Computing Jacobi Symbols in Algebraic Number Fields

to Willem Kuyk

H.W. Lenstra, Jr.[1]
Department of Mathematics
University of California
Berkeley, CA 94720-3840

It is shown that there is an efficient algorithm for computing quadratic residue symbols in algebraic number fields.

1. Introduction

The *Jacobi symbol* or *quadratic residue symbol* $\left(\frac{a}{b}\right)$ is defined for integers a and b, with b odd and positive. It extends the Legendre symbol, which is only defined if b is prime, by means of the rule $\left(\frac{a}{b_1 b_2}\right) = \left(\frac{a}{b_1}\right)\left(\frac{a}{b_2}\right)$. It is well-known that there exists an efficient algorithm for calculating the Jacobi symbol (cf. [7, Exercise 4.5.4.23]). The main ingredients of this algorithm are the reciprocity law for the Jacobi symbol and the Euclidean division algorithm.

Let K be an algebraic number field, with ring of integers A. There is again a quadratic residue symbol $\left(\frac{a}{\mathfrak{b}}\right)$, which is defined for $a \in A$ and for $\mathfrak{b}$ an ideal of A of odd norm (see [4, Exercise 1, with $m = 2$], and Section 3 below). It does satisfy a reciprocity law, but the latter is restricted to principal ideals $\mathfrak{b}$ and it involves the norm residue symbol (see [4, Exercise 2]). Since the Euclidean division algorithm in general algebraic number fields leaves also something to be desired, we find that the tools that enable us to calculate $\left(\frac{a}{\mathfrak{b}}\right)$ efficiently in the case that K is the field of rational numbers are lacking for general K. In the present paper I exhibit an efficient algorithm that works in general.

Theorem. *There is a deterministic polynomial time algorithm that, given an algebraic number field K, an order A in K, an element $a \in A$, and an ideal $\mathfrak{b} \subset A$ of odd index in A, computes $\left(\frac{a}{\mathfrak{b}}\right)$.*

What it means for K, A, a, $\mathfrak{b}$ to be "given" is explained in [9, Section 2]. Imprecisely speaking, it means that numerical data specifying K, A, a, $\mathfrak{b}$ form the input to the algorithm. In particular, the polynomial bound for the run time of the algorithm is not just valid for a fixed number field K, but it holds

[1] The author was supported by NSF under grant No. DMS 92-24205.

uniformly for all number fields. For the definition of orders and Jacobi symbols for orders I refer to Section 3.

My algorithm, as described in 3.2, may not be immediately digestible by an electronic computer, but there is no doubt that it can be turned into a practical method for computing $\left(\frac{a}{b}\right)$, should the need ever arise.

The cardinality of a set S is denoted by $\#S$. Rings are supposed to be commutative with 1. We write $\mathbb{Z}$ for the ring of integers.

2. Signs of endomorphisms

In this section we denote by M a finite abelian group of *odd* order. It will be written additively. For any endomorphism ε of M, we define the symbol $(\varepsilon, M) \in \{0, 1, -1\}$ as follows. If ε is not an automorphism of M, then we let $(\varepsilon, M) = 0$. Suppose next that ε is an automorphism. Then we put $(\varepsilon, M) = 1$ if ε is even as a permutation of the underlying set of M, and $(\varepsilon, M) = -1$ if it is odd. Clearly, we have $(\varepsilon_1\varepsilon_2, M) = (\varepsilon_1, M)(\varepsilon_2, M)$ for any two endomorphisms ε_1, ε_2 of M.

Proposition 2.1. *Let $0 \to M' \xrightarrow{i} M \xrightarrow{f} M'' \to 0$ be a short exact sequence, and let ε be an endomorphism of M. Suppose that ε induces endomorphisms ε' and ε'' of M' and M'', in the sense that $\varepsilon i = i\varepsilon'$ and $\varepsilon'' f = f\varepsilon$. Then we have $(\varepsilon, M) = (\varepsilon', M')(\varepsilon'', M'')$.*

Proof. It is easy to show that ε is an automorphism of M if and only if ε' is an automorphism of M' and ε'' is an automorphism of M''. Thus the formula is true if one of the symbols equals 0. Let it now be assumed that we have three automorphisms. Using that M'' has no elements of order 2, one easily constructs a right inverse $g\colon M'' \to M$ to f with the property that $g(-z) = -g(z)$ for all $z \in M''$. Then any $x \in M$ has a unique representation $x = i(y) + g(z)$, with $y \in M'$, $z \in M''$. Define permutations ρ, σ of M by $\rho(i(y) + g(z)) = i(\varepsilon' y) + g(z)$ and $\sigma(i(y) + g(z)) = i(y) + g(\varepsilon'' z)$; these are not necessarily automorphisms of M, but they do commute with the map $-1\colon M \to M$ sending x to $-x$. Hence the permutation τ of M for which $\varepsilon = \rho\sigma\tau$ commutes with -1 as well.

The permutation ρ acts on M in the same way as ε' acts on the union of $\#M''$ disjoint copies of M'. Since $\#M''$ is odd, this implies that ρ and ε' have the same sign. Likewise, σ and ε'' have the same sign. Thus, to finish the proof of 2.1 it suffices to show that τ is even.

By construction, τ induces the identity permutations of both M' and M''. That is, τ is the identity on the set $iM' = f^{-1}0$, and for each $z \in M''$ it permutes the set $f^{-1}z = iM' + g(z)$. Since τ commutes with -1, its actions on $f^{-1}z$ and on $f^{-1}(-z)$ are isomorphic, so its action on the union $f^{-1}z \cup f^{-1}(-z)$ is even, for each $z \in M''$, $z \neq 0$. Hence τ is even. This proves 2.1. □

Proposition 2.2. *Let k be a finite field of odd characteristic, and let $a \in k$. Denote by ε_a the endomorphism of the additive group of k that is defined by $\varepsilon_a(x) = ax$. Then we have $(\varepsilon_a, k) = a^{(\#k-1)/2}$, where we consider $\{0, 1, -1\}$ as*

a subset of k.

PROOF. For $a = 0$ the formula is clear. Next let a be a generator of the multiplicative group k^* of k. Then ε_a is, as a permutation, the product of a cycle of length 1 and a cycle of even length $\#k - 1$. Hence ε_a is odd, and $(\varepsilon_a, k) = -1$. Also, $a^{(\#k-1)/2}$ has order 2 in k^*, so $a^{(\#k-1)/2} = -1$. This proves the formula if a generates k^*. To prove the formula for general $a \in k^*$ it suffices to remark that each element of k^* can be written as a power of a generator. This proves 2.2. □

If $M = (\mathbb{Z}/n\mathbb{Z})^t$ for some positive integers n and t, then each endomorphism ε of M can be written as a $t \times t$ matrix with coefficients in $\mathbb{Z}/n\mathbb{Z}$. In this situation we define the determinant $\det \varepsilon$ of ε to be the determinant of that matrix; so $\det \varepsilon \in \mathbb{Z}/n\mathbb{Z}$. The Jacobi symbol in the following result is the traditional one.

PROPOSITION 2.3. *Suppose that $M = (\mathbb{Z}/n\mathbb{Z})^t$ for some positive integers n and t, with n odd. Then for each endomorphism ε of M the symbol (ε, M) equals the Jacobi symbol $\left(\frac{\det \varepsilon}{n}\right)$.*

PROOF. Assume first that $n = p$ is prime. For $t = 1$ the formula follows from 2.2, with $k = \mathbb{Z}/p\mathbb{Z}$. If ε is given by an upper or lower triangular matrix, then one uses 2.1 to prove the formula by induction on t. Since any square matrix over a field is a product of finitely many upper and lower triangular matrices we obtain the formula for all ε.

For general n we argue by induction on the number u of prime factors of n, counted with multiplicities. For $u = 0$ the formula is trivial, and for $u = 1$ we just proved it. Suppose that $u \geq 2$, and choose a non-trivial factorization $n = n'n''$. With $M' = (\mathbb{Z}/n'\mathbb{Z})^t$ and $M'' = (\mathbb{Z}/n''\mathbb{Z})^t$ we have a short exact sequence $0 \to M' \xrightarrow{i} M \xrightarrow{f} M'' \to 0$, where f is the natural map and i is induced by multiplication by n''. If the entries of the matrix giving ε are reduced modulo n' and n'', respectively, then one obtains matrices that give endomorphisms ε' and ε'' of M' and M'' as in 2.1. Hence 2.1 and the induction hypothesis imply that

$$(\varepsilon, M) = (\varepsilon', M')(\varepsilon'', M'') = \left(\frac{\det \varepsilon'}{n'}\right)\left(\frac{\det \varepsilon''}{n''}\right) = \left(\frac{\det \varepsilon}{n'}\right)\left(\frac{\det \varepsilon}{n''}\right) = \left(\frac{\det \varepsilon}{n}\right),$$

as required. This proves 2.3. □

We shall now give a formula for (ε, M) that applies to general M. Since M is a finite abelian group of odd order, there are positive odd integers $n_1, n_2, \ldots, n_t$ such that with $m_i = \prod_{h=1}^{i} n_h$ we have an isomorphism $M \cong \bigoplus_{i=1}^{t} (\mathbb{Z}/m_i\mathbb{Z})$; moreover, the n_i are uniquely determined by M if we also require that $n_1 > 1$. Choose such an isomorphism, and denote by e_i the element of M that corresponds to the ith unit vector in $\bigoplus_{i=1}^{t} (\mathbb{Z}/m_i\mathbb{Z})$. Let ε be an endomorphism of M. Then $\varepsilon(e_i) = \sum_{j=1}^{t} a_{ij} e_j$ for certain integers a_{ij}, uniquely determined modulo m_j; a given system of integers a_{ij} corresponds to an endomorphism of M if and only if $a_{ij} \equiv 0 \bmod m_j/m_i$ whenever $j > i$.

PROPOSITION 2.4. *Let M be a finite abelian group of odd order, and let ε be an endomorphism of M. Suppose that the pair M, ε is specified, as just described, by a sequence $n_1, n_2, \ldots, n_t$ and a $t \times t$ matrix (a_{ij}). Then we have*

$$(\varepsilon, M) = \prod_{h=1}^{t} \left(\frac{\det(a_{ij})_{h \le i,j \le t}}{n_h} \right).$$

PROOF. The proof is by induction on t, the case $t = 0$ being trivial. Let $t > 0$. The isomorphism $M \cong \bigoplus_{i=1}^{t} (\mathbb{Z}/m_i\mathbb{Z})$ induces isomorphisms $n_1 M \cong \bigoplus_{i=2}^{t} (\mathbb{Z}/(m_i/n_1)\mathbb{Z})$ and $M/n_1 M \cong (\mathbb{Z}/n_1\mathbb{Z})^t$. We apply 2.1 to the short exact sequence $0 \to n_1 M \to M \to M/n_1 M \to 0$, with ε'' given by the $t \times t$ matrix $(a_{ij})_{1 \le i,j \le t}$ and ε' by the $(t-1) \times (t-1)$ matrix $(a_{ij})_{2 \le i,j \le t}$. We find that $(\varepsilon, M) = (\varepsilon', n_1 M)(\varepsilon'', M/n_1 M)$. Applying the induction hypothesis to $(\varepsilon', n_1 M)$ and 2.3 to $(\varepsilon'', M/n_1 M)$ we obtain 2.4. □

Determinants of integer matrices can be computed in polynomial time (see [10, Corollary 3.3a]), and the same applies to Jacobi symbols (as in [7, Exercise 4.5.4.23]). It follows that the formula in 2.4 can be evaluated in polynomial time.

3. JACOBI SYMBOLS

Let A be a ring. For an element $a \in A$ and an ideal $\mathfrak{b} \subset A$ for which $\#(A/\mathfrak{b})$ is finite and odd we define the Jacobi symbol $\left(\frac{a}{\mathfrak{b}}\right) \in \{0, 1, -1\}$ as follows. If $\mathfrak{b} = \mathfrak{m}$ is a maximal ideal, then $\left(\frac{a}{\mathfrak{m}}\right)$ is the unique element of $\{0, 1, -1\}$ that is congruent to $a^{(\#(A/\mathfrak{m})-1)/2}$ modulo $\mathfrak{m}$. For general $\mathfrak{b}$, one puts $\left(\frac{a}{\mathfrak{b}}\right) = \prod_{\mathfrak{m}} \left(\frac{a}{\mathfrak{m}}\right)^{l_{\mathfrak{m}}(A/\mathfrak{b})}$, where $\mathfrak{m}$ ranges over all maximal ideals of A with $2 \notin \mathfrak{m}$, and $l_{\mathfrak{m}}(A/\mathfrak{b})$ denotes the number of composition factors of the A-module $A/\mathfrak{b}$ that are isomorphic to $A/\mathfrak{m}$ (cf. [3, Section 7]); equivalently, $l_{\mathfrak{m}}(A/\mathfrak{b})$ equals the length of the module $A_{\mathfrak{m}}/\mathfrak{b}_{\mathfrak{m}}$ over the local ring $A_{\mathfrak{m}}$ (cf. [1]). We have $l_{\mathfrak{m}}(A/\mathfrak{b}) = 0$ for almost all $\mathfrak{m}$, so the infinite product makes sense (with $0^0 = 1$).

For $A = \mathbb{Z}$ and $\mathfrak{b} = b\mathbb{Z}$, with b a positive odd integer, the Jacobi symbol $\left(\frac{a}{\mathfrak{b}}\right)$ defined above is clearly equal to the traditional Jacobi symbol $\left(\frac{a}{b}\right)$. If A is the ring of integers of an algebraic number field K, then the Jacobi symbol defined above is equal to the traditional quadratic residue symbol in K.

The connection with the symbol from the previous section is as follows.

PROPOSITION 3.1. *Let A be a ring, let $a \in A$, and let $\mathfrak{b} \subset A$ be an ideal for which $\#(A/\mathfrak{b})$ is finite and odd. Denote by ε_a the endomorphism of $A/\mathfrak{b}$ defined by $\varepsilon_a(x) = ax$. Then we have $\left(\frac{a}{\mathfrak{b}}\right) = (\varepsilon_a, A/\mathfrak{b})$.*

PROOF. We prove the following more general formula. Let M be a finite A-module of odd cardinality. Then for any $a \in A$ we have $(\varepsilon_a, M) = \prod_{\mathfrak{m}} \left(\frac{a}{\mathfrak{m}}\right)^{l_{\mathfrak{m}}(M)}$, where $\mathfrak{m}$ ranges over all maximal ideals of A, and ε_a and $l_{\mathfrak{m}}(M)$ are defined as in the case $M = A/\mathfrak{b}$. The proof is by induction on $\#M$. If $M = 0$ then the formula is trivial, and if $M \cong A/\mathfrak{n}$ for some maximal ideal $\mathfrak{n}$ of A then it

suffices to apply 2.2. In all other cases M has a non-trivial submodule M', and one can use 2.1 and the induction hypothesis to finish the proof. This proves 3.1. □

3.2 *Computing the Jacobi symbol*
Let K be an algebraic number field, and denote by d its degree over the field of rational numbers. An *order* in K is a subring A of K of which the additive group is isomorphic to $\mathbb{Z}^d$. Let an order A in an algebraic number field be given (in the sense of [9, Section 2]), along with an element $a \in A$ and a non-zero ideal $\mathfrak{b} \subset A$ for which $\#(A/\mathfrak{b})$ is odd. Suppose that one wishes to compute $\left(\frac{a}{\mathfrak{b}}\right)$. By 3.1, one can apply the formula of 2.4 for this purpose, provided that one knows integers $n_1, n_2, \ldots, n_t$ and a $t \times t$ matrix (a_{ij}) that specify the abelian group $A/\mathfrak{b}$ and its endomorphism ε_a in the way indicated in Section 2. One can compute such n_i and a_{ij} by means of standard techniques of linear algebra over $\mathbb{Z}$ (see [2, Section 5] and [5, Chapter 2]).

One verifies in a straightforward way that the algorithm for computing $\left(\frac{a}{\mathfrak{b}}\right)$ that we just described runs in polynomial time. This proves the theorem stated in the introduction.

3.3 *The mth power residue symbol*
Our definition of the symbol (ε, M) depends on the notion of parity of permutations, so that it may not be obvious how to define a generalization that applies to higher power residue symbols. One can proceed in the following way. Let m be an integer, $m > 1$, and let ζ be a primitive mth root of unity in some extension field of the field of rational numbers. Instead of finite abelian groups of odd order, one now considers finite modules M over the ring $\mathbb{Z}[\zeta]$ for which $\gcd(m, \#M) = 1$. Let M be such a module. Write $\langle\zeta\rangle$ for the multiplicative group generated by ζ; it is cyclic of order m. One can show that there is a set S of non-zero elements of M such that every non-zero element of M has a unique expression of the form ηs with $\eta \in \langle\zeta\rangle$, $s \in S$; in particular, one has $\#M \equiv 1 \bmod m$. Let ε be an endomorphism of M, or, more generally, any map $M \to M$ that commutes with the map sending x to ζx. Then one defines the symbol $(\varepsilon, M)_m \in \{0\} \cup \langle\zeta\rangle$ as follows. If ε is not bijective, one puts $(\varepsilon, M)_m = 0$. Next suppose that ε is bijective. For each $s \in S$, let $\eta(s)$ be the unique element of $\langle\zeta\rangle$ for which $\varepsilon(s)\eta(s)^{-1}$ belongs to S. Then one puts $(\varepsilon, M)_m = \prod_{s\in S} \eta(s)$. Note the similarity with the definition of the transfer map in group theory (see [6, Kapitel IV, Abschnitt 1]). One readily verifies that the definition is independent of the choice of S, and that for $m = 2$ one recovers the symbol (ε, M). All results that we obtained for (ε, M) generalize to $(\varepsilon, M)_m$, although with different proofs. The algorithms in 2.4 and 3.2 do not generalize completely; all one finds is that *the computation of the mth power residue symbol $\left(\frac{a}{\mathfrak{b}}\right)_m$, where a belongs to a $\mathbb{Z}[\zeta]$-algebra A that is an order in a number field, and $\mathfrak{b}$ is a non-zero ideal of A with $\gcd(m, \#(A/\mathfrak{b})) = 1$, can be reduced to the case that $A = \mathbb{Z}[\zeta]$*. This suggests that for fixed m there is a polynomial time algorithm for calculating the mth power residue symbol in algebraic number fields containing ζ. It would be of interest to prove the same result for variable m, and to find efficient algorithms for computing norm

residue symbols and Artin symbols as well.

References

1. M.F. Atiyah and I.G. Macdonald, 1969, *Introduction to commutative algebra*, Addison-Wesley, Reading, Mass..
2. J.A. Buchmann and H.W. Lenstra, Jr., 1994, Approximating rings of integers in number fields, *Journal de Théorie des Nombres de Bordeaux* **6**, 221–260.
3. J.P. Buhler, H.W. Lenstra, Jr., and C. Pomerance, *Factoring integers with the number field sieve*, pp. 50–94 in [8].
4. J.W.S. Cassels and A. Fröhlich (eds), 1967, *Algebraic number theory, Proceedings of an Instructional Conference*, Academic Press.
5. H. Cohen, 1993, *A course in computational algebraic number theory*, Springer-Verlag, Berlin.
6. B. Huppert, 1967, *Endliche Gruppen I*, Springer-Verlag, Berlin.
7. D.E. Knuth, 1981, *The art of computer programming*, Vol. 2, *Seminumerical algorithms*, Addison-Wesley, Reading, Mass., second edition.
8. A. K. Lenstra and H.W. Lenstra, Jr. (eds), 1993, *The development of the number field sieve*, Lecture Notes in Math. **1554**, Springer-Verlag, Berlin.
9. H.W. Lenstra, Jr., 1992, Algorithms in algebraic number theory, *Bull. Amer. Math. Soc.* **26**, 211–244.
10. A. Schrijver, 1986, *Theory of linear and integer programming*, John Wiley, Chichester.