International Journal of Number Theory

AN EFFICIENT SEVENTH POWER RESIDUE SYMBOL ALGORITHM

PERLAS C. CARANAY and RENATE SCHEIDLER

Department of Mathematics and Statistics, University of Calgary
2500 University Drive NW, Calgary, Alberta, Canada T2N 1N4
{*pcaranay, rscheidl*}*@math.ucalgary.ca*

Received (10 December 2009)
Accepted (21 December 2009)

Communicated by xxx

Power residue symbols and their reciprocity laws have applications not only in number theory, but also in other fields like cryptography. A crucial ingredient in certain public key cryptosystems is a fast algorithm for computing power residue symbols. Such algorithms have only been devised for the Jacobi symbol as well as for cubic and quintic power residue symbols, but for no higher powers. In this paper, we provide an efficient procedure for computing 7-th power residue symbols. The method employs arithmetic in the field $\mathbb{Q}(\zeta)$, with ζ a primitive 7-th root of unity, and its ring of integers $\mathbb{Z}[\zeta]$. We give an explicit characterization for an element in $\mathbb{Z}[\zeta]$ to be primary, and provide an algorithm for finding primary associates of integers in $\mathbb{Z}[\zeta]$. Moreover, we formulate explicit forms of the complementary laws to Kummer's 7-th degree reciprocity law, and use Lenstra's norm-Euclidean algorithm in the cyclotomic field.

Keywords: Cyclotomic field, power residue symbol, primary, reciprocity and complementary laws, norm-Euclidean division

Mathematics Subject Classification 2000: 11R18 11A15 11A05 11Y16

1. Introduction

Characters and reciprocity laws have a rich history and many uses in number theory. One of the simplest applications of classical reciprocity is in the evaluation of Jacobi symbols. Using the definition, one would have to factor the modulus and apply Euler's criterion to compute the Legendre symbols modulo the individual prime factors. However, combining the Euclidean algorithm with quadratic reciprocity and the accompanying complementary laws eliminates the need for this factorization. This is particularly important when the modulus is too big to factor, which is the case in cryptographic applications. Efficient Jacobi symbol computation is required, for example, in the Rabin-Williams [26] and the Goldwasser-Micali [6] public key cryptosystems as well as Blum's protocol for coin flipping by telephone [1]. The security of all these systems resides in the computational impossibility of factoring

the underlying modulus.

It is natural to ask to what extent this method can be generalized to characters of higher order. This question is not only of mathematical interest in its own right, but once again has cryptographic applications. The above idea has in fact been employed to evaluate cubic and quintic power residue symbols which are used in higher power generalizations of the Rabin-Williams scheme [22,23,27]. Here, the Jacobi symbol is replaced by the power residue symbol $(\alpha/\beta)_\lambda$ where $\lambda = 3$ or 5, and α, β are integers in the cyclotomic field $\mathbb{Q}(\zeta)$ with ζ a primitive λ-th root of unity. An explicit algorithm that generalizes the procedure for Jacobi symbols — which is just the case $\lambda = 2$ — was described for the cases $\lambda = 3$ and 5, but for no higher values of λ. As λ grows, the technical details becomes increasingly complicated. To point out the obstacles and motivate this work, we first recall the efficient Jacobi symbol algorithm referred to above, and then illustrate how this technique can be used to evaluate higher power residue symbols.

Computing Jacobi Symbols – Basic Idea

Suppose we wish to find the Jacobi symbol (a/b) for two rational integers a, b, with b odd and positive. If $\gcd(a, b) > 1$, then $(a/b) = 0$, so suppose that a and b are coprime. We first apply the absolute least remainder Euclidean algorithm to find $q, r \in \mathbb{Z}$ with $a = qb + r$ and $|r| \leq b/2$. Next, write $r = (-1)^k 2^l c$ with $k \in \{0, 1\}$, $l \geq 0$, and c odd and positive. We recall that

$$\left(\frac{b}{c}\right) = (-1)^{\frac{b-1}{2}\frac{c-1}{2}} \left(\frac{c}{b}\right), \quad \left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}}, \quad \left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}} .$$

The first of these three identities is known as the *quadratic law of reciprocity*, and the latter two are the *complementary laws*. We now obtain

$$\left(\frac{a}{b}\right) = \left(\frac{r}{b}\right) = \left(\frac{-1}{b}\right)^k \left(\frac{2}{b}\right)^l \left(\frac{c}{b}\right) = (-1)^{k\frac{b-1}{2}} (-1)^{l\frac{b^2-1}{8}} (-1)^{\frac{b-1}{2}\frac{c-1}{2}} \left(\frac{b}{c}\right) .$$

Now replace a by b and b by c and start over. Since the "numerator" of the symbol decreases by a factor of at least 2 in each iteration, we eventually arrive at a Jacobi symbol of the form $(1/b) = 1$, at which point the algorithm terminates. The number of iterations is therefore no more than the number of divisions with remainder required to compute $\gcd(a, b)$, which is linear in the size of b, i.e. linear in $\log(b)$.

Computing Higher Power Residue Symbols – Basic Idea

In the λ-th power residue symbol, the rational integers a, b are replaced by algebraic integers in the cyclotomic field $\mathbb{Q}(\zeta)$ obtained by adjoining a primitive λ-th root of unity ζ to the rationals $\mathbb{Q}$. Note that if β and β' differ by a unit factor in $\mathbb{Z}[\zeta]$, then $(\alpha/\beta)_\lambda = (\alpha/\beta')_\lambda$. One first needs to assume that $\mathbb{Z}[\zeta]$ is norm-Euclidean; a list of values of λ for which $\mathbb{Z}[\zeta]$ is known to satisfy this condition can be found in [15]. Next, one requires complementary laws for units in $\mathbb{Z}[\zeta]$ and for the "special"

prime $\omega = 1 - \zeta \in \mathbb{Z}[\zeta]$ lying above λ. Finally, Kummer's reciprocity law states that $(\gamma/\beta)_\lambda = (\beta/\gamma)_\lambda$ if γ and β are *primary*, i.e. satisfy certain normalization conditions. Every algebraic integer β in $\mathbb{Q}(\zeta)$ has a primary associate β', i.e. there exists a unit ε (that is in fact unique up to sign) such that $\beta = \varepsilon\beta'$ and β' is primary.

Once again, assume that α and β are coprime. To compute $(\alpha/\beta)_\lambda$ with β not divisible by ω, first replace β by a primary associate which we also denote by β; this does not change the value of the residue symbol. Next, use the norm-Euclidean algorithm to find $\rho \in \mathbb{Z}[\zeta]$ with $\alpha \equiv \rho \pmod{\beta}$ and $\mathbf{N}(\rho) < \mathbf{N}(\beta)$; here, $\mathbf{N}(\cdot)$ denotes the norm function of $\mathbb{Q}(\zeta)/\mathbb{Q}$. Finally, find a unit $\eta \in \mathbb{Z}[\zeta]$ and a primary element $\gamma \in \mathbb{Z}[\zeta]$ such that $\rho = \eta\omega^l\gamma$ where $l \geq 0$ and γ is primary. As above, we obtain

$$\left(\frac{\alpha}{\beta}\right)_\lambda = \left(\frac{\rho}{\beta}\right)_\lambda = \left(\frac{\eta}{\beta}\right)_\lambda \left(\frac{\omega}{\beta}\right)_\lambda^l \left(\frac{\beta}{\gamma}\right)_\lambda .$$

The first two residue symbols on the right hand side above are evaluated directly using the comlementaries. Now replace α by β and β by γ and start over. Since the norm of the "numerator" decreases in each iteration, one eventually reaches a power residue symbol of the form $(\pm 1/\beta) = 1$, since 1 and -1 can be shown to be the only primary units of $\mathbb{Q}(\zeta)$. At this point, the algorithm terminates, and the total number of iterations is linear in $\log(\mathbf{N}(\beta))$.

Overview of this Work

We note that the above algorithm requires four major ingredients:

- simple explicit conditions for a cyclotomic integer to be primary;
- an algorithm for finding a primary associate of a cyclotomic integer, and the corresponding unit factor;
- complementary laws for units and the cyclotomic prime lying above λ;
- a norm-Euclidean algorithm.

As mentioned earlier, all this machinery was previously provided for $\lambda = 2, 3$ and 5 only. The case $\lambda = 2$ is classical. The case $\lambda = 3$ is discussed in [22] and [26] and uses a description of primary cubic cyclotomic integers and cubic complementary laws due to Eisenstein [4,5]. Finally, the case $\lambda = 5$ was first presented in [22] and [23]. It is based on an explicit formulation of the quintic complementary laws due to Williams [28] and employs the same norm-Euclidean algorithm used for our work here.

In this paper, we provide explicit details for the case $\lambda = 7$. That is, we develop an efficient method for computing residue symbols $(\alpha/\beta)_7$ in the cyclotomic field $\mathbb{Q}(\zeta)$, with ζ a primitive 7-th root of unity, without factoring the modulus β. We introduce a set of precise simple conditions for elements in the ring of integers $\mathbb{Z}[\zeta]$ to be primary. We give an efficient technique for finding primary associates and show that these associates are unique up to sign. We also provide an explicit proof that

Kummer's general reciprocity law, stated only for primary primes in [9], holds for composite primary cyclotomic integers as well. We derive explicit complementary laws for the elements excluded from Kummer's reciprocity law, using the results of [10]. These elements include $\lambda = 7$, $\omega = 1 - \zeta$, and the units ± 1, ζ, $\zeta + \zeta^6$, $\zeta^2 + \zeta^5$, and $\zeta^3 + \zeta^4$; any two of the latter three are fundamental units of $\mathbb{Q}(\zeta)$. The final ingredient is an explicit norm-Euclidean algorithm in $\mathbb{Q}(\zeta)$ that was first stated in [22] and is based on work by Lenstra [16]. All these tools are then combined to provide a fast algorithm for computing power residue symbols of order 7.

A review of basic properties of cyclotomic fields and primary elements is given in Section 2. In Section 3, we present the λ-th residue symbol as well as Kummer's law of reciprocity and its accompanying complementary laws. We then specialize to the case $\lambda = 7$, giving an an explicit characterization of primary elements in $\mathbb{Z}[\zeta]$ in Section 4, and an algorithm for finding primary associates in $\mathbb{Z}[\zeta]$ in Section 5. This is followed by an explicit description of the complementary laws for the 7-th power residue symbol in Section 6. A norm-Euclidean division algorithm for $\lambda \leq 11$ due to Lenstra is described in Section 7. All these results are combined into an efficient algorithm for computing 7-th power residue symbols in Section 8, where we also provide a numerical example. We conclude with some remarks on possible future research directions in Section 9.

2. Cyclotomic Fields

We recall some elementary properties of cyclotomic fields; for a good overview, see for example Chapters 1 and 2 of [25]. Throughout this and the next section, let λ be an odd rational prime and $\zeta = e^{2\pi i/\lambda}$ a primitive λ-th root of unity, so

$$1 + \zeta + \zeta^2 + \cdots + \zeta^{\lambda-1} = 0 \ .$$

The cyclotomic field $\mathbb{Q}(\zeta)$ formed by adjoining ζ to the rational numbers $\mathbb{Q}$ is a Galois extension of degree $\lambda - 1$ over $\mathbb{Q}$. The $\lambda - 1$ conjugate mappings of $\mathbb{Q}(\zeta)/\mathbb{Q}$ are given by $\sigma_i(\zeta) = \zeta^i$ for $1 \leq i \leq \lambda - 1$. For any $\alpha = a_1\zeta + a_2\zeta^2 + \cdots + a_{\lambda-1}\zeta^{\lambda-1} \in \mathbb{Q}(\zeta)$, with $a_i \in \mathbb{Q}$, we thus have

$$\sigma_i(\alpha) = a_1\zeta^i + a_2\zeta^{2i} + \cdots + a_{\lambda-1}\zeta^{(\lambda-1)i} \ .$$

The norm and trace of α are the rational numbers $\mathbf{N}(\alpha) = \prod_{i=1}^{\lambda-1} \sigma_i(\alpha)$ and $\mathbf{T}(\alpha) = \sum_{i=1}^{\lambda-1} \sigma_i(\alpha)$, respectively. Since $\sigma^{\lambda-i}(\alpha)$ is the complex conjugate of $\sigma^i(\alpha)$, we see that $\mathbf{N}(\alpha) > 0$ for all non-zero $\alpha \in \mathbb{Q}(\zeta)$.

The maximal order of $\mathbb{Q}(\zeta)$ is the ring $\mathbb{Z}[\zeta]$, so any $\lambda - 1$ distinct powers of ζ form an integral basis of $\mathbb{Q}(\zeta)$. We will be using both the integral bases $\{\zeta^k \mid 1 \leq k \leq \lambda - 1\}$ and $\{\zeta^k \mid 0 \leq k \leq \lambda - 2\}$. Since all the $\lambda - 1$ conjugate mappings are complex embeddings of $\mathbb{Q}(\zeta)$, the unit rank of $\mathbb{Q}(\zeta)$ is $r = (\lambda - 3)/2$, so the unit group of $\mathbb{Z}[\zeta]$ is of the form $\mathbb{Z}[\zeta]^* = \langle -1, \zeta \rangle \times \mathcal{E}$ where $\mathcal{E}$ is an infinite cyclic group of rank r. For any $\alpha, \beta \in \mathbb{Z}[\zeta]$, we write $\alpha \simeq \beta$ if $\alpha\beta^{-1} \in \mathbb{Z}[\zeta]^*$, i.e. α and β are associates.

The discriminant of $\mathbb{Q}(\zeta)$ is $(-1)^{(\lambda-1)/2}\lambda^{\lambda-2}$, so the only rational prime that ramifies in $\mathbb{Q}(\zeta)$ is λ, which is in fact totally ramified. Specifically, $\lambda \simeq \omega^{\lambda-1}$ where $\omega = 1-\zeta$ is a prime in $\mathbb{Z}[\zeta]$. Note that the powers ω^k with $0 \le k \le \lambda-2$ also form an integral basis of $\mathbb{Q}(\zeta)$. For every $\alpha = \sum_{i=1}^{\lambda-1} a_i\zeta^i \in \mathbb{Z}[\zeta]$, we define the quantities

$$b = b(\alpha) = \sum_{i=1}^{\lambda-1} a_i = -\mathbf{T}(\alpha)\,, \qquad c = c(\alpha) = \sum_{i=1}^{\lambda-1} ia_i\ , \tag{2.1}$$

which we will use extensively. Then we have the following useful identity.

Lemma 2.1. *$\alpha \equiv b(\alpha) - c(\alpha)\omega \pmod{\omega^2}$ for all $\alpha \in \mathbb{Z}[\zeta]$.*

Proof. Write $\alpha = \sum_{i=1}^{\lambda-1} a_i\zeta^i$ with $a_i \in \mathbb{Z}$ for $1 \le i \le \lambda-1$. Then

$$\alpha = \sum_{i=1}^{\lambda-1} a_i(1-\omega)^i \equiv \sum_{i=1}^{\lambda-1} a_i(1-i\omega) \equiv b(\alpha) - c(\alpha)\omega \pmod{\omega^2}\ . \qquad \square$$

Corollary 2.2.

(a) $\alpha \equiv 0 \pmod{\omega}$ if and only if $b(\alpha) \equiv 0 \pmod{\lambda}$.
(b) $\alpha \equiv b \pmod{\omega^2}$ if and only if $c(\alpha) \equiv 0 \pmod{\lambda}$.

Corollary 2.3. *Let $\alpha, \beta \in \mathbb{Z}[\zeta]$. Then*

$$b(\alpha\beta) \equiv b(\alpha)b(\beta) \pmod{\lambda}\,, \qquad c(\alpha\beta) \equiv c(\alpha)b(\beta) + b(\alpha)c(\beta) \pmod{\lambda}\ .$$

Proof. By Lemma 2.1,

$$\begin{aligned} b(\alpha\beta) - c(\alpha\beta)\omega &\equiv \alpha\beta \equiv \big(b(\alpha) - c(\alpha)\omega\big)\big(b(\beta) - c(\beta)\omega\big) \\ &\equiv b(\alpha)b(\beta) - \big(c(\alpha)b(\beta) + b(\alpha)c(\beta)\big)\omega \pmod{\omega^2}. \end{aligned}$$

Now simply use the fact that two rational integers are congruent modulo ω if and only if they are congruent modulo λ. $\square$

Corollary 2.4. *Let $\alpha \in \mathbb{Z}[\zeta]$. Then for all $n \in \mathbb{N}$,*

$$b(\alpha^n) \equiv b(\alpha)^n \pmod{\lambda}\,, \qquad c(\alpha^n) \equiv nc(\alpha)b(\alpha)^{n-1} \pmod{\lambda}\ .$$

Primary Elements

An important element in our λ-th power residue symbol algorithm is Kummer's reciprocity law [9]. However, this law only applies to primes that satisfy certain normalization conditions.

Definition 2.5 (Primary elements). Let $\alpha \in \mathbb{Z}[\zeta]$. Then α is said to be *primary* if there exists $B \in \mathbb{Z}$ such that the following hold:

$$\alpha \not\equiv 0 \pmod{\omega}\,, \qquad \alpha \equiv B \pmod{\omega^2}\,, \qquad \alpha\overline{\alpha} \equiv B^2 \pmod{\lambda}\ .$$

This definition can be found on p. 350 of [9] and p. 118 of [24]. Note that every rational integer not divisible by λ is primary. The first two conditions in Definition 2.5 can be simplified using Corollary 2.2 above, which also shows that the integer B above is in fact $B = b(\alpha)$ as given in (2.1). Note that the last condition of Definition 2.5 generally does not have an obvious simplification along the same lines as Corollary 2.2.

Lemma 2.6 (Properties of primary elements).

(a) If $\alpha, \beta \in \mathbb{Z}[\zeta]$ are primary, then $\alpha\beta$ is primary.
(b) Let $\alpha \in \mathbb{Z}[\zeta]$ with $\alpha \not\equiv 0 \pmod{\omega}$. Then $\alpha^\lambda \equiv b^\lambda \pmod{\lambda}$, so α^λ is primary.
(c) Every $\alpha \in \mathbb{Z}[\zeta]$ with $\alpha \not\equiv 0 \pmod{\omega}$ has a primary associate. Furthermore, if $\alpha \in \mathbb{Z}[\zeta]$ is primary, then $\alpha' \in \mathbb{Z}[\zeta]$ is a primary associate of α if and only if $\alpha' = \alpha\varepsilon^\lambda$ for some unit $\varepsilon \in \mathbb{Z}[\zeta]^*$.
(d) Let $\eta_1, \eta_2, \ldots, \eta_r$ be a system of fundamental units of $\mathbb{Q}(\zeta)$. Then every $\alpha \in \mathbb{Z}[\zeta]$ with $\alpha \not\equiv 0 \pmod{\omega}$ has a primary associate of the form $\alpha' = \pm\zeta^{e_0}\eta_1^{e_1}\eta_2^{e_2}\cdots\eta_r^{e_r}\alpha$ where $0 \le e_0, e_1, \ldots, e_r \le \lambda - 1$. Moreover, α' is unique up to sign.

Proof. Part (a) is easily verified using Definition 2.5. For part (b), $\alpha^\lambda \equiv b^\lambda \pmod{\lambda}$ can be obtained by writing $\alpha = b + \gamma\omega$ for suitable $\gamma \in \mathbb{Z}[\zeta]$, so that binomial expansion yields $\alpha^\lambda \equiv b^\lambda + \gamma^\lambda\omega^\lambda \equiv b^\lambda \pmod{\lambda}$. Since $\overline{\alpha}^\lambda \equiv \overline{b}^\lambda \equiv b^\lambda \pmod{\lambda}$, we see that α^λ is primary.

The assertion of part (c) that every $\alpha \in \mathbb{Z}[\zeta]$ with $\alpha \not\equiv 0 \pmod{\omega}$ has a primary associate, and that any two such associates differ by a λ-th unit power is proved in [10] and on p. 288 of [8]. For the converse, note that α is primary by assumption and ε^λ is primary by part (b), so $\alpha' = \alpha\varepsilon^\lambda$ is a primary associate of α by part (a).

Finally, to obtain part (d), let α'' be a primary associate of α, and write $\alpha'' = \pm\zeta^{k_0}\eta_1^{k_1}\eta_2^{k_2}\cdots\eta_r^{k_r}\alpha$ with $k_0, k_1, \ldots, k_r \in \mathbb{Z}$. Write $k_i = e_i + m_i\lambda$ with $0 \le e_i \le \lambda - 1$ and $m_i \in \mathbb{Z}$ for $0 \le i \le r$, and set $\varepsilon = \zeta^{m_0}\eta_1^{m_1}\eta_2^{m_2}\cdots\eta_r^{m_r} \in \mathbb{Z}[\zeta]^*$ and $\alpha' = \zeta^{e_0}\eta_1^{e_1}\eta_2^{e_2}\cdots\eta_r^{e_r}\alpha$. Then $\alpha' = \alpha''\varepsilon^{-\lambda}$ is a primary associate of α by part (c) that is of the desired form.

Now let $\alpha_1 = \pm\zeta^{e_0}\eta_1^{e_1}\eta_2^{e_2}\cdots\eta_r^{e_r}\alpha$ and $\alpha_2 = \pm\zeta^{f_0}\eta_1^{f_1}\eta_2^{f_2}\cdots\eta_r^{f_r}\alpha$ be two primary associates of α with $0 \le e_i, f_i \le \lambda - 1$ for $0 \le i \le r$. By part (c), $\alpha_1\alpha_2^{-1}$ is the λ-th power of a unit in $\mathbb{Z}[\zeta]^*$, so since $-\lambda < e_i - f_i < \lambda$ for $0 \le i \le r$, this unit must be ± 1. □

Corollary 2.7. *The units 1 and -1 are the only primary units of $\mathbb{Q}(\zeta)$.*

Proof. Certainly both 1 and -1 are primary. By part(d) of Lemma 2.6, $\pm\zeta^0\eta_1^0\cdots\eta_r^0 = \pm 1$ are the only two primary associates of 1 and -1. □

3. λ-th Power Residue Symbols

Henceforth, we assume that $\mathbb{Z}[\zeta]$ be a unique factorization domain; this is the case exactly when $\lambda \leq 19$ [17]. Let $\pi \in \mathbb{Z}[\zeta]$ be a prime. Then $\mathbb{Z}[\zeta]/\pi\mathbb{Z}[\zeta]$ is a field of order $\mathbf{N}(\pi)$, so $\alpha^{\mathbf{N}(\pi)-1} \equiv 1 \pmod{\pi}$ for any non-zero $\alpha \in \mathbb{Z}[\zeta]$ with $\pi \nmid \alpha$. It follows that $\alpha^{(\mathbf{N}(\pi)-1)/\lambda} \equiv \zeta^i \pmod{\pi}$ for some unique $i \in \{0, 1, \ldots, \lambda-1\}$. The exponent i is referred to as the *index* of α with respect to π, denoted by $\mathrm{ind}_\pi(\alpha)$. This leads to the following definition.

Definition 3.1. Let $\alpha, \pi \in \mathbb{Z}[\zeta]$, where $\pi \neq \omega$ is a prime. Then the *λ-th power residue symbol* of α modulo π is defined as

$$\left(\frac{\alpha}{\pi}\right)_\lambda = \begin{cases} 0 & \text{if } \pi \mid \alpha\,, \\ \zeta^{\mathrm{ind}_\pi(\alpha)} & \text{if } \pi \nmid \alpha\,. \end{cases}$$

For any non-zero element $\beta \in \mathbb{Z}[\zeta] \setminus \mathbb{Z}[\zeta]^*$ not divisible by ω, the λ-th power residue symbol of α modulo β is defined as

$$\left(\frac{\alpha}{\beta}\right)_\lambda = \prod_{i=1}^{k} \left(\frac{\alpha}{\pi_i}\right)_\lambda^{e_i}\,,$$

where $\beta \simeq \prod_{i=1}^{k} \pi_i^{e_i}$ is the unique factorization (up to order and unit factors) into distinct primes $\pi_i \in \mathbb{Z}[\zeta]$.

The analogue for the $\lambda = 2$ case (which is excluded here) is the Legendre symbol for prime moduli and the Jacobi symbol for composite moduli. It is not hard to show that if $\beta_1 \simeq \beta_2$, then $(\alpha/\beta_1)_\lambda = (\alpha/\beta_2)_\lambda$. Furthermore, $(\alpha/\beta)_\lambda = 0$ if and only if α and β have a common prime factor, and $(\alpha/\pi)_\lambda = 1$ if and only if α is a λ-th power modulo π. The following properties are easily verified:

Lemma 3.2. *Let $\alpha, \beta, \gamma, \delta \in \mathbb{Z}[\zeta]$ with $\omega \nmid \beta\delta$. Then the following hold:*

$$\left(\frac{\alpha}{\beta}\right)_\lambda = \left(\frac{\gamma}{\beta}\right)_\lambda \quad \text{if } \alpha \equiv \gamma \pmod{\beta}\,,$$

$$\left(\frac{\alpha\gamma}{\beta}\right)_\lambda = \left(\frac{\alpha}{\beta}\right)_\lambda \left(\frac{\gamma}{\beta}\right)_\lambda\,, \qquad \left(\frac{\alpha}{\beta\delta}\right)_\lambda = \left(\frac{\alpha}{\beta}\right)_\lambda \left(\frac{\alpha}{\delta}\right)_\lambda\,.$$

Kummer's Law of Reciprocity

Kummer's reciprocity law is a crucial ingredient in our power residue algorithm. It can be found in [9], [14], [12], pp. 120-121 of [24] and pp. 312-313 of [8].

Theorem 3.3 (Kummer's law of reciprocity). *Let π and ψ be two distinct primary primes. Then* $\left(\frac{\pi}{\psi}\right)_\lambda = \left(\frac{\psi}{\pi}\right)_\lambda$.

Kummer stated his reciprocity law for primes only, but it extends easily to composite cyclotomic integers:

Corollary 3.4 (Law of reciprocity for composite elements). *Let $\alpha, \beta \in \mathbb{Z}[\zeta]$ be primary. Then* $\left(\frac{\alpha}{\beta}\right)_\lambda = \left(\frac{\beta}{\alpha}\right)_\lambda$.

Proof. It suffices to prove this statement for elements $\alpha \simeq \pi_1\pi_2$ and $\beta \simeq \psi_1\psi_2$ where $\pi_1, \pi_2, \psi_1, \psi_2$ are primary primes. By part (c) of Lemma 2.6, $\alpha = \varepsilon^\lambda \pi_1\pi_2$ and $\beta = \eta^\lambda \psi_1\psi_2$ for some units $\varepsilon, \eta \in \mathbb{Z}[\zeta]^*$. Then by Lemma 3.2 and Theorem 3.3,

$$\begin{aligned}\left(\frac{\alpha}{\beta}\right)_\lambda &= \left(\frac{\varepsilon}{\beta}\right)_\lambda^\lambda \left(\frac{\pi_1\pi_2}{\beta}\right)_\lambda = \left(\frac{\pi_1\pi_2}{\psi_1\psi_2}\right)_\lambda = \left(\frac{\pi_1}{\psi_1}\right)_\lambda \left(\frac{\pi_2}{\psi_1}\right)_\lambda \left(\frac{\pi_1}{\psi_2}\right)_\lambda \left(\frac{\pi_2}{\psi_2}\right)_\lambda \\ &= \left(\frac{\psi_1}{\pi_1}\right)_\lambda \left(\frac{\psi_2}{\pi_1}\right)_\lambda \left(\frac{\psi_1}{\pi_2}\right)_\lambda \left(\frac{\psi_2}{\pi_2}\right)_\lambda = \left(\frac{\psi_1\psi_2}{\pi_1\pi_2}\right)_\lambda = \left(\frac{\psi_1\psi_2}{\alpha}\right)_\lambda \\ &= \left(\frac{\eta}{\alpha}\right)_\lambda^\lambda \left(\frac{\psi_1\psi_2}{\alpha}\right)_\lambda = \left(\frac{\beta}{\alpha}\right)_\lambda \quad . \end{aligned}$$

□

The Complementary Laws

Kummer's reciprocity law does not apply to units or to the conjugates of the prime ω. For these elements, the residue symbol needs to be explicitly stated via *complementary laws*, which were also provided by Kummer. Before we state these, we note that the complementary laws for the units ± 1 and ζ are obvious:

Lemma 3.5 (Complementary laws for ± 1 and ζ). *Let $\pi \in \mathbb{Z}[\zeta]$ be any prime distinct from ω. Then* $\mathrm{ind}_\pi(\pm 1) = 0$ *and* $\mathrm{ind}_\pi(\zeta) \equiv (\mathbf{N}(\pi) - 1)/\lambda \pmod{\lambda}$.

Proof. The claim that $\mathrm{ind}(\pm 1) = 0$ follows from the fact that $\mathbf{N}(\pm 1) = 1$. The congruence for $\mathrm{ind}_\pi(\zeta)$ follows straight from Definition 3.1. □

Corollary 3.6 (Complementary laws for ± 1 and ζ, composite modulus). *Let $\beta \in \mathbb{Z}[\zeta]$ not be divisible by ω. Then* $(\pm 1/\beta)_\lambda = 1$ *and* $(\zeta/\beta)_\lambda = \zeta^{(\mathbf{N}(\beta)-1)/\lambda}$.

Proof. It suffices to prove the statement for $\beta = \pi\psi$ where π, ψ are primes in $\mathbb{Z}[\zeta]$. The complementary law for ± 1 is obvious, and that for ζ follows from the fact that $(\mathbf{N}(\pi) - 1) + (\mathbf{N}(\psi) - 1) \equiv \mathbf{N}(\pi\psi) - 1 \pmod{\lambda^2}$. □

The remaining complementary laws can be found in Kummer's works [10] and [13], as well as on pp. 121-123 of [24], pp. 107-113 of [7], and pp. 312 and 326-327 of [8]. We take this opportunity to point out that there are discrepancies in these literature sources, as detailed on pp. 61-63 of [2]. However, for the results presented here, none of the formulas that exhibit such inconsistencies were used.

Following Kummer's notation, we write any $\alpha = \sum_{i=1}^{\lambda-1} a_i \zeta^i \in \mathbb{Z}[\zeta]$ as

$$\alpha = A(\zeta) \quad \text{with} \quad A(t) = \sum_{i=0}^{\lambda-2} A_i t^i \in \mathbb{Z}[t] \ .$$

Note that α is now expressed in terms of the integral basis $1, \zeta, \ldots, \zeta^{\lambda-2}$. Then the two representations of α are related via

$$A_0 = -a_{\lambda-1}\,, \qquad A_i = a_i - a_{\lambda-1} \text{ for } 1 \le i \le \lambda - 2\ . \tag{3.1}$$

For $m \ge 0$, the *m-th logarithmic differential quotient* of α is given by

$$D_m(\alpha) = \left.\frac{d^m \ln A(e^v)}{dv^m}\right|_{v=0}\ . \tag{3.2}$$

Kummer's complementary laws can be found on pp. 695-697 of [9] and pp. 122-123 of and [24]. The two laws required for our purposes are given as follows (recall that $r = (\lambda-3)/2$ is the unit rank of $\mathbb{Q}(\zeta)$):

Theorem 3.7 (Complementary laws for λ and units). *Let π be a primary prime in $\mathbb{Z}[\zeta]$. Then the following hold.*

(a) $\operatorname{ind}_\pi(\lambda) \equiv \dfrac{D_\lambda(\pi)}{\lambda} \pmod{\lambda}$.
(b) For any unit $\varepsilon \in \mathbb{Z}[\zeta]^*$,

$$\operatorname{ind}_\pi(\varepsilon) \equiv D_1(\varepsilon)\frac{\mathbf{N}(\pi)-1}{\lambda} + \sum_{k=1}^{r} D_{2k}(\varepsilon)D_{\lambda-2k}(\pi) \pmod{\lambda}\ .$$

Now that since $\lambda = \varepsilon\omega^{\lambda-1}$ for some unit $\varepsilon \in \mathbb{Z}[\zeta]^*$, $\operatorname{ind}_\pi(\omega)$ can be derived from Theorem 3.7 via $\operatorname{ind}_\pi(\omega) \equiv \operatorname{ind}_\pi(\varepsilon) - \operatorname{ind}_\pi(\lambda) \pmod{\lambda}$.

4. Primary Elements, $\lambda = 7$

We now restrict to the case $\lambda = 7$, so ζ is a 7-th primitive root of unity. Let $\alpha = \sum_{i=1}^{6} a_i\zeta^i \in \mathbb{Z}[\zeta]$. We define six linear combinations of the coefficients of α as follows:

$$\begin{aligned}
b = b(\alpha) &= \sum_{i=1}^{6} a_i \ = a_1 + a_2 + a_3 + a_4 + a_5 + a_6\ ,\\
c = c(\alpha) &= \sum_{i=1}^{6} i a_i \ = a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 + 6a_6\ ,\\
a = a(\alpha) &= \sum_{i=1}^{6} i^2 a_i \equiv a_1 - 3a_2 + 2a_3 + 2a_4 - 3a_5 + a_6 \pmod 7\ ,\\
d = d(\alpha) &= \sum_{i=1}^{6} i^3 a_i \equiv a_1 + a_2 - a_3 + a_4 - a_5 - a_6 \pmod 7\ ,\\
e = e(\alpha) &= \sum_{i=1}^{6} i^4 a_i \equiv a_1 + 2a_2 - 3a_3 - 3a_4 + 2a_5 + a_6 \pmod 7\ ,\\
f = f(\alpha) &= \sum_{i=1}^{6} i^5 a_i \equiv a_1 - 3a_2 - 2a_3 + 2a_4 + 3a_5 - a_6 \pmod 7\ .
\end{aligned} \tag{4.1}$$

The quantities b and c were already introduced in (2.1). Inverting the above system modulo 7 yields

$$\begin{aligned} a_1 &\equiv -a-b-c-d-e-f \pmod 7 ,\\ a_2 &\equiv -2a-b+3c-d+3e-2f \pmod 7 ,\\ a_3 &\equiv 3a-b+2c+d-2e-3f \pmod 7 ,\\ a_4 &\equiv 3a-b-2c-d-2e+3f \pmod 7 ,\\ a_5 &\equiv -2a-b-3c+d+3e+2f \pmod 7 ,\\ a_6 &\equiv -a-b+c+d-e+f \pmod 7 . \end{aligned} \tag{4.2}$$

Since $\omega^6 \simeq 7$, it is straightforward to deduce that

$$\begin{aligned} \alpha = \sum_{i=1}^{6} a_i(1-\omega)^i \equiv b - c\omega + 3(c-a)\omega^2 + (2c-3a+d)\omega^3 \\ -(a+2c+2d+2e)\omega^4 + (a-3c+3e-f)\omega^5 \pmod 7 . \end{aligned} \tag{4.3}$$

We investigate the multiplicative behavior of the quantities in (4.1).

Lemma 4.1. *Let $\alpha, \beta \in \mathbb{Z}[\zeta]$ with $c(\alpha) \equiv c(\beta) \equiv 0 \pmod 7$. Then the following hold:*

$$\begin{aligned} b(\alpha\beta) &\equiv b(\alpha)b(\beta) \pmod 7 ,\\ c(\alpha\beta) &\equiv 0 \pmod 7 ,\\ a(\alpha\beta) &\equiv a(\alpha)b(\beta) + b(\alpha)a(\beta) \pmod 7 ,\\ d(\alpha\beta) &\equiv d(\alpha)b(\beta) + b(\alpha)d(\beta) \pmod 7 ,\\ e(\alpha\beta) &\equiv e(\alpha)b(\beta) + b(\alpha)e(\beta) - a(\alpha)a(\beta) \pmod 7 ,\\ f(\alpha\beta) &\equiv f(\alpha)b(\beta) + b(\alpha)f(\beta) + 3\big(d(\alpha)a(\beta) + a(\alpha)d(\beta)\big) \pmod 7 . \end{aligned}$$

Proof. The first two congruences follow immediately from Corollary 2.3. Now $c(\alpha) \equiv 0 \pmod 7$ reduces (4.3) to

$$\alpha \equiv b - 3a\omega^2 + (d-3a)\omega^3 - (a+2d+2e)\omega^4 + (a+3e-f)\omega^5 \pmod 7 ; \tag{4.4}$$

similarly for β. This implies

$$\alpha\beta \equiv b(\alpha)b(\beta) - 3\big(a(\alpha)b(\beta) + b(\alpha)a(\beta)\big)\omega^2 \pmod{\omega^3} .$$

Since $c(\alpha\beta) \equiv 0 \pmod 7$, (4.4) applied to $\alpha\beta$ yields

$$\alpha\beta \equiv b(\alpha\beta) - 3a(\alpha\beta)\omega^2 \pmod{\omega^3} .$$

Comparing the coefficients of ω^2 in the two above congruences for $\alpha\beta \pmod{\omega^3}$ implies the third of the above congruences. Similar coefficient comparisons at ω^3, ω^4 and ω^5 yield the remaining identities. □

Using induction, Lemma 4.1 immediately yields

Corollary 4.2. *Let $\alpha \in \mathbb{Z}[\zeta]$ with $c(\alpha) \equiv 0 \pmod 7$. Then for all $n \in \mathbb{N}$,*

$$a(\alpha^n) \equiv na(\alpha)b(\alpha)^{n-1} \pmod 7 ,$$
$$e(\alpha^n) \equiv ne(\alpha)b(\alpha)^{n-1} + 3n(n-1)a(\alpha)^2 b(\alpha)^{n-2} \pmod 7 .$$

Corollary 2.2 gives simple congruences involving rational (rather than algebraic) integers for two of the three conditions for a cyclotomic integer to be primary. For $\lambda = 7$, we provide a similar simple set of congruences characterizing the third condition.

Theorem 4.3. *Let $\alpha = \sum_{i=1}^{6} a_i\zeta^i \in \mathbb{Z}[\zeta]$, a, b, e as given in (4.1), and suppose that $\alpha \equiv b \pmod{\omega^2}$ and $b \not\equiv 0 \pmod 7$. Then $\alpha\overline{\alpha} \equiv b^2 \pmod 7$ if and only if $a \equiv e \equiv 0 \pmod 7$.*

Proof. Let c, d, f also be as given in (4.1). Then $c \equiv 0 \pmod 7$ by part (b) of Corollary 2.2. Since $\overline{\alpha} = \sum_{i=1}^{6} a_i\zeta^{7-i}$, (4.1) yields $b(\overline{\alpha}) = b$, $c(\overline{\alpha}) \equiv -c \equiv 0 \pmod 7$, $a(\overline{\alpha}) \equiv a \pmod 7$, $d(\overline{\alpha}) \equiv -d \pmod 7$, $e(\overline{\alpha}) \equiv e \pmod 7$, and $f(\overline{\alpha}) \equiv -f \pmod 7$. By Corollary 2.3, $b(\alpha\overline{\alpha}) \equiv b^2 \pmod 7$ and $c(\alpha\overline{\alpha}) \equiv 0 \pmod 7$, and by Lemma 4.1, $a(\alpha\overline{\alpha}) \equiv 2ab \pmod 7$, $e(\alpha\overline{\alpha}) \equiv 2be - a^2 \pmod 7$, and $d(\alpha\overline{\alpha}) \equiv f(\alpha\overline{\alpha}) \equiv 0 \pmod 7$. Thus, by (4.4),

$$\alpha\overline{\alpha} \equiv b^2 + ab\omega^2 + ab\omega^3 - (2ab - 3be - 2a^2)\omega^4 + (2ab - be - 3a^2)\omega^5 \pmod 7 .$$

So $\alpha\overline{\alpha} \equiv b^2 \pmod 7$ if and only if the coefficients of ω^i for $2 \le i \le 5$ vanish modulo 7. Since $b \not\equiv 0 \pmod 7$, this holds if and only if $a \equiv e \equiv 0 \pmod 7$. □

Lemma 4.4. *Let $\alpha = \sum_{i=1}^{6} a_i\zeta^i \in \mathbb{Z}[\zeta]$, a, b, c, d, e defined as in (4.1), and suppose that $b \not\equiv 0 \pmod 7$ and $c \equiv 0 \pmod 7$. Then $a \equiv e \equiv 0 \pmod 7$ if and only if $a_1 + a_6 \equiv a_2 + a_5 \equiv a_3 + a_4 \pmod 7$.*

Proof. Simple verification using (4.1) and (4.2). □

Theorem 4.3, Lemma 4.4 and Corollary 2.2 now provide a simple practical test for elements of $\mathbb{Z}[\zeta]$ to be primary:

Corollary 4.5. *Let $\alpha = \sum_{i=1}^{6} a_i\zeta^i \in \mathbb{Z}[\zeta]$. Then α is primary if and only if the following conditions hold:*

(a) $b \not\equiv 0 \pmod 7$,
(b) $c \equiv 0 \pmod 7$,
(c) $a \equiv e \equiv 0 \pmod 7$, *or equivalently,* $a_1 + a_6 \equiv a_2 + a_5 \equiv a_3 + a_4 \pmod 7$.

5. Finding Primary Associates, $\lambda = 7$

We continue to let ζ be a primitive 7-th root of unity. Then the field $\mathbb{Q}(\zeta)$ has unit rank $r = 2$. By p. 99 of [24],

$$\eta_1 = \zeta + \zeta^6 \quad \text{and} \quad \eta_2 = \sigma_2(\eta_1) = \zeta^2 + \zeta^5$$

form a pair of fundamental units of $\mathbb{Q}(\zeta)$. It is easy to verify that

$$\begin{aligned} b(\eta_1) &\equiv 2 \pmod 7, & b(\eta_2) &\equiv 2 \pmod 7, \\ c(\eta_1) &\equiv 0 \pmod 7, & c(\eta_2) &\equiv 0 \pmod 7, \\ a(\eta_1) &\equiv 2 \pmod 7, & a(\eta_2) &\equiv 1 \pmod 7, \\ d(\eta_1) &\equiv 0 \pmod 7, & d(\eta_2) &\equiv 0 \pmod 7, \\ e(\eta_1) &\equiv 2 \pmod 7, & e(\eta_2) &\equiv 4 \pmod 7, \\ f(\eta_1) &\equiv 0 \pmod 7, & f(\eta_2) &\equiv 0 \pmod 7. \end{aligned} \tag{5.1}$$

Lemma 5.1. *Let $m, n \in \mathbb{Z}$ be non-negative, $\alpha \in \mathbb{Z}[\zeta]$, and a, b, c, e as given in* (4.1) *with $c \equiv 0 \pmod 7$. Then the following hold.*

$$\begin{aligned} b(\alpha\eta_1^m\eta_2^n) &\equiv 2^{m+n} b(\alpha) \pmod 7, \\ c(\alpha\eta_1^m\eta_2^n) &\equiv 0 \pmod 7, \\ a(\alpha\eta_1^m\eta_2^n) &\equiv 2^{m+n-1}\big(b(2m+n)+2a\big) \pmod 7, \\ e(\alpha\eta_1^m\eta_2^n) &\equiv 2^{m+n-2}\big(b(3n^2-2n-2m^2-m-2mn)+a(3m-2n)-3e\big) \pmod 7. \end{aligned}$$

Proof. The first two congruences follow from (5.1) as well as Corollaries 2.3 and 2.4. For the last two identities, we use (5.1) as well as Corollaries 2.4 and 4.2 to compute

$$\begin{aligned} a(\eta_1^m) &\equiv 2^m m \pmod 7, & a(\eta_2^n) &\equiv 2^{n-1} n \pmod 7, \\ e(\eta_1^m) &\equiv 2^m m(3m-2) \pmod 7, & e(\eta_2^n) &\equiv 2^{n-2} n(3n-2) \pmod 7, \end{aligned}$$

and hence by (5.1) and Lemma 4.1 with $\alpha = \eta_1^m$ and $\beta = \eta_2^n$,

$$\begin{aligned} a(\eta_1^m\eta_2^n) &\equiv 2^{m+n-1}(2m+n) \pmod 7, \\ e(\eta_1^m\eta_2^n) &\equiv 2^{m+n-2}(3n^2-2n-2m^2-m-2mn) \pmod 7. \end{aligned}$$

Applying Lemma 4.1 again with $\beta = \eta_1^m\eta_2^n$ yields the last two congruences of the lemma. □

Corollary 5.2. *Let Let $m, n \in \mathbb{Z}$ be non-negative, $\alpha \in \mathbb{Z}[\zeta]$, a, b, c, e be as given in* (4.1) *with $b \not\equiv 0 \pmod 7$ and $c \equiv 0 \pmod 7$. Then $\alpha\eta_1^m\eta_2^n$ is primary if and only if*

$$m \equiv b^{-1}(a + e - 3a^2b^{-1}) \pmod 7, \tag{5.2}$$

$$n \equiv b^{-1}(3a - 2e - a^2b^{-1}) \pmod 7. \tag{5.3}$$

Proof. By part (c) of Lemma 2.6, we only need to consider values m, n with $0 \le m, n \le 6$. So let m, n be any such integers. By Lemma 5.1, $b(\alpha\eta_1^m\eta_2^n) \not\equiv 0 \pmod 7$ and $c(\alpha\eta_1^m\eta_2^n) \equiv 0 \pmod 7$. By the same lemma and Corollary 4.5, $\alpha\eta_1^m\eta_2^n$ is primary if and only if

$$b(2m+n) + 2a \equiv 0 \pmod 7, \tag{5.4}$$

$$b(3n^2-2n-2m^2-m-2mn) + a(3m-2n) - 3e \equiv 0 \pmod 7. \tag{5.5}$$

Now (5.4) is equivalent to

$$n \equiv -2(m + ab^{-1}) \pmod 7. \tag{5.6}$$

With n as given in (5.6), we obtain

$$3n^2 - 2n - 2m^2 - m - 2mn \equiv 3m - 3ab^{-1} - 2(ab^{-1})^2 \pmod 7$$

and $3m - 2n \equiv -3ab^{-1} \pmod 7$. Thus, by (5.5), $\alpha\eta_1^m\eta_2^n$ is primary if and only if (5.6) holds and

$$(3bm - 3a - 2a^2b^{-1}) - 3a^2b^{-1} - 3e \equiv 0 \pmod 7 .$$

This last congruence is equivalent to (5.2), and then (5.6) is easily seen to be equivalent to (5.3). □

The following algorithm computes for any $\alpha \in \mathbb{Z}[\zeta]$ with $b(\alpha) \not\equiv 0 \pmod 7$ the unique values $k, m, n \in \{0, 1, \ldots, 6\}$ and the unique associate $\alpha' = \zeta^k\eta_1^m\eta_2^n\alpha$ of α such that $\pm\alpha'$ is primary. Note that $(\alpha'/\beta)_\lambda = (-\alpha'/\beta)_\lambda$ by Lemma 3.2 and Corollary 3.6, so for computing 7-th residue symbols, it does not matter which of the two associates α' and $-\alpha'$ is used.

Algorithm 5.3 (Finding primary associates, $\boldsymbol{\lambda = 7}$).
Input: $\alpha \in \mathbb{Z}[\zeta]$ such that $b(\alpha) \not\equiv 0 \pmod 7$.
Output: $k, m, n \in \mathbb{Z}$ with $0 \le k, m, n \le 6$ and $\alpha' \in \mathbb{Z}[\zeta]$ such that $\alpha' = \zeta^k\eta_1^m\eta_2^n\alpha$ is primary.

(1) Compute $b \equiv b(\alpha) \pmod 7$ and $c \equiv c(\alpha) \pmod 7$ via (4.1).
(2) Compute $k \equiv -b^{-1}c \pmod 7$, $0 \le k \le 6$, and $\alpha'' = \zeta^k\alpha$.
(3) Compute $a \equiv a(\alpha'') \pmod 7$ and $e \equiv e(\alpha'') \pmod 7$ via (4.1).
(4) Compute m and n with $0 \le m, n \le 6$ via (5.2) and (5.3), respectively, and $\alpha' = \eta_1^m\eta_2^n\alpha''$.
(5) Output k, m, n, α'.

Theorem 5.4. *Algorithm 5.3 is correct.*

Proof. Note that $b(1) = -6$ and $b(\zeta^k) = 1$ for $1 \le k \le 6$, so $b(\zeta^k) \equiv 1 \pmod 7$ for $0 \le k \le 6$. It follows that $b(\alpha\zeta^k) \equiv b \pmod 7$ by Corollary 2.3. Furthermore, $c(1) = -21 \equiv 0 \pmod 7$ and $c(\zeta^k) \equiv k \pmod 7$ for $1 \le k \le 6$, so $c(\zeta^k) \equiv k \pmod 7$ for $0 \le k \le 6$. Again by Corollary 2.2, $c(\alpha\zeta^k) \equiv c+bk \pmod 7$. Thus, if α'' is defined as in step 2, we have $b(\alpha'') \equiv b \pmod 7$ and $c(\alpha'') \equiv 0 \pmod 7$. By Corollary 5.2, α' as defined in step 4 is primary. □

6. Complementary Laws, $\boldsymbol{\lambda = 7}$

Using Theorem 3.7, we now derive explicit complementary laws for $\lambda = 7$, $\eta_1 = \zeta + \zeta^6$, $\eta_2 = \zeta^2 + \zeta^5$, and $\eta_3 = \zeta^3 + \zeta^4$; note that the complementary law for η_3 could also be derived from the identity $\eta_3 = (\eta_1\eta_2)^{-1}$. We will then employ these results to find the complementary law for ω. Since $r = 2$, Theorem 3.7 now reads

$$\operatorname{ind}_\pi(7) \equiv \frac{D_7(\pi)}{7} \pmod 7 , \tag{6.1}$$

$$\operatorname{ind}_\pi(\varepsilon) \equiv D_1(\varepsilon)\frac{\mathbf{N}(\pi) - 1}{7} + D_2(\varepsilon)D_5(\pi) + D_4(\varepsilon)D_3(\pi) \pmod 7 \tag{6.2}$$

for any unit $\varepsilon \in \mathbb{Z}[\zeta]^*$, where $\pi \in \mathbb{Z}[\zeta]$ is a primary prime. So we need to find $D_j(\eta_i) \pmod 7$ for $j = 1, 2, 4$ and $i = 1, 2, 3$, as well as $D_3(\pi)$, $D_5(\pi)$, $D_7(\pi)/7 \pmod 7$ for $j = 3, 5, 7$. We obtain

$$\begin{array}{lll} D_1(\eta_1) \equiv 0 \pmod 7, & D_2(\eta_1) \equiv 1 \pmod 7, & D_4(\eta_1) \equiv 5 \pmod 7, \\ D_1(\eta_2) \equiv 0 \pmod 7, & D_2(\eta_2) \equiv 4 \pmod 7, & D_4(\eta_2) \equiv 3 \pmod 7, \\ D_1(\eta_3) \equiv 0 \pmod 7, & D_2(\eta_3) \equiv 2 \pmod 7, & D_4(\eta_3) \equiv 6 \pmod 7. \end{array} \tag{6.3}$$

As in Section 3, we write $\pi = \sum_{i=1}^{6} a_i \zeta^i \in \mathbb{Z}[\zeta]$ as $\pi = A(\zeta)$ where $A(t) = \sum_{i=0}^{5} A_i t^i \in \mathbb{Z}[t]$. The remaining logarithmic differential quotients require the computation of $\ln A(e^v)$ and its derivatives with respect to v at $v = 0$. This in turn requires the first seven derivatives of $A(t)$ with respect to t at $t = 1$. We compute these derivatives for arbitrary elements π and then restrict to primary primes π. Let a, b, c, d, e, f be given by (4.1). We obtain

$$\begin{array}{ll} \pi(1) = b - 7a_6, & \dfrac{d\pi}{dt}(1) = c - 21a_6, \\ \dfrac{d^2\pi}{dt^2}(1) \equiv a \pmod 7, & \dfrac{d^3\pi}{dt^3}(1) \equiv d \pmod 7, \\ \dfrac{d^4\pi}{dt^4}(1) \equiv e \pmod 7, & \dfrac{d^5\pi}{dt^5}(1) \equiv f \pmod 7, \\ \dfrac{d^6\pi}{dt^6}(1) \equiv b + a_6 \pmod 7, & \dfrac{d^7\pi}{dt^7}(1) \equiv c \pmod 7. \end{array} \tag{6.4}$$

For primary π, Corollary 4.5 states that $b \not\equiv 0 \pmod 7$ and $c \equiv a \equiv e \equiv 0 \pmod 7$. This yields

$$D_3(\pi) \equiv \frac{d}{b} \pmod 7, \qquad D_5(\pi) \equiv \frac{f}{b} \pmod 7, \tag{6.5}$$

$$\frac{D_7(\pi)}{7} \equiv \frac{c}{7b} - \frac{d}{b} + \frac{3f}{b} + 3 \pmod 7. \tag{6.6}$$

We combine the above results:

Lemma 6.1. *Let $\pi \in \mathbb{Z}[\zeta]$ be a primary prime and a, b, c, d, e, f given by (4.1), with π in place of α. Then the following hold:*

(1) $\operatorname{ind}_\pi(7) \equiv \dfrac{c}{7b} - \dfrac{d}{b} + \dfrac{3f}{b} + 3 \pmod 7$,

(2) $\operatorname{ind}_\pi(\omega) \equiv \dfrac{4(\mathbf{N}(\pi) + 6)}{7} - \dfrac{c}{7b} \pmod 7$,

(3) $\operatorname{ind}_\pi(\zeta + \zeta^6) \equiv \dfrac{f - 2d}{b} \pmod 7$,

(4) $\operatorname{ind}_\pi(\zeta^2 + \zeta^5) \equiv \dfrac{3(d - f)}{b} \pmod 7$,

(5) $\operatorname{ind}_\pi(\zeta^3 + \zeta^4) \equiv \dfrac{2f - d}{b} \pmod 7$.

Proof. The first assertion follows immediately from (6.1) and (6.6), and the last three from (6.2), (6.3) and (6.5). Finally, we have

$$7 = \varepsilon\omega^6 \quad \text{with} \quad \varepsilon = -\zeta^4(\zeta+\zeta^6)^7(\zeta^2+\zeta^5)^5(\zeta^3+\zeta^4)^9 \ ,$$

so by parts (1), (4), (5), and Lemma 3.5,

$$\begin{aligned}
\operatorname{ind}_\pi(\omega) &\equiv \operatorname{ind}_\pi(\varepsilon) - \operatorname{ind}_\pi(7) \\
&\equiv \operatorname{ind}_\pi(-1) + 4\operatorname{ind}_\pi(\zeta) + 5\operatorname{ind}_\pi(\zeta^2+\zeta^5) + 2\operatorname{ind}_\pi(\zeta^3+\zeta^4) - \operatorname{ind}_\pi(7) \\
&\equiv 4\,\frac{\mathbf{N}(\pi)-1}{7} + 5\,\frac{3(d-f)}{b} + 2\,\frac{2f-d}{b} - \left(\frac{c}{7b} - \frac{d}{b} + \frac{3f}{b} + 3\right) \\
&\equiv 4\,\frac{\mathbf{N}(\pi)-1}{7} - \frac{c}{7b} + \frac{49-21}{7} \equiv \frac{4(\mathbf{N}(\pi)+6)}{7} - \frac{c}{7b} \pmod 7 \ . \qquad \square
\end{aligned}$$

Before we extend all the complementary laws for the case $\lambda = 7$ to composite moduli, we require a refinement of Corollary 2.3:

Lemma 6.2. *Let $\alpha, \beta \in \mathbb{Z}[\zeta]$ be primary. Then*

$$c(\alpha\beta) \equiv c(\alpha)b(\beta) + b(\alpha)c(\beta) + 21b(\alpha)b(\beta) \pmod{49} \ .$$

Proof. Write $\alpha = A(\zeta)$ and $\beta = B(\zeta)$ with $A(t) = \sum_{i=0}^5 A_i t^i$, $B(t) = \sum_{i=0}^5 B_i t^i$, and set $A(t)B(t) = \sum_{i=0}^{10} C_i t^i$. For brevity, denote the first derivative with respect to t of any of these polynomials $F(t)$ by $F'(t)$. Then by the first line of (6.4),

$$\begin{aligned}
c(\alpha\beta) &= (\alpha\beta)'(1) - 21C_0 = \alpha'(1)\beta(1) + \alpha(1)\beta'(1) - 21C_0 \\
&= (c(\alpha)+21A_0)(b(\beta)+7B_0) + (b(\alpha)+7A_0)(c(\beta)+21B_0) - 21C_0 \\
&\equiv c(\alpha)b(\beta) + b(\alpha)c(\beta) + 21(b(\alpha)B_0 + b(\beta)A_0 - C_0) \pmod{49} \ ,
\end{aligned}$$

so it suffices to show that $b(\alpha)B_0 + b(\beta)A_0 - C_0 \equiv b(\alpha\beta) \pmod 7$. Now by (3.1), the last congruence of (4.1), and Lemma 4.1, we have

$$\begin{aligned}
b(\alpha)B_0 + b(\beta)A_0 &\equiv b(\alpha)\big(b(\beta) - d(\beta) - f(\beta)\big) + b(\beta)\big(b(\alpha) - d(\alpha) - f(\alpha)\big) \\
&\equiv 2b(\alpha)b(\beta) - b(\alpha)d(\beta) - b(\beta)d(\alpha) - b(\alpha)f(\beta) - b(\beta)f(\alpha) \\
&\equiv 2b(\alpha\beta) - d(\alpha\beta) - f(\alpha\beta) \equiv b(\alpha\beta) + C_0 \pmod 7 \ . \qquad \square
\end{aligned}$$

Theorem 6.3 (Complementary laws, $\boldsymbol{\lambda = 7}$). *Let $\beta \in \mathbb{Z}[\zeta]$ be primary and a, b, c, d, e, f given by (4.1) (with β in place of α). Then the following hold:*

$$\left(\frac{\pm 1}{\beta}\right)_7 = 1 \,, \qquad \left(\frac{\zeta}{\beta}\right)_7 = \zeta^{\frac{\mathbf{N}(\beta)-1}{7}} \ ,$$

$$\left(\frac{7}{\beta}\right)_7 = \zeta^{\frac{c}{7b} - \frac{d+3f}{b} + 3} \,, \qquad \left(\frac{\omega}{\beta}\right)_7 = \zeta^{\frac{4(\mathbf{N}(\beta)+6)}{7} - \frac{c}{7b}} \ ,$$

$$\left(\frac{\zeta+\zeta^6}{\beta}\right)_7 = \zeta^{\frac{f-2d}{b}} \,, \qquad \left(\frac{\zeta^2+\zeta^5}{\beta}\right)_7 = \zeta^{\frac{3(d-f)}{b}} \,, \qquad \left(\frac{\zeta^3+\zeta^4}{\beta}\right)_7 = \zeta^{\frac{2f-d}{b}} \ .$$

Proof. The complementaries for ± 1 and ζ are just a re-statement of Corollary 3.6. It suffices to prove the remaining results for $\beta = \pi\psi$ where π and ψ are primary primes. Note that Corollary 2.3 and Lemma 4.1 imply

$$\frac{F(\pi\psi)}{b(\pi\psi)} \equiv \frac{F(\pi\psi)}{b(\pi)b(\psi)} \equiv \frac{F(\pi)}{b(\pi)} + \frac{F(\psi)}{b(\psi)} \pmod 7$$

for $F = d$ and $F = f$. Furthermore, by Corollary 2.3 and Lemma 6.2,

$$\frac{c(\pi\psi)}{7b(\pi\psi)} \equiv \frac{c(\pi\psi)}{7b(\pi)b(\psi)} \equiv \frac{c(\pi)}{7b(\pi)} + \frac{c(\psi)}{7b(\psi)} + 3 \pmod 7 \ .$$

Finally, note that 49 divides

$$(\mathbf{N}(\pi) - 1)(\mathbf{N}(\psi) - 1) = (\mathbf{N}(\pi\psi) - 1) - (\mathbf{N}(\pi) - 1) - (\mathbf{N}(\psi) - 1) \ ,$$

so

$$\frac{\mathbf{N}(\pi\psi) - 1}{7} \equiv \frac{\mathbf{N}(\pi) - 1}{7} + \frac{\mathbf{N}(\psi) - 1}{7} \pmod 7 \ .$$

The above identities are sufficient to verify all the claims of the theorem. □

7. A Norm-Euclidean Algorithm, $\lambda \leq 11$

The ring $\mathbb{Z}[\zeta]$, with ζ a primitive λ-th root of unity and λ an odd prime, is known to be norm-Euclidean for $\lambda \leq 13$. For $\lambda \leq 11$, a very efficient norm-Euclidean algorithm was provided in [22,23], based on the work of Lenstra [16]; see also Chapter 6 of [2]. This is the method that we will use here. For completeness, we mention that a norm-Euclidean algorithm for $\lambda = 13$ was given in [18].

If $\mathbb{Z}[\zeta]$ is norm-Euclidean, then there exists for all $\alpha, \beta \in \mathbb{Z}[\zeta]$ with $\beta \neq 0$ an element $\rho \in \mathbb{Z}[\zeta]$ such that $\alpha \equiv \rho \pmod \beta$ and $\mathbf{N}(\rho) < \mathbf{N}(\beta)$. By setting $x = \alpha/\beta \in \mathbb{Q}(\zeta)$ and $y = (\alpha - \rho)/\beta = x - \rho/\beta \in \mathbb{Z}[\zeta]$, this is equivalent to finding for any $x \in \mathbb{Q}(\zeta)$ an element $y \in \mathbb{Z}[\zeta]$ with $\mathbf{N}(x - y) < 1$. In other words, one needs to generate $y \in \mathbb{Z}[\zeta]$ "close" to $x \in \mathbb{Q}(\zeta)$ with respect to the norm.

Assume henceforth that $\lambda \leq 11$. For any element $x \in \mathbb{Z}[\zeta]$, define

$$\mu(x) = \mathbf{T}(x\overline{x}) = \sum_{i=1}^{\lambda-1} |\sigma_i(x)|^2 \ .$$

Then the arithmetic-geometric mean inequality yields

$$\mathbf{N}(x) \leq \left(\frac{\mu(x)}{\lambda - 1}\right)^{(\lambda-1)/2} \ .$$

Lenstra's method finds for every $x \in \mathbb{Q}(\zeta)$ an element $y \in \mathbb{Z}[\zeta]$ with $\mu(x - y) \leq (\lambda^2 - 1)/12$. This implies

$$\mathbf{N}(x - y) \leq \left(\frac{\lambda + 1}{12}\right)^{(\lambda-1)/2} \ .$$

In the case when $\lambda = 7$, this produces the very good bound $\mathbf{N}(x - y) \leq 8/27 < 0.3$.

The idea of the technique is as follows. If $x \in \mathbb{Z}[\zeta]$, then one can simply take $y = x$, so assume that $x \in \mathbb{Q}(\zeta) \setminus \mathbb{Z}[\zeta]$. Write x as a rational linear combination of all the λ powers ζ^i, $0 \leq i \leq \lambda - 1$; note that such a representation is no longer unique. By adding the expression $1 + \zeta + \zeta^2 + \cdots + \zeta^{\lambda-1} = 0$ sufficiently many times to this representation, we may write x as $x = \sum_{i=0}^{\lambda-1} x_i \zeta^i$ with $x_i \geq 0$ for $0 \leq i \leq \lambda - 1$. Set $y = \sum_{i=0}^{\lambda-1} y_i \zeta^i \in \mathbb{Z}[\zeta]$ with $y_i = \lfloor x_i \rfloor$; note that $y_i \in \mathbb{Z}$ and $y_i \geq 0$ for $0 \leq i \leq \lambda - 1$. In addition, set $z = x - y = \sum_{i=0}^{\lambda-1} z_i \zeta^i \in \mathbb{Q}(\zeta)$.

One now systematically adds powers of ζ to z, and subtracts the corresponding power from y to leave x intact. Specifically, sort the z_i in non-descending order, say $0 \leq z_{e_0} \leq z_{e_1} \leq \ldots \leq z_{e_{\lambda-1}}$, where $(e_0, e_1, \ldots, e_{\lambda-1})$ is an appropriate permutation of $(0, 1, \ldots, \lambda-1)$. Now set $z^{(0)} = z$, $z^{(k)} = z^{(k-1)} + \zeta^{e_k}$, $y^{(0)} = y$, $y^{(k)} = y^{(k-1)} - \zeta^{e_k}$ for $0 \leq k \leq \lambda - 1$. Then $x = y + z = y^{(k)} + z^{(k)}$ for all k, and $z^{(\lambda-1)} = z^{(0)}$. Lenstra proved that at least one of the values $z^{(k)}$ satisfies $\mu(z^{(k)}) \leq (\lambda^2 - 1)/12$, in which case $\mathbf{N}(x - y^{(k)}) < 1$ by our above remarks. (For $\lambda = 11$, equality is theoretically possible here, but this can only happen if $x \in \mathbb{Z}[\zeta]$, which was ruled out from the beginning.)

For the development of his theory, Lenstra specified $x_i \geq 0$; however, for the actual algorithm, this is in fact unnecessary. This is because for any $M \in \mathbb{Z}$, $x = \sum_{i=0}^{\lambda-1} (x_i + M)\zeta^i$. The order of the elements $z_i + M$ is the same as that of the x_i, and the value of y does not change. The overall algorithm is given below (see Algorithm 6.4 of [22] and Algorithm 5.1 of [23]).

Algorithm 7.1 (Approximating a cyclotomic number by a cyclotomic integer, $\lambda \leq 11$).
Input: An element $x = \sum_{i=0}^{\lambda-1} x_i \zeta^i \in \mathbb{Q}(\zeta)$.
Output: An element $y \in \mathbb{Z}[\zeta]$ such that $\mathbf{N}(x - y) < 1$.

(1) If $x \in \mathbb{Z}[\zeta]$, then output $y = x$ and terminate.
(2) For $0 \leq i \leq \lambda - 1$ set $y_i = \lfloor x_i \rfloor$ and $z'_i = x_i - y_i$. Set $z = \displaystyle\sum_{i=0}^{\lambda-1} z'_i \zeta^i$, $y = \displaystyle\sum_{i=0}^{\lambda-1} y_i \zeta^i$.
(3) Sort the z'_i in non-descending order: set $z_i = z'_{e_i}$ such that $z_0 \leq z_1 \leq \cdots \leq z_{\lambda-1}$.
(4) While $\mu(z) > (\lambda^2 - 1)/12$ do
   (a) Replace y by $y - \zeta^{e_0}$ and z by $z + \zeta^{e_0}$.
   (b) Set $t = z_0$, $z_0 = z_1$, $\ldots z_{\lambda-2} = z_{\lambda-1}$, $z_{\lambda-1} = t + 1$.

The algorithm finds $y \in \mathbb{Z}[\zeta]$ with $\mathbf{N}(x - y) < 1$ after at most λ tests of the "while" condition in step 4. The following is a formulation of the norm-Euclidean algorithm that is suitable for our purposes.

Algorithm 7.2 (Norm-Euclidean division, $\lambda \leq 11$).
Input: $\alpha, \beta \in \mathbb{Z}[\zeta]$ with β non-zero.
Output: $\rho \in \mathbb{Z}[\zeta]$ such that $\alpha \equiv \rho \pmod{\beta}$ and $\mathbf{N}(\rho) < \mathbf{N}(\beta)$.

(1) Set $x = \alpha/\beta = \alpha\sigma_2(\beta)\sigma_3(\beta)\ldots\sigma_{\lambda-1}(\beta)/\mathbf{N}(\beta)$.
(2) Find $y \in \mathbb{Z}[\zeta]$ such that $\mathbf{N}(x - y) < 1$ using Algorithm 7.1.

(3) Output $\rho = \alpha - y\beta$.

8. Efficient Residue Symbol Computation, $\lambda = 7$

We now have all the necessary tools to evaluate 7-th power residue symbols. The following algorithm explicitly computes the residue symbol $(\alpha/\beta)_7$. Note that $(\alpha/\beta)_7 = 0$ if and only $\gcd(\mathbf{N}(\alpha), \mathbf{N}(\beta)) > 1$, so we may assume that α and β are coprime. We also need to ensure that $\mathbf{T}(\beta) \not\equiv 0 \pmod 7$ as otherwise the residue symbol is not defined.

Algorithm 8.1 (Computing Residue Symbols, $\lambda = 7$).
Input: $\alpha, \beta \in \mathbb{Z}[\zeta]$ with $\mathbf{T}(\beta) \not\equiv 0 \pmod 7$ and $\gcd(\alpha, \beta) \simeq 1$.
Output: $s \in \mathbb{Z}$ with $0 \le s \le 6$ and $\left(\dfrac{\alpha}{\beta}\right)_7 = \zeta^s$.

(1) Initialize $s = 0$.
(2) Find a primary associate β' of β using Algorithm 5.3.
(3) While $\mathbf{N}(\alpha) > 1$ do
   (a) Find $\gamma \in \mathbb{Z}[\zeta]$ such that $\alpha \equiv \gamma \pmod\beta$ and $\mathbf{N}(\gamma) < \mathbf{N}(\beta')$ using Algorithm 7.2.
   (b) Write $\mathbf{N}(\gamma) = 7^i N$ with $N \not\equiv 0 \pmod 7$ and $i \ge 0$ and set $\gamma'' = \gamma\omega^{-i}$.
   (c) Find k, m, n, γ' so that $\gamma' = \zeta^k \eta_0^m \eta_1^n \gamma''$ is a primary associate of γ'', using Algorithm 5.3.
   (d) Compute

$$\begin{aligned} b &\equiv b(\beta') \pmod 7, & c &\equiv c(\beta') \pmod{49}, \\ d &\equiv d(\beta') \pmod 7, & f &\equiv f(\beta') \pmod 7, \end{aligned}$$

   and $b^{-1} \pmod 7$. Replace s by

$$s + i\left(\frac{6c}{7b} + \frac{4(\mathbf{N}(\beta')+6)}{7}\right) - k\frac{\mathbf{N}(\beta')-1}{7} - m\left(\frac{5d+f}{b}\right) - n\left(\frac{3d+4f}{b}\right) \pmod 7 .$$

   (e) Replace α by β' and β' by γ'.
(4) Output s.

Note that i as given in step 3 (b) is exactly the power of ω contained in γ, while k, m, and n are the powers of ζ, η_1, and η_2, respectively, which γ'' needs to be multiplied by to obtain a primary associate γ' of γ''. So we need to add the appropriate multiple of i as given by Theorem 6.3 to s in step 3 (d), while subtracting the suitable multiples of k, m, and n as given in the same theorem from s.

It is clear that $N(\alpha)$ strictly decreases in each iteration of the while loop, and since the input values are coprime, the algorithm eventually reaches a value of α that is a primary associate of $\gcd(\alpha, \beta) \simeq 1$. So α is a primary unit, and hence must

be ± 1 by Corollary 2.7. At that point $(\alpha/\beta)_7 = 1$ by Theorem 6.3. The number of iterations of the while loop is no more than the number of steps required when applying the norm-Euclidean algorithm to α and β, and is hence linear in $\log(N(\beta))$.

We implemented this algorithm on a Pentium(R) 4 laptop using the computer algebra system PARI/GP [3]. Even on inputs with norms as large as 150 decimal digits, the method took no more than a few milliseconds to find the 7-th power residue symbol.

An Example for $\lambda = 7$

We illustrate Algorithm 8.1 by computing the residue symbol $(\alpha/\beta)_7$ for

$$\alpha = 128\zeta + 80\zeta^2 + 44\zeta^3 + 161\zeta^4 - 21\zeta^5 + 189\zeta^6 \quad \text{and} \quad \beta = -3\zeta - 2\zeta^2 \ .$$

(1) Initialize $s = 0$.
(2) Algorithm 5.3 produces the primary associate

$$\beta' = \eta_1^4\beta = -17\zeta - 12\zeta^2 + \zeta^3 - 9\zeta^4 - 17\zeta^5 - 5\zeta^6$$

of β.
(3) The while condition is checked for the first time. We have $\mathbf{N}(\alpha) = 695653 > 1$, so the loop is entered.
   (a) Algorithm 7.2 finds

$$x = \frac{\alpha}{\beta'} = -\frac{25799}{463} - \frac{5513}{463}\zeta - \frac{16722}{463}\zeta^2 - \frac{16966}{463}\zeta^3 - \frac{5074}{463}\zeta^4 - \frac{25966}{463}\zeta^5 \ ,$$

   and after four iterations,

$$\begin{aligned} y &= \left\lfloor -\frac{25799}{463} \right\rfloor + \left\lfloor -\frac{5513}{463} \right\rfloor \zeta + \left\lfloor -\frac{16722}{463} \right\rfloor \zeta^2 + \left\lfloor -\frac{16966}{463} \right\rfloor \zeta^3 \\ &\quad + \left\lfloor -\frac{5074}{463} \right\rfloor \zeta^4 + \left\lfloor -\frac{25966}{463} \right\rfloor \zeta^5 - 1 - \zeta - \zeta^4 - \zeta^6 \\ &= -57 - 13\zeta - 37\zeta 62 - 37\zeta^3 - 12\zeta^4 - 57\zeta^5 - \zeta^6 \ . \end{aligned}$$

   Therefore, $\gamma = \alpha - y\beta' = -2\zeta - 10\zeta^2 - 6\zeta^3 + 2\zeta^4 - 7\zeta^5 - 10\zeta^6$, and $\mathbf{N}(\gamma) = 71 < 463) = \mathbf{N}(\beta)$.
   (b) Since $\mathbf{N}(\gamma) = 71 \not\equiv 0 \pmod 7$, we see that $i = 0$, so $\gamma'' = \gamma$.
   (c) Algorithm 5.3 finds $k = 4$, $m = 6$, $n = 3$, and

$$\gamma' = \zeta^4\eta_1^6\eta_2^3 = 73\zeta + 25\zeta^2 + 39\zeta^3 + 62\zeta^4 + 6\zeta^5 + 84\zeta^6 \ .$$

   (d) One easily computes $b(\beta') = -59 \equiv 4 \pmod 7$, $c(\beta') = -189 \equiv 7 \pmod{49}$, $d(\beta') \equiv 4 \pmod 7$, $f(\beta') \equiv 2 \pmod 7$ and $b^{-1}(\beta') \equiv 2 \pmod 7$. So recalling that $\mathbf{N}(\beta') = 463$, one obtains $s = 3$.
   (e) Set

$$\begin{aligned} \alpha &= -17\zeta - 12\zeta^2 + \zeta^3 - 9\zeta^4 - 17\zeta^5 - 5\zeta^6 \, , \\ \beta' &= 73\zeta + 25\zeta^2 + 39\zeta^3 + 62\zeta^4 + 6\zeta^5 + 84\zeta^6 \, . \end{aligned}$$

(3) The while condition is checked for the second time. We have: $\mathbf{N}(\alpha) = 463 > 1$, so the loop is entered.

(a) Algorithm 7.2 finds

$$x = \frac{\alpha}{\beta'} = +\frac{1093}{71} + \frac{922}{71}\zeta - \frac{151}{71}\zeta^2 + \frac{405}{71}\zeta^3 + \frac{1168}{71}\zeta^4 + \frac{289}{71}\zeta^5 \ ,$$

and after two iterations,

$$y = \left\lfloor \frac{1093}{71} \right\rfloor + \left\lfloor \frac{922}{71} \right\rfloor \zeta + \left\lfloor -\frac{151}{71} \right\rfloor \zeta^2 \left\lfloor \frac{405}{71} \right\rfloor \zeta^3 + \left\lfloor \frac{1168}{71} \right\rfloor \zeta^4 + \left\lfloor \frac{289}{71} \right\rfloor \zeta^5 \\ -\zeta^5 - \zeta^6 \ .$$

Therefore, $\gamma = \alpha - y\beta' = -48\zeta - 39\zeta^3 - 17\zeta^4 - 17\zeta^5 - 39\zeta^6$ and $\mathbf{N}(\gamma) = 1 < 71 = \mathbf{N}(\beta)$.

(b) Since $\mathbf{N}(\gamma) = 1 \not\equiv 0 \pmod 7$, we see that $i = 0$, so $\gamma'' = \gamma$.

(c) Algorithm 5.3 finds $k = 6$, $m = 2$, $n = 0$, and

$$\gamma' = \zeta^6\eta_1^2 = 157\zeta + 31\zeta^2 + 101\zeta^3 + 101\zeta^4 + 31\zeta^5 + 157\zeta^6 \ .$$

(d) We compute $b(\beta') = 289 \equiv 2 \pmod 7$, $c(\beta') = 1022 \equiv 42 \pmod{49}$, $d(\beta') \equiv 3 \pmod 7$, $f(\beta') \equiv 6 \pmod 7$ and $b^{-1}(\beta') \equiv 4 \pmod 7$. So recalling that $\mathbf{N}(\beta') = 71$, we obtain $s = 3 + 3 = 6$.

(e) Set

$$\alpha = 73\zeta + 25\zeta^2 + 39\zeta^3 + 62\zeta^4 + 6\zeta^5 + 84\zeta^6 \, , \\ \beta' = 157\zeta + 31\zeta^2 + 101\zeta^3 + 101\zeta^4 + 31\zeta^5 + 157\zeta^6 \, .$$

(3) The while condition is checked for the third time. We have $\mathbf{N}(\alpha) = 1$, so the while loop is skipped.

(4) The algorithm outputs $s = 6$.

The algorithm computes $(\alpha/\beta)_7 = \zeta^6$ after only two iterations of the while loop. Typically, many more iterations are required; we simply chose this example for its compactness. Note also that $\mathbf{N}(\beta) = 463 = 7 \cdot 66 + 1$ is a prime. So in this case, the residue symbol could also have been computed using Definition 3.1. That is, $(\alpha/\beta)_7 \equiv \alpha^{66} \pmod \beta$. PARI indeed verifies that $\alpha^{66} - \zeta^6$ is divisible by β; since the actual quotient is very large, we forego reproducing it here.

9. Conclusion

We developed a fast and effective algorithm for computing residue symbols of the form $(\alpha/\beta)_7$ in the cyclotomic field $\mathbb{Q}(\zeta)$, where ζ is a primitive 7-th root of unity. Just as in the efficient computation of Jacobi symbols, our method does not require the factorization of β, and has an analogous running time that is linear in $\log(\mathbf{N}(\beta))$ when expressed in terms of rational integer operations. The four major ingredients employed in our technique were:

- an explicit characterization of primary cyclotomic integers in $\mathbb{Z}[\zeta]$, together with an algorithm for finding a primary associate (unique up to sign) of any cyclotomic integer whose trace is not divisible by 7;
- Kummer's reciprocity law;
- explicit forms of Kummer's complementary laws for 7, the ramified prime $1-\zeta$, and the units ± 1, ζ, as well as the two fundamental units $\zeta + \zeta^6$ and $\zeta^2 + \zeta^5$ (along with the redundant complementary law for the unit $\zeta^3 + \zeta^4$);
- an efficient norm-Euclidean algorithm.

Our conditions for testing if a cyclotomic integer is primary, as well as the method for finding primary associates, involves only basic arithmetic on rational integers modulo 7. Similarly, our explicit form of the complementary laws requires only the computation of some very simple functions modulo 7 and 49 of the basis coefficients of the modulus when represented as a linear combination of the powers ζ^k for $1 \leq k \leq 6$. Moreover, they do not require the modulus to be prime. Finally, the norm-Euclidean method that we employed is based on work of Lenstra [16] and was first stated in explicit algorithmic form in [22] and [23]. For $\lambda = 7$, it generates a remainder whose norm is smaller than that of the divisor by a factor of at least $8/27$.

In principle, our method can be extended to other cyclotomic rings $\mathbb{Z}[\zeta]$ with ζ a primitive λ-th root of unity. Kummer's work assumes λ to be a regular prime. Lenstra's technique [16] extends to values of λ with $\varphi(\lambda) \leq 10$ and $\lambda \neq 16, 24$; here, φ denotes Euler's totient function. With these two restrictions, the above technique applies to the values $\lambda = 2, 3, 5, 7$ and 11. The only other regular prime for which $\mathbb{Q}(\zeta)$ is known to be norm-Euclidean is $\lambda = 13$. For this scenario, McKenzie [18] provided a highly combinatorial norm-Euclidean algorithm; the cases $\lambda = 17$ and $\lambda = 19$ remain undetermined.

Even for the case $\lambda = 11$, for which Euclidean division remains straightforward, the other details of the method get increasingly complicated. Finding explicit conditions for a cyclotomic integer to be primary becomes more and more technical, as does an algorithm to find a primary associate. The cyclotomic field generated by an 11-th primitive root of unity has four fundamental units, so complementary laws need to be found for three of them as well as for the ramified prime lying above 11 (or for 11 itself).

Finally, we remark that our method can be used to extend Williams' quadratic [26] and cubic [27] public key cryptosystem as well as the quintic system of [23] to the case $\lambda = 7$.

References

[1] M. Blum, Coin flipping by telephone. *Advances in Cryptology: A Report on CRYPTO 81*, University of California Santa Barbara, Dept. of Elec. and Computer Eng., ECE Report No 82-04, ed. A. Gersho, 1982, pp. 11-15.

[2] P. Caranay, *On Residue Symbols and Kummer's Reciprocity Law of Degree Seven*. MSc Thesis, University of Calgary (Canada), 2009. Available at `http://math.ucalgary.ca/profiles/perlas-caranay`

[3] H. Cohen, *PARI/GP Computer Algebra System*. Available for download at `http://pari.math.u-bordeaux.fr`.

[4] G. Eisenstein, Beweis des Reciprocitätssatzes für die cubischen Reste in der Theorie der aus dritten Wurzeln der Einheit zusammengesetzten complexen Zahen. *J. Reine Angew. Math.* **27** (1844), 289–310.

[5] G. Eisenstein, Nachtrag zum cubischen Reciprocitätssatze für die aus dritten Wurzeln der Einheit zusammengesetzten complexen Zahen. Criterien des cubischen Characters der Zahl 3 und ihrer Theiler. *J. Reine Angew. Math.* **28** (1844), 28–35.

[6] S. Goldwasser and S. Micali, Probabilistic Encryption. *J. Computer System Sci.* **28** (1984), 270–299

[7] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper; Teil 2: Reziprozitätsgesetz*. 2nd ed., Physica-Verlag, Vienna 1965.

[8] D. Hilbert, *The Theory of Algebraic Number Fields*. Translated from the German by I. T. Adamson with an Introduction by F. Lemmermeyer and N. Schappacher. Springer-Verlag, Berlin 1998.

[9] E. E. Kummer, Allgemeine Reziprozitätsgesetze für beliebig hohe Potenzreste. In *Collected Papers*, Vol. 1, ed. A. Weil, Springer-Verlag, Berlin 1975, 345–357.

[10] E. E. Kummer, Über die Ergänzungssätze zu den allgemeinen Reziprozitätsgesetzen. In *Collected Papers*, Vol. 1, ed. A. Weil, Springer-Verlag, Berlin 1975, 485–538.

[11] E. E. Kummer, Über die allgemeinen Reziprozitätsgesetze der Potenzreste. In *Collected Papers*, Vol. 1, ed. A. Weil, Springer-Verlag, Berlin 1975, 673–687.

[12] E. E. Kummer, Zwei neue Beweise der allgemeinen Reziprozitätsgesetze unter den Resten und Nichtresten der Potenzen, deren Grad eine Primzahl ist. In *Collected Papers*, Vol. 1, ed. A. Weil, Springer-Verlag, Berlin 1975, 842–882.

[13] E. E. Kummer, Über die Ergänzungssätze zu den allgemeinen Reziprozitätsgesetzen. In *Collected Papers*, Vol. 1, ed. A. Weil, Springer-Verlag, Berlin 1975, 688–698.

[14] E. E. Kummer, Über die allgemeinen Reziprozitätsgesetze unter den Resten und Nichtresten der Potenzen, deren Grad eine Primzahl ist. In *Collected Papers*, Vol. 1, ed. A. Weil, Springer-Verlag, Berlin 1975, 699–839.

[15] F. Lemmermeyer, The Euclidean algorithm in algebraic number fields. An update of an article published in *Expo. Math.* **13** (1995) 385–416. Available at `http://www.fen.bilkent.edu.tr/~franz/publ/survey.pdf`.

[16] H. W. Lenstra, Jr., Euclid's algorithm in cyclotomic fields. *J. London Math. Soc.* **10** (1975) 457–465.

[17] J. M. Masley and H. L. Montgomery, Cyclotomic fields with unique factorization. *J. Reine Angew. Math.* **286-287** (1976) 248–256.

[18] R. G. McKenzie, *The Ring of Cyclotomic Integers of Modulus Thirteen is Norm-Euclidean*. PhD Dissertation, Michigan State University (USA), 1988.

[19] M. O. Rabin, *Digitized signatures and public-key functions as intractable as factorization*. MIT Lab for Computer Science Technical Report LCS/TR-212, 1979.

[20] P. Ribenboim, *Classical Theory of Algebraic Numbers*. Springer-Verlag, New York 2001.

[21] R. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems. *Comm. ACM* **21** (1978), 120–126.

[22] R. Scheidler, *Applications of Algebraic Number Theory to Cryptography*. PhD Dissertation, University of Manitoba (Canada), 1993.

[23] R. Scheidler and H. C. Williams, A public-key cryptosystem utilizing cyclotomic fields. *Designs, Codes, and Cryptography* **6** (1995), 117–131.

[24] H. J. S. Smith, Report on the Theory of Numbers. In *Collected Mathematical Papers*,

Vol. 1, Chelsea Publishing Company, 1979.

[25] L. C. Washington, *Introduction to Cyclotomic Fields*. 2nd. ed., Springer-Verlag, New York 1997.

[26] H. C. Williams, A modification of the RSA public-key encryption procedure. *IEEE Trans. Inf. Theory* **IT-26** (6) (1980), 726-729.

[27] H. C. Williams, An M^3 public-key encryption scheme. In *CRYPTO '85 Proceedings*, *Lect. Notes Comp. Sci* **218**, Springer-Verlag, Berlin 1986, 358–368.

[28] K. S. Williams, Explicit forms of Kummer's complementary theorems to his law of quintic reciprocity. *J. Reine Angew. Math.* **288** (1976) 207–210.