MATIMYÁS MATEMATIKA
ISSN 0115-6926

Journal of the Mathematical Society of the Philippines
Vol. 41 No. 1 (2018) pp. 1-8

On the greatest common divisor in imaginary quadratic fields

Eric Anthony C. Arances
Institute of Mathematics
University of the Philippines Diliman
Quezon City, Philippines
eaarances@math.upd.edu.ph

Julius M. Basilla
Institute of Mathematics
University of the Philippines Diliman
Quezon City, Philippines
jbasilla@math.upd.edu.ph

Abstract

We present an algorithm that determines whether an ideal $\mathfrak{I}$ of the ring of integers $\mathfrak{O}_K$ of an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-d})$, where d is a positive squarefree integer, is principal or not. It is known that $\mathfrak{I}$ is generated over $\mathfrak{O}_K$ by at most two elements of $\mathfrak{O}_K$, say α and β so that $\mathfrak{I} = (\alpha, \beta)$. If $\mathfrak{I}$ is a principal ideal, then $\mathfrak{I} = (\gamma)$, for some $\gamma \in \mathfrak{O}_K$, which is also a greatest common divisor of α and β. And we compute this generator γ. The process is based on the algorithm of Cornacchia and appears to require minimal computations.

Keywords: greatest common divisor, principal ideal, quadratic number field

2010 MSC: Primary 11R04; Secondary 11Y40

1 Introduction

A number field K is a finite extension of $\mathbb{Q}$. Denote by $\mathfrak{O}_K$ its ring of integers. The ideal class group H_K of K is the quotient group J_K/P_K, where J_K and P_K are the groups of fractional ideals and principal ideals of K, respectively. H_K is known to be finite and $h_K := |H_K|$ is the class number K. The class number is a measure of how far $\mathfrak{O}_K$ is from being a principal ideal domain. In particular, $\mathfrak{O}_K$ is a principal ideal domain if and only if $h_K = 1$.

The ring $\mathfrak{O}_K$ is a Dedekind domain, hence any ideal $\mathfrak{I}$ of $\mathfrak{O}_K$ is generated by at most two elements, say $\mathfrak{I} = (\alpha, \beta) = \alpha\mathfrak{O}_K + \beta\mathfrak{O}_K$, where α, $\beta \in \mathfrak{O}_K$ (cf. [7], [2]). It is interesting to know if, given an ideal $\mathfrak{I} \subset \mathfrak{O}_K$, we can find $\gamma \in \mathfrak{O}_K$ such that $\mathfrak{I} = (\gamma)$. If $h_K = 1$, such a γ always exists. If $h_K > 1$, such a γ exists if and only if the ideal belongs to the trivial class of H_K. The algebraic integer γ is also a greatest common divisor of α and β. This paper addresses the said problem for imaginary quadratic fields $\mathbb{Q}(\sqrt{-d})$, where d is a positive squarefree integer.

2 Review of Related Literature

A Euclidean function on an integral domain R is a function $\phi : R \to \mathbb{N}$ with the property that for all $\alpha, \beta \in R$, $\beta \neq 0$, there exist γ, $\rho \in R$ such that $\alpha = \gamma\beta + \rho$ and either $\rho = 0$ or $\phi(\rho) < \phi(\beta)$. An integral domain R is said to be Euclidean if there exists a Euclidean function on R. By abuse of language, we say that a number field K is Euclidean if its ring of integers $\mathfrak{O}_K$ is Euclidean. Note that a Euclidean domain is also a principal ideal domain but not the other way around.

In a principal ideal domain, any ideal $\mathfrak{I} = (\gamma)$, for some $\gamma \in \mathfrak{O}_K$. For instance, the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-d})$, where d is a positive squarefree integer, has class number 1 if and only if

$$d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}.$$

But K is Euclidean if and only if $d = \{1, 2, 3, 7, 11\}$. The Euclidean function in these cases can be taken to be the field norm N (cf. [10]).

For the real quadratic fields, $K = \mathbb{Q}(\sqrt{d})$ is Euclidean with respect to the absolute value of the field norm if and only if

$$d \in \{2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}.$$

However, there are Euclidean real quadratic fields but not with respect to the absolute of the field norm. One such field is $\mathbb{Q}(\sqrt{69})$, as shown by D. Clark (cf. [4]).

In any quadratic ring $\mathfrak{O}_K$, a greatest common divisor (gcd) of two non-zero elements $\alpha, \beta \in \mathfrak{O}_K$ is an element $\gamma \in \mathfrak{O}_K$ such that

1. $\gamma \mid \alpha$ and $\gamma \mid \beta$,
2. if $\delta \in \mathfrak{O}_K \setminus \{0\}$ such that $\delta \mid \alpha$ and $\delta \mid \beta$, then $\delta \mid \gamma$.

In general, a gcd of two algebraic integers α and β may not exist. However, for principal ideal domains, $(\alpha, \beta) = (\gamma)$, if and only if $\gcd(\alpha, \beta) = \gamma$. For domains that are not principal ideal domains, we compute ideal gcd's.

In a Euclidean number field, with Euclidean function ϕ, the gcd γ of $\rho_0 := \alpha$ and $\rho_1 := \beta$ can be computed from the remainder sequence $\{\rho_i\}_{i=0}^{n-1}$ satisfying

$$\rho_{i+2} = \rho_i - \gamma_{i+1}\rho_{i+1},$$

where $\rho_i, \gamma_i \in \mathfrak{O}_K$, $\phi(\rho_1) > \phi(\rho_2) > \cdots > \phi(\rho_n) > 0$, and $\rho_{n+1} = 0$, for some $n \in \mathbb{N}$. In this case, $\gamma = \rho_n = \gcd(\alpha, \beta)$. If $K = \mathbb{Q}$, such sequence can be constructed explicitly for any α, $\beta \in \mathbb{Z}$, $\beta \neq 0$.

However, M. Harper showed that $\mathbb{Q}(\sqrt{14})$ is Euclidean using a criterion of Euclideanity by Motzkin (cf. [6]). No Euclidean function was explicitly defined. It is conjectured that there are infinitely many real quadratic fields with class number 1. And under the assumption of the generalized Riemann hypothesis, Weinberger showed that these number fields are Euclidean (cf. [12]). Thus, we need other methods of computing gcds.

An analog of the Euclidean algorithm was extended to the Gaussian integers (cf. [8]). The same algorithm can easily be extended to all Euclidean imaginary quadratic fields. Kaltofen and Rolletschek presented an algorithm to compute the gcd for any quadratic field, though the process looks difficult and not straightforward (cf. [9], [1]). Agarwal and Frandsen presented another algorithm based on the relationship between quadratic forms and ideals in quadratic rings (cf. [1]). In this paper, we present a simple algorithm in computing the gcd in an imaginary quadratic field, if such exists, which appears to require less computations.

3 The Algorithm

For the remainder of the paper, we always assume $K = \mathbb{Q}(\sqrt{-d})$, where d is a squarefree positive integer. Its ring of integers $\mathfrak{O}_K$ is

$$\mathfrak{O}_K = \mathbb{Z}[\omega] = \{a + b\omega \,:\, a, b \in \mathbb{Z}\},$$

where

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

Given an algebraic number $\alpha = r + s\sqrt{-d} \in K$, we denote by $R(\alpha) := r$ and $I(\alpha) := s$.

Let $\mathfrak{I}$ be an ideal of $\mathfrak{O}_K$. Since $\mathfrak{O}_K$ is a Dedekind domain, $\mathfrak{I}$ is generated (over $\mathfrak{O}_K$) by at most two elements of $\mathfrak{O}_K$. A module basis for $\mathfrak{I}$ can easily be computed (cf. [5]). In general, we can represent the ideal as

$$\mathfrak{I} = [a, b + c\omega],$$

where $a | N(b + c\omega)$, $c|a$, and $c|b$. Its norm is $N(\mathfrak{I}) = ac$.

The idea of the algorithm is inspired by Cornacchia's (cf. [5], [3]), which allows one to solve for an algebraic integer $\alpha \in \mathfrak{O}_K$ such that $N(\mathfrak{I}) = N(\alpha)$. However, for α to be a generator of $\mathfrak{I}$, we require the additional condition that $\alpha \in \mathfrak{I}$.

3.1 Main Result

We consider the different forms of $\mathfrak{O}_K = \mathbb{Z}[\omega]$.

Proposition 1. *Let $\mathfrak{I} = [a, b + c\sqrt{-d}]$ be a module of $\mathfrak{O}_K$, where $0 \le b < a$. Let $\alpha_0 = -a$, $\alpha_1 = b + c\sqrt{-d}$, and $\alpha_{i+2} = \alpha_i + q_i\alpha_{i+1}$, $q_i = \lfloor -R(\alpha_i)/R(\alpha_{i+1}) \rfloor$ for $0 \le i \le n-1$, where $R(\alpha_n) = \gcd(a, b)$, and $R(\alpha_{n+1}) = 0$. Let k be the integer such that $(R(\alpha_k))^2 < ac < (R(\alpha_{k-1}))^2$.*

If $\mathfrak{I}$ represents an ideal, then it is principal if and only if $d(I(\alpha_k))^2 < ac$. Moreover, if $\mathfrak{I}$ is principal, then α_k is a generator of $\mathfrak{I}$.

We begin the proof with two lemmas on the generators of an ideal as a lattice. Note that the norm of an ideal $\mathfrak{I}$ is $N(\mathfrak{I}) = \#(\mathfrak{O}_K/\mathfrak{I}) = [\mathfrak{O}_K : \mathfrak{I}]$, while the norm of an element $\gamma \in \mathfrak{O}_K$ is $N(\gamma) = \gamma\overline{\gamma}$.

Lemma 1. *Let $\mathfrak{I}$ be an ideal of $\mathfrak{O}_K$ and $\gamma \in \mathfrak{I}$. The ideal $\mathfrak{I} = (\gamma)$ if and only if $N(\mathfrak{I}) = N(\gamma)$.*

Proof: If $\mathfrak{I} = (\gamma)$, clearly $N(\mathfrak{I}) = N(\gamma)$. On the other hand, suppose $\gamma \in \mathfrak{I}$ such that $N(\mathfrak{I}) = N(\gamma)$, so that $(\gamma) \subset \mathfrak{I}$. By definition, $N(\mathfrak{I}) = [\mathfrak{O}_K : \mathfrak{I}]$, and $N(\gamma) = N((\gamma)) = [\mathfrak{O}_K : (\gamma)]$. Therefore,

$$[\mathfrak{O}_K : (\gamma)] = [\mathfrak{O}_K : \mathfrak{I}][\mathfrak{I} : (\gamma)] \Longrightarrow [\mathfrak{I} : (\gamma)] = 1.$$

Thus, $\mathfrak{I} = (\gamma)$. □

Lemma 2. *Let V be a two-dimensional vector space over $\mathbb{R}$. Let $\vec{u} = (u_1, u_2)$, $\vec{v} = (v_1, v_2) \in V$ be generators of a lattice L such that $u_2, v_2 \ge 0$, $|v_1| < |u_1|$, and $u_1 v_1 < 0$. The lattice vector $\vec{w} = (w_1, w_2)$ with the least w_2 such that $w_2 > 0$ and $|w_1| < |v_1|$ is given by $\vec{w} = \vec{u} + q\vec{v}$, where $q = \lfloor -u_1/v_1 \rfloor$. Moreover, the vectors $\vec{v}$ and $\vec{w}$ generate the same lattice as the vectors $\vec{u}$ and $\vec{v}$.*

Proof: Without loss of generality, assume $0 < v_1 < -u_1$ so that $-\frac{u_1}{v_1} > 1$. Let $\vec{w} = a\vec{u} + b\vec{v} \in L$, a, $b \in \mathbb{Z}$ such that $au_2 + bv_2 > 0$ and $|au_1 + bv_1| < v_1$.

If $a \leq 0$, $b \leq 0$, then $au_2 + bv_2 \leq 0$. If $a \leq 0$, $b > 0$, then $au_1 + bv_1 > v_1$. Both of these contradict the properties of $\vec{w}$.

Therefore, $a > 0$ so that

$$\begin{aligned} -v_1 < au_1 + bv_1 < v_1 \\ -v_1 - au_1 < bv_1 < v_1 - au_1 \\ -1 + a\Big(-\frac{u_1}{v_1}\Big) < b < 1 + a\Big(-\frac{u_1}{v_1}\Big). \end{aligned}$$

Note that $-1 + a < -1 + a\,(-u_1/v_1)$. To minimize $au_2 + bv_2$, we take $a = 1$ and $b = \lfloor -u_1/v_1 \rfloor$. □

The idea of the proof is similar to that in [11]. Lemma (2) will answer the ideal membership problem.

Note that $\mathfrak{I} = [a, b + c\sqrt{-d}] = [-a, b + c\sqrt{-d}]$. Also, we can view $\mathfrak{I}$ as a lattice generated by $-a$ and $b + c\sqrt{d}$.

Construct the sequence $\{\alpha_i\}$ as in Proposition (1). Lemma (2) tells us that $\{|R(\alpha_i)|\}$ is a decreasing sequence and $\{I(\alpha_i)\}$ is an increasing sequence. Since $\alpha_i \in \mathfrak{I}$ for $0 \leq i \leq n+1$, then $(\alpha_i) \subset \mathfrak{I}$ so that $N(\mathfrak{I})|N(\alpha_i)$. That is, $N(\alpha_i) \equiv 0 \pmod{ac}$.

Suppose that $\mathfrak{I}$ is an ideal that is principal, say $\mathfrak{I} = (\gamma)$, so that $N(\gamma) = ac$. And $(R(\gamma))^2 \leq (R(\gamma))^2 + d(I(\gamma))^2 = ac < (R(\alpha_{k-1}))^2$. Therefore, $|R(\gamma)| < |R(\alpha_{k-1})|$.

By repeatedly applying Lemma (2) to $\mathfrak{I} = [\alpha_0, \alpha_1]$, one can arrive at $[\alpha_{k-1}, \alpha_k]$ as a module basis for $\mathfrak{I}$, where $\alpha_k \in \mathfrak{I}$ has the least value of $I(\alpha_i)$, among all the α_i s, such that $(R(\alpha_i))^2 < ac < (R(\alpha_{k-1}))^2$.

Since $|R(\gamma)| < |R(\alpha_{k-1})|$, it follows that $I(\alpha_k) \leq I(\gamma)$. Therefore, $d(I(\alpha_k))^2 \leq d(I(\gamma))^2 < ac$.

On the other hand, suppose $d(I(\alpha_k))^2 < ac$. Since $N(\alpha_k) = (R(\alpha_k))^2 + d(I(\alpha_k))^2 \equiv 0 \pmod{ac}$ and $(R(\alpha_k))^2 < ac$, then $N(\alpha_k) = ac$ so that Lemma (1) tells us that $\mathfrak{I} = (\alpha_k)$. This proves Proposition (1).

If $-d \equiv 2, 3 \pmod 4$, an ideal of $\mathfrak{O}_K$ has the form $[a, b + c\sqrt{d}]$ and Proposition (1) can be applied.

We will now consider the case of $\mathfrak{O}_K$, where $-d \equiv 1 \pmod 4$.

Proposition 2. *Let $\mathfrak{I} = [a, b + c\omega]$ be an ideal of $\mathfrak{O}_K$, where $0 \leq b < a$. Let $\alpha_0 = -2a$, $\alpha_1 = 2b + c + c\sqrt{-d}$, and $\alpha_{i+2} = \alpha_i - q_i\alpha_{i+1}$, $q_i = \lfloor -R(\alpha_i)/R(\alpha_{i+1}) \rfloor$ for $0 \leq i \leq n-1$, where $R(\alpha_n) = \gcd(2a, 2b+c)$, and $R(\alpha_{n+1}) = 0$. Let k be the integer such that $(R(\alpha_k))^2 < 4ac < (R(\alpha_{k-1}))^2$.*

The ideal $\mathfrak{I}$ is a principal ideal if and only if $d(I(\alpha_k))^2 < 4ac$. Moreover, if $\mathfrak{I}$ is principal, then $\frac{1}{2}\alpha_k$ is a generator of $\mathfrak{I}$.

Proof: Let $\mathfrak{I} = [a, b + c\omega]$ be an ideal of $\mathfrak{O}_K$. Note that $N(\mathfrak{I}) = ac$.

We will apply Proposition (1) to the ideal $2\mathfrak{I} = [2a, 2b + c + c\sqrt{-d}]$ to determine whether it is principal or not. If $2\mathfrak{I}$ is not principal, then $\mathfrak{I}$ is not principal. The first part of the result of the proposition then follows.

Suppose $2\mathfrak{I}$ is principal, so that $2\mathfrak{I} = (\alpha_k)$ and $4ac = N(2\mathfrak{I}) = N(\alpha_k)$. Thus, for some

$m, n \in \mathbb{Z}$,

$$\begin{aligned}
\alpha_k &= 2am + (2b + c + c\sqrt{-d})n \\
\frac{1}{2}\alpha_k &= \frac{1}{2}\Big(2am + (2b + c + c\sqrt{-d})n\Big) \\
&= am + \Big(b + c\Big(\frac{1+\sqrt{-d}}{2}\Big)\Big)n \\
&= am + (b + c\omega)n \in \mathfrak{I}
\end{aligned}$$

Note that $ac = N(\mathfrak{I}) = \frac{1}{4}N(\alpha_k) = \left(\frac{1}{2}\alpha_k\right)\left(\frac{1}{2}\overline{\alpha_k}\right) = N\left(\frac{1}{2}\alpha_k\right)$. Thus, $\mathfrak{I} = \left(\frac{1}{2}\alpha_k\right)$.

3.2 Examples

We now illustrate the algorithm through the following examples.

Example 1. *Let $K = \mathbb{Q}(\sqrt{-21})$, which is not a principal ideal domain. The ring of integers of K is $\mathfrak{O}_K = \mathbb{Z}(\sqrt{-21})$.*

Let $\mathfrak{I} = (\alpha, \beta)$, where $\alpha = -2576 + 343\sqrt{-21}$ and $\beta = -1596 + 227\sqrt{-21}$.

A module basis for $\mathfrak{I}$ is $[217, 14 + \sqrt{-21}]$ so that $N(\mathfrak{I}) = 217$. The sequence $\{\alpha_i\}$ is

$$\begin{aligned}
\alpha_0 &= -217 \\
\alpha_1 &= 14 + \sqrt{-21}
\end{aligned}$$

with $(R(\alpha_1))^2 = 14^2 = 196 < N(\mathfrak{I})$. Also, $d(I(\alpha_1))^2 = 21 < N(\mathfrak{I})$. Thus, the ideal is principal, and is generated by $\alpha = 14 + \sqrt{-21} = \gcd(\alpha, \beta)$.

Example 2. *Let $K = \mathbb{Q}(\sqrt{-21})$. Let the ideal $\mathfrak{I} = (\alpha, \beta)$, where $\alpha = -1032 + 1146\sqrt{-21}$ and $\beta = 6690 - 1395\sqrt{-21}$.*

A module basis for $\mathfrak{I}$ is $[103785, 21189 + 3\sqrt{-21}]$ so that $N(\mathfrak{I}) = 103785(3) = 311355$. The sequence $\{\alpha_i\}$ is

$$\begin{aligned}
\alpha_0 &= -103785 \\
\alpha_1 &= 21189 + 3\sqrt{-21} \\
\alpha_2 &= -19029 + 12\sqrt{-21} \\
\alpha_3 &= 2160 + 15\sqrt{-21} \\
\alpha_4 &= -1749 + 132\sqrt{-21} \\
\alpha_5 &= 411 + 147\sqrt{-21}
\end{aligned}$$

with $(R(\alpha_5))^2 = 411^2 = 168921 < N(\mathfrak{I}) < (R(\alpha_4))^2$. But $d(I(\alpha_5))^2 = 453789 > N(\mathfrak{I})$. Thus, the ideal is not principal.

Example 3. *Let $K = \mathbb{Q}(\sqrt{-11})$, which is a principal ideal domain. The ring of integers of K is $\mathfrak{O}_K = \mathbb{Z}(\omega)$ where $\omega = \frac{1}{2}(1 + \sqrt{-11})$.*

Let $\mathfrak{I} = [12885, 339 + 3\omega]$, with $N(\mathfrak{I}) = 38665$. The sequence $\{\alpha_i\}$ is

$$\begin{aligned}
\alpha_0 &= -25770 \\
\alpha_1 &= 681 + 3\sqrt{-11} \\
\alpha_2 &= -573 + 111\sqrt{-11} \\
\alpha_3 &= 108 + 114\sqrt{-11}
\end{aligned}$$

with $(R(\alpha_3))^2 = 11664 < 154620 = 4N(\mathfrak{I}) < (R(\alpha_2))^2$. *Being a principal ideal domain, the generator of* $\mathfrak{I}$ *is* $\frac{1}{2}\alpha_3 = 54 + 57\sqrt{-11} = -3 + 114\omega$ *and* $\gcd(12885, 339 + 3\omega) = -3 + 114\omega$. *Note that* $d(I(\alpha_3))^2 = 142956 < 4N(\mathfrak{I})$.

Example 4. *Let* $K = \mathbb{Q}(\sqrt{-15})$, *which is not a principal ideal domain. The ring of integers of* K *is* $\mathfrak{O}_K = \mathbb{Z}(\omega)$ *where* $\omega = \frac{1}{2}(1 + \sqrt{-15})$.

Let $\mathfrak{I} = (\alpha, \beta)$, *where* $\alpha = 4184 + 2072\omega$ *and* $\beta = 5180 + 2420\omega$. *A module basis for* I *is* $[50640, 38428 + 4\omega]$, *with* $N(\mathfrak{I}) = 202560$. *The sequence* $\{\alpha_i\}$ *is*

$$\begin{aligned}
\alpha_0 &= -101280 \\
\alpha_1 &= 76860 + 4\sqrt{-15} \\
\alpha_2 &= -24420 + 4\sqrt{-15} \\
\alpha_3 &= 3600 + 16\sqrt{-15} \\
\alpha_4 &= -2820 + 100\sqrt{-15} \\
\alpha_5 &= 780 + 116\sqrt{-15}
\end{aligned}$$

with $(R(\alpha_5))^2 = 608400 < 4N(\mathfrak{I}) < (R(\alpha_4))^2$. *Now,* $d(I(\alpha_5))^2 = 201840 < 4N(\mathfrak{I})$, *so that the ideal is principal and*

$$\gcd(4184 + 2072\omega, 5180 + 2420\omega) = \tfrac{1}{2}\alpha_5 = 390 + 58\sqrt{-15} = 332 + 116\omega.$$

Example 5. *Let* $K = \mathbb{Q}(\sqrt{-23})$, *which is not a principal ideal domain. The ring of integers of* K *is* $\mathfrak{O}_K = \mathbb{Z}(\omega)$ *where* $\omega = \frac{1}{2}(1 + \sqrt{-23})$.

Let $\mathfrak{I} = [3627, 147 + \omega]$, *with* $N(\mathfrak{I}) = 3627$. *The sequence* $\{\alpha_i\}$ *is*

$$\begin{aligned}
\alpha_0 &= -7254 \\
\alpha_1 &= 295 + \sqrt{-23} \\
\alpha_2 &= -174 + 24\sqrt{-23} \\
\alpha_3 &= 121 + 25\sqrt{-23} \\
\alpha_4 &= -53 + 49\sqrt{-23}
\end{aligned}$$

with $(R(\alpha_4))^2 < 14508 = 4N(\mathfrak{I}) < (R(\alpha_3))^2$. *Since* $d(I(\alpha_4))^2 = 55223 > 14508$, *the ideal is not principal.*

4 References

[1] S. Agarwal and G.S. Frandsen. *A new GCD algorithm for quadratic number rings with unique factorization.* Lecture Notes in Comput. Sci., 3887, Springer, Berlin, 2006.

[2] S. Alaca and K.S. Williams. *Introductory Algebraic Number Theory.* Cambridge University Press, Cambridge, 2004.

[3] J.M. Basilla. *On the solution of* $x^2 + dy^2 = m$. Proc. Japan Acad. Ser. A. Math. Sci. **80** (2004), no. 5, 40–41.

[4] D.A. Clark. *A quadratic field which is Euclidean but not norm-Euclidean*, Manuscripta Math. **83** (1994), no. 3–4, 327–330.

[5] H. Cohen. *A Course in Computational Algebraic Number Theory*. Graduate Texts in Mathematics, 138. Springer-Verlag, Berlin, 1993.

[6] M. Harper. $\mathbb{Z}[\sqrt{14}]$ *is Euclidean*, Canad. J. Math. **56** (2004), no. 1, 55–70.

[7] D. Hilbert. *The Theory of Algebraic Number Fields [Translated from German by I.A. Adamson. With an Introduction by F. Lemmermeyer and N. Schappacher]*. Springer-Verlag, Berlin, 1998.

[8] K. Ireland and M. Rosen. *A Classical Introduction to Modern Number Theory*. Second edition. Graduate Texts in Mathematics, 84. Springer-Verlag, New York, 1990.

[9] E. Kaltofen and H. Rolletschek. *Computing greatest common divisors and factorizations in quadratic number fields*. Math. Comp. **53** (1989), no. 188, 697–720.

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

[11] H. Wada. *A note on the Pell equation*. Tokyo J. Math. **2** (1979), no. 1, 133–136.

[12] P. Weinberger. *On Euclidean rings of algebraic integers*. Proc. Sympos. Pure Math. Vol. 24 (1973), 321–332.

This page is intentionally left blank