ON FUNDAMENTAL UNITS OF CLASS NUMBER ONE 
QUADRATIC FIELDS 

ANDREJ DUJELLA AND FLORIAN LUCA 

Abstract. In this paper, we give a nontrivial lower bound for the 
fundamental unit of norm $-1$ of a real quadratic field of class num-
ber 1. As a corollary, we find parametric families of real quadratic 
fields of class number larger than 1. 

1. Introduction 

Throughout this note, $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ is a real quadratic field. Here, 
$d > 1$ is a squarefree positive integer. We let $\mathcal{O}_K$ be the ring of algebraic 
integers in $\mathbb{K}$ and $\zeta_K = \frac{U + \sqrt{\Delta_K}}{2}$ be a fundamental unit (the smallest unit 
$> 1$). We assume that $\zeta_K$ has norm $-1$. We then have the following 
theorem. In what follows we use the Vinogradov symbols $\asymp$ and $\ll$ and 
the Landau symbols $O$ and $o$ with their regular meaning. 

Theorem 1.1. Let $d > 2$. Assume that $d$ and $U$ are not both odd. If $\mathbb{K}$ 
has class number 1, then 

$$\zeta_K \asymp 2^{-1/3} \Delta_K^{2/3},$$

where $\Delta_K$ is the discriminant of $\mathbb{K}$. 

Before proving our result and giving some applications, let us first 
see that it is nontrivial. Indeed, writing 

$$\zeta_K = \frac{u + v\sqrt{\Delta_K}}{2}$$

for some positive integers $u$, $v$, we see that the trivial inequality is 
$\zeta_K \gg \Delta_K^{1/2}$. The reverse inequality, namely 

$$\zeta_K \ll \Delta_K^{1/2}$$

also holds for infinitely many $\mathbb{K}$. Indeed it holds for those ones for 
which $\Delta_K$ is a squarefree integer of the form $a^2 + 1$ (or $a^2 + 4$, or more 
generally $(ak)^2 + 4k$, $k$ odd) for some integer $a$. However, by results 
of Biró [1, 2] and Biró and Lapkova [3], there are only finitely many 
such real quadratic number fields of class number 1. Furthermore, a
well-known conjecture in analytic number theory asserts that writing $h_K$ for the class number of $K$, the estimate
\[ h_K \log \zeta_K \gg \Delta_K^{1/2} \]
should hold. In particular, if there are infinitely many real quadratic fields of class number 1 (a conjecture of Gauss), then for such fields $K$, $\zeta_K$ should be at least as large as $\exp(c_0 \Delta_K^{1/2})$ for some absolute constant $c_0$. In particular, we see that our Theorem 1.1 is a modest contribution in this direction.

In Section 3, we give an application of our general result to a concrete parametric family of quadratic fields.

2. The proof of Theorem 1.1

We treat in detail the case when $d$ is even and we shall only sketch the case when $d$ is odd. Since $d$ is even, $\Delta_K = 4d$, and $O_K = \mathbb{Z} + \mathbb{Z}\sqrt{d}$. We write
\[ \zeta_K = U + \sqrt{d}V, \]
where
\[ (2.1) \quad U^2 - dV^2 = -1. \]
Since $d$ is even, it follows that $U$ is odd. Let $p$ be any prime divisor of $U$. Equation (2.1) reduced modulo $p$ shows that $\left( \frac{d}{p} \right) = 1$, where we use $\left( \frac{\cdot}{p} \right)$ for the Legendre symbol with respect to $p$. Since the above equality holds for all prime factors $p$ of $U$, it follows that $U$ splits completely in $K$. Since $K$ has class number 1 and a unit of norm $-1$, it follows that the Diophantine equation
\[ (2.2) \quad x^2 - dy^2 = U \]
has at least one (hence, infinitely many) positive integer solutions $(x, y)$ with $x$ and $y$ coprime. Let $(x, y)$ be such a solution. Put $V_2 = V/\gcd(y, V)$ and $y_1 = y/\gcd(y, V)$. Multiplying both sides of equation (2.2) by $V_2^2$ we get
\[ (2.3) \quad (xV_2)^2 - (dV_2^2)y_1^2 = UV_2^2. \]
Let $D = dV_2$ and note that $D = U^2 + 1$. Thus, equation (2.3) is of the form
\[ (2.4) \quad X^2 - DY^2 = UV_2^2, \]
where $X = xV_2$, $Y = y_1$ are coprime and may be assumed arbitrarily large. Equation (2.4) can be rewritten as

\begin{equation}
(2.5) \quad \left| \frac{X}{Y} - \sqrt{D} \right| = \frac{UV_2^2}{Y^2(X/Y + \sqrt{D})} = \frac{1}{Y^2} \left( \frac{1}{2\sqrt{D}} + o(1) \right) UV_2^2
\end{equation}

as $X \to \infty$. We use the fact that $\sqrt{D} = \sqrt{U^2 + 1} > U$, choose $\varepsilon > 0$ sufficiently small such that

\begin{equation}
\left( \frac{1}{2\sqrt{D}} + \varepsilon \right) UV_2^2 < \frac{V_2^2 + 1}{2}
\end{equation}

holds, then choose $X$ and $Y$ sufficiently large so that the amount indicated by $o(1)$ in (2.5) is in absolute value smaller than $\varepsilon$, to conclude that if we put

\begin{equation}
(2.6) \quad K = \frac{V_2^2 + 1}{2},
\end{equation}

then

\begin{equation}
(2.7) \quad \left| \frac{X}{Y} - \sqrt{D} \right| < \frac{K}{Y^2}.
\end{equation}

By results of Dujella [4] and Worley [6], there exist integers $n$, $r$, $s$ with $r$ positive and $r|s| < 2K = V_2^2 + 1$ such that $X = r p_n + sp_{n-1}$ and $Y = r q_n + sq_{n-1}$. Here, $p_k/q_k$ is the $k$th convergent to $\sqrt{D} = \sqrt{U^2 + 1}$. With these values for $X$ and $Y$ we have

\begin{equation}
(2.8) \quad UV_2^2 = X^2 - DY^2 = (r p_n + sp_{n-1})^2 - D(r q_n + sq_{n-1})^2
\end{equation}

It is easy to prove that

\begin{equation}
(2.9) \quad p_n = \frac{\alpha^{n+1} + \beta^{n+1}}{2} \quad \text{and} \quad q_n = \frac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta}
\end{equation}

hold for all $n \geq 0$, where

\begin{equation}
(\alpha, \beta) = (U + \sqrt{U^2 + 1}, U - \sqrt{U^2 + 1}).
\end{equation}

Using (2.9), one checks that

\begin{equation}
p_n^2 - Dq_n^2 = (-1)^{n+1} \quad \text{and} \quad p_n p_{n-1} - Dq_n q_{n-1} = (-1)^n 2U
\end{equation}

hold for all $n \geq 0$. Thus, relation (2.8) is

\begin{equation}
UV_2^2 = (-1)^n (s^2 - r^2 + 2rsU)
\end{equation}

(see also [5, Lemma 1]). In particular, $r^2 \equiv s^2 \pmod{U}$. If $r^2 = s^2$, we then get $UV_2^2 = \pm 2r^2 U$, therefore $2r^2 = \pm V_2^2$, which does not have
an integer solution $r$. Thus, $r^2 \neq s^2$, which together with the fact that $r^2 \equiv s^2 \pmod{U}$ shows that $\max\{r, |s|\} \geq (U + 1)^{1/2}$. In particular,

$$(U + 1)^{1/2} \leq \max\{r, |s|\} \leq r|s| \leq V_2^2,$$

therefore $V \geq V_2 \geq (U + 1)^{1/4}$. Since $\sqrt{dV} = \sqrt{U^2 + 1}$, we get $\sqrt{U^2 + 1} \geq \sqrt{dV} \geq \sqrt{d(U + 1)^{1/4}}$. We have $U > 1$ since $d > 2$. Hence, $d^2 \leq \frac{U^4 + 2U^2 + 1}{U + 1} < U^3$. Since $\zeta_K > 2U$, we get

$$\zeta_K > 2d^{2/3} = 2^{-1/3}\Delta_K^{2/3}.$$ 

We now sketch the proof of the remaining cases. Assume that $d$ is odd. It is clear that every prime factor of $d$ is congruent to 1 modulo 4, therefore $\Delta_K = d$ and $\{1, (1 + \sqrt{d})/2\}$ is a basis for $O_K$. Write

$$\zeta_K = \frac{U + \sqrt{dV}}{2}.$$ 

Assume that $U$ is even. Write $U = 2U_1$, $V = 2V_1$ and then

$$U_1^2 - dV_1^2 = -1. \quad (2.10)$$

If $U_1$ is odd, a proof completely analogous to the previous one shows that $U_1 > d^{2/3}$ and $\zeta_K > 2U_1 > 2d^{2/3} = 2\Delta_K^{2/3}$.

If $4 \mid U_1$, equation $(2.10)$ shows that $dV_1^2 \equiv 1 \pmod{16}$. In particular, $d \equiv 1 \pmod{8}$. In this case, $\left(\frac{2}{d}\right) = 1$, therefore $U_1$ splits completely in $K$. Now a proof completely analogous to the previous one shows that $\zeta_K > 2U_1 > 2d^{2/3} = 2\Delta_K^{2/3}$.

Assume now that $2 \mid U_1$. In this case, $U_1/2$ is odd and splits completely in $K$ therefore the equation

$$x^2 - dy^2 = U_1/2$$

has one (hence, infinitely many) positive integer solutions $(x, y)$ with $\gcd(x, y) = 1$. An analysis similar to the one used above conducts to an equation of the form

$$\frac{U_1}{2}V_2^2 = \pm(s^2 - r^2 + 2rsU_1).$$

where $V_2 = V_1 / \gcd(y, V_1)$. Hence, $s^2 \equiv r^2 \pmod{U_1/2}$. If $r = \pm s$, we get $4r^2 = V_2^2$, so $2r = V_2$, which is impossible since $V_2$ is odd. After concluding that $r^2 = s^2$ is not possible, the proof is analogous as in the previous cases. \qed
Remark 2.1. In the case in which both $d$ and $U$ are odd, we cannot exclude the possibility that $r^2 = s^2 = 1$. That possibility corresponds to the equation $x^2 - (U^2 + 4)y^2 = 4U$ which indeed has (infinitely many) solutions, and in fact if $U$ is a prime power, then all solutions come from $r^2 = s^2 = 1$.

3. Applications

Recall that Biró proved that there are only finitely many real quadratic fields of class number 1 and discriminant of the form $a^2 + 1$ or $a^2 + 4$ for some integer $a$, and Biró and Lapkova [3] proved analogous result for the discriminant of the form $(ak)^2 + 4k$, where $a$ and $k$ are odd positive integers. One may ask if there are other polynomials $f(X) \in \mathbb{Z}[X]$ for which one can prove that there are only finitely many real quadratic fields having class number 1 of the form $\mathbb{Q}(\sqrt{f(a)})$ for some integer $a$ such that $f(a)$ is squarefree.

Here is an example of such family of polynomials:

$$g_c(X) = (2c^2 + 2c + 1)^2 X^2 + 2(4c + 2)(c^2 + c + 1) X + 4c^2 + 4c + 5, \quad c \in \mathbb{Z}_{\geq 0}.$$  

Note that $g_0(X) = X^2 + 4X + 5 = (X + 2)^2 + 1$ which is Biró’s example.

**Theorem 3.1.** For each $c \geq 0$, there are only finitely many real quadratic fields of class number 1 of the form $\mathbb{Q}(\sqrt{g_c(k)})$ for some positive integer $k$ such that $g_c(k)$ is squarefree. More precisely, any such $k$ satisfies

$$k \leq 16(2c^2 + 2c + 1)^2 - 1.$$  

**Proof.** Let $d = g_c(k)$. The case $c = 0$ is solved in [1], so we may assume that $c \geq 1$. Putting

$$\alpha = \frac{\lfloor \sqrt{d} \rfloor + \sqrt{d}}{2},$$

the quadratic number $\alpha$ is purely periodic of period 3, namely

$$\alpha = \{(2c^2 + 2c + 1) k + 2c + 1, 2c + 1, 2c + 1\}.$$  

Thus, in particular, the fundamental unit in $K = \mathbb{Q}(\sqrt{g_c(k)})$ is $\zeta_K = \frac{U + V \sqrt{g_c(k)}}{2}$, where

$$U = ((2c^2 + 2c + 1) k + 2c + 1)((2c + 1)^2 + 1) + 4c + 2,$$

$$V = (2c + 1)^2 + 1 = 4c^2 + 4c + 2.$$  

It has norm $-1$ since the length of the period of $\alpha$ is odd. Thus,

$$\zeta_K < 2\sqrt{g_c(k)} V,$$
while $\Delta_K = g_c(k)$ for $k$ even, and $\Delta_K = 4g_c(k)$ for $k$ odd. Since $U$ is even, we can apply Theorem 1.1. Theorem 1.1 implies that under the assumption that $K$ has class number 1, we should have $\zeta_K \geq 2^{-1/3}\Delta_K^{2/3}$. This implies $g_c(k) < 4V_0$, so

$$k \leq 16(2c^2 + 2c + 1)^2 - 1.$$ 

Thus, for fixed $c$ there are only finitely many real quadratic number fields of the form $\mathbb{Q}(\sqrt{g_c(k)})$ with $g_c(k)$ squarefree of class number 1. One may ask whether indeed there are infinitely many values for $k$ such that $g_c(k)$ is squarefree. But it is well-known that if $f(X) = \alpha X^2 + \beta X + \gamma$ is quadratic with simple roots such that there is no positive integer $\delta > 1$ with $\delta | f(n)$ for all integers $n$, then indeed $f(n)$ is squarefree for infinitely many positive integers $n$. For us, $g_c(X)$ as a quadratic polynomial has discriminant $-4$. Thus, it has simple roots. Further, suppose that $\delta$ divides $g_c(n)$ for all $n$. Assuming $\delta > 1$, let $p$ be a prime factor of $\delta$. Then $p | g_c(0)$, so $p | 4c^2 + 4c + 5 = (2c + 1)^2 + 4$. Also, $p | g_c(\pm 1)$, and since $p | 4c^2 + 4c + 5$, we get that $p|(8c - 5)$ and $p|(8c + 13)$, and so $p|18$. It follows that $p = 2$ or $p = 3$, contradicting $p|(2c + 1)^2 + 4$. Thus, there is no integer $\delta > 1$ dividing $g_c(n)$ for all integers $n$. Therefore, indeed there are infinitely many positive integers $k$ with $g_c(k)$ squarefree.

**Corollary 3.2.** Let $k$ be a positive integer such that $d = 25k^2 + 36k + 13$ is squarefree and let $K = \mathbb{Q}(\sqrt{d})$. If $k \neq 4$, then $h_K > 1$.

**Proof.** By taking $c = 1$ in Theorem 3.1, we conclude that if $h_K = 1$, then $k \leq 399$. It is easy to check, e.g. by PARI/GP, that among 371 squarefree values of $d$ in the range $1 \leq k \leq 399$ we always have $h_K > 1$, except for $k = 4$, i.e., for $d = 557$. \qed

**Acknowledgements**

We thank Professor Yasuhiro Kishi for comments which improved the quality of this paper.

The second author would like to thank the Max Planck Institute for Mathematics, Bonn for hospitality and support during the period when this paper was written.

The first author was supported by the Croatian Science Foundation under the project no. 6422 and the QuantiXLie Center of Excellence. The second author was supported in part by NRF (South Africa) Grants CPRR160325161141 and an A-rated researcher award and by CGA (Czech Republic) Grant 17-02804S.
ON FUNDAMENTAL UNITS OF CLASS NUMBER ONE QUADRATIC FIELDS

REFERENCES


DEPARTMENT OF MATHEMATICS, FACULTY OF SCIENCE, UNIVERSITY OF ZAGREB, BIJENIČKA CESTA 30, 10000 ZAGREB, CROATIA

E-mail address: duje@math.hr

SCHOOL OF MATHEMATICS, UNIVERSITY OF THE WITWATERSRAND, PRIVATE BAG X3, WITS 2050, SOUTH AFRICA; MAX PLANCK INSTITUTE FOR MATHEMATICS, VIVATGASSE 7, 53111 BONN, GERMANY; DEPARTMENT OF MATHEMATICS, FACULTY OF SCIENCES, UNIVERSITY OF OSTRAVA, 30 DUBNA 22, 701 03 OSTRAVA 1, CZECH REPUBLIC

E-mail address: florian.luca@wits.ac.za