Journal of Symbolic Computation 44 (2009) 683–699

Contents lists available at ScienceDirect

Journal of Symbolic Computation

journal homepage: www.elsevier.com/locate/jsc

Lower bounds for decision problems in imaginary, norm-Euclidean quadratic integer rings[☆]

J. Busch [1]

The Archer School for Girls, Mathematics Department, 11725 Sunset Boulevard, Los Angeles, CA 90049, USA

ARTICLE INFO

Article history:
Received 4 November 2007
Accepted 22 November 2008
Available online 28 November 2008

Keywords:
Arithmetic complexity
Computational complexity
Coprimality
Eisenstein integers
Gaussian integers
gcd
Lower bounds

ABSTRACT

We prove lower bounds for the complexity of deciding several relations in imaginary, norm-Euclidean quadratic integer rings, where computations are assumed to be relative to a basis of piecewise-linear operations. In particular, we establish lower bounds for deciding coprimality in these rings, which yield lower bounds for gcd computations. In each imaginary, norm-Euclidean quadratic integer ring, a known binary-like gcd algorithm has complexity that is quadratic in our lower bound.

1. Introduction

1.1. Background and scope

The greatest common divisor (gcd) of two integers is a fundamental number-theoretic notion. It can be computed using the ancient Euclidean algorithm, which iteratively performs division with remainder. Presented in Stein (1967) is a modern, so-called binary gcd algorithm which also computes the gcd of two integers, but uses only comparisons, subtraction, multiplication by 2, and division by 2, and requires no general division operation. The optimality of this algorithm relative to these primitive operations is shown in van den Dries and Moschovakis (2004).

The notion of gcd generalizes to arbitrary Euclidean domains, because Euclidean domains are unique factorization domains. Given two elements x, y of a Euclidean domain D, $d \in D$ is a gcd of

[☆] This research was partly supported by the National Science Foundation grant DMS-0502315.

E-mail address: buschje@gmail.com.

[1] Tel.: +1 310 873 7000; fax: +1 310 873 7070.

0747-7171/$ – see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jsc.2008.11.001

x and y if $d \mid x, y$, and if $z \in D$ is also such that $z \mid x, y$, then $z \mid d$. A gcd is unique up to multiplication by a unit (invertible element). The binary gcd algorithm for $\mathbb{Z}$ has been generalized in Weilert (2000), Agarwal and Frandsen (2004), and Damgård and Frandsen (2005) to each of the five imaginary, norm-Euclidean quadratic integer rings, which are the rings of integers of certain second-degree algebraic extensions of $\mathbb{Q}$ that are Euclidean domains with respect to the field norm. Such rings are discussed in more detail in Section 1.2. Greatest common divisor computations have applications in rational complex arithmetic, and in computing a generator of a finitely-generated ideal. They are also useful in computing discrete logarithms in finite fields, see, e.g., Coppersmith et al. (1986) and LaMacchia and Odlyzko (1991).

The binary-like algorithms compute a gcd using subtraction, multiplication and division by a small, fixed set of algebraic integers, and roughly, comparison of norms. We prove lower bounds, for a natural measure of complexity, on gcd computation by algorithms which use as given a set of primitive operations in terms of which these algorithms can be naturally expressed. The notion that we are using of computation relative to a fixed set of basic functions will be made precise in Section 2.2, and the lower bounds that we prove hold for many uniform models of computation from a fixed basis of given functions.

We use the following standard notation for expressing the asymptotic growth rate of functions. Let $\mathbb{R}^+ = [0, \infty)$. Given two functions $f, g : \mathbb{R}^+ \to \mathbb{R}^+$, we have that $f = O(g)$ if there are constants $x_0, M > 0$ such that for all $x > x_0, f(x) \leq Mg(x)$. We have that $f = \Omega(g)$ if there are constants $x_0, M > 0$ such that for all $x > x_0, f(x) \geq Mg(x)$. If $f, g : D \to \mathbb{R}^+$ for some arbitrary set D, we have that $f = \Omega_\infty(g)$ if there is a constant $M > 0$, and an infinite set $\{x_n\}_{n \in \mathbb{N}} \subseteq D$, such that for all $n \in \mathbb{N}$, $f(x_n) \geq Mg(x_n)$.

We prove an $\Omega_\infty(\log \max\{N(\zeta), N(\xi)\})$-lower bound for deciding if ζ and ξ are coprime in a ring of integers under consideration. Here, two algebraic integers are coprime iff their gcd is a unit, and $N(\zeta) = |\zeta|^2$ (absolute value squared) is the norm of ζ. We obtain a lower bound for computing gcd's by reducing coprimality to gcd computation. Each of the binary-like gcd algorithms has complexity that is $O(\log^2 \max\{N(\zeta), N(\xi)\})$ in our model. Before establishing these bounds, we prove $\Omega_\infty(\log N(\zeta))$-lower bounds for some natural unary decision problems which are of independent interest, and certain technical steps followed to establish these lower bounds will set the pattern for coprimality.

There are few results in the literature which give complexity lower bounds for algorithms relative to a fixed set of basic functions. Related work in this area includes Mansoor et al. (1991a,b) and Meidânis (1991), where lower bounds are obtained for the depth of computation trees and the time complexity of random access machines which compute certain number-theoretic functions. Also related is van den Dries and Moschovakis (in press), which includes lower bounds for term complexity in addition to many other results for arithmetic algorithms. The lower bounds proved below are established in the framework of van den Dries and Moschovakis (2004), and make particular use of the powerful embedding technique developed there. This technique reduces the problem of proving lower bounds to constructing certain embeddings, and is isolated and further described in Moschovakis (2005). Closely related to the present work is Busch (2007), where lower bounds are obtained for the arithmetic operations of modular exponentiation, deciding pseudoprimality, and computing the Legendre and Jacobi symbols.

1.2. Results from algebraic number theory

Let $D \in \mathbb{Z}$ be negative and squarefree. The number field $\mathbb{Q}(\sqrt{D}) \subseteq \mathbb{C}$ has degree 2 over $\mathbb{Q}$, and its ring of integers $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ consists of algebraic numbers of the form $a + b\omega$, where $a, b \in \mathbb{Z}$, and ω has the following dependence on D,

$$\omega = \begin{cases} \sqrt{D} & \text{if } D \equiv 2, 3 \pmod 4, \\ \dfrac{-1 + \sqrt{D}}{2} & \text{if } D \equiv 1 \pmod 4. \end{cases} \tag{1}$$

In particular, $\mathbb{Z} \subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$.

These rings inherit from $\mathbb{Q}(\sqrt{D})$ the algebraic field norm $N(\zeta) = \zeta\overline{\zeta}$, where $\overline{\zeta}$ is the Galois conjugate of ζ, which is the same as the complex conjugate of ζ since each $\mathbb{Q}(\sqrt{D})$ is a quadratic extension and $D < 0$. The ring of integers $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ is norm-Euclidean if the field norm N is also a Euclidean norm on $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$, i.e., if for all $\zeta, \xi \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$, $\xi \neq 0$, there exist $\theta, \rho \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ such that

$$\zeta = \theta\xi + \rho, \quad \text{with } \rho = 0 \text{ or } N(\rho) < N(\xi). \tag{2}$$

A classical result, included in standard texts such as Stewart and Tall (1987), is that for $D < 0$, the ring of integers $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ of the imaginary, quadratic extension $\mathbb{Q}(\sqrt{D})$ is norm-Euclidean iff $D \in \{-1, -2, -3, -7, -11\}$. For such values of D, $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ is said to be an *imaginary, norm-Euclidean quadratic integer ring*. The Gaussian integers $\mathbb{Z}[\mathrm{i}] = \mathcal{O}_{\mathbb{Q}(\sqrt{-1})}$, and for a primitive cube root of unity ζ, the Eisenstein integers $\mathbb{Z}[\zeta] = \mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$, are well-known examples of such rings. Our focus will be exclusively on imaginary, norm-Euclidean quadratic integer rings, and when not otherwise qualified, the symbol '$\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$' will always refer to one.

We list here some properties of the norm of $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ which are easily verified, and which will be used frequently, often without explicit mention. If $|\zeta|$ is the absolute value of the complex number ζ, then $N(\zeta) = |\zeta|^2$ for all $\zeta \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$, and it follows by the triangle inequality in $\mathbb{C}$ that for all $\zeta, \xi \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$,

$$N(\zeta + \xi) \leq N(\zeta) + N(\xi) + 2\sqrt{N(\zeta)N(\xi)}. \tag{3}$$

Since $N(a + b\omega) = (a + b\omega)(a + b\overline{\omega})$, we easily obtain from (1) the following explicit formula for the norm,

$$N(a + b\omega) = \begin{cases} a^2 - Db^2 & \text{if } D \equiv 2, 3 \pmod 4, \\ a^2 + \dfrac{1 - D}{4}b^2 - ab & \text{if } D \equiv 1 \pmod 4. \end{cases}$$

In particular, if $a \in \mathbb{Z}$, then $N(a) = a^2$. Clearly, $N(-\zeta) = N(\zeta)$ and $N(\zeta) = 0$ iff $\zeta = 0$. It follows easily that the norm of non-zero $\zeta \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ is a positive rational integer. The norm satisfies $N(\zeta\xi) = N(\zeta)N(\xi)$, and so, in particular, for $a \in \mathbb{Z}$,

$$N(a\zeta) = a^2N(\zeta).$$

Observe that for $\zeta \neq 0$, if $\xi \mid \zeta$ in $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$, then $N(\xi) \leq N(\zeta)$, because $\zeta = \theta\xi$ implies that $N(\zeta) = N(\theta)N(\xi)$ with $N(\theta) \geq 1$.

Since $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ is discrete, every subset of $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ that consists of elements which are bounded in norm is finite. Each $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ has a finite, explicitly known group of units,

$$\mathcal{O}^{\times}_{\mathbb{Q}(\sqrt{D})} = \{\zeta \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})} \mid (\exists \xi \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})})\ \zeta\xi = 1\}.$$

It is easy to verify that $\zeta \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ is a unit iff $N(\zeta) = 1$.

Given non-zero $\zeta, \xi \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$, (2) guarantees the existence of a quotient θ and remainder ρ in a division of ζ by ξ. It is well known, however, that a quotient and remainder are not uniquely determined, e.g., in the Gaussian integers $\mathcal{O}_{\mathbb{Q}(\sqrt{-1})}$, we have that

$$\begin{aligned} 5 + 12\sqrt{-1} &= 2(4 + 4\sqrt{-1}) + (-3 + 4\sqrt{-1}), \\ &= (2 + \sqrt{-1})(4 + 4\sqrt{-1}) + 1, \end{aligned}$$

with $N(1) = 1$, and $N(-3 + 4\sqrt{-1}) = 25 < 32 = N(4 + 4\sqrt{-1})$. We assume that algorithms can apply functions to perform division by elements from a fixed finite set. Our results are independent of how a particular quotient and remainder are chosen in a division by some ξ, provided the choice is made uniformly for each ξ. The approach we take is to fix a systematic method of choosing a remainder, and then to define the quotient in terms of it. There are many possible ways of deterministically choosing a remainder, e.g., by picking one of least norm, one of greatest norm, one that is right-most in the complex plane, etc. These choices are all somewhat arbitrary, and are generalized in Busch (2008). We would get the same complexity lower bounds for each choice, and for all others in which the resulting remainder function is constant on residue classes, i.e.,

$$\text{if } \zeta \equiv \zeta' \pmod{\xi}, \text{ then } \mathrm{rem}_\xi(\zeta) = \mathrm{rem}_\xi(\zeta'). \tag{4}$$

For each ξ for which we allow division, fix any function $\mathrm{rem}_\xi(\zeta)$ that satisfies (4), and is such that, for every $\zeta \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$, there is a $\theta \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ such that

$$\zeta = \theta\xi + \mathrm{rem}_\xi(\zeta), \quad N(\mathrm{rem}_\xi(\zeta)) < N(\xi).$$

For the present purposes, it will be necessary to fix only finitely many such functions. Let

$$\mathrm{quo}_\xi(\zeta) = \frac{\zeta - \mathrm{rem}_\xi(\zeta)}{\xi},$$

and notice that this uniquely defines a quotient because $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ is an integral domain. We clearly have, for all $\zeta \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$,

$$\zeta = \mathrm{quo}_\xi(\zeta)\xi + \mathrm{rem}_\xi(\zeta), \quad N(\mathrm{rem}_\xi(\zeta)) < N(\xi).$$

2. Model of computation

2.1. Imaginary, norm-Euclidean quadratic algebras

For each $M > 1$, let

$$\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})} = (\mathcal{O}_{\mathbb{Q}(\sqrt{D})}, 0, 1, +, -, \chi_=, \zeta \mapsto \overline{\zeta}, \{\zeta \mapsto \xi\zeta, \mathrm{quo}_\xi(\zeta), \mathrm{rem}_\xi(\zeta)\}_{0<N(\xi)<M})$$

be the imaginary, norm-Euclidean quadratic algebra with underlying set $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$, distinguished constants $0, 1 \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$, and the functions displayed, where $+, -$ are addition and subtraction respectively, $\chi_=$ is the characteristic function of equality, $\zeta \mapsto \overline{\zeta}$ is the function which takes $\zeta \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ to its complex conjugate $\overline{\zeta}$, and $\zeta \mapsto \xi\zeta$ is the function which takes $\zeta \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ to the product of ξ with ζ. Notice that $\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})}$ contains functions to perform multiplication, and division with remainder, by only those elements from a fixed, finite set of algebraic integers, and that the size of this set depends on the parameter M.

Let

$$E'_{\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})}} = \prod_{0<N(\xi)<M} \xi.$$

Then $E'_{\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})}} \in \mathbb{Z}$, since $N(\xi) < M$ implies that $N(\overline{\xi}) < M$. Let

$$E = E_{\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})}} = \left| E'_{\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})}} \right|, \tag{5}$$

and observe that if $N(\xi) < M$, then $N(\xi) \le E$.

2.2. Programs and complexity

We work in the framework for programs and complexity developed in van den Dries and Moschovakis (2004). The terms t of $\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})}$ are generated by the recursion

$$t ::= 0 \mid 1 \mid \mathsf{v} \mid \text{if } t_0 = 0 \text{ then } t_1 \text{ else } t_2 \mid \phi(t_0 \cdots t_m) \mid \mathsf{p}(t_0 \cdots t_n),$$

where v is an individual variable, ϕ is a symbol for a function of $\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})}$, and p is a function variable. A recursive program γ in $\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})}$ is a system of mutually-recursive term equations

$$\gamma : \begin{cases} \mathsf{p}_0(\vec{\mathsf{v}}_0) = t_0(\vec{\mathsf{v}}_0, \mathsf{p}_1, \ldots, \mathsf{p}_k), \\ \mathsf{p}_1(\vec{\mathsf{v}}_1) = t_1(\vec{\mathsf{v}}_1, \mathsf{p}_1, \ldots, \mathsf{p}_k), \\ \quad\vdots \\ \mathsf{p}_k(\vec{\mathsf{v}}_k) = t_k(\vec{\mathsf{v}}_k, \mathsf{p}_1, \ldots, \mathsf{p}_k), \end{cases} \tag{6}$$

where the variables of each term t_i are among those displayed. The program γ computes the (possibly partial) function $[\![\gamma]\!] : \mathcal{O}^n_{\mathbb{Q}(\sqrt{D})} \rightharpoonup \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$, the least fixed point of the head equation of γ.

If γ converges on input $\vec{\zeta} \in \mathcal{O}^n_{\mathbb{Q}(\sqrt{D})}$, then the basic parallel complexity $c_\gamma(\vec{\zeta})$ of γ on input $\vec{\zeta}$ is the maximum number of nested calls to the functions of $\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})}$ in the "computation" of $[\![\gamma]\!](\vec{\zeta})$. In more detail, for each term t of the program γ, the basic parallel complexity $C(t)$ is determined by (C1)–(C4) below. In each of these clauses, the parameters and function variables of a term are suppressed for brevity, and $[\![t]\!]$ is the value (denotation) of the term t in the expansion of $\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})}$ in which the partial function variables are interpreted as the least fixed points of the program.

(C1) $C(0) = C(1) = C(x) = 0$, if x is any parameter,

(C2) $C(\phi(t_1, \ldots, t_m)) = \max\{C(t_i)\} + 1$, if ϕ is a function of $\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})}$,

(C3) $C(\mathsf{p}(t_1, \ldots, t_n)) = \max\{C(t_i)\} + C(E_{\mathsf{p}}([\![t_1]\!], \ldots, [\![t_n]\!]))$, if p is a function variable and E_{p} defines p in the program γ,

(C4) $C(\text{if } (t_0 = 0) \text{ then } t_1 \text{ else } t_2)$

$$= \begin{cases} \max\{C(t_0), C(t_1)\} & \text{if } [\![t_0]\!] = 0, \\ \max\{C(t_0), C(t_2)\} & \text{if } [\![t_0]\!]\downarrow\neq 0. \end{cases}$$

The basic parallel complexity of γ on input $\vec{\zeta}$ is the complexity of the term that results by substituting the values of the vector $\vec{\zeta}$ for the individual variables of head term of γ:

$$c_\gamma(\vec{\zeta}) = C(t_0\{\mathsf{v}_{0,0} := \zeta_0, \ldots, \mathsf{v}_{0,n} := \zeta_n\}),$$

for γ as in (6), $\vec{\mathsf{v}}_0 = (\mathsf{v}_{0,0}, \ldots, \mathsf{v}_{0,n})$, $\vec{\zeta} = (\zeta_0, \ldots, \zeta_n)$.

This complexity does not count logical steps, and is an abstract measure of strict, parallel, call-by-value time complexity. With respect to this complexity, non-trivial computations like evaluating $\chi_=(\zeta, \xi)$ are performed in one step, regardless of the size of ζ and ξ. Of course, when considering lower bounds, the assumption that strong operations can be carried out in constant time increases the strength of the results. Regardless, because the methods that we use are insensitive to logical operations, we obtain exactly the same lower bounds whether or not $\chi_=$ is included as a given function. In fact, it can be shown that the lower bounds that we obtain in $\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})}$ also hold in extensions which contain logical datatypes such as lists and trees. The class of such logical extensions includes random access machines. For more details, see van den Dries and Moschovakis (2004).

It is convenient to use the model-theoretic notation,

$$\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})} \models \gamma(\vec{\zeta})^{(m)} = w \iff [\![\gamma]\!](\vec{\zeta}) = w \;\&\; c_\gamma(\vec{\zeta}) \leq m.$$

For every $X \subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$, let

$$G_0(X) = \{0, 1\} \cup X,$$

$$G_{m+1}(X) = G_m(X) \cup \Big\{\phi(\zeta_1, \ldots, \zeta_n) \mid \zeta_1, \ldots, \zeta_n \in G_m(X) \text{ and } \phi \text{ is a function of the algebra } \mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})}\Big\}$$

so that $G_m(X)$ consists precisely of those elements of $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ that can be generated from X by the functions of $\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})}$ in m steps.

Our main tools for obtaining lower bounds are the Absoluteness and Embedding Lemmas of van den Dries and Moschovakis (2004). The Absoluteness Lemma states that if γ is a recursive program in $\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})}$ and $\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})} \models \gamma(\vec{\zeta})^{(m)} = w$, then $w \in G_m(\vec{\zeta})$, and

$$\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})} \restriction G_m(\vec{\zeta}) \models \gamma(\vec{\zeta})^{(m)} = w.$$

Here, the generated subalgebra $\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})} \upharpoonright G_m(\vec{\zeta})$ is defined so that for every function ϕ of $\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})}$,

$$\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})} \upharpoonright G_m(\vec{\zeta}) \models \phi(\xi_1, \ldots, \xi_n) = w$$
$$\iff \xi_1, \ldots, \xi_n, \quad w \in G_m(\vec{\zeta}) \;\&\; \mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})} \models \phi(\xi_1, \ldots, \xi_n) = w.$$

The Absoluteness Lemma expresses the fact that convergent computations are finite and "take place" in the subalgebra generated by the input.

An embedding

$$j : \mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})} \upharpoonright G_m(X) \hookrightarrow \mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})}$$

is a function $j : G_m(X) \to \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ such that j is injective, $j(0) = 0, j(1) = 1$, and j respects each function ϕ of $\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})}$:

$$\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})} \upharpoonright G_m(X) \models \phi(\vec{\zeta}) = w \Longrightarrow \mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})} \models \phi(j(\vec{\zeta})) = j(w). \tag{7}$$

In (7) (and elsewhere), if $\vec{\zeta} = (\zeta_1, \ldots, \zeta_n)$, then $j(\vec{\zeta}) = (j(\zeta_1), \ldots, j(\zeta_n))$.

The Embedding Lemma implies that if γ is a recursive program and

$$j : \mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})} \upharpoonright G_m(X) \hookrightarrow \mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})}$$

is an embedding, then

$$\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})} \upharpoonright G_m(x) \models \gamma(\vec{\zeta})^{(m)} = w \Longrightarrow \mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})} \models \gamma(j(\vec{\zeta}))^{(m)} = j(w).$$

This Lemma expresses the fact that embeddings preserve both structure and complexity.

3. Primality and squarefreeness

Let $\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})}$ be an imaginary, norm-Euclidean algebra, and let $E = \left|\prod_{0<N(\xi)<M} \xi\right|$. Define for all $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ and $m \in \mathbb{N}$,

$$B_m(\alpha) = \left\{ \frac{\zeta_0 + \zeta_1\alpha}{E^m} \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})} \mid \zeta_0, \zeta_1 \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})} \;\&\; N(\zeta_0), N(\zeta_1) < (2E)^{3m+1} \right\}.$$

Observe that all $\zeta \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ with norm $< 2E$ belong to $B_0(\alpha)$. In particular, if $N(\xi) < M$, then for all $\zeta \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$, $\mathrm{rem}_\xi(\zeta) \in B_0(\alpha)$.

Lemma 1. *If $\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})}$ is an imaginary norm-Euclidean algebra and $\alpha \in \mathbb{N}$, then for all $m \in \mathbb{N}$, $G_m(\alpha) \subseteq B_m(\alpha)$.*

Proof. The proof is by induction on m. The basis is obvious. For the inductive step, assume that $G_m(\alpha) \subseteq B_m(\alpha)$ for some fixed $m \geq 0$. As noted above, the images of the remainder functions are contained in $B_0(\alpha)$, and are therefore included in every $B_m(\alpha)$. We take cases on the other functions ϕ of $\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})}$ which generate $\phi(\zeta_1, \ldots, \zeta_n) \in G_{m+1}(\alpha)$ from $\zeta_1, \ldots, \zeta_n \in G_m(\alpha)$.

Suppose that $\zeta + \xi \in G_{m+1}(\alpha)$, with $\zeta, \xi \in G_m(\alpha)$. By induction, we have the expressions

$$\zeta = \frac{\zeta_0 + \zeta_1\alpha}{E^m}, \quad \xi = \frac{\xi_0 + \xi_1\alpha}{E^m}, \tag{8}$$

with $N(\zeta_k), N(\xi_k) < (2E)^{3m+1}, k = 0, 1$. Then

$$\zeta + \xi = \frac{E(\zeta_0 + \xi_0) + E(\zeta_1 + \xi_1)\alpha}{E^{m+1}},$$

and by (3),

$$N(E(\zeta_k + \xi_k)) < 4E^2(2E)^{3m+1} = (2E)^{3m+3} < (2E)^{3(m+1)+1}, \quad k = 0, 1,$$

so $\zeta + \xi \in B_{m+1}(\alpha)$. A similar computation shows that $\zeta - \xi \in B_{m+1}(\alpha)$ whenever $\zeta, \xi \in G_m(\alpha)$.

If $\overline{\zeta} \in G_{m+1}(\alpha)$ with $\zeta \in G_m(\alpha)$ expressed as in (8), then

$$\overline{\zeta} = \frac{\overline{\zeta_0 + \zeta_1\alpha}}{E^m} = \frac{E\overline{\zeta_0} + E\overline{\zeta_1}\alpha}{E^{m+1}}.$$

Since $N(\overline{\zeta}) = N(\zeta)$ for all $\zeta \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$, we have that

$$N(E\overline{\zeta_k}) < E^2(2E)^{3m+1} < (2E)^{3(m+1)+1}, \quad k = 0, 1,$$

and therefore $\overline{\zeta} \in B_{m+1}(\alpha)$.

For multiplication by some fixed $\xi \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$, $N(\xi) < M$, suppose that $\xi\zeta \in G_{m+1}(\alpha)$ with $\zeta \in G_m(\alpha)$ expressed as in (8). Then

$$\xi\zeta = \frac{\xi E\zeta_0 + \xi E\zeta_1\alpha}{E^{m+1}},$$

and

$$N(\xi E\zeta_k) < E^3(2E)^{3m+1} < (2E)^{3(m+1)+1}, \quad k = 0, 1,$$

so $\xi\zeta \in B_{m+1}(\alpha)$.

For the quotient functions, let $\xi \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ be non-zero and such that $N(\xi) < M$. Suppose that $\mathrm{quo}_\xi(\zeta) \in G_{m+1}(\alpha)$ with $\zeta \in G_m(\alpha)$ expressed as in (8). We have that

$$\mathrm{quo}_\xi(\zeta) = \frac{\zeta_0 - E^m\mathrm{rem}_\xi(\zeta) + \zeta_1\alpha}{\xi E^m} = \frac{E}{\xi}\frac{(\zeta_0 - E^m\mathrm{rem}_\xi(\zeta)) + \zeta_1\alpha}{E^{m+1}},$$

and

$$\begin{aligned} N\left(\frac{E}{\xi}\left(\zeta_0 - E^m\mathrm{rem}_\xi(\zeta)\right)\right) &< E^2\left((2E)^{3m+1} + E^{2m+1} + 2\sqrt{(2E)^{3m+1}E^{2m+1}}\right) \\ &\leq 4E^2(2E)^{3m+1} \\ &< (2E)^{3(m+1)+1}. \end{aligned} \tag{9}$$

It is even simpler to establish that

$$N(E\zeta_1/\xi) < (2E)^{3(m+1)+1},$$

hence $\mathrm{quo}_\xi(\zeta) \in B_{m+1}(\alpha)$. □

Lemma 1 shows that elements of $G_m(\alpha)$ have convenient representations when α is rational. The following Lemma implies that this representation is unique when α is sufficiently large relative to m.

Lemma 2. *Suppose that $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ is an imaginary, norm-Euclidean quadratic ring of integers.*

(i) *If $\alpha, \zeta_0, \zeta_1 \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ are such that*

$$N(\zeta_0) < N(\alpha),$$

then

$$\zeta_0 + \zeta_1\alpha = 0 \iff \zeta_0 = \zeta_1 = 0.$$

(ii) *If $\alpha, \zeta_k \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$, $k = 0, 1, 2, 3$, are such that*

$$N(\zeta_0), N(\zeta_2) < N(\alpha)/4,$$

then

$$\zeta_0 + \zeta_1\alpha = \zeta_2 + \zeta_3\alpha \iff \zeta_k = \zeta_{k+2}, \quad \textit{for } k = 0, 1.$$

Proof. (i) If $\zeta_1 = 0$, then $\zeta_0 = 0$, so assume that $\zeta_1 \neq 0$ so that $N(\zeta_1) \geq 1$. If $\zeta_0 + \zeta_1\alpha = 0$, then $\zeta_0 = -\zeta_1\alpha$. Taking norms yields the contradictory $N(\zeta_0) = N(\zeta_1)N(\alpha) \geq N(\alpha)$.

(ii) If $\zeta_0 + \zeta_1\alpha = \zeta_2 + \zeta_3\alpha$, then $\zeta_0 - \zeta_2 + (\zeta_1 - \zeta_3)\alpha = 0$. Now,

$$\begin{aligned} N(\zeta_0 - \zeta_2) &\leq N(\zeta_0) + N(\zeta_2) + 2\sqrt{N(\zeta_0)N(\zeta_2)} \\ &< \frac{N(\alpha)}{4} + \frac{N(\alpha)}{4} + 2\sqrt{\frac{N(\alpha)^2}{16}} = N(\alpha), \end{aligned}$$

so the result follows by (i). □

The key to obtaining lower bounds for the unary relations that we consider in this section is the embedding furnished by the following Lemma.

Lemma 3. *Let $\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})}$ be an imaginary, norm-Euclidean quadratic algebra, and let E be defined as in (5). If $m > 0$ and $\alpha \in \mathbb{N}$ satisfies $N(\alpha) > (2E)^{3m+8}$, then for all $\mu \in \mathbb{N}$ such that $\mu \equiv 1 \pmod{E^{m+2}}$, there exists an embedding*

$$j : \mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})} \restriction G_m(\alpha) \hookrightarrow \mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})},$$

such that $j(\alpha) = \mu\alpha$.

Proof. Let m and α be as in the statement of the Lemma. We begin by defining a function

$$j : G_{m+1}(\alpha) \to \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$$

on the larger set $G_{m+1}(\alpha) \supseteq G_m(\alpha)$, on which it is not necessarily an embedding, but does respect differences. We will show that the restriction of j to $G_m(\alpha)$ is an embedding. Fix any $\mu \in \mathbb{N}$ such that $\mu \equiv 1 \pmod{E^{m+2}}$, and let q^* be such that $\mu = q^*E^{m+2} + 1$. Let

$$j\left(\frac{\zeta_0 + \zeta_1\alpha}{E^{m+1}}\right) = \frac{\zeta_0 + \mu\zeta_1\alpha}{E^{m+1}}.$$

By Lemmas 1 and 2, j is a well-defined injection. It is clear that $j(0) = 0$ and $j(1) = 1$ because, in general, algebraic numbers of the form

$$\frac{\zeta_0 + \zeta_1\alpha}{E^{m+1}}$$

with $\zeta_1 = 0$ and $N(\zeta_0) < (2E)^{3m+4}$ are fixed by j. We have that image(j) $\subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$, because if

$$\frac{\zeta_0 + \zeta_1\alpha}{E^{m+1}} \in G_{m+1}(\alpha),$$

then $E^{m+1} \mid \zeta_0 + \zeta_1\alpha$, so

$$E^{m+1} \mid \zeta_0 + \zeta_1\alpha + q^*E^{m+2}\zeta_1\alpha = \zeta_0 + \mu\zeta_1\alpha,$$

hence

$$j\left(\frac{\zeta_0 + \zeta_1\alpha}{E^{m+1}}\right) = \frac{\zeta_0 + \mu\zeta_1\alpha}{E^{m+1}} \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}.$$

Let $\zeta, \xi \in G_{m+1}(\alpha)$, and suppose that $\zeta - \xi \in G_{m+1}(\alpha)$. These algebraic integers have representations

$$\zeta = \frac{\zeta_0 + \zeta_1\alpha}{E^{m+1}}, \qquad \xi = \frac{\zeta_2 + \zeta_3\alpha}{E^{m+1}}, \qquad \zeta - \xi = \frac{\zeta_4 + \zeta_5\alpha}{E^{m+1}},$$

with $N(\zeta_k) < (2E)^{3(m+1)+1}$, $0 \leq k \leq 5$. For $k = 0, 1$, we have that

$$N(\zeta_k - \zeta_{k+2}) < 4(2E)^{3(m+1)+1} \leq \frac{(2E)^{3(m+1)+5}}{4} < \frac{N(\alpha)}{4},$$

and therefore, by Lemma 2,

$$\zeta_0 - \zeta_2 = \zeta_4, \quad \zeta_1 - \zeta_3 = \zeta_5.$$

Thus

$$j(\zeta - \xi) = \frac{\zeta_4 + \mu\zeta_5\alpha}{E^{m+1}} = \frac{\zeta_0 - \zeta_2 + \mu(\zeta_1 - \zeta_3)\alpha}{E^{m+1}} = j(\zeta) - j(\xi). \tag{10}$$

We proceed to show that $j \restriction G_m(\alpha)$ is an embedding. First, observe that for $\zeta \in G_m(\alpha)$, we have the formula

$$j(\zeta) = j\left(\frac{\zeta_0 + \zeta_1\alpha}{E^m}\right) = j\left(\frac{E\zeta_0 + E\zeta_1\alpha}{E^{m+1}}\right) = \frac{E\zeta_0 + \mu E\zeta_1\alpha}{E^{m+1}} = \frac{\zeta_0 + \mu\zeta_1\alpha}{E^m}.$$

This is because

$$N(E\zeta_k) < E^2(2E)^{3m+1} < (2E)^{3(m+1)+1}, \quad k = 0, 1,$$

and hence, if ζ is uniquely represented in $B_m(\alpha)$ as $(\zeta_0 + \zeta_1\alpha)/E^m$ with

$$N(\zeta_0), N(\zeta_1) < (2E)^{3m+1},$$

then ζ is uniquely represented in $B_{m+1}(\alpha)$ as $(E\zeta_0 + E\zeta_1\alpha)/E^{m+1}$ with

$$N(E\zeta_0), N(E\zeta_1) < (2E)^{3(m+1)+1}.$$

To see that j respects complex conjugation, suppose that

$$\frac{\zeta_0 + \zeta_1\alpha}{E^m}, \quad \overline{\frac{\zeta_0 + \zeta_1\alpha}{E^m}} = \frac{\xi_0 + \xi_1\alpha}{E^m} \in G_m(\alpha),$$

so that $\overline{\zeta_k} = \xi_k$, $k = 0, 1$. Then

$$\overline{j\left(\frac{\zeta_0 + \zeta_1\alpha}{E^m}\right)} = \overline{\frac{\zeta_0 + \mu\zeta_1\alpha}{E^m}} = \frac{\overline{\zeta_0} + \mu\overline{\zeta_1}\alpha}{E^m} = j\left(\frac{\xi_0 + \xi_1\alpha}{E^m}\right).$$

If $N(\xi) < M$, then the remainder in the division by ξ is fixed by j, because for every ζ,

$$\mathrm{rem}_\xi(\zeta) = \frac{E^m \mathrm{rem}_\xi(\zeta) + 0\alpha}{E^m},$$

with

$$N(E^m \mathrm{rem}_\xi(\zeta)) \le E^{2m+1} < (2E)^{3m+1}.$$

Therefore,

$$j(\mathrm{rem}_\xi(\zeta)) = \mathrm{rem}_\xi(\zeta). \tag{11}$$

We next show that j is a congruence for residue classes of small moduli in the following sense: if $\xi \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ is such that $N(\xi) < M$, and $\zeta \in G_{m+1}(\alpha)$, then,

$$\begin{aligned} \xi \mid \zeta = \frac{\zeta_0 + \zeta_1\alpha}{E^{m+1}} &\iff \xi E^{m+1} \mid \zeta_0 + \zeta_1\alpha \iff \xi E^{m+1} \mid \zeta_0 + \zeta_1\alpha + q^* E^{m+2}\zeta_1\alpha \\ &\iff \xi E^{m+1} \mid \zeta_0 + \mu\zeta_1\alpha \iff \xi \mid \frac{\zeta_0 + \mu\zeta_1\alpha}{E^{m+1}} = j(\zeta). \end{aligned} \tag{12}$$

To see that j respects the remainder functions, let $\zeta \in G_m(\alpha)$, and fix some non-zero $\xi \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ with $N(\xi) < M$. Now, $N(\mathrm{rem}_\xi(\zeta)), N(\mathrm{rem}_\xi(j(\zeta))) < N(\xi) < M$, hence $\mathrm{rem}_\xi(\zeta), \mathrm{rem}_\xi(j(\zeta)) \in G_1(\alpha) \subseteq G_m(\alpha)$. Since $\mathrm{rem}_\xi(\zeta)$ is the remainder in a division of ζ by ξ, $\xi \mid \zeta - \mathrm{rem}_\xi(\zeta)$. Clearly, $\zeta - \mathrm{rem}_\xi(\zeta) \in G_{m+1}(\alpha)$, and therefore we have by (10), (11), and (12) that

$$\xi \mid j(\zeta - \mathrm{rem}_\xi(\zeta)) = j(\zeta) - j(\mathrm{rem}_\xi(\zeta)) = j(\zeta) - \mathrm{rem}_\xi(\zeta).$$

Thus,

$$j(\zeta) \equiv \zeta \pmod{\xi},$$

and therefore, $\mathrm{rem}_\xi(j(\zeta)) = \mathrm{rem}_\xi(\zeta) = j(\mathrm{rem}_\xi(\zeta))$.

To see that j respects the quotient functions, let $\xi \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ be such that $N(\xi) < M$, and assume that $\zeta, \psi = \mathrm{quo}_\xi(\zeta) \in G_m(\alpha)$, where

$$\zeta = \frac{\zeta_0 + \zeta_1\alpha}{E^m}, \qquad \psi = \frac{\psi_0 + \psi_1\alpha}{E^m}.$$

Then

$$\begin{aligned}\mathrm{quo}_\xi(\zeta) &= \frac{\zeta_0 - E^m\mathrm{rem}_\xi(\zeta) + \zeta_1\alpha}{\xi E^m}\\ &= \frac{E}{\xi}\frac{(\zeta_0 - E^m\mathrm{rem}_\xi(\zeta)) + \zeta_1\alpha}{E^{m+1}}\\ &= \frac{E\psi_0 + E\psi_1\alpha}{E^{m+1}}.\end{aligned}$$

As in (9),

$$N\left(\frac{E}{\xi}(\zeta_0 - E^m\mathrm{rem}_\xi(\zeta))\right) < (2E)^{3(m+1)+1} < \frac{N(\alpha)}{4},$$

so we have that

$$\frac{E}{\xi}(\zeta_0 - E^m\mathrm{rem}_\xi(\zeta)) = E\psi_0, \qquad \frac{E}{\xi}\zeta_1 = E\psi_1.$$

Therefore

$$\begin{aligned}\mathrm{quo}_\xi(j(\zeta)) &= \frac{\zeta_0 - E^m\mathrm{rem}_\xi(j(\zeta)) + \mu\zeta_1\alpha}{\xi E^m}\\ &= \frac{E}{\xi}\frac{(\zeta_0 - E^m\mathrm{rem}_\xi(j(\zeta))) + \mu\zeta_1\alpha}{E^{m+1}}\\ &= \frac{E}{\xi}\frac{(\zeta_0 - E^m\mathrm{rem}_\xi(\zeta)) + \mu\zeta_1\alpha}{E^{m+1}}\\ &= \frac{\psi_0 + \mu\psi_1\alpha}{E^m}\\ &= j(\mathrm{quo}_\xi(\zeta)).\end{aligned}$$

For multiplication by $\xi \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ with $N(\xi) < M$, suppose that

$$\zeta, \psi = \xi\zeta \in G_m(\alpha).$$

We have the representations

$$\xi\zeta = \frac{\xi\zeta_0 + \xi\zeta_1\alpha}{E^m} = \frac{\psi_0 + \psi_1\alpha}{E^m} = \psi,$$

and since

$$N(\xi\zeta_k) \le E(2E)^{3m+1} < \frac{N(\alpha)}{4}, \quad k = 0, 1,$$

we have that $\xi\zeta_k = \psi_k$, $k = 0, 1$. Therefore,

$$\xi j(\zeta) = \frac{\xi\zeta_0 + \xi\mu\zeta_1\alpha}{E^m} = \frac{\psi_0 + \mu\psi_1\alpha}{E^m} = j(\xi\zeta). \quad \square$$

A non-zero algebraic integer $\pi \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ is prime in $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ if π is not a unit, and is irreducible, i.e., if $\pi = \xi\theta$ in $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ then one of ξ, θ is a unit. An algebraic integer $\zeta \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ is squarefree if there is no prime $\pi \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ such that $\pi^2 \mid \zeta$.

Notice that rational primes $p \in \mathbb{N}$ may fail to be prime in certain $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$, e.g., $2 = (1+\sqrt{-1})(1-\sqrt{-1})$ in $\mathcal{O}_{\mathbb{Q}(\sqrt{-1})}$. Despite this, if $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ is an imaginary, norm-Euclidean quadratic integer ring, then there are infinitely many $p \in \mathbb{N}$ such that p is prime in $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$. In the case $D = -1$, this can be seen as follows. By Dirichlet's Theorem on the primes of an arithmetic progression, there are infinitely many rational primes $p \in \mathbb{N}$ such that $p \equiv 3 \pmod 4$. If p factors as $p = \zeta\xi$ in $\mathcal{O}_{\mathbb{Q}(\sqrt{-1})}$ with neither ζ nor ξ a unit, then we must have for $\zeta = a + b\sqrt{-1}$ that $N(\zeta) = a^2 + b^2 = p$. It is easy to check that $a^2 + b^2 \equiv 3 \pmod 4$ has no integer solutions, so p is prime in $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$.

Theorem 4. *There is an infinite set $\{\alpha_k\}_{k\in\mathbb{N}} \subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ such that if γ is a recursive program in the imaginary, norm-Euclidean quadratic algebra $\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})}$ that decides either of the relations "α is prime" or "α is squarefree", then for all $k \in \mathbb{N}$,*

$$c_\gamma(\alpha_k) > \frac{1}{4\log_2 2E}\log_2 N(\alpha_k),$$

where E is defined as in (5).

Proof. Let $\{\alpha_k\}_{k\in\mathbb{N}}$ consist of infinitely many primes in $\mathbb{N}$ such that, for each k, α_k is prime in $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$, and $N(\alpha_k) > (2E)^{32}$. Let γ be a recursive program in $\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})}$ that decides either primality or squarefreeness. Fix $k \in \mathbb{N}$, and let $\alpha = \alpha_k$. Let $m = c_\gamma(\alpha) > 0$ and assume for a contradiction that $(2E)^{3m+8} < N(\alpha)$. Let j be an embedding as in the statement of Lemma 3, with $\mu = (1 + E^{m+2})^2$.

Since γ decides primality or squarefreeness in $\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})}$,

$$\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})} \models \gamma(\alpha)^{(m)} = 1,$$

hence, by Absoluteness,

$$\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})} \restriction G_m(\alpha) \models \gamma(\alpha)^{(m)} = 1.$$

Therefore, by the Embedding Lemma,

$$\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})} \models \gamma(j(\alpha))^{(m)} = 1,$$

i.e., $j(\alpha) = \mu\alpha$ is either prime or squarefree, but it is neither. Thus $(2E)^{3m+8} \geq N(\alpha)$, hence

$$c_\gamma(\alpha) \geq \frac{\log_{2E} N(\alpha)}{3} - \frac{8}{3} > \frac{1}{4}\log_{2E} N(\alpha) = \frac{1}{4\log_2 2E}\log_2 N(\alpha). \quad \square$$

The problem of deciding whether an element of $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ is prime can be reduced to the corresponding problem in $\mathbb{N}$, it can be solved in polynomial time, and the asymptotic complexity is the same for both domains. As with the rational integers, there do not appear to be any algorithms that decide squarefreeness in $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ without resorting to factoring.

4. Coprimality and gcd

The main result of this section is a lower bound for deciding coprimality in imaginary, norm-Euclidean quadratic algebras. As in the previous section, the lower bound is obtained through the construction of an appropriate embedding, and the one defined in this section is a generalization of the embedding from Busch (2007).

Define for all $\alpha, \beta \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ and $m \in \mathbb{N}$,

$$B_m(\alpha, \beta) = \left\{ \frac{\zeta_0 + \zeta_1\alpha + \zeta_2\beta}{E^m} \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})} \mid \zeta_k \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})} \,\&\, N(\zeta_k) < (2E)^{3m+1} \right\}.$$

For every $x \in \mathbb{R}$, let $\lfloor x \rfloor$ be the greatest integer $\leq x$. The following Lemma is analogous to Lemma 1, and because $\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})}$ contains only piecewise-linear functions, its proof is essentially the same.

Lemma 5. *If $\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})}$ is an imaginary norm-Euclidean algebra, E is defined as in (5), $\alpha \in \mathbb{N}$ is non-zero, and $\beta = E^{\lfloor \log_E 2N(\alpha) \rfloor + 1}$, then for all $m \in \mathbb{N}$, $G_m(\alpha, \beta) \subseteq B_m(\alpha, \beta)$.*

The following Lemma implies the representation of an element of $G_m(\alpha, \beta)$ as a member of $B_m(\alpha, \beta)$ is unique, provided certain conditions on α and β are satisfied.

Lemma 6. *Suppose that $\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})}$ is an imaginary, norm-Euclidean algebra, $\alpha, \mu \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ are non-zero, and*

$$\beta = E^{\lfloor \log_E 2N(\alpha) \rfloor + 1}.$$

(i) *If $\zeta_0, \zeta_1, \zeta_2 \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ are such that*

$$N(\zeta_0), N(\zeta_1) < N(\alpha),$$

then

$$\zeta_0 + \zeta_1\alpha + \mu\zeta_2\beta = 0 \iff \zeta_k = 0 \quad \text{for } k = 0, 1, 2.$$

(ii) *If $\zeta_k, \xi_k \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$, $k = 0, 1, 2$ are such that*

$$N(\zeta_0), N(\xi_0), N(\zeta_1), N(\xi_1) < N(\alpha)/4,$$

then

$$\zeta_0 + \zeta_1\alpha + \mu\zeta_2\beta = \xi_0 + \xi_1\alpha + \mu\xi_2\beta \iff \zeta_k = \xi_k, \quad \text{for } k = 0, 1, 2.$$

Proof. (i) If $\zeta_2 = 0$, then $\zeta_0 = \zeta_1 = 0$ as in Lemma 2. So assume that $\zeta_2 \neq 0$. Then

$$-\mu\zeta_2\beta = \zeta_0 + \zeta_1\alpha,$$

so, by taking norms,

$$\begin{aligned} N(\beta) &\leq N(\mu\zeta_2\beta) \\ &\leq N(\zeta_0) + N(\zeta_1)N(\alpha) + 2\sqrt{N(\zeta_0)N(\zeta_1)N(\alpha)} \\ &< N(\alpha) + N(\alpha)^2 + 2N(\alpha)\sqrt{N(\alpha)} \\ &\leq 4N(\alpha)^2. \end{aligned}$$

On the other hand,

$$N(\beta) = N(E^{\lfloor \log_E 2N(\alpha) \rfloor + 1}) \geq (2N(\alpha))^2 = 4N(\alpha)^2,$$

a contradiction.

(ii) follows from (i) as in the proof of Lemma 2. □

The embedding that we define on $G_m(\alpha, \beta)$ below is asymmetric in the sense that it fixes α, but moves β.

Lemma 7. *Let $\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})}$ be an imaginary, norm-Euclidean quadratic algebra, with E defined as in (5). If $m > 0$, $\alpha \in \mathbb{N}$ satisfies $N(\alpha) > (2E)^{3m+8}$, and*

$$\beta = E^{\lfloor \log_E 2N(\alpha) \rfloor + 1},$$

then for all non-zero $\mu \in \mathbb{N}$, there exists an embedding

$$j : \mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})} \restriction G_m(\alpha, \beta) \hookrightarrow \mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})},$$

such that

$$j(\alpha) = \alpha, \quad j(\beta) = \mu\beta.$$

Proof. Let m, α, β be as in the statement of the Lemma. As in the proof of Lemma 3, we begin by defining a function

$$j : G_{m+1}(\alpha, \beta) \to \mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})}$$

on a slightly larger set and then show that the restriction of this map to $G_m(\alpha, \beta)$ is an embedding. Let

$$j\left(\frac{\zeta_0 + \zeta_1\alpha + \zeta_2\beta}{E^{m+1}}\right) = \frac{\zeta_0 + \zeta_1\alpha + \mu\zeta_2\beta}{E^{m+1}}.$$

We first observe that

$$\lfloor \log_E 2N(\alpha) \rfloor + 1 \geq \log_E 2N(\alpha) > \log_E N(\alpha) > \log_{2E} N(\alpha) > 3m + 8,$$

hence $E^{m+2} \mid \beta = E^{\lfloor \log_E 2N(\alpha) \rfloor + 1}$. From this we conclude that

$$\begin{aligned} &E^{m+1} \mid \zeta_0 + \zeta_1\alpha + \zeta_2\beta \\ &\qquad\qquad \Longrightarrow E^{m+1} \mid \zeta_0 + \zeta_1\alpha + \zeta_2\beta + (\mu - 1)\zeta_2\beta = \zeta_0 + \zeta_1\alpha + \mu\zeta_2\beta, \end{aligned}$$

so image$(j) \subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$.

By Lemma 6, j is an injection. It is clear that j fixes 0 and 1, because in general, j fixes all elements of $G_{m+1}(\alpha, \beta)$ of the form

$$\frac{\zeta_0 + \zeta_1\alpha + \zeta_2\beta}{E^{m+1}},$$

with $\zeta_1 = \zeta_2 = 0$, and $N(\zeta_0) < (2E)^{3m+4}$.

It is straightforward to verify, through calculations similar to those in the proof of Lemma 3, that j respects differences on $G_{m+1}(\alpha, \beta)$, and that the restriction of j to $G_m(\alpha, \beta)$ respects sums, complex conjugates, and products. It is easy to verify that $j \upharpoonright G_m(\alpha, \beta)$ fixes all the values of the remainder functions $\mathrm{rem}_\xi(\zeta)$, $N(\xi) < M$.

It will follow, as in the proof of Lemma 3, that the restriction of j to $G_m(\alpha, \beta)$ respects the quotient functions, once we show that it respects the remainder functions. This in turn will follow once we show for all $\xi \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$, $N(\xi) < M$, and for all $\zeta \in G_{m+1}(\alpha, \beta)$,

$$\xi \mid \zeta \Longleftrightarrow \xi \mid j(\zeta).$$

So fix $\xi \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ with $N(\xi) < M$, and let $\zeta \in G_{m+1}(\alpha, \beta)$. Again using that $E^{m+2} \mid \beta$, we have that

$$\begin{aligned} \xi \mid \zeta = {} & \frac{\zeta_0 + \zeta_1\alpha + \zeta_2\beta}{E^{m+1}} \\ \Longleftrightarrow {} & \xi E^{m+1} \mid \zeta_0 + \zeta_1\alpha + \zeta_2\beta \\ \Longleftrightarrow {} & \xi E^{m+1} \mid \zeta_0 + \zeta_1\alpha + \zeta_2\beta + (\mu - 1)\zeta_2\beta = \zeta_0 + \zeta_1\alpha + \mu\zeta_2\beta \\ \Longleftrightarrow {} & \xi \mid \frac{\zeta_0 + \zeta_1\alpha + \mu\zeta_2\beta}{E^{m+1}} = j(\zeta). \quad \square \end{aligned}$$

Since $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ admits unique factorization, if $\pi \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ is a prime such that $\pi \mid \zeta^m$, for some non-zero $m \in \mathbb{N}$ and $\zeta \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$, then $\pi \mid \zeta$. This fact is used in the proof of the following Theorem.

Theorem 8. *There is an infinite set $\{(\alpha_k, \beta_k)\}_{k\in\mathbb{N}} \subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ such that if γ is a recursive program in the imaginary, norm-Euclidean quadratic algebra $\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})}$ that decides coprimality, then for all $k \in \mathbb{N}$,*

$$c_\gamma(\alpha_k, \beta_k) > \frac{1}{9\log_2 2E} \log_2 \max\{N(\alpha_k), N(\beta_k)\},$$

where E is defined as in (5).

Proof. For each $k \in \mathbb{N}$, let $\alpha_k = (E+1)^k$ and $\beta_k = E^{\lfloor \log_E 2N(\alpha_k)\rfloor+1}$, so that $N(\beta_k) = \max\{N(\alpha_k), N(\beta_k)\}$. Now, E and $E+1$ are coprime because $(E+1)-E = 1$, and so for every k, α_k is coprime to β_k. Suppose that γ decides coprimality in $\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})}$. Fix $k \in \mathbb{N}$, and let $(\alpha, \beta) = (\alpha_k, \beta_k)$. Let $m = c_\gamma(\alpha, \beta) > 0$, and suppose that $(2E)^{3m+8} < N(\alpha)$. Let j be an embedding as in the statement of Lemma 7 with $\mu = \alpha$.

Since γ decides coprimality,

$$\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})} \models \gamma(\alpha, \beta)^{(m)} = 1,$$

so by Absoluteness,

$$\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})} \restriction G_m(\alpha, \beta) \models \gamma(\alpha, \beta)^{(m)} = 1.$$

By the Embedding Lemma,

$$\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})} \models \gamma(j(\alpha), j(\beta))^{(m)} = 1,$$

which contradicts that γ decides coprimality, because $j(\alpha) = \alpha$ and $j(\beta) = \alpha\beta$ are not coprime. Thus $(2E)^{3m+8} \geq N(\alpha)$, and if we assume that $N(\alpha) > (2E)^{32}$, then, as in the proof of Theorem 4,

$$c_\gamma(\alpha, \beta) > \frac{1}{4}\log_{2E} N(\alpha).$$

A simple estimate yields $N(\beta) \leq 4E^2 N(\alpha)^2$, and so by a straightforward calculation,

$$\frac{1}{4}\log_{2E} N(\alpha) > \frac{1}{9}\log_{2E} N(\beta) = \frac{1}{9\log_2 2E}\log_2 N(\beta),$$

where we have used that $N(\beta) > N(\alpha) > (2E)^{18}$. The result follows once we delete a finite subset of $\{(\alpha_k, \beta_k)\}_{k\in\mathbb{N}}$ and re-index so that for all $k \in \mathbb{N}$, $N(\alpha_k) > (2E)^{32}$. □

Since a gcd algorithm in $\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})}$ decides coprimality by first computing a gcd and then checking in constant time whether it is a unit, Theorem 8 immediately gives the following.

Corollary 9. *If γ is a recursive program in an imaginary, norm-Euclidean quadratic algebra $\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})}$ that computes a gcd of its arguments, then*

$$c_\gamma(\zeta, \xi) = \Omega_\infty(\log\max\{N(\zeta), N(\xi)\}).$$

The real quadratic case is substantially different from the imaginary case in two important ways: (i) the unit group is infinite, and so there is no constant-time reduction of coprimality to gcd computation like the one used above, and (ii) the Galois conjugate in the real case is not the complex conjugate, and so the norm does not satisfy an inequality like (3). The proofs of the present paper therefore do not directly carry over to the real case, and it remains an open question whether the corresponding results hold.

5. Relevance for known algorithms

The complexity lower bound for gcd computation that appears in the statement of Corollary 9 applies to the large class of gcd algorithms which can be expressed as recursive programs in $\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})}$. We show in this section that known algorithms belong to this class, and have complexity that is quadratic in our lower bound.

We first consider the binary-like gcd algorithm from Weilert (2000), which computes a gcd in the Gaussian integers $\mathbb{Z}[\mathrm{i}] = \mathcal{O}_{\mathbb{Q}(\sqrt{-1})}$. It is easiest to understand in the following terms, where we write $\mathrm{i} = \sqrt{-1}$. If one of the arguments is 0, the algorithm outputs the other argument. If both arguments are non-zero, the algorithm extracts factors of the prime $(1+\mathrm{i})$ from both arguments until they are each relatively prime to $(1+\mathrm{i})$. When this stage is reached, the argument that is larger in norm is replaced with a certain difference, which is smaller in norm and divisible by $(1+\mathrm{i})$. The algorithm continues recursively, and terminates after finitely many steps because the norms of the arguments decrease in each stage. The strong similarity of this algorithm with the binary gcd algorithm for $\mathbb{Z}$ is evident.

This description is an oversimplification because the algorithm is optimized not to compute norms exactly, but only to compute them approximately. Specifically, when both arguments are relatively prime to $(1+\mathrm{i})$, the algorithm does not replace the argument that is larger in norm, but instead, replaces the argument which is approximately larger in norm. Suitable norm approximations suffice for the algorithm's correctness, and lead to a reduction in its complexity. The approximations are determined from the lengths of the arguments and the values of their most-significant bits, and these are complex values in our model. Consequently, we express the algorithm below in its non-optimized form, in which norms are computed exactly and compared in logtime. Norm computations and comparisons are complex; the authors of each of the binary-like gcd algorithms considered in this section use clever approximations, and the embeddings defined in Lemmas 3 and 7 do not respect norm comparisons.

Proposition 10 (Weilert, 2000). *There is a recursive program η in $\mathfrak{O}^5_{\mathbb{Q}(\sqrt{-1})}$ such that for all $\zeta, \xi \in \mathcal{O}_{\mathbb{Q}(\sqrt{-1})}$, $[\![\eta]\!](\zeta, \xi)$ is a gcd of ζ, ξ, and $c_\eta(\zeta, \xi) = O(\log^2 \max\{N(\zeta), N(\xi)\})$.*

Proof. Let η be the following recursive program in $\mathfrak{O}^5_{\mathbb{Q}(\sqrt{-1})}$.

$$\mathsf{p}(\zeta,\xi) = \begin{cases} \xi & \text{if } \zeta = 0, \\ \zeta & \text{if } \xi = 0, \\ (1+\mathrm{i})\mathsf{p}(\mathrm{quo}_{1+\mathrm{i}}(\zeta), \mathrm{quo}_{1+\mathrm{i}}(\xi)) & \text{if } \mathrm{rem}_{1+\mathrm{i}}(\zeta) = 0, \text{ and} \\ & \qquad \mathrm{rem}_{1+\mathrm{i}}(\xi) = 0, \\ \mathsf{p}(\mathrm{quo}_{1+\mathrm{i}}(\zeta), \xi) & \text{if } \mathrm{rem}_{1+\mathrm{i}}(\zeta) = 0, \text{ and} \\ & \qquad \mathrm{rem}_{1+\mathrm{i}}(\xi) \neq 0, \\ \mathsf{p}(\zeta, \mathrm{quo}_{1+\mathrm{i}}(\xi)) & \text{if } \mathrm{rem}_{1+\mathrm{i}}(\zeta) \neq 0, \text{ and} \\ & \qquad \mathrm{rem}_{1+\mathrm{i}}(\xi) = 0, \\ \mathsf{p}(\zeta - \varepsilon\xi, \xi) & \text{if } N(\xi) \leq N(\zeta) \text{ and } \varepsilon \in \mathcal{O}^\times_{\mathbb{Q}(\sqrt{-1})} \\ & \qquad \text{minimizes } N(\zeta - \varepsilon\xi), \\ \mathsf{p}(\zeta, \xi - \varepsilon\zeta) & \text{if } N(\zeta) < N(\xi) \text{ and } \varepsilon \in \mathcal{O}^\times_{\mathbb{Q}(\sqrt{-1})} \\ & \qquad \text{minimizes } N(\xi - \varepsilon\zeta). \end{cases}$$

Here, $M = 5$ is chosen to allow multiplication and division by $(1+\mathrm{i})$ and 2. As discussed above, multiplication and division by $(1+\mathrm{i})$ is central to the algorithm. Operations involving 2 are used to multiply algebraic integers – specifically ζ and $\overline{\zeta}$ to obtain $N(\zeta)$ – in logtime.

The correctness of η is established in Weilert (2000), and uses the fact that if $(1+\mathrm{i}) \nmid \zeta, \xi$, then $(1+\mathrm{i}) \mid (\zeta - \varepsilon\xi)$ for every $\varepsilon \in \mathcal{O}^\times_{\mathbb{Q}(\sqrt{-1})}$. To estimate the running time of the algorithm, notice that the norm of an argument is reduced by a factor of $N(1+\mathrm{i}) = 2$ at least as often as every other step. For the other steps, suppose that $N(\xi) \leq N(\zeta)$ and that $\varepsilon \in \mathcal{O}^\times_{\mathbb{Q}(\sqrt{-1})}$ minimizes $N(\zeta - \varepsilon\xi)$. A geometric argument in Weilert (2000) shows that $N(\zeta - \varepsilon\xi) < N(\zeta)$. Thus the number of steps is $O(\log \max\{N(\zeta), N(\xi)\})$.

Each step involves either removing a factor of $(1+\mathrm{i})$ from one or both arguments, or computing and comparing norms. The former can be done in constant time. For the latter, observe that norms can be computed in logtime by the familiar technique of multiplication by halving, and two natural numbers can be compared in logtime.[2] Hence $c_\eta(\zeta, \xi) = O(\log^2 \max\{N(\zeta), N(\xi)\})$. □

[2] In fact, if $\chi_{\mathbb{N}_<}(m, n)$ is the characteristic function of $<$ on $\mathbb{N}$, which is undefined for arguments $\notin \mathbb{N}$, then we can take $\chi_{\mathbb{N}_<}$ as a primitive operation and work in the expansion $(\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})}, \chi_{\mathbb{N}_<})$. It can be shown that all of the results about $\mathfrak{O}^M_{\mathbb{Q}(\sqrt{D})}$ obtained above also go through for this expansion, and so we get the same lower bounds when natural numbers can be compared in

The gcd algorithms of Agarwal and Frandsen (2004) and Damgård and Frandsen (2005) compute gcd's in $\mathfrak{D}^M_{\mathbb{Q}(\sqrt{D})}$ for small M and $D \in \{-2, -3, -7, -11\}$. They are similar in spirit to Weilert's algorithm above, and have the same asymptotic complexity.

6. Future work

The lower bound expressed by Theorem 8 is the best known, however it is an open question whether it is the best possible. In particular, it is unknown whether there is an $\Omega_\infty(\log^2 \max\{N(\zeta), N(\xi)\})$-lower bound for gcd computation in $\mathfrak{D}^M_{\mathbb{Q}(\sqrt{D})}$. Proving that one holds would imply the optimality of the binary-like algorithms, and likely would require a new technique, since the one used in the present paper does not seem to yield superlogarithmic lower bounds.

Another direction for future work involves proving lower bounds for the class of algorithms which use as primitive full multiplication and division, not simply multiplication and division by finitely-many algebraic integers. In the framework of this paper, this amounts to considering recursive programs in

$$\mathfrak{D}^{\div}_{\mathbb{Q}(\sqrt{D})} = (\mathcal{O}_{\mathbb{Q}(\sqrt{D})}, 0, 1, \times, +, -, \chi_=, \zeta \mapsto \overline{\zeta}, \mathrm{quo}(\zeta, \xi), \mathrm{rem}(\zeta, \xi)),$$

where × is multiplication, and $\mathrm{quo}(\zeta, \xi)$ and $\mathrm{rem}(\zeta, \xi)$ are respectively the quotient and remainder in a division of ζ by non-zero ξ. Proving lower bounds in this algebra is more difficult than in $\mathfrak{D}^M_{\mathbb{Q}(\sqrt{D})}$ because useful representations of the elements of finitely-generated subalgebras are more complex. No lower bounds are known for this structure, but related results likes those of van den Dries and Moschovakis (in press) suggest the following.

Conjecture 11. *There is a rational constant $r > 0$, and an infinite set $\{(\alpha_k, \beta_k)\}_{k \in \mathbb{N}} \subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ such that if γ is a recursive program in the imaginary, norm-Euclidean quadratic algebra $\mathfrak{D}^{\div}_{\mathbb{Q}(\sqrt{D})}$ that decides coprimality, then for all $k \in \mathbb{N}$,*

$$c_\gamma(\alpha_k, \beta_k) > r\sqrt{\log_2 \log_2 \max\{N(\alpha_k), N(\beta_k)\}}.$$

Acknowledgements

The main results of this paper come from a chapter of the author's doctoral dissertation (Busch, 2008) which was written in the UCLA Mathematics Department under the supervision of Yiannis N. Moschovakis. The author is very grateful to the anonymous referees for their many helpful remarks and suggestions.

References

Agarwal, S., Frandsen, G.S., 2004. Binary GCD like algorithms for some complex quadratic rings. In: Algorithmic Number Theory. In: Lecture Notes in Comput. Sci., vol. 3076. Springer, Berlin, pp. 57–71.

Busch, J., 2007. On the optimality of the binary algorithm for the Jacobi symbol. Fundamenta Informaticae 76 (1–2), 1–11.

Busch, J., 2008. Lower bounds in arithmetic complexity via asymmetric embeddings. Ph.D. Thesis, University of California, Los Angeles.

Coppersmith, D., Odlzyko, A.M., Schroeppel, R., 1986. Discrete logarithms in $\mathrm{GF}_{(p)}$. Algorithmica 1 (1), 1–15.

Damgård, I.B., Frandsen, G.S., 2005. Efficient algorithms for the gcd and cubic residuosity in the ring of Eisenstein integers. Journal of Symbolic Computation 39 (6), 643–652.

van den Dries, L., Moschovakis, Y.N., 2004. Is the euclidean algorithm optimal among its peers? Bulletin of Symbolic Logic 10 (3), 390–418.

van den Dries, L., Moschovakis, Y.N., 2008. Arithmetic complexity. ACM Transactions on Computational Logic (in press).

one step. This does nothing to improve the asymptotic complexity of the known binary-like gcd algorithms, and increases the conceptual complexity of the model of computation by introducing the *partial* algebra $(\mathfrak{D}^M_{\mathbb{Q}(\sqrt{D})}, \chi_{\mathbb{N}_<})$, which contains a function that diverges on some input values.

LaMacchia, B.A., Odlyzko, A.M., 1991. Computation of discrete logarithms in prime fields. Designs, Codes and Cryptography 1 (1), 47–62.

Mansoor, Y., Schieber, B., Tiwari, P., 1991a. A lower bound for integer greatest common divisor computations. Journal of the Association for Computing Machinery 38, 453–471.

Mansoor, Y., Schieber, B., Tiwari, P., 1991b. Lower bounds for computations with the floor operation. SIAM Journal on Computing 20, 315–327.

Meidânis, J., 1991. Lower bounds for arithmetic problems. Information Processing Letters 38, 83–87.

Moschovakis, Y.N., 2005. Recursion and complexity. In: Cooper, S.B., Löwe, B., Torenvliet, L. (Eds.), New Computational Paradigms: First Conference on Computability in Europe. CiE 2005, Amsterdam, The Netherlands, June 8–12, 2005, Proceedings. In: Springer Lecture Notes in Computer Science, vol. 3526/2005. pp. 350–357.

Stein, J., 1967. Computational problems associated with Racah algebra. Journal of Computational Physics 1, 397–405.

Stewart, I., Tall, D., 1987. Algebraic Number Theory, 2nd ed. In: Chapman and Hall Mathematics Series, Chapman & Hall, London.

Weilert, A., 2000. $(1+\mathrm{i})$-ary GCD computation in $\mathbf{Z}[\mathrm{i}]$ is an analogue to the binary GCD algorithm. Journal of Symbolic Computation 30 (5), 605–617.