Gauss bounds of quadratic extensions

By FRANZ LEMMERMEYER (Saarbrücken)

Abstract. We give a simple proof of results of Lubelski and Lakein on Gauss bounds for quadratic extensions of imaginary quadratic Euclidean number fields.

1. Preliminaries

Let $k$ be a number field with class number 1; in the following, $N$ will denote the absolute value of the norm, i.e. $N\alpha = |N_{k/Q}\alpha|$. We define the Euclidean minimum $M(k)$ by $M(k) = \inf \{ \delta > 0 : \forall \xi \in k \exists \eta \in \mathbb{Z}_k \text{ such that } N(\xi - \eta) < 1 \}$. An ideal $I$ in the maximal order $\mathbb{Z}_K$ of a quadratic extension $K/k$ is called primitive if it is not divisible by any non-unit $a \in \mathbb{Z}_k$. Since $h(k) = 1$, there exists a relative integral basis $\{1, \omega\}$ of $\mathbb{Z}_K$.

The following lemma and its proof are well known for $k = \mathbb{Q}$ ([2], 14.12):

Lemma 1. Let $k$ be a number field with class number 1, and suppose that $K/k$ is a quadratic extension. Then every primitive ideal $I$ has the form $I = (\alpha + c\omega)\mathbb{Z}_k + c\mathbb{Z}_k$ for algebraic integers $\alpha, c \in \mathbb{Z}_k$, where $c$ is a generator of the ideal $c\mathbb{Z}_K = N_{K/k}I$.

Proof. Choose $\alpha = a + b\omega$ such that $I = (\alpha, c)$ (cf. [2], 6.19). Writing $c\omega \in I$ as a linear combination of $a + b\omega$ and $c$ shows easily that $b | a$ and $b | c$. Since $I$ is primitive, $b$ must be a unit, and we may assume without loss of generality that $b = 1$. \qed

Mathematics Subject Classification: 11 R 11, 11 R 16, 11 R 29.
Key words and phrases: Quadratic Fields, Ideal Classes, Discriminants.
2. Quadratic number fields

The following theorem is well known (see e.g. Holzer [3]); we will give a very simple proof which we will generalize in the next section.

**Theorem 2.** Let \( K = \mathbb{Q}(\sqrt{m}) \) be a quadratic number field with ring of integers \( \mathbb{Z}_K = \mathbb{Z}[\omega] \) and discriminant \( \Delta \), where

\[
\begin{align*}
\omega &= \begin{cases} 
\sqrt{m}, & \text{if } m \equiv 2, 3 \mod 4, \\
\frac{1 + \sqrt{m}}{2}, & \text{if } m \equiv 1 \mod 4.
\end{cases} \\
\Delta &= \begin{cases} 
4m, & \text{if } m \equiv 2, 3 \mod 4, \\
m, & \text{if } m \equiv 1 \mod 4.
\end{cases}
\end{align*}
\]

Let \( \mu_K \) be defined by

\[
\mu_K = \begin{cases} 
1, & \text{if } \Delta = 5 \\
\sqrt{\Delta}/8, & \text{if } \Delta \geq 8 \\
\sqrt{-\Delta/3}, & \text{if } \Delta < 0.
\end{cases}
\]

Then each ideal class of \( K \) contains an integral ideal of norm \( \leq \mu_K \).

**Proof.** Let \([I]\) be an ideal class generated by an integral ideal \( I \) which we may assume to be primitive. Then \( I = (\gamma, c) = N_{K/\mathbb{Q}}I \) and \( \gamma = a + \omega = s + \frac{1}{2}\sqrt{\Delta} \), where \( 2s \in \mathbb{Z} \). Applying the Euclidean algorithm to the pair \((s, c)\) we see that there exists a \( \gamma = r + \frac{1}{2}\sqrt{\Delta} \in I \) such that

\[
\begin{align*}
|r| &\leq \frac{c}{2} \quad \text{if } \Delta < 0, \\
\frac{c}{2} &\leq |r| \leq c \quad \text{if } c^2 > \frac{\Delta}{5}, \\
c &\leq |r| \leq \frac{3}{2}c \quad \text{if } \frac{\Delta}{8} < c^2 < \frac{\Delta}{5}.
\end{align*}
\]

We claim that \( |N\gamma| \leq \frac{1}{2}(c^2 - \Delta) < c^2 \) provided that \( c^2 > \mu_K \); this shows that \( I_1 = \gamma'c^{-1}I \sim I \) (where \( \gamma' \) denotes the algebraic conjugate of \( \gamma \)) is an integral ideal such that \( [I_1] = [I] \) and \( NI_1 < NI \). Repeating this procedure if necessary we eventually arrive at an integral ideal \( I_n \sim I \) with norm \( \leq \mu_K \).

The claimed inequality is proved by going through all the cases:

1. \( \Delta < 0 \): here \( |N\gamma| = |r^2 - \frac{\Delta}{4}| \leq \frac{c^2 + |\Delta|}{4} < 1 \) since \( c^2 > \mu_K = |\Delta|/3 \).
2. \( c^2 > \frac{\Delta}{5} \): here \( -c^2 = \frac{c^2 - 5c^2}{4} < r^2 - \frac{\Delta}{4} < c^2 \).
3. \( \frac{\Delta}{8} < c^2 < \frac{\Delta}{5} \): then \( -c^2 = c^2 - \frac{8c^2}{4} < r^2 - \frac{\Delta}{4} < \frac{9c^2 - 5c^2}{4} = c^2 \).
The only possibility not covered by the proof is \( c^2 = \Delta/5 \); since the odd part of \( \Delta \) is squarefree, this will happen if and only if \( \Delta = 5 \) and \( c = \pm 1 \). This completes the proof of the theorem. \( \square \)

### 3.2. Quadratic extensions of imaginary quadratic fields

Let \( k = \mathbb{Q}(\sqrt{-n}) \), where \( n \in \{-1, -2, -3, -7, -11\} \). These are the Euclidean among the imaginary quadratic fields, and it is known (cf. [5]) that for all \( \xi \in k \) there exist integers \( \eta \in \mathbb{Z}_k \) such that
\[
N(\xi - \eta) \leq M,
\]
where the Euclidean minimum \( M = M(k) \) is given by
\[
M = \begin{cases} 
\frac{|n| + 1}{4}, & \text{if } \Delta \equiv 0 \mod 4, \\
\frac{(|n| + 1)^2}{16|n|}, & \text{if } \Delta \equiv 1 \mod 4.
\end{cases}
\]

Fix an embedding of \( k \) into \( \mathbb{C} \); then \( N\xi = |\xi|^2 \) for all \( \xi \in k \), and the above result translates into

**Lemma 3.** Let \( k = \mathbb{Q}(\sqrt{-n}) \) be Euclidean; then for all \( \xi \in k \) there exist \( \eta \in \mathbb{Z}_k \) such that \( |\xi - \eta|^2 \leq M \).

Now we redo our computations in the proof of Theorem 1, assuming \( a, c, m, \) etc. to be integers (resp. half-integers) in \( k \); the discriminant \( \Delta \) is now replaced by the relative discriminant \( d = \text{disc}_{K/k}(1, \omega) \), and we have
\[
\Delta = \text{disc}(K/\mathbb{Q}) = d_0^2 N d, \quad \text{where } d_0 = \text{disc}(k/\mathbb{Q}).
\]

Now
\[
\frac{|r^2 - d/4|}{|c|^2} \leq \frac{4|\xi|^2 + |d|}{4|c|^2} \leq \frac{4M|c|^2 + |d|}{4|c|^2},
\]
and this expression is \(< 1\) if and only if

\[
|c|^2 > \frac{|d|}{4(1 - M)} = \frac{\sqrt{\Delta}}{4d_0(1 - M)}.
\]

For \( k = \mathbb{Q}(\sqrt{-1}) \) we have \( M(k) = \frac{1}{2} \) and \( d_0 = -4 \), hence \( \mu_K = \sqrt{\Delta}/8 \). Evaluating (1) for the other fields gives

**Theorem 4.** Let \( k = \mathbb{Q}(\sqrt{-n}) \) be Euclidean, and let \( K/k \) be a quadratic extension with absolute discriminant \( \Delta \). Then every ideal class of \( K \) contains an integral ideal of norm \( \leq \mu_K \), where
\[
\mu_K = \frac{\sqrt{\Delta}}{4d_0(1 - M)} = \begin{cases} 
\sqrt{\Delta}/8, & \text{if } n \in \{-1, -2, -3, -11\}; \\
\sqrt{\Delta}/12, & \text{if } n = -7.
\end{cases}
\]
These are exactly the bounds given by Lakein [4]; another proof is due to Mordell [7]. The result in the special case $k = \mathbb{Q}(\sqrt{-1})$ was already known to S. Kuroda and J. A. Nyman (cf. [4]). After the completion of this article I discovered that S. Lubelsky (in his posthumously published paper [6]) had already found the formula connecting the bounds given in Theorem 2 with the Euclidean minima of imaginary quadratic number fields; his results remained unnoticed, probably because he used the language of quadratic forms.

In [1], Robin Chapman has generalized Theorem 2 to quadratic extensions of imaginary quadratic fields with class number 1.

Acknowledgement. I would like to thank Sachar Paulus, Felicity George, and Chris Smyth for some helpful discussions on Euclidean-like algorithms in quadratic number fields from which this note originated, and Robin Chapman for considerably simplifying the proofs. I also thank the referee for his careful reading of the manuscript.

References


FRANZ LEMMERMEYER
UNIVERSITÄT DES SAARLANDES
FB 14 INFORMATIK
D–66041 SAARBRÜCKEN
GERMANY
E-MAIL: lemmermf@cs.uni-sb.de

(Received August 6, 1996)