The Thirteenth Power Residue Symbol

Eric Brier[1] and David Naccache[2]

[1] Ingenico, Alixan, France
eric.brier@ingenico.com
[2] DIENS, École normale supérieure, CNRS, PSL University, Paris, France
david.naccache@ens.fr

Abstract. This paper presents an efficient deterministic algorithm for computing 13^{th}-power residue symbols in the cyclotomic field $\mathbb{Q}(\zeta_{13})$, where ζ_{13} is a primitive 13^{th} root of unity.

The new algorithm finds applications in the implementation of certain cryptographic schemes and closes a gap in the *corpus* of algorithms for computing power residue symbols.

1 Introduction

Quadratic and higher-order residuosity are useful cryptographic building-blocks which applications include encryption [6, 19, 15, 14], digital signature and authentication primitives [1, 13, 2].

A central operation underlying those algorithms is the evaluation of a residue symbol $\left[\frac{\alpha}{\lambda}\right]_p$ 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 $p = 2$, 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 λ.

The cases $p = \{3, 4, 5, 7, 8, 11\}$ are discussed in the following references:

$p = 3 \rightsquigarrow$ [19, 4, 15]	$p = 4 \rightsquigarrow$ [18, 4]	$p = 5 \rightsquigarrow$ [15]
$p = 7 \rightsquigarrow$ [3]	$p = 8 \rightsquigarrow$ [10, § 9]	$p = 11 \rightsquigarrow$ [7]

Caranay and Scheidler describe a generic algorithm in [3, § 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 general case is addressed probabilistically in a recent algorithm by de Boer and Pagano [5].

So far no efficient and deterministic algorithm for $p = 13$ was known although the ring of cyclotomic integers modulo 13 is norm-Euclidean [12]. The following sections present such an algorithm. Subsection 1.1 is reproduced with minor modifications from [7] to avoid unnecessary reformulation.

1.1 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* [11, 9] (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

$$\alpha = \sum_{j=1}^{p-1} a_j \, \zeta^j \quad \text{with} \quad a_j \in \mathbb{Z}$$

The norm and trace of $\alpha \in \mathbb{Z}[\zeta]$ are the rational integers respectively given by

$$\mathbf{N}(\alpha) = \prod_{k=1}^{p-1} \sigma_k(\alpha) \quad \text{and} \quad \mathbf{T}(\alpha) = \sum_{k=1}^{p-1} \sigma_k(\alpha) \quad \text{where} \quad \sigma_k \colon \zeta \mapsto \zeta^k$$

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 [8, p. 158]) in $\mathbb{Z}[\zeta]$.

Definition 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 1 ([3, Lemma 2.6]). *Every element $\alpha \in \mathbb{Z}[\zeta]$ with $\alpha \not\equiv 0 \pmod{\omega}$ has a primary associate α^* of the form*

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

Moreover, α^* is unique up to its sign. □

1.2 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 $\text{ind}_\pi(\alpha)$. 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

$$\lambda = \prod_j \pi_j^{e_j} \quad \text{for primes} \quad \pi_j \in \mathbb{Z}[\zeta]$$

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 [8] stated the reciprocity law in 1850 (see also [16, Art. 54]). It is restricted to so-called "regular" primes,[3] 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 1 (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 Primary Elements

Let ζ be a 13^{th} root of unity, $K := \mathbb{Q}(\zeta)$ the 13^{th} cyclotomic field, and define $\omega = 1 - \zeta$. We choose the following generating units for $\mathbb{Z}[\zeta]$:

$$\eta_i = 1 + \zeta^i \quad \text{for} \quad i = 1, \ldots, 5$$

We suppose that $\alpha, \beta \in \mathbb{Z}[\zeta]$ and denote by α^*, β^* their primary associates. Let the e_i be defined by:

$$\alpha^* = \zeta^{e_0}\alpha\prod_{i=1}^{5}\eta_i^{e_i}$$

We then have

$$\left[\frac{\alpha}{\beta}\right]_{13} = \left[\frac{\alpha}{\beta^*}\right]_{13} = \left[\frac{\alpha^*}{\beta^*}\right]_{13} \cdot \left[\frac{\zeta}{\beta^*}\right]_{13}^{-e_0} \cdot \left[\frac{\eta_1}{\beta^*}\right]_{13}^{-e_1} \cdot \left[\frac{\eta_2}{\beta^*}\right]_{13}^{-e_2} \cdot \left[\frac{\eta_3}{\beta^*}\right]_{13}^{-e_3} \cdot \left[\frac{\eta_4}{\beta^*}\right]_{13}^{-e_4} \cdot \left[\frac{\eta_5}{\beta^*}\right]_{13}^{-e_5}$$

The problem is thus two-fold: *identifying the primary associate* and *having additional laws*.

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

(1) The first part can be solved by an algorithm based on the definition of primary elements and some special units. A primary element is congruent to a natural integer modulo ω^2 and its complex norm is congruent to a natural integer modulo 13. One must keep in mind that 13 is equal to ω^{12} up to a unit. By definition, we have $\zeta = 1 - \omega$ and $v_1, z_1 \in \mathbb{N}$ such that

$$\zeta^{v_1} \cdot \alpha \equiv z_1 \bmod \omega^2$$

(2) The next step consists in using the unit $\zeta^{11}\eta_4$. This unit is $\equiv 2 \mod \omega^2$ and its complex norm is $\equiv 4 + \omega^2 \mod \omega^4$. So $\exists v_2, z_2 \in \mathbb{N}$ such that

$$\zeta^{v_1}(\zeta^{11}\eta_4)^{v_2} \cdot \alpha \equiv z_2 \bmod \omega^2 \quad \text{and} \quad \mathcal{N}_{\mathbb{C}/\mathbb{R}}(\zeta^{v_1}(\zeta^{11}\eta_4)^{v_2} \cdot \alpha) \equiv z_2^2 \bmod \omega^4$$

(3) The third step consists in using the unit $\zeta^3\eta_1\eta_2^3$. This unit is $\equiv 3 \mod \omega^2$ and its complex norm is $\equiv 9 + 3\omega^4 \mod \omega^6$. So $\exists v_3, z_3 \in \mathbb{N}$ such that

$$\zeta^{v_1}(\zeta^{11}\eta_4)^{v_2}(\zeta^3\eta_1\eta_2^3)^{v_3} \cdot \alpha \equiv z_2 \bmod \omega^2 \quad \text{and} \quad \mathcal{N}_{\mathbb{C}/\mathbb{R}}(\zeta^{v_1}(\zeta^{11}\eta_4)^{v_2}(\zeta^3\eta_1\eta_2^3)^{v_3} \cdot \alpha) \equiv z_2^2 \bmod \omega^6$$

(4)(5)(6) The fourth, fifth, and sixth steps use the units $\zeta^{10}\eta_1^2\eta_2^7\eta_3$, $\eta_1\eta_2^4\eta_3^4\eta_5$ and $\zeta^4\eta_1^2\eta_2^{10}\eta_3^6\eta_4^3\eta_5$ till the complex norm is equal to a natural integer modulo ω^{12} which is equal to 13 modulo a multiplicative unit. Since the units used are another set of generators of the unit group, the existence of a primary associate for any algebraic integer in the number field ensures that there is no term to cancel modulo odd powers of ω.

(7) To finalize the primary representative algorithm, we reconstruct the e_i exponents. One can also reduce these numbers modulo 13 since it does not spoil the primary nature of the result.

3 Additional Laws

One way to address the needed additional laws is to rely on Ray Class Field Theory and on an isomorphism which is based on the Artin map and its link with the power residue symbols. We shall not prove the result here and limit ourselves to mention that we consider the Abelian extension L/K of conductor $\mathfrak{f} = \langle\omega^{14}\rangle$ with

$$L := K(\sqrt[13]{\omega},\ \sqrt[13]{\zeta},\ \sqrt[13]{\eta_1},\ \sqrt[13]{\eta_2},\ \sqrt[13]{\eta_3},\ \sqrt[13]{\eta_4},\ \sqrt[13]{\eta_5})$$

We will build an algorithm for computing the additional laws based on the following proposition: let $\alpha \in \{\omega, \zeta, \eta_1, \eta_2, \eta_3, \eta_4, \eta_5\}$, let $\beta, \gamma \in \mathbb{Z}[\zeta]$ be non-unit and coprime to ω. If, in addition, $\beta \equiv \gamma \mod \omega^{14}$, then we have:

$$\left[\frac{\alpha}{\beta}\right]_{13} = \left[\frac{\alpha}{\gamma}\right]_{13}$$

Being given a cyclotomic integer β for which one wants to compute the 13^{th} residue symbol, we build a cyclotomic integer γ for which the computation is easy and which is $\equiv \beta \mod \omega^{14}$. To that end, we define units:

$$\begin{aligned}
\lambda_0 = \eta_1 &\equiv 2 && \bmod \omega \\
\lambda_1 = \eta_1^{12} &\equiv 1 + 7\omega && \bmod \omega^2 \\
\lambda_2 = \eta_1^{35}\eta_4 &\equiv 1 + 8\omega^2 && \bmod \omega^3
\end{aligned}$$

We also need some particular primes in K to fully generate $\mathbb{Z}_K \bmod \omega^{14}$. An automated search yields the primes $\lambda_i = 1 + \omega^i + \psi_i\omega^{14}$ for $3 \le i \le 13$ where the constants ψ_i are given in Appendix A.

We have the property that, for $0 \le i \le 13$, $\lambda_i = 1 \mod \omega^i$ and $\lambda_i \neq 1 \mod \omega^{i+1}$. This ensures that if β is coprime to ω, there exists natural integers e_i such that

$$\beta \equiv \prod_{i=0}^{13} \lambda_i^{e_i} \bmod \omega^{14}$$

From the above proposition, this implies (by multiplicativity of the residue symbols):

$$\left[\frac{\alpha}{\beta}\right]_{13} = \prod_{i=0}^{13} \left[\frac{\alpha}{\lambda_i}\right]_{13}^{e_i}, \forall \alpha \in \{\omega, \zeta, \eta_1, \eta_2, \eta_3, \eta_4, \eta_5\}$$

Taking into account that only the exponents e_i depend on β, one can pre-compute the residue symbols on the right-hand side. One can also make a direct link between the exponents e_i and the coefficients of β when expressed as a polynomial in ω, using developments and the Newton formula to turn exponents in polynomials. The following framed paragraph summarizes this process in a synthetic way.

Using the above-mentioned units, $\exists u_\beta, v_\beta, w_\beta \in \mathbb{N}$ such that

$$\eta_1^{u_\beta} \cdot \beta \equiv 1 \bmod \omega \quad \text{and} \quad \eta_1^{u_\beta} \zeta^{v_\beta} \cdot \beta \equiv 1 \bmod \omega^2$$

$$\gamma := \eta_1^{u_\beta} \zeta^{v_\beta} (\eta_1^4 \eta_2^3 \eta_3^4 \eta_4)^{w_\beta} \cdot \beta \equiv 1 \bmod \omega^3$$

Let the numbers $d_0, \ldots, d_{11}$ be the ω-expansion of γ, i.e. $\gamma = \sum_{i=0}^{11} d_i \omega^i$

Let us furthermore define $d_{12} = \dfrac{1 - d_0}{13}$ and $d_{13} = \dfrac{6(1 - d_0) - d_1}{13}$

We then have (for the Δ_i polynomials cf. to the Druidic Grimoire of Appendix A):

$$\left[\frac{\omega}{\beta}\right]_{13} = \zeta^{\Delta_0} \qquad \left[\frac{\zeta}{\beta}\right]_{13} = \zeta^{\Delta_1} \qquad \left[\frac{\eta_i}{\beta}\right]_{13} = \zeta^{\Delta_{i+1}}, \text{ for } 1 \leq i \leq 5.$$

4 Further Research: Beyond Thirteen?

The natural question that comes to the mind is what happens for $p > 13$?

While considerably complex, the formulae for $p = 17$ and $p = 19$ should remain manageable. The real problem is – however – the lack of Euclidean division for $p = 17$ and $p = 19$. In other words, we have no deterministic way to decrease the norm of elements.

The next barrier is $p \geq 23$ (and beyond) for which the class number is $\neq 1$. This ensures in particular that no Euclidean division can exist. It however does not prevent Kummer reciprocity nor establishing additional laws.

Finally, for $p = 37$ we stumble on a hardcore issue: a class number which is a multiple of 37. The prime 37 is not a regular and we cannot rely on Kummer reciprocity anymore.

We propose as a future research direction the following workaround:

Observe that

$$\left[\frac{a}{b}\right]_p = \left[\frac{a + br}{b}\right]_p$$

Hence, if we can find an r such that $c = a + br$ is prime in $\mathbb{Q}(\zeta)$, we can apply the definition to get

$$\left[\frac{b}{c}\right]_p \text{ and, using reciprocity, obtain } \left[\frac{c}{b}\right]_p$$

For the resulting algorithm to be a deterministic polynomial time algorithm, we would need theoretical results ensuring the existence of such rs under a given bound depending on the norms of a and b.

References

[1] William D. Banks, Daniel Lieman, and Igor E. Shparlinski. An extremely small and efficient identification scheme. In E. Dawson et al., editors, *Information Security and Privacy (ACISP 2000)*, volume 1841 of *Lecture Notes in Computer Science*, pages 378–384. Springer, 2000. doi:10.1007/10718964_31.

[2] Éric Brier, Houda Ferradi, Marc Joye, and David Naccache. New number-theoretic cryptographic primitives. To appear in Number-Theoretic Methods in Cryptology (NutMiC 2019), Paris, France, June 24–27, 2019. Preprint available at URL https://ia.cr/2019/484.

[3] Perlas C. Caranay and Renate Scheidler. An efficient seventh power residue symbol algorithm. *International Journal of Number Theory*, 6(8):1831–1853, 2010. doi:10.1142/s1793042110003770.

[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(6):643–652, 2005. doi:10.1016/j.jsc.2004.02.006.

[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 $\mathfrak{p}$-adic number field completion. In M. A. Burr et al., editors, *42nd International Symposium on Symbolic and Algebraic Computation*, pages 117–124. ACM, 2017. doi:10.1145/3087604.3087637.

[6] Shafi Goldwasser and Silvio Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28(2):270–299, 1984. doi:10.1016/0022-0000(84)90070-9.

[7] Marc Joye, Oleksandra Lapiha, Ky Nguyen, and David Naccache. The eleventh power residue symbol. Preprint available at URL https://ia.cr/2019/870.

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

[9] Franz Lemmermeyer. The Euclidean algorithm in algebraic number fields. *Expositiones Mathematicæ*, 13(5):385–416, 1995. URL http://www.rzuser.uni-heidelberg.de/~hb3/publ/survey.pdf. Updated version, February 14, 2004.

[10] Franz Lemmermeyer. *Reciprocity Laws: From Euler to Eisenstein*. Springer Monographs in Mathematics. Springer, 2000. doi:10.1007/978-3-662-12893-0.

[11] Hendrik W. Lenstra, Jr. Euclid's algorithm in cyclotomic fields. *Journal of the London Mathematical Society (2)*, 10(4):457–465, 1975. doi:10.1112/jlms/s2-10.4.457.

[12] Robert George McKenzie. *The Ring of Cyclotomic Integers of Modulus Thirteen is Norm-Euclidean*. PhD thesis, Michigan State University (USA), 1988. PhD Dissertation.

[13] Jean Monnerat and Serge Vaudenay. Short undeniable signatures based on group homomorphisms. *Journal of Cryptology*, 24(3):545–587, 2011. doi:10.1007/s00145-010-9070-1.

[14] Renate Scheidler. A public-key cryptosystem using purely cubic fields. *Journal of Cryptology*, 11(2): 109–124, 1998. doi:10.1007/s001459900038.

[15] Renate Scheidler and Hugh C. Williams. A public-key cryptosystem utilizing cyclotomic fields. *Designs, Codes and Cryptography*, 6(2):117–131, 1995. doi:10.1007/BF01398010.

[16] Henry J. S. Smith. Report on the theory of numbers (Part II). In J. W. L. Glaisher, editor, *Collected Mathematical Papers*, volume 1, pages 93–162. The Clarendon Press, 1894.

[17] André Weil, editor. *Collected Papers I: Contributions to Number Theory*. Springer-Verlag, 1975. URL https://www.springer.com/gp/book/9783662488324.

[18] André Weilert. Fast computation of the biquadratic residue symbol. *Journal of Number Theory*, 96 (1):133–151, 2002. doi:10.1006/jnth.2002.2783.

[19] Hugh C. Williams. An M^3 public-key encryption scheme. In H. C. Williams, editor, *Advances in Cryptology – CRYPTO '85*, volume 218 of *Lecture Notes in Computer Science*, pages 358–368. Springer, 1986. doi:10.1007/3-540-39799-X_26.

A Druidic Grimoire

$$\Delta_0 = 12(d_{13}+d_4^2d_5+d_3d_5^2+d_3^2d_7)+11d_3d_4d_6+d_{10}d_3+d_3^3d_4+d_6d_7+d_5d_8+d_4d_9$$

$$\Delta_1 = 12\sum_{i=3}^{5} d_i\phi^1_{i+1,12-i}+d_3(3d_3^3+2d_4d_5+d_3\phi^1_{4,6}+d_4^2)+9\phi^3_{3,4}+6\phi^2_{3,6}+\phi^1_{3,12} \quad \text{where} \quad \phi^k_{u,v}=\sum_{i=u}^{v} d_i^k$$

$$\Delta_2 = 12d_7+11(d_4^3+d_8)+10(d_{11}+d_3d_4^2+d_3^2d_5+d_3^2)+9d_9+8(d_3^4+d_4+d_4d_6+d_3d_7)+7(d_{12}+d_3^2d_6)+6(d_5d_7+d_6+d_4d_8+d_3d_9)+3(d_3^3+d_5+d_5d_6+d_6^2+d_4d_7+d_3d_8)+5(d_{10}+d_3^2d_4)+4(d_3+d_4d_5+d_5^2+d_3d_6)+2d_3d_5+d_3d_4+d_4^2+d_3d_4d_5$$

$$\Delta_3 = 12(d_3d_9+d_4d_8+d_5d_7)+10(d_3d_5+d_5^2)+9(d_4^3+d_4)+7(d_3(d_6+d_7)+d_4(d_5+d_6))+6(d_{10}+d_9+d_6^2+d_3^2d_4)+5(d_4^2+d_6+d_5)+4d_3^2+3(d_8+d_3^4)+2(d_3^3+d_3d_4d_5)+d_{12}+d_3^2d_6$$

$$\Delta_4 = 12(d_3d_4+d_8)+11d_3^4+10(d_4d_6+d_3d_7)+9(d_{11}+d_3d_4^2+d_3^2d_5+d_6^2)+8(d_{12}+d_3^2d_6+d_9)+7(d_3^3+d_4^2+d_4^3+d_6)+6d_4+5(d_4d_5+d_5^2+d_3d_6+d_5d_7+d_4d_8+d_3d_9)+4(d_5d_6+d_4d_7+d_3d_8)+3(d_{10}+d_3+d_3^2+d_3^2d_4+d_3d_4d_5)+d_3d_5+d_7+2d_5$$

$$\Delta_5 = 12d_6^2+11(d_{11}+d_4+d_3d_4^2+d_3^2d_5+d_5d_7+d_4d_8+d_3d_9)+9(d_{10}+d_3^2+d_3^2d_4+d_5)+8d_6+7(d_7+d_8)+6(d_3^4+d_3d_4+d_3d_5)+5d_4^3+4(d_3d_4d_5+d_4d_6+d_3d_7)+3d_4^2+2(d_{12}+d_5^2+d_3^2d_6+d_5d_6+d_4d_7+d_3d_8)+d_3$$

$$\Delta_6 = 11(d_{10}+d_3^2d_4+d_6)+10d_7+9(d_{12}+d_3^2d_6)+7(d_5d_6+d_4d_7+d_8+d_3d_8)+6(d_{11}+d_3d_4^2+d_3d_5+d_3^2d_5)+5(d_5+d_3d_4d_5)+4(d_5d_7+d_4d_8+d_3d_9)+3(d_3+d_4+d_3d_4+d_4^2+d_4^3)+2(d_4d_6+d_6^2+d_3d_7)+d_3^2+d_3^4+d_5^2$$

$$\tau = \begin{pmatrix} 1 & 11 & 3 & 10 & 0 & 4 \\ 0 & 0 & 1 & 2 & 1 & 2 \\ 0 & 0 & 3 & 7 & 4 & 10 \\ 0 & 0 & 0 & 1 & 4 & 6 \\ 0 & 1 & 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

$$\eta_i = 1+\zeta^i \quad \text{for } 1 \le i \le 5$$

$$\mu_0 = 1 \qquad \mu_1 = 0 \qquad \mu_2 = 0$$

$$\chi = \sum_{i=0}^{12} \zeta^i$$

$$\begin{aligned} z_0 &= \zeta^{11}\eta_4 \\ z_1 &= \zeta^3\eta_1\eta_2^3 \\ z_2 &= \zeta^{10}\eta_1^2\eta_2^7\eta_3 \\ z_3 &= \eta_1\eta_2^4\eta_3^4\eta_5 \\ z_4 &= \zeta^4\eta_1^2\eta_2^{10}\eta_3^6\eta_4^3\eta_5 \end{aligned}$$

$$\begin{aligned} s_0 &= 1+\zeta \\ s_1 &= \zeta \\ s_2 &= \eta_1^4\eta_2^3\eta_3^4\eta_4 \end{aligned}$$

$$\begin{aligned} \psi_3 &= 107 \\ \psi_4 &= 7436 \\ \psi_5 &= 1000 \\ \psi_6 &= 2300 \\ \psi_7 &= 8632 \\ \psi_8 &= 4496 \\ \psi_9 &= 2307 \\ \psi_{10} &= 2123 \\ \psi_{11} &= 9183 \\ \psi_{12} &= 6929 \\ \psi_{13} &= 3194 \end{aligned}$$

Let P, Q be two polynomials, we denote by $P \bmod Q$ the reduction of P modulo Q.

$x \mod y$ denotes the usual modular reduction of integers.

Let $P(\zeta)$ be a polynomial in the variable ζ. We denote by $P[\![\ell]\!]$ the polynomial P in which ζ was replaced by ℓ. ℓ may be an integer, a polynomial in ζ or any other expression.

Let $\alpha(\zeta)$ be a polynomial, we define:

$$f[\alpha, k] = \prod_{k}^{12} \alpha[\![\zeta^i]\!] \bmod \chi$$

The function `Coefficient` isolates the coefficient of a specific term in a polynomial, i.e.:

$$\texttt{Coefficient}[\sum_{i=0}^{u} \epsilon_i x^i, x^j] = \epsilon_j \quad \text{or equivalently:} \quad \texttt{Coefficient}[\sum_{i=0}^{u} \epsilon_i x^i, x, j] = \epsilon_j$$

whereas `CoefficientList` returns the list of all the coefficients in the indicated variable, i.e.:

$$\texttt{CoefficientList}[\sum_{i=0}^{u} \epsilon_i x^i, x] = \{\epsilon_0, \ldots, \epsilon_u\}$$

B Code in Mathematical Form

```
Function PrimaryRep[α]
```

$\alpha^* = \alpha$
$\{e_1, e_2, e_3, e_4, e_5, e_6\} = \{0, 0, 0, 0, 0, 0\}$
While[Coefficient[$\alpha^* \llbracket 1 - \omega \rrbracket, \omega$] $\not\equiv 0 \mod 13$,
$\alpha^* = \zeta \alpha^*$ MOD χ
$e_1 ++$
]
For[$j = 1, j \leq 5, j++$,
While[Coefficient[$(\alpha^*(\alpha^* \llbracket \zeta^{12} \rrbracket)$ MOD $\chi) \llbracket 1 - \omega \rrbracket, \omega^{2j}$] $\not\equiv 0 \mod 13$,
$\alpha^* = \alpha^* z_j$ MOD χ
$e_{j+1} ++$
]
]
$e = \tau \cdot e \mod 13$
$\alpha^* = \alpha \zeta^{e_1} \prod_{i=1}^{5} \eta_i^{e_{i+1}}$ MOD χ
Return[$\{\alpha^*, e\}$]

```
Function AdditionalLaws[α]
```

$\gamma = \alpha$
For[$u = 0, u \leq 2, u++$,
While[
Coefficient[γ MOD $(1 - \zeta)^{u+1}, \zeta, u$] $\not\equiv \mu_u \mod 13$,
$\gamma = s_{u+1} \gamma$ MOD χ
]
]
{$d_0, \ldots, d_{12}$}=CoefficientList[$(\omega^{12} + \gamma) \llbracket 1 - \omega \rrbracket, \omega$]
$d_{12} = (1 - d_0)/13$
$d_{13} = 6d_{12} - d_1/13$
Return[$\{\Delta_0 \ldots, \Delta_6\} \mod 13$]

```
Function Resid[α, β]
```

$n = f[\beta, 1]$
$\gamma = f[\beta, 2]$
$\eta = \alpha^{(n-1)/13}$ MOD $\chi \mod n$
Let $0 \leq q \leq 12$ such that $(\eta - \zeta^q)\gamma$ MOD $\chi \equiv 0 \mod n$
Return[q]

C Activation Code & Execution Trace in Mathematical Form

```
Activation Code
```

```
For[j = 1, j ≤ 2, j++,
 p_j = 4
 While[p_j is composite,
  {ρ_0, ..., ρ_11} ∈_R [−min, +max] for some moderate min, max
  r_j = Σ_{i=0}^{11} ρ_i ζ^i
  p_j = f[r_j, 1]
 ]
]

Print["α : ", α = r_1, "\nβ : ", β = r_2]

Print["Residues␣␣:␣", {Resid[α, β], Resid[β, α]}]

{α*, m} = PrimaryRep[α]

β* = PrimaryRep[β][[1]]

Print["Primaries␣:␣", {Resid[α*, β*], Resid[β*, α*]}]

Print["Recovered␣:␣", Resid[α*, β*] - Prepend[m, 0].AdditionalLaws[β*] mod 13]
```

```
Execution Trace
```

$$
\begin{aligned}
\alpha &: \quad 6 - 5\zeta - \zeta^2 - 7\zeta^3 + 8\zeta^4 - 2\zeta^5 + 2\zeta^6 + 9\zeta^7 + 10\zeta^8 - 7\zeta^9 - 10\zeta^{10} - 4\zeta^{11} \\
\beta &: \quad -9 - \zeta + 3\zeta^3 - 2\zeta^4 + \zeta^5 + 9\zeta^6 + 2\zeta^7 + 9\zeta^8 + 9\zeta^9 - 5\zeta^{10} - 4\zeta^{11} \\
\texttt{Residues} &: \{12, 1\} \\
\texttt{Primaries} &: \{10, 10\} \\
\texttt{Recovered} &: 12
\end{aligned}
$$

D Executable Code

```
In[•]:= Mod𝛘[p_, n_: 0] := PolynomialRemainder[p,
          Sum[𝛇^i, {i, 0, 12}], 𝛇, Modulus → n];
        f := Mod𝛘[Product[(#1 /. 𝛇 → 𝛇^i), {i, #2, 12}]] &[#1, #2] &;
        PolynomialPowerMod :=
          Mod𝛘[If[#2 == 0, 1, #0[Mod𝛘[#1^2, #3], Floor[#2 / 2], #3]
                #1^Mod[#2, 2]], #3] &[#1, #2, #3] &;
        (* Generating units *)
        {𝛈1, 𝛈2, 𝛈3, 𝛈4, 𝛈5} = Table[1 + 𝛇^i, {i, 1, 5}];

        𝛕 = ⎛1  11  3  10  0  4⎞
            ⎜0  0   1  2   1  2⎟
            ⎜0  0   3  7   4  10⎟
            ⎜0  0   0  1   4  6⎟
            ⎜0  1   0  0   0  3⎟
            ⎝0  0   0  0   1  1⎠;

        PrimaryRep[𝛂_] :=
          Module[{𝛂s = 𝛂, e = Array[0 &, 6], j,
            z = {𝛇^11 𝛈4 , 𝛇^3 𝛈1 𝛈2^3, 𝛇^10 𝛈1^2 𝛈2^7 𝛈3 , 𝛈1 𝛈2^4 𝛈3^4 𝛈5 ,
              𝛇^4 𝛈1^2 𝛈2^10 𝛈3^6 𝛈4^3 𝛈5 }},
           While[Coefficient[𝛂s /. 𝛇 → 1 - 𝜔, 𝜔, Modulus → 13] ≠ 0,
            𝛂s = Mod𝛘[𝛇 𝛂s];
            e[[1]]++;
           ];
           For[j = 1, j ≤ 5, j++,
            While[Coefficient[Mod𝛘[𝛂s (𝛂s /. 𝛇 → 𝛇^12)] /. 𝛇 → 1 - 𝜔,
                𝜔^2j, Modulus → 13] ≠ 0,
              𝛂s = Mod𝛘[𝛂s z[[j]]];
              e[[j + 1]]++;
             ];
           ];
            e = Mod[𝛕.e, 13];
           𝛂s = Mod𝛘[𝛂 𝛇^e[[1]] 𝛈1^e[[2]] 𝛈2^e[[3]] 𝛈3^e[[4]] 𝛈4^e[[5]] 𝛈5^e[[6]]];
            Return[{𝛂s, e}];
           ];
```



```
        AdditionalLaws[𝛂_] :=
          Module[{𝛄 = 𝛂, z = {1 + 𝛇, 𝛇, 𝛈1^4 𝛈2^3 𝛈3^4 𝛈4 }, u, d0,
            d1, d2, d3, d4, d5, d6, d7, d8, d9, d10, d11, d12, d13},
           (* Reducing 𝛂 to 1 modulo 𝜔^3 *)
           For[u = 0, u ≤ 2, u++,
            While[
              Coefficient[PolynomialRemainder[𝛄, (1 - 𝛇)^u+1, 𝛇],
                𝛇, u, Modulus → 13] ≠ {1, 0, 0}[[u + 1]],
              𝛄 = Mod𝛘[z[[u + 1]] 𝛄];
             ];
           ];
           (* Computing special 𝜔 polynomial *)
           {d0, d1, d2, d3, d4, d5, d6, d7, d8, d9, d10, d11, d12} =
            CoefficientList[𝜔^12 + 𝛄 /. (𝛇 → 1 - 𝜔), 𝜔];
           {d12, d13} = {(1 - d0) / 13, 6 (1 - d0) / 13 - d1 / 13};
           (* Computing addional laws through polynomials *)
           Return[
            Mod[{12 d13 + d10 d3 + d3^3 d4 + 12 d4^2 d5 + 12 d3 d5^2 +
                11 d3 d4 d6 + 12 d3^2 d7 + d6 d7 + d5 d8 + d4 d9,
               d10 + d11 + d12 + d3 + 6 d3^2 + 9 d3^3 + 3 d3^4 + d4 +
                12 d3 d4 + d3^2 d4 + 6 d4^2 + d3 d4^2 + 9 d4^3 + d5 +
                12 d3 d5 + d3^2 d5 + 12 d4 d5 + 2 d3 d4 d5 + 6 d5^2 +
                d6 + 12 d3 d6 + d3^2 d6 + 12 d4 d6 + 12 d5 d6 + 6 d6^2 +
                d7 + 12 d3 d7 + 12 d4 d7 + 12 d5 d7 + d8 + 12 d3 d8 +
                12 d4 d8 + d9 + 12 d3 d9,
               5 d10 + 10 d11 + 7 d12 + 4 d3 + 10 d3^2 + 3 d3^3 + 8 d3^4 +
                8 d4 + d3 d4 + 5 d3^2 d4 + d4^2 + 10 d3 d4^2 + 11 d4^3 +
                3 d5 + 2 d3 d5 + 10 d3^2 d5 + 4 d4 d5 + d3 d4 d5 +
                4 d5^2 + 6 d6 + 4 d3 d6 + 7 d3^2 d6 + 8 d4 d6 + 3 d5 d6 +
                3 d6^2 + 12 d7 + 8 d3 d7 + 3 d4 d7 + 6 d5 d7 + 11 d8 +
                3 d3 d8 + 6 d4 d8 + 9 d9 + 6 d3 d9,
               6 d10 + d12 + 4 d3^2 + 2 d3^3 + 3 d3^4 + 9 d4 + 6 d3^2 d4 +
                5 d4^2 + 9 d4^3 + 5 d5 + 10 d3 d5 + 7 d4 d5 + 2 d3 d4 d5 +
                10 d5^2 + 5 d6 + 7 d3 d6 + d3^2 d6 + 7 d4 d6 + 6 d6^2 +
```

```
      7 d3 d7 + 12 d5 d7 + 3 d8 + 12 d4 d8 + 6 d9 + 12 d3 d9,
     3 d10 + 9 d11 + 8 d12 + 3 d3 + 3 d3^2 + 7 d3^3 + 11 d3^4 +
      6 d4 + 12 d3 d4 + 3 d3^2 d4 + 7 d4^2 + 9 d3 d4^2 + 7 d4^3 +
      2 d5 + d3 d5 + 9 d3^2 d5 + 5 d4 d5 + 3 d3 d4 d5 + 5 d5^2 +
      7 d6 + 5 d3 d6 + 8 d3^2 d6 + 10 d4 d6 + 4 d5 d6 + 9 d6^2 +
      d7 + 10 d3 d7 + 4 d4 d7 + 5 d5 d7 + 12 d8 + 4 d3 d8 +
      5 d4 d8 + 8 d9 + 5 d3 d9,
     9 d10 + 11 d11 + 2 d12 + d3 + 9 d3^2 + 6 d3^4 + 11 d4 +
      6 d3 d4 + 9 d3^2 d4 + 3 d4^2 + 11 d3 d4^2 + 5 d4^3 + 9 d5 +
      6 d3 d5 + 11 d3^2 d5 + 4 d3 d4 d5 + 2 d5^2 + 8 d6 +
      2 d3^2 d6 + 4 d4 d6 + 2 d5 d6 + 12 d6^2 + 7 d7 + 4 d3 d7 +
      2 d4 d7 + 11 d5 d7 + 7 d8 + 2 d3 d8 + 11 d4 d8 + 11 d3 d9,
    11 d10 + 6 d11 + 9 d12 + 3 d3 + d3^2 + d3^4 + 3 d4 +
      3 d3 d4 + 11 d3^2 d4 + 3 d4^2 + 6 d3 d4^2 + 3 d4^3 + 5 d5 +
      6 d3 d5 + 6 d3^2 d5 + 5 d3 d4 d5 + d5^2 + 11 d6 +
      9 d3^2 d6 + 2 d4 d6 + 7 d5 d6 + 2 d6^2 + 10 d7 + 2 d3 d7 +
      7 d4 d7 + 4 d5 d7 + 7 d8 + 7 d3 d8 + 4 d4 d8 + 4 d3 d9},
    13]];
 ];

Resid[α_, β_] := Module[{n = f[β, 1], γ = f[β, 2], η, q},
   η = PolynomialPowerMod[α, (n - 1) / 13, n];
   For[q = 0, q ≤ 12, q++,
    If[ModX[(η - ζ^q) γ, n] == 0, Return[q]];
   ];
  ];
(* Generating to prime elements in cyclotomic field *)
SeedRandom[1122];
For[j = 1, j ≤ 2, j++,
  p[j] = 4;
  While[! PrimeQ[p[j]],
   r[j] = Sum[RandomInteger[{-10, 10}] ζ^i, {i, 0, 11}];
   p[j] = f[r[j], 1];
  ];
 ];
```



```
Print["α : ", α = r[1], "\nβ : ", β = r[2]];
(* Checking residue values using associates *)
Print["Residues  : ", {Resid[α, β], Resid[β, α]}];
{αs, m} = PrimaryRep[α];
βs = PrimaryRep[β][[1]];
Print["Primaries : ", {Resid[αs, βs], Resid[βs, αs]}];
Print["Recovered : ",
  Mod[Resid[αs, βs] - Prepend[m, 0].AdditionalLaws[βs],
   13]];
```

```
α : 6 - 5 ζ - ζ^2 - 7 ζ^3 + 8 ζ^4 -
  2 ζ^5 + 2 ζ^6 + 9 ζ^7 + 10 ζ^8 - 7 ζ^9 - 10 ζ^10 - 4 ζ^11
β : -9 - ζ + 3 ζ^3 - 2 ζ^4 + ζ^5 + 9 ζ^6 + 2 ζ^7 + 9 ζ^8 + 9 ζ^9 - 5 ζ^10 - 4 ζ^11
Residues  : {12, 1}
Primaries : {10, 10}
Recovered : 12
```