COMPUTATION OF k–DIMENSIONAL RESIDUES AND AN APPLICATION TO PROBABILISTIC ENCRYPTION

ANTONIO COSENTINO & FRANCESCO PAPPALARDI

Abstract. The goal of this survey is to explain how to use reciprocity laws to compute residues. We will concentrate on the case of cubic, quartic and octic residues and in these cases we will describe algorithms which are analogues of the classical recursive algorithm for computing Jabobi symbols. We will illustrate implementations of these algorithms comparing execution timings in the various case. As a motivation, we will illustrate how to extend the Goldwasser–Micali probabilistic encryption to general residues.

1. Introduction

The RSA cryptosystem, introduced in 1978 by Rivest, Shamir and Adleman [11], is one of the most popular ones. Its security is believed to rely on the difficulty of factorizing integers. The problem of factoring is so old that we can affirm that Euclid, Gauss and many others contributed in guaranteeing the security of RSA.

Another cryptosystem that uses the difficulty of factoring is the *Goldwasser-Micali probabilistic encryption scheme* [5]. Basic facts on probabilistic public–key systems can be found in [14] and [15].

1.1. Goldwasser - Micali probabilistic encryption scheme.

The scheme works as follows:

Bob chooses an RSA module $M = pq$, with p and q random primes, and an integer[1] $a \in_{\mathbf{R}} (\mathbb{Z}/M\mathbb{Z})^*$ with the properties that $\left(\frac{a}{M}\right) = 1$ and a is a quadratic non–residue modulo M. Then he publishes the public key (M, a).

Alice, in order to encrypt a bit P, picks an element $c \in_{\mathbf{R}} (\mathbb{Z}/M\mathbb{Z})^*$. The encrypted message $C \in (\mathbb{Z}/M\mathbb{Z})^*$ is defined by

$$C = \begin{cases} c^2 a \bmod M & \text{if } P = 1 \\ c^2 \bmod M & \text{if } P = 0 \end{cases}$$

After this computation **Alice** transmits C to **Bob** that will decrypt the message by computing $\epsilon = \left(\frac{C}{p}\right)$ and setting $P = 0$, if $\epsilon = 1$ and $P = 1$ otherwise.

The Goldwasser–Micali cryptosystem is probabilistic in the sense that the same message is encrypted in several different ways. The security of the scheme is based on the problem of quadratic residuosity (see for example [15, §3.4]) that in order to be able to guess whether an element e in $\mathbb{Z}/M\mathbb{Z}$ (M composed) with Jacobi symbol $\left(\frac{e}{M}\right) = 1$ is a square, one has to completely factor M.

Date: August 3, 2003.

1991 *Mathematics Subject Classification.* 11T71, 14G50.

Key words and phrases. probabilistic encryption, identification protocols, reciprocity law; power residue symbol.

the second author was supported in part by COFIN–PRIN 2002 from MIUR and by GNSAGA from INDAM.

[1] the notation $\in_{\mathbf{R}}$ reads "randomly chosen in"

Decryption in the Goldwasser–Micali requires the computation of a Jacobi symbol. It is very well known that if m, m' and n are coprime integers with n odd and $\mathbf{JAC}(m,n) = \left(\frac{m}{n}\right)$ is the Jacobi symbol, then the 5 fundamental properties:

(1) $\left(\frac{m}{n}\right) = \left(\frac{m \bmod n}{n}\right)$;
(2) $\left(\frac{mm'}{n}\right) = \left(\frac{m}{n}\right) \cdot \left(\frac{m'}{n}\right)$;
(3) $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$;
(4) $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$;
(5) $\left(\frac{m}{n}\right) = (-1)^{(n-1)(m-1)/4}\left(\frac{n}{m}\right)$ if m is also odd (quadratic reciprocity law);

lead to the algorithm

COMPUTING **JAC**		$m, n \in \mathbb{Z}, 2 \nmid n, \gcd(m,n) = 1$
$\mathbf{JAC}(m,n) =$	`if` $(m = \pm 1)$	`then return` $\left(m^{\frac{n-1}{2}}\right)$
	`if` $(2 \mid m)$	`then` $\mathbf{JAC}(m/2, n) * (-1)^{\frac{n^2-1}{8}}$
	`else`	$\mathbf{JAC}(n \bmod m, m) * (-1)^{\frac{(m-1)(n-1)}{4}}$

that runs in quadratic time.

Remark. Here $n \bmod m$ denotes the (unique) remainder of the division of n by m. A possibility to speed up a the algorithm is to replace the modular reduction in the last line with s

$$\begin{array}{ll} n \bmod m & \text{if} \quad n \bmod m \leq m/2 \\ n \bmod m - m & \text{if} \quad n \bmod m > m/2. \end{array}$$

The algorithm implicitly computes the gcd of m and n. In fact one can drop the hypotheses that m and n are coprime, by adding the line (before the first)

`if` $(m = 0)$ `then return` (0)

See [9] for other better inexpensive improvements.

The Goldwasser-Micali probabilistic scheme can be extended in the following natural way.

1.2. k–**residues probabilistic encryption.** Let k be a fixed small integer (in practice $k = 2, 3, 4, 6, 8$).

Bob computes an `RSA` module $M = pq$ with the extra property that $p \equiv 1 \bmod k$ and $q \equiv 1 \bmod k$. Further he fixes two prime ideals $\mathfrak{p}$ and $\mathfrak{q}$ of the ring of cyclotomic integers $\mathbb{Z}[\zeta]$ ($\zeta = e^{2\pi i/k}$ is a primitive k–th root of 1) with $\mathfrak{p} | p$ and $\mathfrak{q} | q$.

Next he picks $a \in_{\mathbf{R}} (\mathbb{Z}/M\mathbb{Z})^*$ with the properties that

(1) a is not a k–residue modulo M;
(2) $\left[\frac{a}{\mathfrak{p}}\right]_k = \left[\frac{a}{\mathfrak{q}}\right]_k^{-1}$ is a primitive root of unity.

Here $\left[\frac{\cdot}{\cdot}\right]_k$ is the k–th residue symbol and it is defined in the following way (for details see for example [8]).

Definition 1.1. *Let $\mathfrak{p}$ be a prime ideal of $\mathbb{Z}[\zeta]$ such that $\mathfrak{p} \nmid k$ and consider the residue finite field $\mathbb{Z}[\zeta]/\mathfrak{p}\mathbb{Z}[\zeta]$ with $N(\mathfrak{p})$ elements. The k–th roots of unity $\zeta, \zeta^2, \ldots, \zeta^k = 1$ have distinct image, therefore for any $\alpha \in \mathbb{Z}[\zeta]$ we have the identity*

$$\alpha^{\frac{N(\mathfrak{p})-1}{k}} = \zeta^j \pmod{\mathfrak{p}}$$

*for a unique $j = j(\alpha) \in \mathbb{Z}/k\mathbb{Z}$. For such j, we define the k–*residue symbol

$$\left[\frac{\alpha}{\mathfrak{p}}\right]_k = \zeta^j.$$

Note that $N(\mathfrak{p}) = p^f \equiv 1 \bmod k$. *If* $f = 1$ *(i.e.* $p \equiv 1 \bmod k$*) and* $\alpha \in \mathbb{Z}$, *then all the* k *possible values of* $\left[\frac{\alpha}{\mathfrak{p}}\right]_k$ *are equiprobable.*

Bob's public key is now (M, a).

In order to encrypt a message P (represented as an element of $\mathbb{Z}/k\mathbb{Z}$), **Alice** picks $c \in_{\mathbf{R}} (\mathbb{Z}/M\mathbb{Z})^*$ and encrypts it according to the rule

$$C = E(P) \equiv c^k \cdot a^P \bmod M.$$

Finally, **Bob** decrypts the message by computing the k–residue symbol

$$\left[\frac{C}{\mathfrak{p}}\right]_k = \zeta^j,$$

and setting

$$P = D(C) = j \cdot t^* \bmod k$$

where $\left[\frac{a}{\mathfrak{p}}\right]_k = \zeta^t$ and t^* is the inverse of t module k.

Note that the scheme works since (by the properties of k–residue symbols that will be reviewed later)

$$\left[\frac{E(P)}{\mathfrak{p}}\right]_k = \left[\frac{c}{\mathfrak{p}}\right]_k^k \left[\frac{a}{\mathfrak{p}}\right]_k^P = \zeta^{tP}.$$

As for the classical Goldwasser-Micali scheme, the k–residues probabilistic scheme is based on *the* k*–residuosity assumption* that will be stated later in Section 2.

The probability that a third party, trying to decrypt the message sent by **Alice**, guesses the right values is $\frac{1}{k}$ while, when using Goldwasser-Micali scheme, the probability is $\frac{1}{2}$.

In order to be practical, the k–residue probabilistic encryption requires a fast way to compute residues. Although is generally know that higher reciprocity laws allow one fast computations of k–residue symbols at least for small values of k (see [13]), much to our surprise we could not find any reference in which the necessary algorithms are explicitly stated.

The goal of this note is to survey such algorithms deducing them from the classical theory and compare their relative efficiency.

1.3. **Fast Legendre identification protocol and its k–residue analogue.** The principle of the Goldwasser–Micali scheme is also behind the *fast Legendre identification protocol* `FLIP` that was considered by Banks, Lieman and Shparlinski in [2] and works as follows:

Irina chooses an `RSA` module $M = pq$ with p and q random primes, and integers $a, b \in (\mathbb{Z}/M\mathbb{Z})^*$ with the properties that $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = 1$ and $\left(\frac{b}{p}\right) = \left(\frac{b}{q}\right) = -1$. She then publishes her public key (M, a, b).

Victor, in order to test the identity of **Irina**, picks $c_1, \ldots, c_l \in_{\mathbf{R}} (\mathbb{Z}/M\mathbb{Z})^*$, and a sequence $(d_1, \ldots, d_l) \in_{\mathbf{R}} \{a, b\}^l$. After having computed $C_i \equiv c_i^2 d_i \bmod M$ for $i = 1, \ldots, l$, he transmits $C_1, \ldots, C_l$ to **Irina** that will prove her identity by computing $\epsilon_i = \left(\frac{C_i}{p}\right)$ for $i = 1, \ldots, l$ and sending the resulting sequence $(\epsilon_1, \ldots, \epsilon_l)$ of bits to **Victor**. Finally **Irina**'s identity is verified if, for all i, $\epsilon_i = 1$ when $d_i = a$ and $\epsilon_i = -1$ when $d_i = b$.

We observe that `FLIP` is fast, for the party who's proving its identity, because the only calculations that **Irina** has to perform are Legendre symbols calculations.

The identification protocol `FLIP` can be extended in the following natural way. **Irina** computes an `RSA` module $M = pq$ with the extra properties that $p \equiv 1 \bmod k$ and $q \equiv 1 \bmod k$. Further she fixes two prime ideals $\mathfrak{p}$ and $\mathfrak{q}$ of the ring of cyclotomic integers $\mathbb{Z}[\zeta]$ ($\zeta = e^{2\pi i/k}$ is a primitive k–th root of 1) with $\mathfrak{p}|p$ and $\mathfrak{q}|q$.

Next she chooses $a_1 \dots a_k \in (\mathbb{Z}/M\mathbb{Z})^*$ that verify the following:

$$\left[\frac{a_j}{\mathfrak{p}}\right]_k = \zeta^j = \left[\frac{a_j}{\mathfrak{q}}\right]_k^{-1}, \quad j = 1, \dots k.$$

The public key is now $(M, a_1, \dots, a_k)$.

In order to test **Irina**'s identity, **Victor** picks

$$c_1, \dots, c_l \in_{\mathbf{R}} \mathbb{Z}/M\mathbb{Z}, \ (d_1, \dots, d_l) \in_{\mathrm{R}} \{a_1, \dots, a_k\}^l.$$

Then he computes and sends

$$C_i \equiv c_i^k \cdot d_i \pmod{M}, \quad i = 1, \dots, l.$$

Finally, **Irina** proves her identity by computing and sending the k–residues symbols

$$\left[\frac{C_i}{\mathfrak{p}}\right]_k = \zeta^{j_i}, \quad i = 1, \dots, l.$$

Victor knows that **Irina** is really **Irina** only if $d_i = a_{j_i}$ for all $i = 1, \dots, l$.

The probability that a third party, trying to convince **Victor** that he is **Irina**, guesses all the right values $j_1, \dots, j_l$ is $\frac{1}{k^l}$ while, when using `FLIP`, the probability is $\frac{1}{2^l}$. From this observation we deduce, that with "equal security" but under different hardness assumption (k–residuosity for different values of k), the k-residues identification protocols needs a value of l which is approximately $\frac{\log 2}{\log k}$ times the value required for `FLIP`. If for example $k = 4$, then, with the quartic residues identification protocol, only half of the residues need to be computed by **Irina**. Finally it would be desirable to be able to compute a k–residue symbol in at most $\frac{\log k}{\log 2}$ times the time needed to compute a Jacobi symbol.

2. k–dimensional residue symbols

As we observed above, if $\mathfrak{p}$ is any non trivial prime ideal of $\mathbb{Z}[\zeta]$ with $\mathfrak{p} \nmid k$ (ζ a primitive k–th root of 1), and $\alpha \in \mathbb{Z}[\zeta]$, then the k–dimensional residue symbol is defined by the identity

$$\left[\frac{\alpha}{\mathfrak{p}}\right]_k \equiv \alpha^{\frac{N(\mathfrak{p})-1}{k}} \pmod{\mathfrak{p}}.$$

and it is understood that $\left[\frac{\alpha}{\mathfrak{p}}\right] = 0$ if $\mathfrak{p}|\alpha$.

The fact that, in general, $\mathbb{Z}[\zeta]$ is not Euclidean makes things more technical in the general case. For this reason, from now on, we will restrict our attention here to the values of k:

$$2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 18, 20, 21, 22, 24$$

which are the values of k for which $\mathbb{Z}[\zeta]$ is known to be Euclidean (see [7] for a complete account on the problem).

If $\mathfrak{p} = (\pi)$, with $\pi \in \mathbb{Z}[\zeta]$ irreducible, then we will use the symbol $\left[\frac{\cdot}{\pi}\right]_k$ for $\left[\frac{\cdot}{\mathfrak{p}}\right]_k$ so that if π_1 and π_2 are associated, then for any $\alpha \in \mathbb{Z}[\zeta]$,

$$\left[\frac{\alpha}{\pi_1}\right]_k = \left[\frac{\alpha}{\pi_2}\right]_k.$$

It is clear from the definition that $\left[\frac{\alpha}{\pi}\right]_k$ can be computed in cubic time by a modular exponentiation. However this is unsatisfactory for the practical purposes.

Consider a non-unit $\beta \in \mathbb{Z}[\zeta]$ such that no prime dividing k contain (β). As for the Legendre Symbol with the Jacobi symbol, we extend the k–dimensional residue

symbol to β by the rule:

$$\left[\frac{\alpha}{\beta}\right]_k = \prod_{j=1}^{t} \left[\frac{\alpha}{\pi_j}\right]_k^{a_j}$$

where $\beta = \pi_1^{a_1} \cdots \pi_t^{a_t}$ is the factorization of β into irreducibles. If β is a unit, we also set $\left[\frac{\alpha}{\beta}\right]_k = 1$. Note that from the definition follows immediately that

$$\left[\frac{\alpha}{\beta}\right]_k = \left[\frac{\alpha \bmod \beta}{\beta}\right]_k, \quad \left[\frac{\alpha_1\alpha_2}{\beta}\right]_k = \left[\frac{\alpha_1}{\beta}\right]_k \cdot \left[\frac{\alpha_2}{\beta}\right]_k,$$
$$\left[\frac{\alpha}{\beta}\right]_k = 0 \text{ if } \gcd(\alpha,\beta) \neq 1 \text{ and } \left[\frac{\alpha}{\beta_1}\right]_k = \left[\frac{\alpha}{\beta_2}\right]_k$$

if β_1 and β_2 are associated.

To achieve a fast algorithm to compute $\left[\frac{\alpha}{\beta}\right]_k$ one needs four ingredient:

- a reciprocity law;
- a formula to compute $\left[\frac{\alpha}{\beta}\right]_k$ when α is a product of ramified primes in $\mathbb{Z}[\zeta]$;
- a formula to compute $\left[\frac{\alpha}{\beta}\right]_k$ when α is a unit $\mathbb{Z}[\zeta]$;
- an efficient algorithm to compute the Euclidean division in $\mathbb{Z}[\zeta]$.

A lengthy literature addresses these problems but to our knowledge there is not yet a general answer. However the Eisenstein reciprocity law [8] provides the first ingredient at least in the case when k is prime. As for the last ingredient, see for example [16, 17]

We conclude this section by stating the

The k–residuosity assumption: *Given $\alpha, \beta \in \mathbb{Z}[\zeta]$ (where β is not a unit and such that no prime dividing k contain (β)) with $\left[\frac{\alpha}{\beta}\right]_k = 1$, to determine if α is a k–power modulo β is as hard as to factor the norm $N(\beta)$.*

3. Classical Reciprocity Laws and derived algorithms

We will analyze the three possible values $k = 3, 4, 8$. A similar analysis can be done for $k = 6$.

3.1. **Cubic residues - the ring $\mathbb{Z}[(-1+\sqrt{-3})/2]$.** Let $\omega = \frac{-1+\sqrt{-3}}{2}$ be a complex cubic root of 1. The Euclidean domain $\mathbb{Z}[\omega]$ contains 6 units, namely $\pm 1, \pm\omega$ and $\pm\omega^2$.

The prime $1-\omega$ of $\mathbb{Z}[\omega]$ satisfies the relation $(1-\omega)^2 = -3\omega$, that will be useful for the cubic residue computation. From the definition of norm $N(a+\omega b) = (a+b)^2 - 3ab$, we deduce that if $\alpha = a + b\omega \in \mathbb{Z}[\omega]$, then $1-\omega | \alpha$ if and only if $3 | a+b$. Furthermore

$$\frac{\alpha}{1-\omega} = \frac{2a-b}{3} + \frac{a+b}{3}\omega.$$

We say that $\alpha = a + b\omega \in \mathbb{Z}[\omega]$ is *primary* if $\alpha \equiv 1 \bmod 3$. That is if $a \equiv 1 \bmod 3$ and $3 \mid b$. The only primary unit of $\mathbb{Z}[\omega]$ is 1. For any $\alpha \in \mathbb{Z}[\omega]$ with $1-\omega \nmid \alpha$, among the six associates of α

$$\alpha = a + b\omega, \quad -\alpha = -a - b\omega, \quad \omega\alpha = -b + (a-b)\omega,$$
$$-\omega\alpha = b + (b-a)\omega, \quad \omega^2\alpha = (b-a) - a\omega, \quad -\omega^2\alpha = (a-b) + a\omega$$

there is a unique primary one. Therefore, if $1-\omega \nmid \alpha$, we can write

$$\alpha = \pm\omega^{c(\alpha)} P(\alpha)$$

where $P(\alpha)$ and $c(\alpha)$ are uniquely determined by the requirements that $P(\alpha) \in \mathbb{Z}[\omega]$ is primary and $c(\alpha) \in \mathbb{Z}/3\mathbb{Z}$. Concretely, if $(a', b') \in \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ is the reduction of (a, b) modulo 3 then in the following table we can read out the values

(a', b')	$(1,0)$	$(2,0)$	$(2,2)$	$(1,1)$	$(0,1)$	$(0,2)$
$P(\alpha)$	$a+\omega b$	$-a-b\omega$	$-b+(a-b)\omega$	$b+(b-a)\omega$	$(b-a)-a\omega$	$(a-b)+a\omega$
$c(\alpha)$	0	0	2	2	1	1

From this table we deduce that the computation of $P(\alpha)$ and that of $c(\alpha)$ can be done in linear time.

Primary elements play an important role in the reciprocity law. The following statement can be found in several references as for example [1, 6, 8].

Theorem 3.1 (Cubic reciprocity law)**.** *Let $\alpha, \beta \in \mathbb{Z}[\omega]$ be relatively prime and primary $\beta = c + d\omega$. Then*

$$\left[\frac{\alpha}{\beta}\right]_3 = \left[\frac{\beta}{\alpha}\right]_3, \quad \left[\frac{\omega}{\beta}\right]_3 = \omega^{(1-c-d)/3}, \quad \left[\frac{1-\omega}{\beta}\right]_3 = \omega^{(c-1)/3},$$

$$\left[\frac{3}{\beta}\right]_3 = \omega^{d/3}, \quad \left[\frac{\pm 1}{\beta}\right]_3 = 1. \square$$

From the above discussion and from (1) we deduce the following algorithm for

$$\mathbf{CR}(\alpha, \beta) = \left[\frac{\alpha}{\beta}\right]_3 :$$

COMPUTING **CR**		$\alpha = a + \omega b, \beta = c + \omega d \in \mathbb{Z}[\omega]$ $1 - \omega \nmid \beta, \beta = P(\beta)$ $\gcd(\alpha, \beta) = 1$
$\mathbf{CR}(\alpha, \beta) =$	`if` $(\alpha = 1)$	`then return` (1)
	`if` $(1 - \omega \mid \alpha)$	`then` $\mathbf{CR}(\alpha/(1-\omega), \beta) * \omega^{(c-1)/3}$
	`else`	$s = c(\alpha), \alpha = P(\alpha)$ $\mathbf{CR}(\beta \,(\mathrm{mod}\, \alpha), \alpha) * \omega^{(s(1-c-d))/3}$

With the notation $\beta \,(\mathrm{mod}\, \alpha)$ we denote any remainder of the Euclidean division of β by α. That is an element γ in $\mathbb{Z}[\omega]$ such that $\gamma \equiv \beta \,(\mathrm{mod}\, \alpha)$ and $N(\gamma) < N(\alpha)$. In general there is more then one such element. The best is to choose the one with least norm. The element γ equals $\beta - \rho \cdot \alpha$ where ρ is an the element of the lattice $\mathbb{Z}[\omega]$ which is closest to $\frac{\beta}{\alpha}$.

We can speed up the algorithm by adding between the first and the second line

	`if` $(3 \mid \alpha)$	`then` $\mathbf{CR}(\alpha/3^{v_3(\alpha)}, \beta) * \omega^{dv_3(\alpha)/3}$

where $v_3(\alpha)$ denotes the exponent of the largest power of 3 dividing α.

3.2. **Quartic residues - the ring $\mathbb{Z}[i]$.** The units of Euclidean domain $\mathbb{Z}[i]$ are ± 1 and $\pm i$. In $\mathbb{Z}[i]$, $1+i$ is a special prime and has the property that $2 = -i(1+i)^2$. If $\alpha = a + ib \in \mathbb{Z}[i]$, then it is immediate to see that $1 + i | \alpha$ if and only if $2 | a + b$ (i.e. a and b have the same parity). In that case

$$\frac{\alpha}{1+i} = \frac{a+b}{2} + \frac{a-b}{2} i.$$

We say that $\alpha = a + bi \in \mathbb{Z}[i]$ is *primary* if $\alpha \equiv 1 \pmod{2 + 2i}$. If α is primary, then $1 + i \nmid \alpha$ and also α is primary if and only if

$$a - 1 \equiv b \equiv 0 \bmod 4 \qquad \text{or} \qquad a - 1 \equiv b \equiv 2 \bmod 4.$$

The only primary unit of $\mathbb{Z}[i]$ is 1. Furthermore for any $\alpha \in \mathbb{Z}[i]$ with $1+i \nmid \alpha$, among the four associates of α

$$\alpha = a+bi, \quad -\alpha = -a-bi, \quad i\alpha = -b+ai, \quad -i\alpha = b-ai$$

there is exactly a primary one. Therefore, if $1+i \nmid \alpha$, we can write

$$\alpha = i^{c(\alpha)} P(\alpha)$$

where $P(\alpha)$ and $c(\alpha)$ are uniquely determined by the requirements that $P(\alpha) \in \mathbb{Z}[i]$ is primary and $c(\alpha) \in \mathbb{Z}/4\mathbb{Z}$. Concretely, if $(a', b') \in \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ is the reduction of (a, b) modulo 4 then in the following table we can read out the values of $c(\alpha)$ and $P(\alpha)$:

(a', b')	$(1,0),(3,2)$	$(0,1),(2,3)$	$(1,2),(3,0)$	$(2,1),(0,3)$
$P(\alpha)$	$a+bi$	$b-ai$	$-a-bi$	$-b+ai$
$c(\alpha)$	0	1	2	3

The computation of $P(\alpha)$ and that of $c(\alpha)$ takes a linear number of bit operations.

Primary elements play again an important role in the reciprocity law. The following statement can be found in several references as for example [1, 6, 8].

Theorem 3.2 (Quartic reciprocity law)**.** *Let $\alpha, \beta \in \mathbb{Z}[i]$ be relatively prime and primary with $\alpha = a+bi$ and $\beta = c+di$. Then*

$$\left[\frac{\alpha}{\beta}\right]_4 = \left[\frac{\beta}{\alpha}\right]_4 i^{(1-a)\frac{1-c}{2}} = (-1)^{\frac{bd}{4}},$$

$$\left[\frac{i}{\beta}\right]_4 = i^{(1-c)/2}, \quad \left[\frac{1+i}{\beta}\right]_4 = i^{(c-d-d^2-1)/4}, \quad \left[\frac{2}{\beta}\right]_4 = i^{-d/2}. \square$$

From the above discussion and from (1) we deduce the following algorithm for

$$\mathbf{QR}(\alpha, \beta) = \left[\frac{\alpha}{\beta}\right]_4 :$$

COMPUTING **QR**		$\alpha = a+ib, \beta = c+id \in \mathbb{Z}[i]$ $1+i \nmid \beta, \beta = P(\beta)$ $\gcd(\alpha, \beta) = 1$
$\mathbf{QR}(\alpha, \beta) =$	`if` $(\alpha = 1)$	`then return` (1)
	`if` $(1+i \mid \alpha)$	`then` $\mathbf{QR}(\alpha/(1+i), \beta) * i^{(c-d-d^2-1)/4}$
	`else`	$s = c(\alpha), \alpha = P(\alpha)$ $\mathbf{QR}(\beta \,(\mathrm{mod}\alpha), \alpha) * i^{(1-a+s)*(1-c)/2}$

Further, note that

$$(c-d-d^2-1)/4 \pmod 4 = \begin{cases} (c-d-1)/4 \pmod 4 & \text{if } 4 \mid d, \\ (c-d-5)/4 \pmod 4 & \text{if } 2 \| d. \end{cases}$$

Also here, with the notation $\beta \,(\mathrm{mod}\alpha)$, we denote any remainder of the Euclidean division in $\mathbb{Z}[i]$ of β by α. That is an element γ in $\mathbb{Z}[i]$ such that $\gamma \equiv \beta \,(\mathrm{mod}\alpha)$ and $N(\gamma) < N(\alpha)$. In general there is more then one such element. We can speed up the algorithm by adding between the first and the second line

`if` $(2 \mid \alpha)$	`then` $\mathbf{QR}(\alpha/2^{v_2(\alpha)}, \beta) * i^{-dv_2(\alpha)/2}$

where $v_2(\alpha)$ denotes the exponent of the largest power of 2 dividing α.

3.3. **Octic residues - the ring $\mathbb{Z}[\frac{\sqrt{2}}{2}(1+i)]$.** Let $\tau = \frac{\sqrt{2}}{2}(1+i)$ and $\alpha = a + b\tau + c\tau^2 + d\tau^3 \in \mathbb{Z}[\tau]$. The norm $N(\alpha)$ of $\alpha \in \mathbb{Z}[\tau]$ is $N(\alpha) = \alpha_1\alpha_3\alpha_5\alpha_7$, with $\alpha_n = a + b\tau^n + c\tau^{2n} + d\tau^{3n}$. The domain $\mathbb{Z}[\tau]$ is a Euclidean ring and $1+\tau$ is a prime. It has the property that

$$(1+\tau)^4(1+\sqrt{2})^{-2}\tau^6 = 2.$$

Note that $\epsilon = 1+\sqrt{2} = 1+\tau+\tau^7$ is a fundamental unit of infinite order in $\mathbb{Z}[\tau]$ so that every unit can be written uniquely as $\tau^s\epsilon^t$, with $s \in \mathbb{Z}/8\mathbb{Z}$ and $t \in \mathbb{Z}$. If $\alpha = a + b\tau + c\tau^2 + d\tau^3 \in \mathbb{Z}[\tau]$, then it is immediate to see that $1+\tau|\alpha$ if and only if $2|a+b+c+d$. In that case, if $e = (a+b+c+d)/2$

$$\frac{\alpha}{1+\tau} = (e-c) + (e-a-d)\tau + (e-b)\tau^2 + (e-a-c)\tau^3.$$

We say that $\alpha = a + b\tau + c\tau^2 + d\tau^3 \in \mathbb{Z}[\tau]$ is *primary* if $\alpha \equiv 1 \pmod{2+2\tau}$. This is equivalent to

$$a - 1 \equiv b \equiv c \equiv d \equiv 0 \,(\mathrm{mod}2) \quad \text{and} \quad a+b+c+d \equiv 1 \bmod 4.$$

The ring $\mathbb{Z}[\tau]/(2+2\tau)\mathbb{Z}[\tau]$ has 32 elements and the 32 classes can be represented either by the 16 elements

$$\tau^s\epsilon^t(1+\tau), \quad s \in \mathbb{Z}/8\mathbb{Z}, \quad t \in \{0,1\}$$

that are 0 divisors, or by the 16 elements $\tau^s\epsilon^t, \quad s \in \mathbb{Z}/8\mathbb{Z}, \quad t \in \{0,1\}$ that are units. From this observation we deduce that if $\alpha \in \mathbb{Z}[\tau]$ with $1+\tau \nmid \alpha$, then there exists $s(\alpha) \in \mathbb{Z}/8\mathbb{Z}$, $t(\alpha) \in \{0,1\}$ such that

$$\alpha \equiv \tau^{s(\alpha)}\epsilon^{t(\alpha)} \pmod{2+2\tau}.$$

So, α has an associate of the form

$$\alpha = \tau^{s(\alpha)}\epsilon^{t(\alpha)}P(\alpha),$$

where $P(\alpha)$, $s(\alpha)$ and $t(\alpha)$ are uniquely determined by the requirements that $P(\alpha) \in \mathbb{Z}[\tau]$ is primary, $s(\alpha) \in \mathbb{Z}/8\mathbb{Z}$ and $t(\alpha) \in \{0,1\}$. Note that from the fact that the unit $3-2\sqrt{2}$ is primary, follows that every element has infinitely many primary associates.

Suppose $\alpha \in \mathbb{Z}[\tau]$ is such that $1+\tau \nmid \alpha$ and let $\overline{v}_\alpha \in (\mathbb{Z}/4\mathbb{Z})^4$ be the vector obtained reducing the components of α modulo 4. We can always read the values of $P(\alpha)$, $s(\alpha)$ and $t(\alpha)$ from the following table:

$\overline{v}_\alpha$	$(1,0,0,0),(3,2,2,2)$ $(1,2,2,0),(3,0,0,2)$ $(1,2,0,2),(3,0,2,0)$ $(1,0,2,2),(3,2,0,0)$	$(0,1,0,0),(2,3,2,2)$ $(0,1,2,2),(2,3,0,0)$ $(2,1,2,0),(0,3,0,2)$ $(2,1,0,2),(0,3,2,0)$	$(0,0,1,0),(2,2,3,2)$ $(2,0,1,2),(0,2,3,0)$ $(0,2,1,2),(2,0,3,0)$ $(2,2,1,0),(0,0,3,2)$	$(0,0,0,1),(2,2,2,3)$ $(2,2,0,1),(0,0,2,3)$ $(2,0,2,1),(0,2,0,3)$ $(0,2,2,1),(2,0,0,3)$
$P(\alpha)$	$a+b\tau+c\tau^2+d\tau^3$	$b+c\tau+d\tau^2-a\tau^3$	$c+d\tau-a\tau^2-b\tau^3$	$d-a\tau-b\tau^2-c\tau^3$
$s(\alpha)$	0	1	2	3
$t(\alpha)$	0	0	0	0
$\overline{v}_\alpha$	$(1,2,0,0),(3,0,0,0)$ $(1,0,2,0),(3,2,0,2)$ $(1,0,0,2),(3,2,2,0)$ $(1,2,2,2),(3,0,2,2)$	$(2,1,0,0),(0,3,2,2)$ $(0,1,2,0),(2,3,0,2)$ $(0,1,0,2),(2,3,2,0)$ $(2,1,2,2),(0,3,0,0)$	$(2,0,1,0),(0,2,3,2)$ $(0,2,1,0),(2,0,3,2)$ $(0,0,1,2),(2,2,3,0)$ $(2,2,1,2),(0,0,3,0)$	$(2,0,0,1),(0,2,2,3)$ $(0,2,0,1),(2,0,2,3)$ $(0,0,2,1),(2,2,0,3)$ $(2,2,2,1),(0,0,0,3)$
$P(\alpha)$	$-a-b\tau-c\tau^2-d\tau^3$	$-b-c\tau-d\tau^2+a\tau^3$	$-c-d\tau+a\tau^2+b\tau^3$	$-d+a\tau+b\tau^2+c\tau^3$
$s(\alpha)$	4	5	6	7
$t(\alpha)$	0	0	0	0
$\overline{v}_\alpha$	$(1,1,0,1),(3,3,2,3)$ $(3,1,0,3),(1,3,2,1)$ $(1,3,0,3),(3,1,2,1)$ $(3,3,0,1),(1,1,2,3)$	$(1,3,1,0),(3,1,3,2)$ $(1,1,3,0),(3,3,1,2)$ $(3,1,1,0),(1,3,3,2)$ $(3,3,3,0),(1,1,1,2)$	$(0,1,3,1),(2,3,1,3)$ $(0,3,1,1),(2,1,3,3)$ $(0,1,1,3),(2,3,3,1)$ $(0,3,3,3),(2,1,1,1)$	$(3,0,1,1),(1,2,3,3)$ $(1,0,3,1),(3,2,1,3)$ $(1,0,1,3),(3,2,3,1)$ $(3,0,3,3),(1,2,1,1)$
$P(\alpha)$	$k_0+k_1\tau+k_2\tau^2+k_3\tau^3$	$k_1+k_2\tau+k_3\tau^2-k_0\tau^3$	$k_2+k_3\tau-k_0\tau^2-k_1\tau^3$	$k_3-k_0\tau-k_1\tau^2-k_2\tau^3$
$s(\alpha)$	0	1	2	3
$t(\alpha)$	1	1	1	1
$\overline{v}_\alpha$	$(3,1,0,1),(1,3,2,3)$ $(1,3,0,1),(3,1,2,3)$ $(1,1,0,3),(3,3,2,1)$ $(3,3,0,3),(1,1,2,1)$	$(3,1,1,0),(1,3,3,2)$ $(1,3,1,0),(3,1,3,2)$ $(1,1,3,0),(3,3,1,2)$ $(3,3,3,0),(1,1,1,2)$	$(0,3,1,1),(2,1,3,3)$ $(0,1,3,1),(2,3,1,3)$ $(0,1,1,3),(2,3,3,1)$ $(0,3,3,3),(2,1,1,1)$	$(3,0,1,1),(1,2,3,3)$ $(1,0,3,1),(3,2,1,3)$ $(1,0,1,3),(3,2,3,1)$ $(3,0,3,3),(1,2,1,1)$
$P(\alpha)$	$-k_0-k_1\tau-k_2\tau^2-k_3\tau^3$	$-k_1-k_2\tau-k_3\tau^2+k_0\tau^3$	$-k_2-k_3\tau+k_0\tau^2+k_1\tau^3$	$-k_3+k_0\tau+k_1\tau^2+k_2\tau^3$
$s(\alpha)$	4	5	6	7
$t(\alpha)$	1	1	1	1

where

$$\begin{array}{lcllcl} k_0 &=& -a+b+d & k_1 &=& a-b+c \\ k_2 &=& b-c+d & k_3 &=& -a+c-d. \end{array}$$

From this table we deduce that the computation of $P(\alpha)$ and that of $s(\alpha)$ can be done in linear time.

As for the quartic and cubic case, primary elements play an important role in the octic reciprocity law. The octic reciprocity law was exposed by Goldscheider in [4]. The following statement can be found in [8].

Theorem 3.3. *Let $\alpha, \beta \in \mathbb{Z}[\tau]$ be relatively prime and primary with $\alpha = a + b\tau + c\tau^2 + d\tau^3$ and $\beta = e + f\tau + g\tau^2 + h\tau^3$. Consider the auxiliary functions:*

$$\begin{array}{lcllcl} A = A_\alpha &=& a^2 - c^2 + 2bd, & B = B_\alpha &=& b^2 - d^2 - 2ac, \\ C = C_\alpha &=& a^2 - b^2 + c^2 - d^2, & D = D_\alpha &=& ab - bc + cd + da, \\ E = E_\alpha &=& a^2 + b^2 + c^2 + d^2, & F = F_\alpha &=& ab + bc + cd - da. \end{array}$$

Then

$$\left[\frac{\alpha}{\beta}\right]_8 = \left[\frac{\beta}{\alpha}\right]_8 \tau^{D_\alpha * F_\beta - D_\beta * F_\alpha + (N(\alpha)-1)(N(\beta)-1)/16}.$$

Furthermore

$$\left[\frac{\tau}{\alpha}\right]_8 = \tau^{(A-1+4B+2BD+2D^2)/4}, \quad \left[\frac{1+\tau}{\alpha}\right]_8 = \tau^{(A-1+B+6D+B^2+2BD+D^4/2)/4},$$

$$\left[\frac{\epsilon}{\alpha}\right]_8 = \tau^{(D-3B-BD-2D^2)/2}. \square$$

A special discussion needs to be made for the symbol $\left[\frac{\theta}{\alpha}\right]_8$ where θ is a primary unit of $\mathbb{Z}[\tau]$. In this case it can be seen that $\theta = \epsilon^{2r}$, where

$$r = r_\theta \equiv \begin{cases} 0 \pmod 4 & \text{if } \theta \equiv 1 \pmod 8 \\ 1 \pmod 4 & \text{if } \theta \equiv \epsilon \pmod 8 \\ 2 \pmod 4 & \text{if } \theta \equiv 1 + 4\sqrt{2} \pmod 8 \\ 3 \pmod 4 & \text{if } \theta \equiv 3 + 6\sqrt{2} \pmod 8. \end{cases}$$

From the above we deduce the following algorithm for

$$\mathbf{OR}(\alpha, \beta) = \left[\frac{\alpha}{\beta}\right]_8 :$$

COMPUTING **OR**	$\alpha = a + b\tau + c\tau^2 + d\tau^3$, $\beta = e + f\tau + g\tau^2 + h\tau^3 \in \mathbb{Z}[\tau]$ $1 + \tau \nmid \beta, \beta = P(\beta)$ $\gcd(\alpha, \beta) = 1$

$$\begin{array}{lll} \mathbf{OR}(\alpha,\beta) = & \texttt{if } (N(\alpha) = 1) & \texttt{then } \theta = \alpha \,(\mathrm{mod} 8), r = r_\theta \\ & & \texttt{return}\left(\tau^{2r * Z}\right) \\ & \texttt{if } (1+\tau \vert \alpha) & \texttt{then } \mathbf{OR}(\alpha/(1+\tau), \beta) * \tau^W \\ & \texttt{else} & s = s(\alpha), t = t(\alpha), \alpha = P(\alpha) \\ & & \mathbf{OR}(\beta \,(\mathrm{mod}\alpha), \alpha) * \tau^{X + s*Y + t*Z} \end{array}$$

where

$$\begin{array}{lcl} W &=& (A - 1 + B + 6D + B^2 + 2BD + D^4/2)/4 \\ X &=& D_\alpha * F_\beta - D_\beta * F_\alpha + (N(\alpha) - 1)(N(\beta) - 1)/16, \\ Y &=& (A - 1 + 4B + 2BD + 2D^2)/4, \\ Z &=& (D - 3B - BD - 2D^2)/2. \end{array}$$

4. Conclusion

The algorithms for cubic and quartic residues of Section 3.1 and Section 3.2 have been implemented. The programs were written in C with the auxiliary help of the library functions of PARI [3]. Tests were performed in the Linux environment on a Pentium III (1100Mhz/256Mb RAM) platform. The codes are available at

`http://www.mat.uniroma3.it/users/pappa/RESIDUES.zip`.

4.1. **Test 1.** For each $n \in \{500, 600, 700, 800, 900, 1000, 1100, 1200\}$, we considered 3000 random pairs of elements in $\mathbb{Z}[\omega]$ (resp. $\mathbb{Z}[i]$). Each pair (x, y) was constructed in such a way that $x = x_1 + x_2\omega$, $y = y_1 + y_2\omega$ (resp. $x = x_1 + x_2 i$, $y = y_1 + y_2 i$) and x_1, x_2, y_1, y_2 each have $\frac{n}{2}$ bits.

The following two tables represent the total time in milliseconds to compute $\left[\frac{x}{y}\right]_3$ and $x^{\frac{Ny-1}{3}} \pmod y$ (resp. $\left[\frac{x}{y}\right]_4$ and $x^{\frac{Ny-1}{4}} \pmod y$) for all 3000 random pairs.

The third row contains the ratio of the times and indicates how much faster is to use reciprocity with respect to exponentiation. Note that the factor is at least 13 for cubic residues (resp. 43 for biquadratic residues).

TABLE 1

n	500	600	700	800	900	1000	1100	1200
# of ms to compute $\left[\frac{x}{y}\right]_3$	5240	6840	8940	11160	14000	16860	19830	22770
# of ms to compute $x^{\frac{Ny-1}{3}} \pmod y$	69150	108770	152540	221310	287550	388410	508390	623010
Exponential/cubic symbol times ratio	13.196	15.902	17.062	19.830	20.539	23.037	26.637	27.361

TABLE 2

n	500	600	700	800	900	1000	1100	1200
# of ms to compute $\left[\frac{x}{y}\right]_4$	1430	1810	2550	2990	3980	4460	5370	6220
# of ms to compute $x^{\frac{Ny-1}{4}} \pmod y$	62180	97300	136660	199110	260630	351620	460240	564210
Exponential/biquadratic symbol times ratio	43.482	53.757	53.592	66.592	65.485	78.838	85.706	90.709

4.2. **Test 2.** For each $n = t \cdot 100$ with $t = 5, \ldots, 25$, we considered 100000 random pairs of elements in $\mathbb{Z}[\omega]$ (resp. $\mathbb{Z}[i]$).

Each pair (x, y) was constructed in such a way that $x = x_1$, $y = y_1 + y_2\omega$ (resp. $x = x_1 + x_2 i$, $y = y_1 + y_2 i$), x and y are coprime, x_1 has n bits (resp. x_1, x_2 each have $\frac{n}{2}$ bits) and y_1, y_2 each have $\frac{n}{2}$ bits.

The following four tables represent the total time in milliseconds to compute $\left[\frac{x}{y}\right]_3$ and $\left[\frac{x}{p}\right]_2$ (resp. $\left[\frac{x}{y}\right]_4$ and $\left[\frac{q}{p}\right]_2$) for all 100000 random pairs. To compute the Jacobi symbol we used the native PARI function (we thought that was the best) with $p = N(y)$ (resp. $q = N(x)$ and $p = N(y)$).

The third row contains the ratio of the times and indicates how much slower it is to compute cubic symbol (resp. biquadratic symbol) with respect to Jacobi symbol. Note that the factor is at most 15 for cubic residues (resp. at least 4 for biquadratic residues).

TABLE 3-1

n	500	600	700	800	900	1000	1100	1200	1300	1400	1500
# of ms to compute $\left[\frac{x}{y}\right]_3$	174890	229440	295560	371130	454910	549790	657350	775330	908860	1054690	1214610
# of ms to compute $\left[\frac{x}{p}\right]_2$	11030	15420	18930	23370	28000	34650	39600	45380	52670	59150	67210
Cubic/Jacobi symbol times ratio	15.855	14.879	15.613	15.880	16.246	15.866	16.599	17.085	17.255	17.830	18.071

TABLE 3-2										
n	1600	1700	1800	1900	2000	2100	2200	2300	2400	2500
# of ms to compute $\left[\frac{x}{y}\right]_3$	1395120	1594930	1809680	2042350	2286100	2556210	2833340	3134690	3452360	3787850
# of ms to compute $\left[\frac{q}{p}\right]_2$	74960	84050	92530	102030	111800	123130	131570	144800	158310	173280
Cubic/Jacobi symbol times ratio	18.611	18.975	19.558	20.017	20.448	20.760	21.534	21.648	21.807	21.859

TABLE 4-1											
n	500	600	700	800	900	1000	1100	1200	1300	1400	1500
# of ms to compute $\left[\frac{x}{y}\right]_4$	44100	55750	69750	89600	109990	131860	155430	179370	202980	228360	255340
# of ms to compute $\left[\frac{q}{p}\right]_2$	11820	15270	19160	24960	30150	36850	43320	51860	60500	67250	78250
Biquadratic/Jacobi symbol times ratio	3.731	3.651	3.640	3.590	3.648	3.578	3.588	3.459	3.355	3.396	3.2631

TABLE 4-2										
n	1600	1700	1800	1900	2000	2100	2200	2300	2400	2500
# of ms to compute $\left[\frac{x}{y}\right]_4$	283110	311020	340510	371720	404980	438020	472970	508140	547250	236480
# of ms to compute $\left[\frac{x}{p}\right]_2$	86670	97960	107110	118420	133050	144030	157970	170000	184190	200330
Biquadratic/Jacobi symbol times ratio	3.266	3.175	3.179	3.139	3.044	3.041	2.994	2.989	2.971	2.914

4.3. **Final Remarks.** The bottleneck of the reciprocity algorithms is the reduction of an element modulo another. We have partially overcome this aspect by replacing $a \bmod b$ with $a \pm b$, where the sign is chosen so to minimize the bit size. We recognize that in order to obtain a serious implementation of the algorithms one should consider more efficient implementations of the Euclidean-chain. For example one could use the Lehmer's trick, k–ary algorithms or even methods based on the Schönage's half gcd technique.

Acknowledgements: The idea that `FLIP` can be extended to higher dimensional residue symbols is contained in the original paper of Banks, Lieman and Shparlinski [2].

A non recursive version of the algorithm for cubic residues is also contained in the paper of R. Scheidler [12] where she defines a cryptosystem that uses pure cubic fields. After this paper was completed we also found out about the result in [18] which deal with efficient implementation of the biquadratic symbol.

References

[1] S. D. Adhikari, *The early reciprocity laws: from Gauss to Eisenstein.* in *Cyclotomic fields and related topics (Pune, 1999)*, 55–74, Bhaskaracharya Pratishthana, Pune, 2000;

[2] W. D. Banks, D. Lieman and I. E. Shparlinski, *An identification Scheme Based on Legendre Symbols.* Preprint.

[3] C. Batut, K. Belabas, D. Bernardi, H. Cohen and M. Olivier, *Pari-GP Versione 2.1.1*, **http://www.parigp-home.de**, 2001.

[4] F. Goldscheider, *Das Reciprocitätsgesetz der achten Potenzrest.* Wiener Ber. **101**, 562–584 (1892).

[5] S. Goldwasser and S. Micali, *Probabilistic encryption.* J. Comput. System Sci. **28** (1984), no. 2, 270–299.

[6] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, Second edition. Graduate Texts in Mathematics, 84. Springer-Verlag, New York, 1990.

[7] F. Lemmermeyer, *The Euclidean algorithm in algebraic number fields.*Exposition. Math. **13** (1995), no. 5, 385–416.

[8] F. Lemmermeyer, *Reciprocity laws*, Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2000.

[9] S. Meyer Eikenberry and J. P. Sorenson *Efficient algorithms for computing the Jacobi symbol*, J. Symbolic Comput. **26** (1998), no. 4, 509–523.

[10] P. Paillier, *Public-key cryptosystems based on composite degree residuosity classes.* Advances in cryptology. EUROCRYPT '99 (Prague), 223–238, Lecture Notes in Comput. Sci., 1592, Springer, Berlin, 1999.

[11] R. L. Rivest, A. Shamir and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*. Comm. ACM **21** (1978), no. 2, 120–126.
[12] R. Scheidler,*A public-key cryptosystem using purely cubic fields*. J. Cryptology **11** (1998), no. 2, 109–124.
[13] R. Scheidler and H. C. Williams,*C. A public-key cryptosystem utilizing cyclotomic fields*. Des. Codes Cryptography **6**, No.2, 117–131 (1995).
[14] D. R. Stinson, *Cryptography, Theory and practice*. CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL, 1995.
[15] A. J. Menezes, P. C. Van Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Boca Raton, FL, 1996.
[16] A. Weilert, $(1 + i)$*–ary GCD computation in* $\mathbb{Z}[i]$ *is an analogue to the binary GCD algorithm*, J. Symbolic Comput. **30** (2000), no. 5, 605–617.
[17] A. Weilert, *Asymptotically fast GCD computation in* $\mathbb{Z}[i]$, in Algorithmic number theory (Leiden 2000), Lecture Notes in Comput. Scie., vol. 1838, Springer, 2000, 595–613.
[18] A. Weilert, *Fast computation of the biquadratic residue symbol*, J. Number Theory **96** (2002), no. 1. 133–151.

Dipartimento di Matematica, Università Roma Tre, Largo S. L. Murialdo 1, I–00146 Roma, ITALIA
E-mail address: cosenti@ciop.mat.uniroma3.it, pappa@mat.uniroma3.it