To appear in *Banach Center Publications.*

FAST COMPUTATION OF THE OCTIC RESIDUE SYMBOL

MARC JOYE
Zama, France

Abstract. This paper presents a deterministic algorithm for the fast evaluation of the 8^{th}-power residue symbol.

Introduction. The r^{th}-power residue symbol for an integer $r \geq 2$ is a generalization of the Jacobi symbol. Algorithms for computing r^{th}-power residue symbols have been devised for $r \in \{2, 3, 4, 5, 7, 11\}$. See [15, 5], [14, 5], [13], [4] and [9] for the cases $r = 3$, 4, 5, 7 and 11, respectively. For prime values of $r \leq 11$, they turned out to follow a generic approach put forward by Caranay and Scheidler [4], building on Lenstra's norm-Euclidean division [11]. However, as noted in [4], as r grows, the technical details become increasingly complicated. The general case is addressed in [6] by de Boer and Pagano with probabilistic methods.

The case r a power of two is important for cryptographic applications. This includes [8, 2] for encryption schemes and [1, 12, 3] for authentication schemes and digital signatures. As aforementioned, efficient algorithms are fully specified for $r = 2$ and $r = 4$. The next value is $r = 8$; namely, the octic residue symbol. An excellent account on the octic reciprocity can be found in [10, Chapter 9]. See also [7].

1. Primary Elements. Let $\zeta \coloneqq \zeta_8 = \frac{\sqrt{2}}{2}(1 + i)$ be a primitive 8^{th} root of unity. Let also $\epsilon = 1 + \sqrt{2} = 1 + \zeta + \zeta^{-1}$. The field $\mathbb{Q}(\zeta) = \mathbb{Q}(i, \sqrt{2})$ is biquadratic and the group of units of its ring of algebraic integers is $\langle \zeta, \epsilon \rangle$. The Galois group of $\mathbb{Q}(\zeta)/\mathbb{Q}$ contains the four automorphisms $\sigma_k \colon \zeta \mapsto \zeta^k$ with $k \in \{1, 3, 5, 7\}$. For an element $\alpha \in \mathbb{Z}[\zeta]$, we write $\alpha_k = \sigma_k(\alpha)$. The (absolute) norm of α is given by $\mathrm{N}(\alpha) = \alpha_1\alpha_3\alpha_5\alpha_7$.

An element $\alpha = a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3 \in \mathbb{Z}[\zeta]$ is said to be *primary* if $\alpha \equiv 1$

2020 *Mathematics Subject Classification*: Primary 11A15; Secondary: 11T71, 11Y16.
Key words and phrases: Number theory, Cryptography, Higher residuosity, Power residue symbols, Implementation.
The paper is in final form and no version of it will be published elsewhere.

(mod $2+2\zeta$) or, equivalently, if

$$\begin{cases} a_0+a_1+a_2+a_3 \equiv 1 \pmod 4\,, \\ a_1 \equiv a_2 \equiv a_3 \equiv 0 \pmod 2\,. \end{cases}$$

Proof. By definition, α must be such that $(\alpha-1) \propto 2(1+\zeta)$. Since $1-\zeta^4=2$, we have $\frac{(a_0-1)+a_1\zeta+a_2\zeta^2+a_3\zeta^3}{2(1+\zeta)} = \frac{((a_0-1)+a_1\zeta+a_2\zeta^2+a_3\zeta^3)(1-\zeta)(1+\zeta^2)}{4} = \frac{a_0-1+a_1-a_2+a_3}{4} + \frac{-a_0+1+a_1+a_2-a_3}{4}\zeta + \frac{a_0-1-a_1+a_2+a_3}{4}\zeta^2 + \frac{-a_0+1+a_1-a_2+a_3}{4}\zeta^3$. The condition is satisfied provided that $a_0-1+a_1-a_2+a_3 \equiv -a_0+1+a_1+a_2-a_3 \equiv a_0-1-a_1+a_2+a_3 \equiv -a_0+1+a_1-a_2+a_3 \equiv 0 \pmod 4$; that is, $a_0+a_1+a_2+a_3 \equiv 1 \pmod 4$ and $2a_1 \equiv 2a_2 \equiv 2a_3 \equiv 0 \pmod 4$. ∎

Proposition 1. *Let $\alpha \in \mathbb{Z}[\zeta]$ such that $(1+\zeta) \nmid \alpha$. Then there is a unit $\upsilon \in \mathbb{Z}[\zeta]$ such that $\alpha = \upsilon\,\alpha^*$ with α^* primary.*

Proof. Let $\alpha = a_0+a_1\zeta+a_2\zeta^2+a_3\zeta^3$. The condition $(1+\zeta) \nmid \alpha$ implies $a_0+a_1+a_2+a_3 \equiv 1 \pmod 2$.

1. Suppose first that $a_0 \not\equiv a_2 \pmod 2$ (and thus $a_1 \equiv a_3 \pmod 2$). Noting that $\alpha \sim \alpha\,\zeta^{-2} = a_2 + a_3\zeta - a_0\zeta^2 - a_1\zeta^3$, we can assume that $a_0 \equiv 1 \pmod 2$ and $a_2 \equiv 0 \pmod 2$.
   (a) If $a_1 \equiv a_3 \equiv 0 \pmod 2$ then $\alpha = a_0+a_1\zeta+a_2\zeta^2+a_3\zeta^3$ with $a_0 \equiv 1 \pmod 2$ and $a_1 \equiv a_2 \equiv a_3 \equiv 0 \pmod 2$.
   (b) If $a_1 \equiv a_3 \equiv 1 \pmod 2$, we replace α with $\alpha\,\epsilon^{-1}$ and get
   $$\alpha\,\epsilon^{-1} = \underbrace{(-a_0+a_1-a_3)}_{\equiv 1 \pmod 2} + \underbrace{(a_0-a_1+a_2)}_{\equiv 0 \pmod 2}\zeta + \underbrace{(a_1-a_2+a_3)}_{\equiv 0 \pmod 2}\zeta^2 + \underbrace{(-a_0+a_2-a_3)}_{\equiv 0 \pmod 2}\zeta^3\,.$$
   By possibly multiplying by $-1=\zeta^{-4}$ yields a primary element.
2. Suppose now that $a_0 \equiv a_2 \pmod 2$ (and $a_1 \not\equiv a_3 \pmod 2$). Then multiplying α by ζ^{-1} yields $\alpha\,\zeta^{-1} = a_1 + a_2\zeta + a_3\zeta^3 - a_0\zeta^3$. We so obtain a case similar to Case 1.

Consequently, in all cases, α can be expressed as $\alpha = \upsilon\,\alpha^*$ with α^* primary and $\upsilon = \zeta^k\epsilon^l$ for some $0 \le k \le 7$ and $l \in \{0,1\}$. ∎

2. Octic Reciprocity Law. The main result is the octic reciprocity law; see [10, Theorem 9.19].

Theorem 1 (Octic Reciprocity). *Let α and λ be co-prime primary elements of $\mathbb{Z}[\zeta]$. Let N_1, N_2 and N_3 respectively denote the relative norms of the extensions $\mathbb{Q}(\zeta)/\mathbb{Q}(i)$, $\mathbb{Q}(\zeta)/\mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\zeta)/\mathbb{Q}(\sqrt{2})$; and write $\mathrm{N}_1(\alpha) = a(\alpha)^2+b(\alpha)^2$, $\mathrm{N}_2(\alpha) = c(\alpha)^2 + 2d(\alpha)^2$, $\mathrm{N}_3(\alpha) = e(\alpha)^2 - 2f(\alpha)^2$, and similarly for λ. Then*[1]

$$\left[\frac{\alpha}{\lambda}\right]_8 = \left[\frac{\lambda}{\alpha}\right]_8 (-1)^{\frac{\mathrm{N}(\alpha)-1}{8}\frac{\mathrm{N}(\lambda)-1}{8}} \zeta^{\frac{d(\lambda)f(\alpha)-d(\alpha)f(\lambda)}{4}}\,.$$

[1] We note that a factor $-\frac{1}{4}$ is missing in the expression given in [10, Theorem 9.19].

Moreover,

$$\left[\frac{1-\zeta}{\alpha}\right]_8 = \zeta^{\frac{5a-5+5b+18d+b^2-2bd+d^4/2}{8}}\,, \qquad \left[\frac{\zeta}{\alpha}\right]_8 = \zeta^{\frac{a-1+4b+2bd+2d^2}{4}}\,,$$
$$\left[\frac{1+\zeta}{\alpha}\right]_8 = \zeta^{\frac{a-1+b+6d+b^2+2bd+d^4/2}{8}}\,, \qquad \left[\frac{\epsilon}{\alpha}\right]_8 = \zeta^{\frac{d-3b-bd-2d^2}{2}}\,,$$
$$\left[\frac{1+\zeta+\zeta^2}{\alpha}\right]_8 = \zeta^{\frac{a-1-2b+2d-2d^2}{4}}\,.$$

∎

Letting $\alpha = a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3$ and $\alpha_k = \sigma_k(\alpha)$, a direct calculation shows that $\alpha_1\alpha_5 = ({a_0}^2 - {a_2}^2 + 2a_1a_3) + (-{a_1}^2 + {a_3}^2 + 2a_0a_2)i$, $\alpha_1\alpha_3 = ({a_0}^2 - {a_1}^2 + {a_2}^2 - {a_3}^2) + (a_0a_1 + a_0a_3 - a_1a_2 + a_2a_3)\sqrt{-2}$, and $\alpha_1\alpha_7 = ({a_0}^2 + {a_1}^2 + {a_2}^2 + {a_3}^2) + (a_0a_1 - a_0a_3 + a_1a_2 + a_2a_3)\sqrt{2}$ [10, Exerc. 5.21]. This yields[2]

$$a(\alpha) = {a_0}^2 - {a_2}^2 + 2a_1a_3\,, \quad b(\alpha) = -{a_1}^2 + {a_3}^2 + 2a_0a_2\,,$$
$$d(\alpha) = a_0a_1 + a_0a_3 - a_1a_2 + a_2a_3\,, \quad f(\alpha) = a_0a_1 - a_0a_3 + a_1a_2 + a_2a_3\,.$$

3. Evaluating Octic Residue Symbols. As stated, the reciprocity law requires α and λ being primary. Suppose that α is such that $(1+\zeta) \nmid \alpha$, but is not necessarily primary. Then from Proposition 1, we can write $\alpha = \zeta^k \epsilon^l\, \alpha^*$ for some $0 \le k \le 7$ and $l \in \{0,1\}$, with α^* primary. We note $\alpha^* = \mathrm{primary}(\alpha)$ and $(k,l) = \nu(\alpha)$. Likewise, suppose that λ is such that $(1+\zeta) \nmid \lambda$ and is not necessarily primary. Then $\lambda = \zeta^{k'}\epsilon^{l'}\lambda^*$ with $\lambda^* = \mathrm{primary}(\lambda)$ and $(k',l') = \nu(\lambda)$.

We assume $(1+\zeta) \nmid \lambda$. Putting it all together, when $(1+\zeta) \nmid \alpha$, we have:

$$\begin{aligned}
\left[\frac{\alpha}{\lambda}\right]_8 &= \left[\frac{\alpha}{\lambda^*}\right]_8 \\
&= \left[\frac{\zeta^k}{\lambda^*}\right]_8 \left[\frac{\epsilon^l}{\lambda^*}\right]_8 \left[\frac{\alpha^*}{\lambda^*}\right]_8 && \text{by Proposition 1} \\
&= \zeta^{\frac{k\left(a(\lambda^*)-1+4b(\lambda^*)+2b(\lambda^*)d(\lambda^*)+2d(\lambda^*)^2\right)}{4}} \zeta^{\frac{l\left(d(\lambda^*)-3b(\lambda^*)-b(\lambda^*)d(\lambda^*)-2d(\lambda^*)^2\right)}{2}} \\
&\qquad \left[\frac{\lambda^*}{\alpha^*}\right]_8 \zeta^{\frac{(\mathrm{N}(\alpha^*)-1)(\mathrm{N}(\lambda^*)-1)}{16} + \frac{d(\lambda^*)f(\alpha^*)-d(\alpha^*)f(\lambda^*)}{4}} && \text{by Theorem 1} \\
&= \left[\frac{\lambda^* \bmod \alpha^*}{\alpha^*}\right]_8 \zeta^{k\,\mathcal{K}(\lambda^*)+l\,\mathcal{L}(\lambda^*)+\mathcal{J}(\alpha^*,\lambda^*)} \pmod 8
\end{aligned}$$

where

$$\mathcal{K}(\lambda^*) = \tfrac{1}{4}\left[a(\lambda^*) - 1 + 4b(\lambda^*) + 2b(\lambda^*)d(\lambda^*) + 2d(\lambda^*)^2\right],$$
$$\mathcal{L}(\lambda^*) = \tfrac{1}{2}\left[d(\lambda^*) - 3b(\lambda^*) - b(\lambda^*)d(\lambda^*) - 2d(\lambda^*)^2\right],$$
$$\mathcal{J}(\alpha^*,\lambda^*) = \tfrac{1}{16}\left[(\mathrm{N}(\alpha^*)-1)(\mathrm{N}(\lambda^*)-1) + 4d(\lambda^*)f(\alpha^*) - 4d(\alpha^*)f(\lambda^*)\right]\,.$$

[2]The first formula listed in [10, Exerc. 5.21] actually corresponds to $-b$.

When $(1+\zeta) \mid \alpha$, we have:

$$\begin{aligned}\left[\frac{\alpha}{\lambda}\right]_8 = \left[\frac{\alpha}{\lambda^*}\right]_8 &= \left[\frac{\alpha/(1+\zeta)}{\lambda^*}\right]_8 \left[\frac{1+\zeta}{\lambda^*}\right]_8 \\ &= \left[\frac{\alpha/(1+\zeta)}{\lambda^*}\right]_8 \zeta^{\mathcal{I}(\lambda^*)} \pmod 8 \qquad \text{by Theorem 1}\end{aligned}$$

where

$$\mathcal{I}(\lambda^*) = \tfrac{1}{8}\big(a(\lambda^*) - 1 + b(\lambda^*) + 6d(\lambda^*) + b(\lambda^*)^2 + 2b(\lambda^*)d(\lambda^*) + d(\lambda^*)^4/2\big) \;.$$

Computation of the 8^{th}*-power residue symbol.* These two observations lead to Algorithm 1.

Algorithm 1: Computing $\left[\frac{\alpha}{\lambda}\right]_8$

Data: $\alpha, \lambda \in \mathbb{Z}[\zeta]$ with α and λ co-prime, and $(1+\zeta) \nmid \lambda$
Result: $\left[\frac{\alpha}{\lambda}\right]_8 \in \{\pm 1, \pm i, \pm\zeta, \pm i\zeta\}$

```
λ ← primary(λ); j ← 0
while N(α) ≠ 1 do
    if (1 + ζ) | α then
        α ← α/(1 + ζ)
        j ← j + I(λ) (mod 8)
    else
        (k, l) ← ν(α); α ← primary(α)
        j ← j + k K(λ) + l L(λ) + J(α, λ) (mod 8)
        (α, λ) ← (λ mod α, α)
    end
end
(k, l) ← ν(α); α ← primary(α)
[u0, u1, u2, u3] ← α mod 8; k ← k + u0 − 1; l ← l + u3
j ← j + k K(λ) + l L(λ) (mod 8)
return ζ^j
```

At the end of the while-loop, α is transformed into a primary unit, say υ^*. Letting $\upsilon^* \bmod 8 = u_0 + u_1\zeta + u_2\zeta^2 + u_3\zeta^3 := [u_0, u_1, u_2, u_3]$, it turns out that the possible values are $[1,0,0,0]$, $[1,4,0,4]$, $[5,6,0,2]$, $[5,2,0,6]$, respectively corresponding to $\left[\frac{\upsilon^*}{\lambda^*}\right]_8 = \left[\frac{1}{\lambda^*}\right]_8$, $\left[\frac{\epsilon^4}{\lambda^*}\right]_8$, $\left[\frac{\zeta^4\epsilon^2}{\lambda^*}\right]_8$, $\left[\frac{\zeta^4\epsilon^6}{\lambda^*}\right]_8$.

Correctness. As a reminder, a ring R is said *norm-Euclidean* or *Euclidean with respect to the norm* N if for every $\alpha, \beta \in R$, $\beta \neq 0$, there exist $\eta, \rho \in R$ such that $\alpha = \beta\,\eta + \rho$ and $\mathrm{N}(\rho) < \mathrm{N}(\beta)$. The correctness of the algorithm is a consequence of the fact that $\mathbb{Z}[\zeta]$ is norm-Euclidean [11]: when α is replaced by $\lambda \bmod \alpha$, its norm decreases. Also, when α is divided by $(1+\zeta)$, its norm is divided by 2 since $\mathrm{N}(1+\zeta) = 2$. Therefore, in all cases, the norm of α is decreasing and eventually becomes 1.

Remark 1. Letting $\alpha = a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3$, the condition $(1+\zeta) \mid \alpha$ simply amounts to verify whether $a_0 + a_1 + a_2 + a_3 \equiv 0 \pmod 2$; in this case, $\alpha/(1+\zeta) = \frac{1}{2}(a_0 + a_1 - a_2 + a_3) + \frac{1}{2}(-a_0 + a_1 + a_2 - a_3)\zeta + \frac{1}{2}(a_0 - a_1 + a_2 + a_3)\zeta^2 + \frac{1}{2}(-a_0 + a_1 - a_2 + a_3)\zeta^3$.

Acknowledgements. I am grateful to Franz Lemmermeyer for providing a copy of [7].

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] Fabrice Benhamouda, Javier Herranz, Marc Joye, and Benoît Libert. Efficient cryptosystems from 2^k-th power residue symbols. *Journal of Cryptology*, 30(2):519–549, 2017. doi:10.1007/s00145-016-9229-5.

[3] Éric Brier, Houda Ferradi, Marc Joye, and David Naccache. New number-theoretic cryptographic primitives. *Journal of Mathematical Cryptology*, 14(1):224–235, 2020. doi:10.1515/jmc-2019-0035.

[4] 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.

[5] 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.

[6] 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.

[7] Franz Goldscheider. Das Reziprozitätsgesetz der achten Potenzreste. *Wissenschaftliche Beilage zum Programm des Luisenstädtischen Realgymnasiums*, 96:1–29, 1889. URL: https://zbmath.org/?q=an%3A21.0178.02.

[8] 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.

[9] Marc Joye, Oleksandra Lapiha, Ky Nguyen, and David Naccache. The eleventh power residue symbol. *Journal of Mathematical Cryptology*, 15(1):111–122, 2021. doi:10.1515/jmc-2020-0077.

[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] 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.

[13] 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.

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

[15] 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.