Research Article

Marc Joye*, Oleksandra Lapiha, Ky Nguyen, and David Naccache

The Eleventh Power Residue Symbol

https://doi.org/10.1515/jmc-2020-0077
Received Jun 05, 2020; accepted Jul 01, 2020

Abstract: This paper presents an efficient algorithm for computing 11^{th}-power residue symbols in the cyclotomic field $\mathbb{Q}(\zeta_{11})$, where ζ_{11} is a primitive 11^{th} root of unity. It extends an earlier algorithm due to Caranay and Scheidler (Int. J. Number Theory, 2010) for the 7^{th}-power residue symbol. The new algorithm finds applications in the implementation of certain cryptographic schemes.

Keywords: Power residue symbol, Cyclotomic field, Reciprocity law, Cryptography

2010 Mathematics Subject Classification: 11A15, 11R18, 11A05, 11Y40, 11T71

1 Introduction

Quadratic and higher-order residuosity is a useful tool that finds applications in several cryptographic constructions. Examples include [6, 13, 14, 19] for encryption schemes and [1, 2, 12] for authentication schemes and digital signatures. A central operation therein is the evaluation of a residue symbol of the form $\left[\frac{a}{\lambda}\right]$ without factoring the modulus λ in the cyclotomic field $\mathbb{Q}(\zeta_p)$, where ζ_p is a primitive p^{th} root of unity.

For the case $p = 2$, it is well known that the Jacobi symbol can be computed by combining Euclid's algorithm with quadratic reciprocity and the complementary laws for -1 and 2; see e.g. [10, Chapter 1]. This eliminates the necessity to factor the modulus. In a nutshell, the computation of the Jacobi symbol $\left(\frac{a}{n}\right)_2$ proceeds by repeatedly performing 3 steps: (i) reduce a modulo n so that the result (in absolute value) is smaller than $n/2$, (ii) extract the sign and the powers of 2 for which the symbol is calculated explicitly with the complementary laws, and (iii) apply the reciprocity law resulting in the 'numerator' and 'denominator' of the symbol being flipped. Eventually, the numerator of the symbol becomes ± 1 and the algorithm terminates with the value of $\left(\frac{a}{n}\right)_2$. Under certain conditions, this methodology naturally extends to higher values for p. The case $p = 3$ is discussed in [4, 14, 19], the case $p = 4$ in [4, 18], the case $p = 5$ in [14], the case $p = 7$ in [3], and the case $p = 8$ in [10, Chapter 9].

Caranay and Scheidler describe a generic algorithm in [3, Section 7] for computing the p^{th}-power residue symbol for any *prime* $p \leq 11$, building on Lenstra's norm-Euclidean algorithm. They also provide a detailed implementation for the case $p = 7$. The case $p = 11$ is difficult. We quote from [3]:

> *"Even for the case $p = 11$, 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)."*

The general case is addressed in a recent algorithm by de Boer and Pagano [5].

***Corresponding Author: Marc Joye:** Zama, Paris, France; Email: marc.joye@zama.ai
Oleksandra Lapiha: École normale supérieure, Paris, France
Ky Nguyen: École normale supérieure, Paris, France
David Naccache: École normale supérieure, Paris, France

Our contributions

This paper takes up the challenge put forward in [3] and presents the first implementation of the Caranay–Scheidler algorithm for the 11^{th}-power residue symbol. The contributions of this paper are three-fold: We provide explicit conditions for primary algebraic integers in $\mathbb{Z}[\zeta_{11}]$; we devise an efficient algorithm for finding a primary associate; and we give explicit complementary laws for a set of four fundamental units and for the special prime $1-\zeta_{11}$.

Organization

The rest of this paper is organized as follows. In Section 2, we review some basic definitions and known results on cyclotomic fields. Section 3 particularizes to the 11^{th} cyclotomic field. We establish and prove an efficient criterion for primary cyclotomic integers. We also define a set of four fundamental units and give explicit formulas to find their index. Section 4 is the core of the paper. We present the ingredients and develop the companion algorithms for the computation of the eleventh power residue symbol.

2 Higher-Order Power Residue Symbols

Throughout this section, $p \le 13$ denotes an odd rational prime.

2.1 Basic definitions and notation

Fix $\zeta := \zeta_p = e^{2\pi i/p}$ a primitive p^{th} root of unity and let $\omega = 1-\zeta$. The number field $\mathbb{Q}(\zeta)$ defines the p^{th} *cyclotomic field*. The ring of integers of $\mathbb{Q}(\zeta)$ is $\mathbb{Z}[\zeta]$ and is *norm-Euclidean* [9, 11] (in particular, it is a unique factorization domain). Since $\zeta, \zeta^2, \ldots, \zeta^{p-1}$ form an integral basis for $\mathbb{Q}(\zeta)$, any element $\alpha \in \mathbb{Z}[\zeta]$ can be expressed as $\alpha = \sum_{j=1}^{p-1} a_j \zeta^j$ with $a_j \in \mathbb{Z}$. The norm and trace of $\alpha \in \mathbb{Z}[\zeta]$ are the rational integers respectively given by $\mathbf{N}(\alpha) = \prod_{k=1}^{p-1} \sigma_k(\alpha)$ and $\mathbf{T}(\alpha) = \sum_{k=1}^{p-1} \sigma_k(\alpha)$, where $\sigma_k : \zeta \mapsto \zeta^k$. The group of units of $\mathbb{Z}[\zeta]$ is the direct product of $\langle \pm\zeta \rangle$ and a free abelian group $\mathcal{E}$ of rank $r = (p-3)/2$. The generators of $\mathcal{E}$ are called *fundamental units* and will be denoted by $\eta_1, \ldots, \eta_r$. Two elements α and β are called *associates* if they differ only by a unit factor. We write $\alpha \sim \beta$.

We follow the approach of Kummer. A central notion is that of primary elements (see [7, p. 158]) in $\mathbb{Z}[\zeta]$.

Definition 2.1. An element $\alpha \in \mathbb{Z}[\zeta]$ is said to be *primary* whenever it satisfies

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

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

Lemma 2.2 ([3, Lemma 2.6])**.** *Every element $\alpha \in \mathbb{Z}[\zeta]$ with $\alpha \not\equiv 0 \pmod{\omega}$ has a primary associate $\alpha^\star$ of the form*

$$\alpha^\star = \pm\zeta^{e_0}\eta_1^{e_1}\cdots\eta_r^{e_r}\alpha \quad \text{where } 0 \le e_0, e_1, \ldots, e_r \le p-1 \ .$$

Moreover, $\alpha^\star$ is unique up to its sign.

2.2 Kummer's reciprocity law

Let $\alpha, \pi \in \mathbb{Z}[\zeta]$ with π prime, $\pi \nmid \omega$, and $\pi \nmid \alpha$. The *p^{th}-power residue symbol* $\left[\frac{\alpha}{\pi}\right]_p$ is then defined to be the p^{th}-root of unity ζ^i such that

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

This exponent i (with $0 \le i \le p-1$) is called the *index* of α w.r.t. π and is noted $\mathrm{ind}_\pi(\alpha)$. If π divides α then $\left[\frac{\alpha}{\pi}\right]_p = 0$.

Analogously to the Legendre symbol, the p^{th}-power residue symbol generalizes: For any $\alpha, \lambda \in \mathbb{Z}[\zeta]$ with λ non-unit and $\gcd(\lambda, \omega) \sim 1$, writing $\lambda = \prod_j \pi_j^{e_j}$ for primes π_j in $\mathbb{Z}[\zeta]$, the generalized p^{th}-power residue symbol $\left[\frac{\alpha}{\lambda}\right]_p$ is defined as $\left[\frac{\alpha}{\lambda}\right]_p = \prod_j \left[\frac{\alpha}{\pi_j}\right]_p^{e_j}$.

Kummer [7] stated the reciprocity law in 1850 (see also [15, Art. 54]). It is restricted to so-called "regular" primes,[1] which include odd primes $p \le 13$. Although initially formulated for primary primes in $\mathbb{Z}[\zeta]$, the reciprocity law readily extends to all primary elements; see [3, Corollary 3.4].

Theorem 2.3 (Kummer's Reciprocity Law)**.** *Let α and λ be two primary elements in $\mathbb{Z}[\zeta]$. Then* $\left[\frac{\alpha}{\lambda}\right]_p = \left[\frac{\lambda}{\alpha}\right]_p$.

2.3 Complementary laws

The special prime ω and its conjugates are excluded from Kummer's reciprocity law. Moreover, it does not apply to units other than ± 1 as they are not primary. For these elements, the p^{th}-power residue symbol is determined through *complementary laws*, also stated by Kummer [7, 8] (see also [15, Art. 55]). The complementary laws rely on the *logarithmic differential quotients* given by

$$\Delta_n(\alpha) = \left.\frac{\mathrm{d}^n \ln\big(F(e^v)\big)}{\mathrm{d}v^n}\right|_{v=0}$$

for any $\alpha = \sum_{j=1}^{p-1} a_j \zeta^j \in \mathbb{Z}[\zeta]$ with $\mathbf{T}(\alpha) \neq 0$ and where $F(X) = \sum_{j=0}^{p-2} b_j X^j \in \mathbb{Z}[X]$ whose coefficients are $b_0 = -a_{p-1}$ and $b_j = a_j - a_{p-1}$ for $1 \le j \le p-2$. Notice that $\alpha = F(\zeta)$.

Theorem 2.4 (Complementary Laws)**.** *Let π be a primary prime in $\mathbb{Z}[\zeta]$. Then,*

1. $\mathrm{ind}_\pi(p) \equiv \frac{\Delta_p(\pi)}{p} \pmod p$;
2. *for any unit $\varepsilon \in \mathbb{Z}[\zeta]^\star$,*

$$\mathrm{ind}_\pi(\varepsilon) \equiv \Delta_1(\varepsilon)\,\tfrac{\mathbf{N}(\pi)-1}{p} + \sum_{i=1}^{r} \Delta_{2i}(\varepsilon)\Delta_{p-2i}(\pi) \pmod p$$

where $r = (p-3)/2$.

For completeness, we give the complementary laws for ± 1 and ζ. Alternatively, they can be obtained directly from the definition of the p^{th}-power residue symbol. The next corollary is a straightforward extension to composite moduli.

Corollary 2.5 ([3, Corollary 3.6])**.** *Let $\lambda \in \mathbb{Z}[\zeta]$ such that $\omega \nmid \lambda$. Then* $\left[\frac{\pm 1}{\lambda}\right]_p = 1$ *and* $\left[\frac{\zeta}{\lambda}\right]_p = \zeta^{\frac{\mathbf{N}(\lambda)-1}{p} \bmod p}$.

3 The Case $p = 11$

This section presents results for the special case $p = 11$. We henceforth assume that $\zeta := \zeta_{11}$ is a primitive 11^{th} root of unity.

1 An odd prime p is said to be *regular* if it does not divide the class number of $\mathbb{Q}(\zeta_p)$.

3.1 Primary elements

Definition 2.1 explicitly characterizes primary elements. The next proposition specializes it for prime $p = 11$ in order to have a simple criterion involving only rational integers.

It is useful to introduce some notation. For $\alpha = \sum_{j=1}^{10} a_j \zeta^j \in \mathbb{Z}[\zeta]$, we define the rational integers $A_k(\alpha) = \sum_{j=1}^{10} a_j j^k$, for $0 \le k \le 9$. Also, when $A_0(\alpha) \not\equiv 0 \pmod{11}$, we define $\mathsf{a}_j(\alpha) = \frac{A_j(\alpha)}{A_0(\alpha)} \bmod 11$, for $1 \le j \le 9$. Notice that $A_0(\alpha) = -\mathbf{T}(\alpha)$.

Proposition 3.1. *Let $\alpha = \sum_{j=1}^{10} a_j \zeta^j \in \mathbb{Z}[\zeta]$ and $A_k := A_k(\alpha)$. Then α is primary if and only if the following conditions hold:*

1. $A_0 \not\equiv 0 \pmod{11}$;
2. $A_1 \equiv 0 \pmod{11}$;
3. $A_2 \equiv A_4 \equiv 0 \pmod{11}$;
4. $A_0 A_6 + {A_3}^2 \equiv 0 \pmod{11}$;
5. $A_3 A_5 - A_0 A_8 \equiv 0 \pmod{11}$.

Proof. Let $\omega = 1 - \zeta$. From Definition 2.1, α is primary if and only if $\alpha \not\equiv 0 \pmod{\omega}$, $\alpha \equiv B \pmod{\omega^2}$, and $\alpha\overline{\alpha} \equiv B^2 \pmod{11}$ for some rational integer B. We have $\sum_{i=1}^{10} a_j \zeta^j \equiv \sum_{j=1}^{10} a_j (1-\omega)^j \equiv \sum_{j=1}^{10} a_j (1 - j\omega) \equiv A_0 - A_1\,\omega \pmod{\omega^2}$. As a result, the condition $\alpha \not\equiv 0 \pmod{\omega}$ is equivalent to $A_0 \not\equiv 0 \pmod{\omega}$, and the condition $\alpha \equiv B \pmod{\omega^2}$ with $B = A_0 \in \mathbb{Z}$ is equivalent to $A_1\,\omega \equiv 0 \pmod{\omega^2} \iff A_1 \equiv 0 \pmod{\omega}$. We observe that rational integers are congruent modulo ω if and only if they are congruent modulo p (in this case 11). We therefore have $A_0 \not\equiv 0 \pmod{\omega} \iff A_0 \not\equiv 0 \pmod{11}$ and $A_1 \equiv 0 \pmod{\omega} \iff A_1 \equiv 0 \pmod{11}$.

It remains to look at the third condition, $\alpha\overline{\alpha} \equiv {A_0}^2 \pmod{11}$. Using matrix notation and defining the Vandermonde matrix

$$\mathbf{V} = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & 2 & 2^2 & \dots & 2^9 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 10 & 10^2 & \dots & 10^9 \end{pmatrix} \pmod{11},$$

we can express $(A_0, \dots, A_9)$ as $(A_0, \dots, A_9) = (a_1, \dots, a_{10})\,\mathbf{V}$. In turn, we can write $\alpha \equiv \sum_{j=1}^{10} a_j (1-\omega)^j \equiv (a_1, \dots, a_{10}) \left(1-\omega, \dots, (1-\omega)^{10}\right)^\intercal \equiv (A_0, \dots, A_9)\,\mathbf{V}^{-1} \left((1-\omega), \dots, (1-\omega)^{10}\right)^\intercal \pmod{11}$. Similarly, we can write $\overline{\alpha} \equiv \sum_{j=1}^{10} a_j \zeta^{11-j} \equiv \sum_{j=1}^{10} a_j (1-\omega)^{11-j} \equiv (A_0, \dots, A_9)\,\mathbf{V}^{-1} \left((1-\omega)^{10}, \dots, (1-\omega)\right)^\intercal$. Hence, noting that $\omega^{10} \sim 11$, the product $\alpha\overline{\alpha} \pmod{11}$ can be put after a little algebra in the form of a degree-9 polynomial in ω:

$$\begin{aligned} \alpha\overline{\alpha} \equiv\ & {A_0}^2 \left(A_0 A_2 - {A_1}^2\right) \omega^2 + \left(A_0 A_2 - {A_1}^2\right) \omega^3 + \left(A_0 A_4 - 4A_1 A_3 + 3{A_2}^2\right) \omega^4 \\ & + \left(-A_0 A_2 + 2A_0 A_4 + {A_1}^2 + 3A_1 A_3 - 5{A_2}^2\right) \omega^5 + \left(4A_0 A_2 + A_0 A_4 - 4A_0 A_6 - 4{A_1}^2 - 4A_1 A_3 + 2A_1 A_5\right. \\ & \left. + 3{A_2}^2 - 5A_2 A_4 - 4{A_3}^2\right) \omega^6 \\ & + \left(4A_0 A_2 - 2A_0 A_4 - A_0 A_6 - 4{A_1}^2 - 3A_1 A_3 - 5A_1 A_5 + 5{A_2}^2 - 4A_2 A_4 - {A_3}^2\right) \omega^7 \\ & + \left(-5A_0 A_4 - A_0 A_6 - 4A_0 A_8 - 2A_1 A_3 - 5A_1 A_5 - A_1 A_7\right. \\ & \left. - 4{A_2}^2 - 4A_2 A_4 - 2A_2 A_6 - {A_3}^2 + 4A_3 A_5 + 3{A_4}^2\right) \omega^8 \\ & + \left(4A_0 A_2 + 5A_0 A_4 - 3A_0 A_6 - 5A_0 A_8 - 4{A_1}^2 + 2A_1 A_3 - 4A_1 A_5\right. \\ & \left. - 4A_1 A_7 + 4{A_2}^2 - A_2 A_4 + 3A_2 A_6 - 3{A_3}^2 + 5A_3 A_5 + {A_4}^2\right) \omega^9 \\ & \pmod{11}\ . \end{aligned} \tag{1}$$

For conciseness, we write C_j the rational coefficient of ω^j in the right hand side of Eq. (1): $\alpha\overline{\alpha} \equiv {A_0}^2 + \sum_{j=2}^{9} C_j\,\omega^j \pmod{11}$. The condition $\alpha\overline{\alpha} \equiv {A_0}^2 \pmod{11}$ can be thus rewritten as $\sum_{j=2}^{9} C_j\,\omega^j \equiv 0 \pmod{11}$. Further, since $\omega^j \mid 11$ for $2 \le j \le 9$, we get $C_2\,\omega^2 \equiv 0 \pmod{\omega^3} \iff C_2 \equiv 0 \pmod{\omega} \iff C_2 \equiv 0 \pmod{11}$, $C_2\,\omega^2 + C_3\,\omega^3 \equiv C_3\,\omega^3 \equiv 0 \pmod{\omega^4} \iff C_3 \equiv 0 \pmod{\omega} \iff C_3 \equiv 0 \pmod{11}$, and so on: $C_4 \equiv 0$

(mod 11), …, $C_9 \equiv 0 \pmod{11}$. Now, assuming $A_0 \not\equiv 0 \pmod{11}$ and $A_1 \equiv 0 \pmod{11}$ in Eq. (1), the congruences $C_2 \equiv C_3 \equiv C_4 \equiv \cdots \equiv C_9 \equiv 0 \pmod{11}$ yield $A_2 \equiv A_4 \equiv A_0A_6 + {A_3}^2 \equiv -A_0A_8 + A_3A_5 \equiv 0 \pmod{11}$. This completes the proof. □

3.2 Fundamental units

For $p = 11$, the `fundamental_units()` function from SageMath [16] provides the set $\{\upsilon_1, \upsilon_2, \upsilon_3, \upsilon_4\}$ of fundamental units, with $\upsilon_1 = \zeta + 1$, $\upsilon_2 = \zeta^2 + 1$, $\upsilon_3 = \zeta^2 + \zeta + 1$, $\upsilon_4 = \zeta^6 + \zeta$.

Every unit can be rendered real by multiplying it by some power of ζ. Another set of fundamental units is so given by $\{\eta_1, \eta_2, \eta_3, \eta_4\}$ with $\eta_1 = \zeta^5\,\upsilon_1$, $\eta_2 = \zeta^{10}\,\upsilon_2$, $\eta_3 = \zeta^{10}\,\upsilon_3$, and $\eta_4 = \zeta^2\,\upsilon_4$. Observe that

$$\eta_1 = \zeta^5 + \zeta^{-5}\,, \qquad \eta_2 = \zeta + \zeta^{-1}\,, \qquad \eta_3 = \zeta^{-1}(1 + \zeta + \zeta^2)\,, \qquad \eta_4 = \zeta^3 + \zeta^{-3}\,,$$

and $\eta_i = \sigma_{-1}(\eta_i)$ for $1 \le i \le 4$, where $\sigma_{-1}\colon \zeta \mapsto \zeta^{-1}$. We will use this set $\{\eta_1, \eta_2, \eta_3, \eta_4\}$ of fundamental units in later computations.

Remark 3.2. Suppose $\alpha \in \mathbb{Z}[\zeta]$ is real (i.e., $\alpha = \overline{\alpha}$). Then $2A_1(\alpha) \equiv A_1(2\alpha) \equiv A_1(\alpha + \overline{\alpha}) \equiv 0 \pmod{11} \iff A_1(\alpha) \equiv 0 \pmod{11}$. Since the units $\eta_1, \ldots, \eta_4$ are real, it follows that $A_1(\eta_1) \equiv A_1(\eta_2) \equiv A_1(\eta_3) \equiv A_1(\eta_4) \equiv 0 \pmod{11}$.

We now apply Theorem 2.4 to find the index of the fundamental units η_i, $1 \le i \le 4$, and of special prime ω.

Proposition 3.3. *Let π be a primary prime in $\mathbb{Z}[\zeta]$. Then*

$$\begin{aligned}
\operatorname{ind}_\pi(\eta_1) &\equiv \mathsf{a}_3(\pi) + 3\mathsf{a}_5(\pi) + 4\mathsf{a}_7(\pi) + 4\mathsf{a}_6(\pi)\mathsf{a}_3(\pi) + 3\mathsf{a}_9(\pi) \pmod{11}\,,\\
\operatorname{ind}_\pi(\eta_2) &\equiv 3\mathsf{a}_3(\pi) + 5\mathsf{a}_5(\pi) - 2\mathsf{a}_7(\pi) + 5\mathsf{a}_6(\pi)\mathsf{a}_3(\pi) + \mathsf{a}_9(\pi) \pmod{11}\,,\\
\operatorname{ind}_\pi(\eta_3) &\equiv 2\mathsf{a}_3(\pi) - 2\mathsf{a}_5(\pi) + 3\mathsf{a}_7(\pi) - 4\mathsf{a}_6(\pi)\mathsf{a}_3(\pi) - 3\mathsf{a}_9(\pi) \pmod{11}\,,\\
\operatorname{ind}_\pi(\eta_4) &\equiv 4\mathsf{a}_3(\pi) + 4\mathsf{a}_5(\pi) + 3\mathsf{a}_7(\pi) + \mathsf{a}_6(\pi)\mathsf{a}_3(\pi) - 2\mathsf{a}_9(\pi) \pmod{11}\,,
\end{aligned}$$

and

$$\operatorname{ind}_\pi(\omega) \equiv 5\mathsf{a}_6(\pi)\mathsf{a}_3(\pi) - 2\mathsf{a}_6(\pi)\mathsf{a}_5(\pi) - \mathsf{A}_1(\pi) - 5\,\tfrac{\mathbf{N}(\pi)-1}{11} - 5 \pmod{11}$$

where $\mathsf{A}_1(\pi) = \frac{\frac{A_1(\pi)}{A_0(\pi)} \bmod 121}{11}$.

Proof. Let $\pi \in \mathbb{Z}[\zeta]$ be a primary prime. Recalling that $A_1(\eta_i) \equiv 0 \pmod{11}$ for $1 \le i \le 4$, we have $\Delta_1(\eta_i) \equiv 0 \pmod{11}$; see Appendix A. Applied to η_i, the general formula for computing the index w.r.t. a primary prime (cf. Theorem 2.4) becomes $\operatorname{ind}_\pi(\eta_i) \equiv \Delta_2(\eta_i)\Delta_9(\pi) + \Delta_4(\eta_i)\Delta_7(\pi) + \Delta_6(\eta_i)\Delta_5(\pi) + \Delta_8(\eta_i)\Delta_3(\pi) \pmod{11}$. An application of the formulas given in Appendix A yields

	$\Delta_2(\eta_i) \bmod 11$	$\Delta_4(\eta_i) \bmod 11$	$\Delta_6(\eta_i) \bmod 11$	$\Delta_8(\eta_i) \bmod 11$
$i = 1$	3	4	3	1
$i = 2$	1	9	5	3
$i = 3$	8	3	9	2
$i = 4$	9	3	4	4

Further, π being primary and thus $A_0(\pi) \not\equiv 0 \pmod{11}$ and $\mathsf{a}_1(\pi) \equiv \mathsf{a}_2(\pi) \equiv \mathsf{a}_4(\pi) \equiv \mathsf{a}_6(\pi) + \mathsf{a}_3(\pi)^2 \equiv 0 \pmod{11}$, those formulas also yield, modulo 11,

$$\begin{aligned}
\Delta_3(\pi) \equiv \mathsf{a}_3(\pi)\,, \quad \Delta_5(\pi) \equiv \mathsf{a}_5(\pi)\,, \quad \Delta_7(\pi) \equiv \mathsf{a}_7(\pi)\,,\\
\Delta_9(\pi) \equiv -\mathsf{a}_3(\pi)^3 + 4\mathsf{a}_6(\pi)\mathsf{a}_3(\pi) + \mathsf{a}_9(\pi) \equiv 5\mathsf{a}_6(\pi)\mathsf{a}_3(\pi) + \mathsf{a}_9(\pi)\,.
\end{aligned}$$

Plugging all these quantities in the above expression for $\operatorname{ind}_\pi(\eta_i)$ gives the desired result.

For ω, since $\omega^{10} \sim 11$, there exists a unit ε such that $\varepsilon\,\omega^{10} = 11$. This holds for $\varepsilon = \prod_{j=1}^{10} \frac{1-\zeta^j}{1-\zeta} = -\zeta^6\,{\eta_1}^4\,{\eta_2}^2\,{\eta_3}^2\,{\eta_4}^{-2}$. As a result, owing to the multiplicative nature of the power residue symbol, we have

$\mathrm{ind}_\pi(\omega) \equiv \mathrm{ind}_\pi(\varepsilon) - \mathrm{ind}_\pi(11) \pmod{11}$ where $\mathrm{ind}_\pi(\varepsilon) \equiv \mathrm{ind}_\pi(-1) + 6\,\mathrm{ind}_\pi(\zeta) + 4\,\mathrm{ind}_\pi(\eta_1) + 2\,\mathrm{ind}_\pi(\eta_2) + 2\,\mathrm{ind}_\pi(\eta_3) - 2\,\mathrm{ind}_\pi(\eta_4) \equiv 0 + 6\frac{\mathbf{N}(\pi)-1}{11} + 6\mathsf{a}_3(\pi) + 10\mathsf{a}_5(\pi) + \mathsf{a}_7(\pi) + 5\mathsf{a}_6(\pi)\mathsf{a}_3(\pi) + \mathsf{a}_9(\pi) \pmod{11}$ from Corollary 2.5 and using the previously obtained expressions for $\mathrm{ind}_\pi(\eta_i)$. The result now follows by plugging the value for $\mathrm{ind}_\pi(11) \equiv \frac{\Delta_{11}(\pi)}{11} \pmod{11}$; see Eq. (A2) in Appendix A. □

4 Computation of the Eleventh Power Residue Symbol

4.1 Obtaining primary associates

We need to investigate the multiplicative properties of the A_k's. Namely, given $\alpha, \beta \in \mathbb{Z}[\zeta]$, how to relate $A_k(\alpha\beta)$ to $A_r(\alpha)$ and $A_s(\beta)$? We also need to express $\mathsf{a}_k(\alpha^n)$ as a function of $\mathsf{a}_j(\alpha)$.

Proposition 4.1. *Let $\alpha, \beta \in \mathbb{Z}[\zeta]$. Then, for $0 \le k \le 9$,*

$$A_k(\alpha\beta) \equiv \sum_{j=0}^{k} \binom{k}{j} A_j(\alpha) A_{k-j}(\beta) \pmod{11} .$$

Proof. Using $\zeta^{11} = 1$, the product of $\alpha = \sum_{j=1}^{10} a_j\,\zeta^j$ and $\beta = \sum_{j=1}^{10} b_j\,\zeta^j$ satisfies $\alpha\beta = \sum_{\ell=2}^{20} c_\ell\,\zeta^\ell = c_{11} + c_{12}\,\zeta + \sum_{j=2}^{9}(c_j + c_{j+11})\,\zeta^j + c_{10}\,\zeta^{10}$, where $c_\ell = \sum_{\substack{m+n=\ell \\ 1\le m,n\le 10}} a_m b_n$. Hence, we get

$$\begin{aligned} A_k(\alpha\beta) &\equiv A_k(c_{11}) + A_k\big(c_{12}\,\zeta + \textstyle\sum_{j=2}^{9}(c_j + c_{j+11})\,\zeta^j + c_{10}\,\zeta^{10}\big) \\ &\equiv A_k(c_{11}) + c_{12} + \textstyle\sum_{j=2}^{9}(c_j + c_{j+11})\,j^k + c_{10}\,10^k \\ &\equiv A_k(c_{11}) + \textstyle\sum_{\substack{2\le\ell\le 20 \\ \ell\neq 11}} c_\ell\,\ell^k \pmod{11} . \end{aligned}$$

Furthermore, $A_k(c_{11}) \equiv A_k\big(c_{11}(-\sum_{j=1}^{10}\zeta^j)\big) \equiv -c_{11}\big(\sum_{j=1}^{10} j^k\big) \pmod{11}$. So, for $k = 0$, we get $A_0(c_{11}) \equiv c_{11} \pmod{11}$ and thus $A_0(\alpha\beta) \equiv \sum_{2\le\ell\le 20} c_\ell \pmod{11}$. For $k \ge 1$, we get $A_k(c_{11}) \equiv 0 \pmod{11}$, which leads to $A_k(\alpha\beta) \equiv \sum_{\substack{2\le\ell\le 20 \\ \ell\neq 11}} c_\ell\,\ell^k \equiv \sum_{2\le\ell\le 20} c_\ell\,\ell^k \pmod{11}$. Therefore, in all cases, we have

$$\begin{aligned} A_k(\alpha\beta) &\equiv \textstyle\sum_{2\le\ell\le 20} c_\ell\,\ell^k \equiv \sum_{2\le\ell\le 20}\big(\sum_{\substack{m+n=\ell \\ 1\le m,n\le 10}} a_m b_n\big)\,\ell^k \\ &\equiv \textstyle\sum_{m=1}^{10}\sum_{n=1}^{10} a_m b_n (m+n)^k \\ &\equiv \textstyle\sum_{m=1}^{10}\sum_{n=1}^{10} a_m b_n \big(\sum_{j=0}^{k}\binom{k}{j} m^j n^{k-j}\big) \\ &\equiv \textstyle\sum_{j=0}^{k}\binom{k}{j}\sum_{m=1}^{10}\sum_{n=1}^{10} a_m b_n\, m^j n^{k-j} \\ &\equiv \textstyle\sum_{j=0}^{k}\binom{k}{j}\big(\sum_{m=1}^{10} a_m\, m^j\big)\big(\sum_{n=1}^{10} b_n\, n^{k-j}\big) \\ &\equiv \textstyle\sum_{j=0}^{k}\binom{k}{j} A_j(\alpha) A_{k-j}(\beta) \pmod{11}, \end{aligned}$$

which completes the proof. □

Corollary 4.2. *Let $\alpha \in \mathbb{Z}[\zeta]$ and let $n \in \mathbb{N}$. Then*

$$A_0(\alpha^n) \equiv A_0(\alpha)^n \pmod{11}$$

and, provided that $A_0(\alpha) \not\equiv 0 \pmod{11}$, for $1 \le k \le 9$,

$$\mathsf{a}_k(\alpha^n) \equiv \sum_{\ell=1}^{k} \binom{n}{\ell} \mathsf{h}_{k,\ell}(\alpha) \pmod{11}$$

where

$$\mathsf{h}_{k,\ell}(\alpha) = \begin{cases} \mathsf{a}_k(\alpha) & \text{for } \ell = 1 \\ \sum_{j=1}^{k-\ell+1}\binom{k}{j}\,\mathsf{h}_{k-j,\ell-1}(\alpha)\,\mathsf{a}_j(\alpha) & \text{for } 2 \le \ell \le k \end{cases} .$$

Proof. This is a direct application of Proposition 4.1. □

Proposition 4.3. *Let* $\eta_1 = \zeta^5 + \zeta^{-5}$, $\eta_2 = \zeta + \zeta^{-1}$, $\eta_3 = \zeta^{-1}(1 + \zeta + \zeta^2)$, *and* $\eta_4 = \zeta^3 + \zeta^{-3}$. *Let also* $\alpha \in \mathbb{Z}[\zeta]$ *with* $A_0(\alpha) \not\equiv 0 \pmod{11}$ *and* $A_1(\alpha) \equiv 0 \pmod{11}$. *If rational integers* $0 \le e_1, e_2, e_3, e_4 \le 10$ *verify*

$$\begin{cases} \sum_{i=1}^4 \mathsf{a}_2(\eta_i)\, e_i \equiv -\mathsf{a}_2(\alpha) \pmod{11} \\ \sum_{i=1}^4 \left(\mathsf{a}_4(\eta_i) - 3\,\mathsf{a}_2(\eta_i)^2\right) e_i \equiv -\mathsf{a}_4(\alpha) + 3\,\mathsf{a}_2(\alpha)^2 \pmod{11} \\ \sum_{i=1}^4 \left(\mathsf{a}_6(\eta_i) - 4\,\mathsf{a}_4(\eta_i)\mathsf{a}_2(\eta_i) - 3\,\mathsf{a}_2(\eta_i)^3\right) e_i \equiv -\mathsf{a}_6(\alpha) + 4\,\mathsf{a}_4(\alpha)\mathsf{a}_2(\alpha) - \mathsf{a}_3(\alpha)^2 + 3\,\mathsf{a}_2(\alpha)^3 \pmod{11} \\ \sum_{i=1}^4 \left(\mathsf{a}_8(\eta_i) + 5\,\mathsf{a}_6(\eta_i)\mathsf{a}_2(\eta_i) - 2\,\mathsf{a}_4(\eta_i)^2 + 2\,\mathsf{a}_4(\eta_i)\mathsf{a}_2(\eta_i)^2 - 3\,\mathsf{a}_2(\eta_i)^4\right) e_i \equiv -\mathsf{a}_8(\alpha) - 5\,\mathsf{a}_6(\alpha)\mathsf{a}_2(\alpha) \\ \qquad +\mathsf{a}_5(\alpha)\mathsf{a}_3(\alpha) + 2\,\mathsf{a}_4(\alpha)^2 - 2\,\mathsf{a}_4(\alpha)\mathsf{a}_2(\alpha)^2 + \mathsf{a}_3(\alpha)^2\mathsf{a}_2(\alpha) + 3\,\mathsf{a}_2(\alpha)^4 \pmod{11} \end{cases} \tag{2}$$

then $\alpha^\star = {\eta_1}^{e_1}\,{\eta_2}^{e_2}\,{\eta_3}^{e_3}\,{\eta_4}^{e_4}\,\alpha$ *is a primary associate of* α.

Proof. Write $\varepsilon = \varepsilon_1\,\varepsilon_2\,\varepsilon_3\,\varepsilon_4$ and $\varepsilon_i = {\eta_i}^{e_i}$. Hence, $\alpha^\star = \varepsilon\,\alpha$ is an associate of α. It is worth noting that ε is real and thus $A_1(\varepsilon) \equiv \mathsf{a}_1(\varepsilon) \equiv 0 \pmod{11}$. Proposition 3.1 lists the conditions for $\alpha^\star$ being primary. From Proposition 4.1 and Corollary 4.2 (see also Appendix A), we get $A_0(\varepsilon) \equiv \prod_{i=1}^4 A_0(\varepsilon_i) \equiv \prod_{i=1}^4 A_0(\eta_i)^{e_i} \pmod{11}$. Therefore, since $A_0(\eta_i) \not\equiv 0 \pmod{11}$, it follows that $A_0(\alpha^\star) \equiv A_0(\varepsilon)A_0(\alpha) \not\equiv 0 \pmod{11}$. Further, since $A_1(\alpha) \equiv A_1(\varepsilon) \equiv 0 \pmod{11}$, we also have $A_1(\alpha^\star) \equiv A_0(\varepsilon)A_1(\alpha) + A_1(\varepsilon)A_0(\alpha) \equiv 0 \pmod{11}$.

Likewise, again from Proposition 4.1 and Corollary 4.2, we find after a little algebra $\mathsf{a}_2(\varepsilon) \equiv \sum_{i=1}^4 \mathsf{a}_2(\varepsilon_i) \equiv \sum_{i=1}^4 \mathsf{a}_2(\eta_i)\, e_i \pmod{11}$. Consequently, since $\alpha^\star = \varepsilon\,\alpha$, the condition $A_2(\alpha^\star) \equiv 0 \pmod{11}$ translates into $A_2(\alpha^\star) \equiv A_0(\varepsilon)A_2(\alpha) + A_2(\varepsilon)A_0(\alpha) \equiv 0 \pmod{11} \iff \mathsf{a}_2(\varepsilon) \equiv \frac{A_2(\varepsilon)}{A_0(\varepsilon)} \equiv -\frac{A_2(\alpha)}{A_0(\alpha)} \equiv -\mathsf{a}_2(\alpha) \pmod{11}$, that is $\sum_{i=1}^4 \mathsf{a}_2(\eta_i)\, e_i \equiv -\mathsf{a}_2(\alpha) \pmod{11}$.

The calculation for $\mathsf{a}_4(\varepsilon)$ is more involved and technical. An application of Proposition 4.1 and Corollary 4.2 yields $\mathsf{a}_4(\varepsilon) \equiv \sum_{i=1}^4 \left(\mathsf{a}_4(\eta_i)\, e_i + 3\,\mathsf{a}_2(\eta_i)^2\, e_i(e_i - 1)\right) + 6\sum_{i=1}^3 \left(\sum_{j=i+1}^4 \mathsf{a}_2(\eta_i)\mathsf{a}_2(\eta_j)\, e_i e_j\right) \pmod{11}$. In turn, as $\sum_{i=1}^4 \mathsf{a}_2(\eta_i)\, e_i \equiv -\mathsf{a}_2(\alpha) \pmod{11}$, we therefore obtain $\mathsf{a}_4(\varepsilon) \equiv \sum_{i=1}^4 \left(\mathsf{a}_4(\eta_i) - 3\mathsf{a}_2(\eta_i)^2\right) e_i + 3\left(\sum_{i=1}^4 \mathsf{a}_2(\eta_i)\, e_i\right)^2 \equiv \left[\sum_{i=1}^4 \left(\mathsf{a}_4(\eta_i) - 3\,\mathsf{a}_2(\eta_i)^2\right) e_i\right] + 3\,\mathsf{a}_2(\alpha)^2 \pmod{11}$. The condition $A_4(\alpha^\star) \equiv 0 \pmod{11}$ so leads to $\mathsf{a}_4(\alpha) + 6\,\mathsf{a}_2(\varepsilon)\,\mathsf{a}_2(\alpha) + \mathsf{a}_4(\varepsilon) \equiv 0 \pmod{11} \iff \mathsf{a}_4(\varepsilon) \equiv -\mathsf{a}_4(\alpha) + 6\,\mathsf{a}_2(\alpha)^2 \pmod{11}$, that is $\sum_{i=1}^4 \left(\mathsf{a}_4(\eta_i) - 3\,\mathsf{a}_2(\eta_i)^2\right) e_i \equiv -\mathsf{a}_4(\alpha) + 3\,\mathsf{a}_2(\alpha)^2 \pmod{11}$.

The two remaining relations are proved similarly as a respective consequence of $A_0(\alpha^\star)A_6(\alpha^\star) + A_3(\alpha^\star)^2 \equiv 0 \pmod{11}$ and $A_3(\alpha^\star)A_5(\alpha^\star) - A_0(\alpha^\star)A_8(\alpha^\star) \equiv 0 \pmod{11}$. Notice that $\mathsf{a}_3(\varepsilon) \equiv \mathsf{a}_5(\varepsilon) \equiv \mathsf{a}_7(\varepsilon) \equiv 0 \pmod{11}$. □

From Lemma 2.2, applied to the case $p = 11$, we know that every $\alpha \in \mathbb{Z}[\zeta]$ with $\alpha \not\equiv 0 \pmod{\omega}$ has a primary associate of the form

$$\alpha^\star = \pm\,\zeta^{e_0}\,{\eta_1}^{e_1}\,{\eta_2}^{e_2}\,{\eta_3}^{e_3}\,{\eta_4}^{e_4}\,\alpha$$

where $0 \le e_0, e_1, e_2, e_3, e_4 \le 10$ and $\alpha^\star$ is unique up to the sign. First, we observe that the sign does not affect the fact of being primary. Indeed, from Proposition 3.1, it is easily seen that if $\alpha^\star$ is primary then so is $-\alpha^\star$. Second, as shown in the proof of Proposition 3.1, we observe that the condition $\alpha \not\equiv 0 \pmod{\omega}$ is equivalent to $A_0(\alpha) \not\equiv 0 \pmod{11}$.

Applying Proposition 4.3 demands that α satisfies $A_0(\alpha) \not\equiv 0 \pmod{11}$ and $A_1(\alpha) \equiv 0 \pmod{11}$. It turns out that if $A_0(\alpha) \not\equiv 0 \pmod{11}$ then

$$\alpha' := \zeta^{-\mathsf{a}_1(\alpha)}\alpha$$

satisfies $A_0(\alpha') \equiv A_0(\zeta^{-\mathsf{a}_1(\alpha)})A_0(\alpha) \equiv A_0(\alpha) \not\equiv 0 \pmod{11}$ and $A_1(\alpha') \equiv A_0(\zeta^{-\mathsf{a}_1(\alpha)})A_1(\alpha) + A_1(\zeta^{-\mathsf{a}_1(\alpha)})A_0(\alpha) \equiv A_1(\alpha) - \mathsf{a}_1(\alpha)A_0(\alpha) \equiv 0 \pmod{11}$. Note that $A_0(\zeta) = A_1(\zeta) = 1$.

Putting all together, we therefore obtain an efficient way to compute a primary associate of an element $\alpha \in \mathbb{Z}[\zeta]$ with $A_0(\alpha) \not\equiv 0 \pmod{11}$. This is depicted in Algorithm 1. With matrix notation, letting (w_1, w_2, w_3, w_4) denote the right-hand side of (2) (i.e., $w_1 = -\mathsf{a}_2(\alpha)$, etc) and replacing the $\mathsf{a}_j(\eta_i)$'s by their respective values, the system of equations (2) can be rewritten as

$$(e_1, e_2, e_3, e_4)\,\mathbf{M} \equiv (w_1, w_2, w_3, w_4) \pmod{11}$$

and so

$$(e_1, e_2, e_3, e_4) \equiv (w_1, w_2, w_3, w_4)\,\mathbf{M}^{-1} \pmod{11}$$

where $\mathbf{M}^{-1} = \begin{pmatrix} -2 & 4 & 1 & -3 \\ -4 & 3 & 5 & -1 \\ 5 & -5 & -3 & 4 \\ -3 & 2 & -3 & 1 \end{pmatrix} \pmod{11}$.

Algorithm 1: Computing $\alpha^\star$ and its representation

Input: $\alpha \in \mathbb{Z}[\zeta]$ with $A_0(\alpha) \not\equiv 0 \pmod{11}$
Output: $\texttt{primary}(\alpha) = \alpha^\star$ and $\texttt{repr}(\alpha) = (e_0, e_1, e_2, e_3, e_4)$ with $\alpha^\star = \zeta^{e_0}\eta_1^{e_1}\eta_2^{e_2}\eta_3^{e_3}\eta_4^{e_4}\alpha$ primary

$e_0 \leftarrow -\mathsf{a}_1(\alpha) \pmod{11}$
$\alpha \leftarrow \zeta^{e_0}\alpha$
$w_1 \leftarrow -\mathsf{a}_2(\alpha) \pmod{11}$
$w_2 \leftarrow -\mathsf{a}_4(\alpha) + 3\,\mathsf{a}_2(\alpha)^2 \pmod{11}$
$w_3 \leftarrow -\mathsf{a}_6(\alpha) + 4\,\mathsf{a}_4(\alpha)\mathsf{a}_2(\alpha) - \mathsf{a}_3(\alpha)^2 + 3\,\mathsf{a}_2(\alpha)^3 \pmod{11}$
$w_4 \leftarrow -\mathsf{a}_8(\alpha) - 5\,\mathsf{a}_6(\alpha)\mathsf{a}_2(\alpha) + \mathsf{a}_5(\alpha)\mathsf{a}_3(\alpha) + 2\,\mathsf{a}_4(\alpha)^2 - 2\,\mathsf{a}_4(\alpha)\mathsf{a}_2(\alpha)^2 + \mathsf{a}_3(\alpha)^2\mathsf{a}_2(\alpha) + 3\,\mathsf{a}_2(\alpha)^4 \pmod{11}$
$e_1 \leftarrow -2w_1 - 4w_2 + 5w_3 - 3w_4 \pmod{11}$
$e_2 \leftarrow 4w_1 + 3w_2 - 5w_3 + 2w_4 \pmod{11}$
$e_3 \leftarrow w_1 + 5w_2 - 3w_3 - 3w_4 \pmod{11}$
$e_4 \leftarrow -3w_1 - w_2 + 4w_3 + w_4 \pmod{11}$
$\alpha^\star \leftarrow \eta_1^{e_1}\eta_2^{e_2}\eta_3^{e_3}\eta_4^{e_4}\alpha$
return $[\alpha^\star, (e_0, e_1, e_2, e_3, e_4)]$

4.2 Norm-Euclidean division

The last ingredient for our algorithm is a norm-Euclidean division. For $p = 11$, the ring $\mathbb{Z}[\zeta]$ is known to be norm-Euclidean, i.e., for all $\alpha, \lambda \in \mathbb{Z}[\zeta]$, there exists some $\rho \in \mathbb{Z}[\zeta]$ such that $\rho \equiv \alpha \pmod{\lambda}$ and $\mathbf{N}(\rho) < \mathbf{N}(\lambda)$. In [11], Lenstra provides an efficient algorithm for approximating an algebraic number $\chi \in \mathbb{Q}(\zeta)$ by an algebraic integer $\iota \in \mathbb{Z}[\zeta]$ satisfying $\mathbf{N}(\chi - \iota) < 1$. See also [14, Algorithm 5.1] or [3, Algorithm 7.1]. Therefore, if we let $\chi = \frac{\alpha}{\lambda} = \frac{\alpha \prod_{j=2}^{10} \sigma_j(\lambda)}{\mathbf{N}(\lambda)} \in \mathbb{Q}(\zeta)$, we obtain $\iota \in \mathbb{Z}[\zeta]$ such that $\mathbf{N}(\chi - \iota) < 1$, and thus $\rho := \alpha - \iota\lambda$ verifies $\rho \equiv \alpha \pmod{\lambda}$ and $\mathbf{N}(\rho) = \mathbf{N}(\lambda)\,\mathbf{N}(\chi - \iota) < \mathbf{N}(\lambda)$. We write $\rho = \texttt{euclid\_div}(\alpha, \lambda)$.

4.3 Our algorithm

The main result is the hendecic reciprocity law.

Theorem 4.4 (Hendecic Reciprocity)**.** *Let α and λ be two primary elements in $\mathbb{Z}[\zeta]$. Then*

$$\left[\frac{\alpha}{\lambda}\right]_{11} = \left[\frac{\lambda}{\alpha}\right]_{11}.$$

Moreover,

$$\left[\frac{+1}{\lambda}\right]_{11} = 1, \quad \left[\frac{\zeta}{\lambda}\right]_{11} = \zeta^{\frac{\mathbf{N}(\lambda)-1}{11}},$$
$$\left[\frac{\zeta^5+\zeta^{-5}}{\lambda}\right]_{11} = \zeta^{\mathsf{a}_3(\lambda)+3\mathsf{a}_5(\lambda)+4\mathsf{a}_7(\lambda)+4\mathsf{a}_6(\lambda)\mathsf{a}_3(\lambda)+3\mathsf{a}_9(\lambda)},$$
$$\left[\frac{\zeta+\zeta^{-1}}{\lambda}\right]_{11} = \zeta^{3\mathsf{a}_3(\lambda)+5\mathsf{a}_5(\lambda)-2\mathsf{a}_7(\lambda)+5\mathsf{a}_6(\lambda)\mathsf{a}_3(\lambda)+\mathsf{a}_9(\lambda)},$$
$$\left[\frac{\zeta^{-1}(1+\zeta+\zeta^2)}{\lambda}\right]_{11} = \zeta^{2\mathsf{a}_3(\lambda)-2\mathsf{a}_5(\lambda)+3\mathsf{a}_7(\lambda)-4\mathsf{a}_6(\lambda)\mathsf{a}_3(\lambda)-3\mathsf{a}_9(\lambda)},$$

$$\left[\frac{\zeta^3+\zeta^{-3}}{\lambda}\right]_{11} = \zeta^{4\mathsf{a}_3(\lambda)+4\mathsf{a}_5(\lambda)+3\mathsf{a}_7(\lambda)+\mathsf{a}_6(\lambda)\mathsf{a}_3(\lambda)-2\mathsf{a}_9(\lambda)},$$

and, letting $\mathsf{A}_1(\lambda) = \frac{A_1(\lambda)/A_0(\lambda) \bmod 121}{11}$,

$$\left[\frac{1-\zeta}{\lambda}\right]_{11} = \zeta^{5\mathsf{a}_6(\lambda)\mathsf{a}_3(\lambda)-2\mathsf{a}_6(\lambda)\mathsf{a}_5(\lambda)-\mathsf{A}_1(\lambda)-5\,\frac{\mathbf{N}(\lambda)-1}{11}-5}.$$

Proof. The first statement is Theorem 2.3 for $p = 11$. The second statement for units ± 1 and ζ is Corollary 2.5 for $p = 11$; note that $\omega \nmid \lambda$ because λ is primary.

The last statements are proved in Proposition 3.3 for a primary prime λ. We need to show that Proposition 3.3 remains valid for any primary element $\lambda \in \mathbb{Z}[\zeta]$. Actually, it is sufficient to consider the case of λ being of the form $\lambda = \pi_1\pi_2$ for two primary primes π_1 and π_2. If π_1 and π_2 are primary then Proposition 3.1 tells that $\mathsf{a}_1(\pi_i) \equiv \mathsf{a}_2(\pi_i) \equiv \mathsf{a}_4(\pi_i) \equiv \mathsf{a}_6(\pi_i) + \mathsf{a}_3(\pi_i)^2 \equiv 0 \pmod{11}$, $i \in \{1,2\}$. Combined with Proposition 4.1, we so obtain for $j \in \{3,5,7\}$, $\mathsf{a}_j(\pi_1\pi_2) \equiv \mathsf{a}_j(\pi_1) + \mathsf{a}_j(\pi_2) \pmod{11}$. We also obtain $\mathsf{a}_6(\pi_1\pi_2)\mathsf{a}_3(\pi_1\pi_2) \equiv \mathsf{a}_6(\pi_1)\mathsf{a}_3(\pi_1) + \mathsf{a}_6(\pi_2)\mathsf{a}_3(\pi_2) + 3\mathsf{a}_6(\pi_1)\mathsf{a}_3(\pi_2) + 3\mathsf{a}_6(\pi_2)\mathsf{a}_3(\pi_1) \pmod{11}$ and $\mathsf{a}_9(\pi_1\pi_2) \equiv \mathsf{a}_9(\pi_1) + \mathsf{a}_9(\pi_2) - 4\mathsf{a}_6(\pi_1)\mathsf{a}_3(\pi_2) - 4\mathsf{a}_6(\pi_2)\mathsf{a}_3(\pi_1) \pmod{11}$. It is now easily checked, for $\eta_1 = \zeta^5 + \zeta^{-5}$, that $\mathsf{a}_3(\pi_1\pi_2) + 3\mathsf{a}_5(\pi_1\pi_2) + 4\mathsf{a}_7(\pi_1\pi_2) + 4\mathsf{a}_6(\pi_1\pi_2)\mathsf{a}_3(\pi_1\pi_2) + 3\mathsf{a}_9(\pi_1\pi_2) \equiv \mathrm{ind}_{\pi_1}(\eta_1) + \mathrm{ind}_{\pi_2}(\eta_1) \equiv \mathrm{ind}_{\pi_1\pi_2}(\eta_1) \pmod{11}$ where the values of $\mathrm{ind}_{\pi_1}(\eta_1)$ and $\mathrm{ind}_{\pi_2}(\eta_1)$ are given by Proposition 3.3; and similarly for the other fundamental units $\eta_2 = \zeta + \zeta^{-1}$, $\eta_3 = \zeta^{-1}(1 + \zeta + \zeta^2)$, and $\eta_4 = \zeta + \zeta^{-3}$. The proof for $\omega = 1 - \zeta$ essentially follows the same lines using a refinement of Proposition 4.1 for $A_1(\alpha\beta) \bmod 121$. □

Theorem 4.4 gives rise to an efficient algorithm for computing the 11^{th}-power residue symbol $\left[\frac{\alpha}{\lambda}\right]_{11}$. It requires α and λ to be co-prime and $\mathbf{T}(\lambda) \not\equiv 0 \pmod{11}$ (as otherwise the symbol is not defined). As a reminder, ω stands for the special prime $1 - \zeta$ and $\eta_1 = \zeta^5 + \zeta^{-5}$, $\eta_2 = \zeta + \zeta^{-1}$, $\eta_3 = \zeta^{-1}(1 + \zeta + \zeta^2)$, $\eta_4 = \zeta^3 + \zeta^{-3}$ are fundamental units.

Algorithm 2: Computing $\left[\frac{\alpha}{\lambda}\right]_{11}$

Input: $\alpha, \lambda \in \mathbb{Z}[\zeta]$ with $\gcd(\alpha, \lambda) \sim 1$ and $\mathbf{T}(\lambda) \not\equiv 0 \pmod{11}$
Output: $\left[\frac{\alpha}{\lambda}\right]_{11}$

$\lambda^\star \leftarrow \mathtt{primary}(\lambda)$
$j \leftarrow 0$
while $\mathbf{N}(\lambda^\star) > 1$ **do**
  $\rho \leftarrow \mathtt{euclid\_div}(\alpha, \lambda^\star)$
  $s \leftarrow 0$
  while $\mathbf{T}(\rho) \equiv 0 \pmod{11}$ **do**
    $s \leftarrow s + 1$
    $\rho \leftarrow \rho \div \omega$
  end
  $[\rho^\star, (e_0, e_1, e_2, e_3, e_4)] \leftarrow [\mathtt{primary}(\rho), \mathtt{repr}(\rho)]$
  // $\rho^\star = \zeta^{e_0}\eta_1^{e_1}\eta_2^{e_2}\eta_3^{e_3}\eta_4^{e_4}\rho$
  $j \leftarrow j + s \times \mathrm{ind}_{\lambda^\star}(\omega) - e_0 \times \mathrm{ind}_{\lambda^\star}(\zeta) - e_1 \times \mathrm{ind}_{\lambda^\star}(\eta_1)$
    $- e_2 \times \mathrm{ind}_{\lambda^\star}(\eta_2) - e_3 \times \mathrm{ind}_{\lambda^\star}(\eta_3) - e_4 \times \mathrm{ind}_{\lambda^\star}(\eta_4) \pmod{11}$
  $\alpha \leftarrow \lambda^\star$; $\lambda^\star \leftarrow \rho^\star$
end
return ζ^j

Proposition 4.5. *Algorithm 2 is correct.*

Proof. Clearly, we have $\left[\frac{\alpha}{\lambda}\right]_{11} = \left[\frac{\alpha}{\lambda^\star}\right]_{11} = \left[\frac{\mathtt{euclid\_div}(\alpha,\lambda^\star)}{\lambda^\star}\right]_{11}$.

Let $\alpha^{(in)}$ and $\lambda^{\star(in)}$ (resp. $\alpha^{(out)}$ and $\lambda^{\star(out)}$) denote the values of α and of $\lambda^\star$ when entering (resp. exiting) the outer while-loop. Define $\varrho := \texttt{euclid\_div}(\alpha^{(in)}, \lambda^{\star(in)})$. At the end of the inner while-loop, we have $\rho^\star = \zeta^{e_0}\eta_1^{e_1}\eta_2^{e_2}\eta_3^{e_3}\eta_4^{e_4}\varrho\,\omega^{-s}$ and so $\left[\frac{\varrho}{\lambda}\right]_{11} = \left[\frac{\rho^\star}{\lambda}\right]_{11} \cdot \zeta^{s\cdot\mathrm{ind}_\lambda(\omega)-e_0\cdot\mathrm{ind}_\lambda(\zeta)-\sum_{i=1}^4 e_i\cdot\mathrm{ind}_\lambda(\eta_i)}$, and wherein $\mathrm{ind}_\lambda(\omega)$, $\mathrm{ind}_\lambda(\zeta)$ and $\mathrm{ind}_\lambda(\eta_i)$ are evaluated using Theorem 4.4 and $\left[\frac{\rho^\star}{\lambda}\right]_{11} = \left[\frac{\lambda^\star}{\rho^\star}\right]_{11}$ by hendecic reciprocity. The last step of the outer while-loop replaces $(\alpha, \lambda^\star)$ with $(\lambda^\star, \rho^\star)$. Since $\mathbb{Z}[\zeta]$ is norm-Euclidean, it follows that the norm of $\lambda^\star$ strictly decreases: $\mathbf{N}(\lambda^{\star(out)}) = \mathbf{N}(\rho^\star) = \mathbf{N}(\varrho)/\mathbf{N}(\omega)^s \le \mathbf{N}(\varrho) < \mathbf{N}(\lambda^{\star(in)})$. It eventually becomes 1 and the algorithm terminates. □

References

[1] William D. Banks, Daniel Lieman and Igor E. Shparlinski, An extremely small and efficient identification scheme, in: *Information Security and Privacy (ACISP 2000)* (E. Dawson et al., eds.), Lecture Notes in Computer Science 1841, pp. 378–384, Springer, 2000.

[2] Éric Brier, Houda Ferradi, Marc Joye and David Naccache, New number-theoretic cryptographic primitives, *Journal of Mathematical Cryptology* (To appear).

[3] Perlas C. Caranay and Renate Scheidler, An efficient seventh power residue symbol algorithm, *International Journal of Number Theory* **6** (2010), 1831–1853.

[4] Ivan Bjerre Damgård and Gudmund Skovbjerg Frandsen, Efficient algorithms for the gcd and cubic residuosity in the ring of Eisenstein integers, *Journal of Symbolic Computation* **39** (2005), 643–652.

[5] Koen de Boer and Carlo Pagano, Calculating the power residue symbol and ibeta: Applications of computing the group structure of the principal units of a p-adic number field completion, in: *42nd International Symposium on Symbolic and Algebraic Computation* (M. A. Burr et al., eds.), pp. 117–124, ACM, 2017.

[6] Shafi Goldwasser and Silvio Micali, Probabilistic encryption, *Journal of Computer and System Sciences* **28** (1984), 270–299.

[7] Ernst E. Kummer, Allgemeine Reziprozitätsgesetze für beliebig hohe Potenzreste, *Monatsberichte der Königlichen Preußischen Akademie der Wissenschaften zu Berlin* (1850), 154–165, Reprinted in [17, pages 345–357].

[8] Ernst E. Kummer, Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen, *Journal für die reine und angewandte Mathematik* **56** (1859), 270–279, Reprinted in [17, pages 688–697].

[9] Franz Lemmermeyer, The Euclidean algorithm in algebraic number fields, *Expositiones Mathematicæ* **13** (1995), 385–416, Updated version, February 14, 2004.

[10] Franz Lemmermeyer, *Reciprocity Laws: From Euler to Eisenstein*, Springer Monographs in Mathematics, Springer, 2000.

[11] Hendrik W. Lenstra, Jr., Euclid's algorithm in cyclotomic fields, *Journal of the London Mathematical Society (2)* **10** (1975), 457–465.

[12] Jean Monnerat and Serge Vaudenay, Short undeniable signatures based on group homomorphisms, *Journal of Cryptology* **24** (2011), 545–587.

[13] Renate Scheidler, A public-key cryptosystem using purely cubic fields, *Journal of Cryptology* **11** (1998), 109–124.

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

[15] Henry J. S. Smith, *Report on the Theory of Numbers (Part II)*, Collected Mathematical Papers (J. W. L. Glaisher, ed.), 1, The Clarendon Press, 1894, pp. 93–162.

[16] The Sage developers, *SageMath, the Sage Mathematics Software System (Version 8.6)*, 2019.

[17] André Weil (ed.), *Collected Papers I: Contributions to Number Theory*, Springer-Verlag, 1975.

[18] André Weilert, Fast computation of the biquadratic residue symbol, *Journal of Number Theory* **96** (2002), 133–151.

[19] Hugh C. Williams, An M^3 public-key encryption scheme, in: *Advances in Cryptology – CRYPTO '85* (H. C. Williams, ed.), Lecture Notes in Computer Science 218, pp. 358–368, Springer, 1986.

A Formulary

In this appendix, we list the general formulas for the logarithmic differential quotients $\Delta_j(\alpha)$ and for the quantities $\mathsf{a}_j(\alpha^n)$.

We use Kummer's notation (cf. Section 2.3) and represent an algebraic integer $\alpha = \sum_{j=1}^{10} a_j\,\zeta^j \in \mathbb{Z}[\zeta]$ with $\mathbf{T}(\alpha) \neq 0$ as $\alpha = F(\zeta)$. The following lemma is useful; it relates $F^{(k)}(1)$ to $A_k(\alpha)$.

Lemma A.1. *Let $\alpha = \sum_{j=1}^{10} a_j\,\zeta^j \in \mathbb{Z}[\zeta]$. Then, letting $F^{(k)}$ denote the k^{th} derivative of F, $F^{(k)}(1) \equiv A_k(\alpha) \pmod{11}$ for $0 \le k \le 9$.*

Proof. The proof is immediate. From the definition of F, we have $F(e^v) = \sum_{j=0}^{9} b_j\,e^{vj}$ where $b_0 = -a_{10}$ and $b_j = a_j - a_{10}$ for $1 \le j \le 9$. Hence, evaluating $F(e^v)$ at $v = 0$, we get $F(1) \equiv \sum_{j=0}^{9} b_j \equiv -a_{10} + \sum_{j=1}^{9}(a_j - a_{10}) \equiv A_0(\alpha) - 11a_{10} \equiv A_0(\alpha) \pmod{11}$. Also, for $1 \le k \le 9$, $F^{(k)}(1) \equiv \sum_{j=1}^{9} j^k\,b_j \equiv \sum_{j=1}^{9} j^k(a_j - a_{10}) \equiv A_k(\alpha) - a_{10}\sum_{j=1}^{10} j^k \equiv A_k(\alpha) \pmod{11}$. □

We assume that $A_0(\alpha) \not\equiv 0 \pmod{11}$. From $\Delta_1(\alpha) = \frac{F'(1)}{F(1)} \iff F'(1) = \Delta_1(\alpha)F(1)$, we get by induction $F^{(k)}(1) = \sum_{j=1}^{k}\binom{k-1}{j-1}\Delta_j(\alpha)F^{(k-j)}(1)$ and therefore

$$\Delta_k(\alpha) = \frac{F^{(k)}(1)}{F(1)} - \sum_{j=1}^{k-1}\binom{k-1}{j-1}\Delta_j(\alpha)\frac{F^{(k-j)}(1)}{F(1)}\ . \tag{A1}$$

So, using Lemma A.1 and letting $\mathsf{a}_j := \mathsf{a}_j(\alpha)$, we obtain the successive logarithmic differential quotients modulo 11.

1. $\Delta_1(\alpha) \equiv \mathsf{a}_1 \pmod{11}$
2. $\Delta_2(\alpha) \equiv -\mathsf{a}_1^2 + \mathsf{a}_2 \pmod{11}$
3. $\Delta_3(\alpha) \equiv 2\mathsf{a}_1^3 - 3\mathsf{a}_2\mathsf{a}_1 + \mathsf{a}_3 \pmod{11}$
4. $\Delta_4(\alpha) \equiv 5\mathsf{a}_1^4 + \mathsf{a}_2\mathsf{a}_1^2 - 4\mathsf{a}_3\mathsf{a}_1 - 3\mathsf{a}_2^2 + \mathsf{a}_4 \pmod{11}$
5. $\Delta_5(\alpha) \equiv 2\mathsf{a}_1^5 - 5\mathsf{a}_2\mathsf{a}_1^3 - 2\mathsf{a}_3\mathsf{a}_1^2 - 3\mathsf{a}_2^2\mathsf{a}_1 - 5\mathsf{a}_4\mathsf{a}_1 + \mathsf{a}_3\mathsf{a}_2 + \mathsf{a}_5 \pmod{11}$
6. $\Delta_6(\alpha) \equiv \mathsf{a}_1^6 - 3\mathsf{a}_2\mathsf{a}_1^4 + \mathsf{a}_3\mathsf{a}_1^3 + 5\mathsf{a}_2^2\mathsf{a}_1^2 - 3\mathsf{a}_4\mathsf{a}_1^2 - \mathsf{a}_3\mathsf{a}_2\mathsf{a}_1 + 5\mathsf{a}_5\mathsf{a}_1 - 3\mathsf{a}_2^3 - 4\mathsf{a}_4\mathsf{a}_2 + \mathsf{a}_3^2 + \mathsf{a}_6 \pmod{11}$
7. $\Delta_7(\alpha) \equiv 5\mathsf{a}_1^7 - \mathsf{a}_2\mathsf{a}_1^5 + 4\mathsf{a}_3\mathsf{a}_1^4 + \mathsf{a}_2^2\mathsf{a}_1^3 - \mathsf{a}_4\mathsf{a}_1^3 + 5\mathsf{a}_3\mathsf{a}_2\mathsf{a}_1^2 - 2\mathsf{a}_5\mathsf{a}_1^2 - 3\mathsf{a}_2^3\mathsf{a}_1 + \mathsf{a}_4\mathsf{a}_2\mathsf{a}_1 - 3\mathsf{a}_3^2\mathsf{a}_1 + 4\mathsf{a}_6\mathsf{a}_1 + \mathsf{a}_3\mathsf{a}_2^2 + \mathsf{a}_5\mathsf{a}_2 - 2\mathsf{a}_3\mathsf{a}_4 + \mathsf{a}_7 \pmod{11}$
8. $\Delta_8(\alpha) \equiv -2\mathsf{a}_1^8 - 3\mathsf{a}_2\mathsf{a}_1^6 + \mathsf{a}_3\mathsf{a}_1^5 + \mathsf{a}_2^2\mathsf{a}_1^4 - 3\mathsf{a}_4\mathsf{a}_1^4 - 2\mathsf{a}_3\mathsf{a}_2\mathsf{a}_1^3 + 5\mathsf{a}_5\mathsf{a}_1^3 + 4\mathsf{a}_2^3\mathsf{a}_1^2 - \mathsf{a}_4\mathsf{a}_2\mathsf{a}_1^2 + 3\mathsf{a}_3^2\mathsf{a}_1^2 + \mathsf{a}_6\mathsf{a}_1^2 - 2\mathsf{a}_3\mathsf{a}_2^2\mathsf{a}_1 - 5\mathsf{a}_5\mathsf{a}_2\mathsf{a}_1 - \mathsf{a}_3\mathsf{a}_4\mathsf{a}_1 + 3\mathsf{a}_7\mathsf{a}_1 - 3\mathsf{a}_2^4 + 2\mathsf{a}_4\mathsf{a}_2^2 - \mathsf{a}_3^2\mathsf{a}_2 + 5\mathsf{a}_6\mathsf{a}_2 - 2\mathsf{a}_4^2 - \mathsf{a}_5\mathsf{a}_3 + \mathsf{a}_8 \pmod{11}$
9. $\Delta_9(\alpha) \equiv 5\mathsf{a}_1^9 + 5\mathsf{a}_2\mathsf{a}_1^7 + 2\mathsf{a}_3\mathsf{a}_1^6 - 2\mathsf{a}_2^2\mathsf{a}_1^5 + 5\mathsf{a}_4\mathsf{a}_1^5 - 5\mathsf{a}_3\mathsf{a}_2\mathsf{a}_1^4 - \mathsf{a}_5\mathsf{a}_1^4 - 5\mathsf{a}_2^3\mathsf{a}_1^3 + \mathsf{a}_4\mathsf{a}_2\mathsf{a}_1^3 - 3\mathsf{a}_3^2\mathsf{a}_1^3 + 2\mathsf{a}_6\mathsf{a}_1^3 + 3\mathsf{a}_3\mathsf{a}_2^2\mathsf{a}_1^2 - 4\mathsf{a}_5\mathsf{a}_2\mathsf{a}_1^2 - 3\mathsf{a}_3\mathsf{a}_4\mathsf{a}_1^2 - 5\mathsf{a}_7\mathsf{a}_1^2 - 2\mathsf{a}_2^4\mathsf{a}_1 + \mathsf{a}_4\mathsf{a}_2^2\mathsf{a}_1 + 5\mathsf{a}_3^2\mathsf{a}_2\mathsf{a}_1 - 2\mathsf{a}_6\mathsf{a}_2\mathsf{a}_1 + 3\mathsf{a}_4^2\mathsf{a}_1 - 4\mathsf{a}_5\mathsf{a}_3\mathsf{a}_1 + 2\mathsf{a}_8\mathsf{a}_1 - 3\mathsf{a}_3\mathsf{a}_2^3 - 3\mathsf{a}_5\mathsf{a}_2^2 + \mathsf{a}_3\mathsf{a}_4\mathsf{a}_2 - 3\mathsf{a}_7\mathsf{a}_2 - 5\mathsf{a}_5\mathsf{a}_4 - \mathsf{a}_3^3 + 4\mathsf{a}_6\mathsf{a}_3 + \mathsf{a}_9 \pmod{11}$

In order to get $\Delta_{11}(\alpha)$ mod 121, we resort on the general relation (A1). We define $\mathsf{f}_j := \mathsf{f}_j(\alpha) = \frac{F^{(j)}(1)}{F(1)}$ and obtain

$$\begin{aligned}\Delta_{11}(\alpha) \equiv 11\big(&-5\mathsf{f}_2\mathsf{f}_1^9 - 2\mathsf{f}_3\mathsf{f}_1^8 - \mathsf{f}_2^2\mathsf{f}_1^7 - 5\mathsf{f}_4\mathsf{f}_1^7 - 4\mathsf{f}_3\mathsf{f}_2\mathsf{f}_1^6 + \mathsf{f}_5\mathsf{f}_1^6 + 5\mathsf{f}_2^3\mathsf{f}_1^5 + 4\mathsf{f}_4\mathsf{f}_2\mathsf{f}_1^5 - \mathsf{f}_3^2\mathsf{f}_1^5 - 2\mathsf{f}_6\mathsf{f}_1^5 - 2\mathsf{f}_3\mathsf{f}_2^2\mathsf{f}_1^4\\ &+ 3\mathsf{f}_5\mathsf{f}_2\mathsf{f}_1^4 + 5\mathsf{f}_4\mathsf{f}_3\mathsf{f}_1^4 + 5\mathsf{f}_7\mathsf{f}_1^4 - \mathsf{f}_2^4\mathsf{f}_1^3 + 4\mathsf{f}_4\mathsf{f}_2^2\mathsf{f}_1^3 - 2\mathsf{f}_3^2\mathsf{f}_2\mathsf{f}_1^3 + 4\mathsf{f}_6\mathsf{f}_2\mathsf{f}_1^3 - 3\mathsf{f}_5\mathsf{f}_3\mathsf{f}_1^3 + 5\mathsf{f}_4^2\mathsf{f}_1^3 - 2\mathsf{f}_8\mathsf{f}_1^3\end{aligned}$$

$$
\begin{aligned}
&- 3\mathsf{f}_3\mathsf{f}_2^3\mathsf{f}_1^2 - 4\mathsf{f}_5\mathsf{f}_2^2\mathsf{f}_1^2 + 5\mathsf{f}_4\mathsf{f}_3\mathsf{f}_2\mathsf{f}_1^2 - 2\mathsf{f}_7\mathsf{f}_2\mathsf{f}_1^2 - 5\mathsf{f}_3^3\mathsf{f}_1^2 - \mathsf{f}_6\mathsf{f}_3\mathsf{f}_1^2 + 4\mathsf{f}_5\mathsf{f}_4\mathsf{f}_1^2 - \mathsf{f}_9\mathsf{f}_1^2 - \mathsf{f}_2^5\mathsf{f}_1 - 3\mathsf{f}_4\mathsf{f}_2^3\mathsf{f}_1 \\
&+ 5\mathsf{f}_3^2\mathsf{f}_2^2\mathsf{f}_1 + 4\mathsf{f}_6\mathsf{f}_2^2\mathsf{f}_1 + 5\mathsf{f}_5\mathsf{f}_3\mathsf{f}_2\mathsf{f}_1 - \mathsf{f}_4^2\mathsf{f}_2\mathsf{f}_1 + 2\mathsf{f}_8\mathsf{f}_2\mathsf{f}_1 - 5\mathsf{f}_4\mathsf{f}_3^2\mathsf{f}_1 - 2\mathsf{f}_7\mathsf{f}_3\mathsf{f}_1 + 2\mathsf{f}_6\mathsf{f}_4\mathsf{f}_1 - \mathsf{f}_5^2\mathsf{f}_1 - \mathsf{f}_{10}\mathsf{f}_1 + 4\mathsf{f}_3\mathsf{f}_2^4 \\
&+ 4\mathsf{f}_5\mathsf{f}_2^3 - 2\mathsf{f}_4\mathsf{f}_3\mathsf{f}_2^2 + 4\mathsf{f}_7\mathsf{f}_2^2 + 4\mathsf{f}_3\mathsf{f}_2 + 4\mathsf{f}_6\mathsf{f}_3\mathsf{f}_2 - 5\mathsf{f}_5\mathsf{f}_4\mathsf{f}_2 - 5\mathsf{f}_9\mathsf{f}_2 + 4\mathsf{f}_5\mathsf{f}_3^2 + 5\mathsf{f}_4^2\mathsf{f}_3 - 4\mathsf{f}_8\mathsf{f}_3 + 3\mathsf{f}_7\mathsf{f}_4 + 2\mathsf{f}_6\mathsf{f}_5\big) \\
&+ \mathsf{f}_{11} + 10\mathsf{f}_1^{11} \pmod{121}.
\end{aligned}
$$

When α is primary, we have $A_0(\alpha) \not\equiv 0 \pmod{11}$ and $\mathsf{f}_1(\alpha) \equiv \mathsf{f}_2(\alpha) \equiv \mathsf{f}_4(\alpha) \equiv \mathsf{f}_3(\alpha)\mathsf{f}_5(\alpha) - \mathsf{f}_8(\alpha) \equiv 0 \pmod{11}$. For $\alpha = \sum_{j=1}^{10} a_j \zeta^j$ primary, the previous relation then yields

$$
\begin{aligned}
\frac{\Delta_{11}(\alpha)}{11} &\equiv 4\mathsf{f}_5\mathsf{f}_3^2 - 4\mathsf{f}_8\mathsf{f}_3 + 2\mathsf{f}_6\mathsf{f}_5 + \frac{\mathsf{f}_{11} \bmod 121}{11} \equiv 2\mathsf{f}_6\mathsf{f}_5 + \frac{\mathsf{f}_{11} \bmod 121}{11} \equiv 2\mathsf{a}_6\mathsf{a}_5 + \frac{\frac{A_{11}(\alpha)}{A_0(\alpha)} - 11a_{10} \bmod 121}{11} \qquad \text{(A2)} \\
&\equiv 2\mathsf{a}_6\mathsf{a}_5 + \frac{\frac{A_{11}(\alpha)}{A_0(\alpha)} \bmod 121}{11} \equiv 2\mathsf{a}_6\mathsf{a}_5 + \mathsf{A}_1 + 5 - 5\mathsf{a}_3 - \mathsf{a}_5 + \mathsf{a}_7 + \mathsf{a}_9 \pmod{11}
\end{aligned}
$$

where $A_{11}(\alpha) = \sum_{j=1}^{10} a_j j^{11}$ and

$$
\mathsf{A}_1 := \mathsf{A}_1(\alpha) = \frac{\frac{A_1(\alpha)}{A_0(\alpha)} \bmod 121}{11},
$$

noting that $A_{11}(\alpha) - A_1(\alpha) \equiv 11(-a_2 - 4a_4 + 2a_5 - 3a_6 + 3a_7 - a_8 - a_{10}) \equiv 11\big(5A_0(\alpha) - 5A_3(\alpha) - A_5(\alpha) + A_7(\alpha) + A_9(\alpha)\big) \pmod{121}$.

We now look at the quantities $\mathsf{a}_j(\alpha^n)$ for $n > 1$. We write $\left\{{n \atop j}\right\}$ as a shortcut to $j!\binom{n}{j} = n(n-1)\dots(n-j+1)$ and again let $\mathsf{a}_j := \mathsf{a}_j(\alpha)$. The next formulas expand those given by Corollary 4.2.

1. $\mathsf{a}_1(\alpha^n) \equiv \left\{{n \atop 1}\right\} \mathsf{a}_1 \pmod{11}$
2. $\mathsf{a}_2(\alpha^n) \equiv \left\{{n \atop 1}\right\} \mathsf{a}_2 + \left\{{n \atop 2}\right\} \mathsf{a}_1^2 \pmod{11}$
3. $\mathsf{a}_3(\alpha^n) \equiv \left\{{n \atop 1}\right\} \mathsf{a}_3 + \left\{{n \atop 2}\right\} 3\mathsf{a}_1\mathsf{a}_2 + \left\{{n \atop 3}\right\} \mathsf{a}_1^3 \pmod{11}$
4. $\mathsf{a}_4(\alpha^n) \equiv \left\{{n \atop 1}\right\} \mathsf{a}_4 + \left\{{n \atop 2}\right\} (4\mathsf{a}_1\mathsf{a}_3 + 3\mathsf{a}_2^2) - \left\{{n \atop 3}\right\} 5\mathsf{a}_1^2\mathsf{a}_2 + \left\{{n \atop 4}\right\} \mathsf{a}_1^4 \pmod{11}$
5. $\mathsf{a}_5(\alpha^n) \equiv \left\{{n \atop 1}\right\} \mathsf{a}_5 + \left\{{n \atop 2}\right\} (5\mathsf{a}_1\mathsf{a}_4 - \mathsf{a}_2\mathsf{a}_3) - \left\{{n \atop 3}\right\} \mathsf{a}_1(\mathsf{a}_1\mathsf{a}_3 - 4\mathsf{a}_2^2) - \left\{{n \atop 4}\right\} \mathsf{a}_1^3\mathsf{a}_2 + \left\{{n \atop 5}\right\} \mathsf{a}_1^5 \pmod{11}$
6. $\mathsf{a}_6(\alpha^n) \equiv \left\{{n \atop 1}\right\} \mathsf{a}_6 - \left\{{n \atop 2}\right\} (5\mathsf{a}_1\mathsf{a}_5 - 4\mathsf{a}_2\mathsf{a}_4 + \mathsf{a}_3^2) + \left\{{n \atop 3}\right\} (4\mathsf{a}_1^2\mathsf{a}_4 + 5\mathsf{a}_1\mathsf{a}_2\mathsf{a}_3 + 4\mathsf{a}_2^3)$
   $- \left\{{n \atop 4}\right\} \mathsf{a}_1^2(2\mathsf{a}_1\mathsf{a}_3 - \mathsf{a}_2^2) + \left\{{n \atop 5}\right\} 4\mathsf{a}_1^4\mathsf{a}_2 + \left\{{n \atop 6}\right\} \mathsf{a}_1^6 \pmod{11}$
7. $\mathsf{a}_7(\alpha^n) \equiv \left\{{n \atop 1}\right\} \mathsf{a}_7 - \left\{{n \atop 2}\right\} (4\mathsf{a}_1\mathsf{a}_6 + \mathsf{a}_2\mathsf{a}_5 - 2\mathsf{a}_3\mathsf{a}_4) - \left\{{n \atop 3}\right\} (\mathsf{a}_1^2\mathsf{a}_5 + 5\mathsf{a}_1\mathsf{a}_2\mathsf{a}_4 - 4\mathsf{a}_1\mathsf{a}_3^2 + 5\mathsf{a}_2^2\mathsf{a}_3)$
   $+ \left\{{n \atop 4}\right\} \mathsf{a}_1(2\mathsf{a}_1^2\mathsf{a}_4 + \mathsf{a}_1\mathsf{a}_2\mathsf{a}_3 - 5\mathsf{a}_2^3) + \left\{{n \atop 5}\right\} \mathsf{a}_1^3(2\mathsf{a}_1\mathsf{a}_3 - 5\mathsf{a}_2^2) - \left\{{n \atop 6}\right\} \mathsf{a}_1^5\mathsf{a}_2 + \left\{{n \atop 7}\right\} \mathsf{a}_1^7 \pmod{11}$
8. $\mathsf{a}_8(\alpha^n) \equiv \left\{{n \atop 1}\right\} \mathsf{a}_8 - \left\{{n \atop 2}\right\} (3\mathsf{a}_1\mathsf{a}_7 + 5\mathsf{a}_2\mathsf{a}_6 - \mathsf{a}_3\mathsf{a}_5 - 2\mathsf{a}_4^2)$
   $- \left\{{n \atop 3}\right\} (5\mathsf{a}_1^2\mathsf{a}_6 - 3\mathsf{a}_1\mathsf{a}_2\mathsf{a}_5 - 5\mathsf{a}_1\mathsf{a}_3\mathsf{a}_4 - \mathsf{a}_2^2\mathsf{a}_4 - 5\mathsf{a}_2\mathsf{a}_3^2)$
   $+ \left\{{n \atop 4}\right\} (\mathsf{a}_1^3\mathsf{a}_5 + 2\mathsf{a}_1^2\mathsf{a}_2\mathsf{a}_4 + 5\mathsf{a}_1^2\mathsf{a}_3^2 + 4\mathsf{a}_1\mathsf{a}_2^2\mathsf{a}_3 - 5\mathsf{a}_2^4)$
   $+ \left\{{n \atop 5}\right\} \mathsf{a}_1^2(4\mathsf{a}_1^2\mathsf{a}_4 - \mathsf{a}_1\mathsf{a}_2\mathsf{a}_3 + 2\mathsf{a}_2^3) + \left\{{n \atop 6}\right\} \mathsf{a}_1^4(\mathsf{a}_1\mathsf{a}_3 + \mathsf{a}_2^2) - \left\{{n \atop 7}\right\} 5\mathsf{a}_1^6\mathsf{a}_2 + \left\{{n \atop 8}\right\} \mathsf{a}_1^8 \pmod{11}$
9. $\mathsf{a}_9(\alpha^n) \equiv \left\{{n \atop 1}\right\} \mathsf{a}_9 - \left\{{n \atop 2}\right\} (2\mathsf{a}_1\mathsf{a}_8 - 3\mathsf{a}_2\mathsf{a}_7 + 4\mathsf{a}_3\mathsf{a}_6 - 5\mathsf{a}_4\mathsf{a}_5)$
   $+ \left\{{n \atop 3}\right\} (3\mathsf{a}_1^2\mathsf{a}_7 - \mathsf{a}_1\mathsf{a}_2\mathsf{a}_6 - 2\mathsf{a}_1\mathsf{a}_3\mathsf{a}_5 - 4\mathsf{a}_1\mathsf{a}_4^2 + 4\mathsf{a}_2^2\mathsf{a}_5 - 5\mathsf{a}_2\mathsf{a}_3\mathsf{a}_4 + 5\mathsf{a}_3^3)$
   $- \left\{{n \atop 4}\right\} (4\mathsf{a}_1^3\mathsf{a}_6 + 3\mathsf{a}_1^2\mathsf{a}_2\mathsf{a}_5 + 5\mathsf{a}_1^2\mathsf{a}_3\mathsf{a}_4 + 2\mathsf{a}_1\mathsf{a}_2^2\mathsf{a}_4 - \mathsf{a}_1\mathsf{a}_2\mathsf{a}_3^2 + 5\mathsf{a}_2^3\mathsf{a}_3)$
   $+ \left\{{n \atop 5}\right\} \mathsf{a}_1(5\mathsf{a}_1^3\mathsf{a}_5 - 5\mathsf{a}_1^2\mathsf{a}_2\mathsf{a}_4 + 4\mathsf{a}_1^2\mathsf{a}_3^2 - 4\mathsf{a}_1\mathsf{a}_2^2\mathsf{a}_3 - \mathsf{a}_2^4) + \left\{{n \atop 6}\right\} \mathsf{a}_1^3(5\mathsf{a}_1^2\mathsf{a}_4 - 5\mathsf{a}_1\mathsf{a}_2\mathsf{a}_3 - 5\mathsf{a}_2^3)$
   $- \left\{{n \atop 7}\right\} \mathsf{a}_1^5(4\mathsf{a}_1\mathsf{a}_3 - 4\mathsf{a}_2^2) + \left\{{n \atop 8}\right\} 3\mathsf{a}_1^7\mathsf{a}_2 + \left\{{n \atop 9}\right\} \mathsf{a}_1^9 \pmod{11}$