# On fundamental units of real quadratic fields of class number 1

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 number 1.

**Mathematics Subject Classification (2010).** Primary 11R29; Secondary 11D09.

**Keywords.** Quadratic fields, class number, continued fractions.

## 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 $\mathcal{O}_{\mathbb{K}}$ be the ring of algebraic integers in $\mathbb{K}$ and $\varepsilon_{\mathbb{K}}$ be a fundamental unit (the smallest unit $> 1$). We assume that $\varepsilon_{\mathbb{K}}$ has norm $-1$. Then the 2-rank of its ideal class group is equal to $t-1$, where $t$ is the number of distinct prime divisors of its discriminant $\Delta_{\mathbb{K}}$ (see e.g. [6, Section 26.8]). Hence $h_{\mathbb{K}}$, the class number of $\mathbb{K}$, is odd if and only if $\Delta_{\mathbb{K}} = 8$ or $\Delta_{\mathbb{K}}$ is a prime congruent to 1 modulo 4.

**Theorem 1.1.** *Let $17 < d \equiv 1 \pmod 4$ be squarefree. Assume that there exists a unit*

$$\varepsilon = \frac{U + V\sqrt{d}}{2} \le (2d)^{2/3}$$

*in $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ with norm equal to $-1$ and with $U, V > 0$ and $U \equiv 0 \pmod 8$. Then $h_{\mathbb{K}} > 1$.*

## 2. The proof of Theorem 1.1

Since $d \equiv 1 \pmod 4$, we have $\Delta_{\mathbb{K}} = d$ and $\{1, (1+\sqrt{d})/2\}$ is a basis for $\mathcal{O}_{\mathbb{K}}$. Write $U = 2U_1,\ V = 2V_1$ and then

$$U_1^2 - dV_1^2 = -1. \tag{2.1}$$

From $U_1^2 = dV_1^2 - 1 \equiv V_1^2 - 1 \pmod 4$, we conclude that $U_1$ is even and $V_1$ is odd. As stated in Theorem 1.1, we will assume that $U_1 \equiv 0 \pmod 4$.

Assume that $h_{\mathbb{K}} = 1$. Let $p$ be an odd prime divisor of $U_1/4$. Equation (2.1) reduced modulo $p$ shows that $\left(\frac{d}{p}\right) = 1$, where we use $\left(\frac{\bullet}{p}\right)$ for the Legendre symbol with respect to $p$. Equation (2.1) shows that $dV_1^2 \equiv 1 \pmod{16}$. In particular, $d \equiv 1 \pmod 8$. It follows that all prime factors $p$ of $U_1/4$ split completely in $\mathbb{K}$. Since $\mathbb{K}$ has class number 1 and a unit of norm $-1$, it follows that the Diophantine equation

$$x^2 - dy^2 = 4 \cdot \frac{U_1}{4} = U_1 \tag{2.2}$$

has at least one (hence, infinitely many) positive integer solutions $(x, y)$ with $\gcd(x, y) = 1$ or 2.

**Lemma 2.1.** *Let $1 < d \equiv 1 \pmod 4$ be squarefree. Assume that there is a unit $\varepsilon = (U + V\sqrt{d})/2$, $U, V > 0$, of the real quadratic field $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ with the norm equal to $-1$ and such that $U = 2U_1$ is even. If the equation*

$$x^2 - dy^2 = U_1 \tag{2.3}$$

*has at least one solution in positive integers, then $U_1 > 2^{-1/3}d^{2/3}$, unless $U_1$ is a perfect square, say $U_1 = r^2$, and gcd$(x, y) = r$.*

*Proof.* Let $(x, y)$ be a positive integer solution of (2.3). Put $V_2 = V_1/\gcd(y,V_1)$ and $y_1 = y/\gcd(y, V_1)$. Multiplying both sides of equation (2.3) by $V_2^2$ we get

$$(xV_2)^2 - (dV_1^2)y_1^2 = 2U_1V_2^2. \tag{2.4}$$

Let $D = dV_1^2$ and note that $D = U_1^2 + 1$. Thus, equation (2.4) is of the form

$$X^2 - DY^2 = U_1V_2^2, \tag{2.5}$$

where $X = xV_2$, $Y = y_1$ may be assumed arbitrarily large. Equation (2.5) can be rewritten as

$$\left|\frac{X}{Y} - \sqrt{D}\right| = \frac{U_1V_2^2}{Y^2(X/Y + \sqrt{D})} = \frac{1}{Y^2}\left(\frac{1}{2\sqrt{D}} + o(1)\right)U_1V_2^2 \tag{2.6}$$

as $X \to \infty$. We use the fact that $\sqrt{D} = \sqrt{U_1^2 + 1} > U_1$, choose $\delta > 0$ sufficiently small such that

$$\left(\frac{1}{2\sqrt{D}} + \delta\right)U_1V_2^2 < \frac{V_2^2 + 1}{2}$$

holds, then choose $X$ and $Y$ sufficiently large so that the amount indicated by $o(1)$ in (2.6) is in absolute value smaller than $\delta$, to conclude that if we put

$$K = \frac{V_2^2 + 1}{2}, \tag{2.7}$$

then

$$\left|\frac{X}{Y} - \sqrt{D}\right| < \frac{K}{Y^2}. \tag{2.8}$$

By results of Dujella [4] and Worley [8], there exist integers $n$, $r$, $s$ with $r$ positive and $r|s| < 2K = 2V_2^2 + 1$ such that $X = rp_n + sp_{n-1}$ and $Y = rq_n + sq_{n-1}$. Here, $p_k/q_k$ is the $k$th convergent to $\sqrt{D} = \sqrt{U_1^2+1}$. With these values for $X$ and $Y$ we have

$$X^2 - DY^2 = (rp_n + sp_{n-1})^2 - D(rq_n + sq_{n-1})^2,$$

which gives

$$U_1V_2^2 = r^2(p_n^2 - Dq_n^2) + s^2(p_{n-1}^2 - Dq_{n-1}^2) + 2rs(p_np_{n-1} - Dq_nq_{n-1}). \quad (2.9)$$

It is easy to prove that

$$p_n = \frac{\alpha^{n+1} + \beta^{n+1}}{2} \qquad \text{and} \qquad q_n = \frac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta} \quad (2.10)$$

hold for all $n \geq 0$, where

$$(\alpha, \beta) = (U_1 + \sqrt{U_1^2+1}, U_1 - \sqrt{U_1^2+1}).$$

Using (2.10), one checks that

$$p_n^2 - Dq_n^2 = (-1)^{n+1} \qquad \text{and} \qquad p_np_{n-1} - Dq_nq_{n-1} = (-1)^nU_1$$

hold for all $n \geq 0$. Thus, relation (2.9) is

$$U_1V_2^2 = (-1)^n(s^2 - r^2 + 2rsU_1) \quad (2.11)$$

(see also [5, Lemma 1]). If $s = 0$, then $U_1 = r^2$ and $\gcd(x, y) = r$. Assume now that $s \neq 0$. From (2.11), we have $r^2 \equiv s^2 \pmod{U_1}$. If $r^2 = s^2$, we then get $U_1V_2^2 = \pm 2r^2U_1$, and therefore $2r^2 = \pm V^2$, which does not have a positive integer solution $r$. Thus, $r^2 \neq s^2$, which together with the fact that $r^2 \equiv s^2 \pmod{U_1}$ shows that $\max\{r, |s|\} \geq \sqrt{U_1}$. In particular,

$$\sqrt{U_1} \leq \max\{r, |s|\} \leq r|s| \leq V_2^2,$$

therefore $V_1 \geq V_2 \geq (U_1)^{1/4}$. Since $\sqrt{d}V_1 = \sqrt{U_1^2+1}$, we get $\sqrt{U_1^2+1} \geq \sqrt{d}(U_1)^{1/4}$. We have $U_1 \geq 4$. Hence, $d^2 \leq \frac{U_1^4+2U_1^2+1}{U_1} < 2U_1^3$ and $U_1 > 2^{-1/3}d^{2/3}$. □

By the discussion at the beginning of this section, the assumptions of Theorem 1.1 imply that equation (2.3) has a solution in positive integers $x, y$ such that $\gcd(x, y) = 1$ or 2. In the case $U_1 = r^2$ and $\gcd(x, y) = r$, we get that $r = 2$ and $dV_1^2 = U_1^2 + 1 = 17$ and thus $d = 17$. Otherwise, since $\varepsilon = U_1 + V_1\sqrt{d} > 2U_1$, we get from Lemma 2.1 that

$$\varepsilon > (2d)^{2/3},$$

which proves Theorem 1.1. □

**Remark 2.2.** In the case $U \equiv 4 \pmod 8$, we cannot conclude that the equation $x^2 - dy^2 = U_1$ is solvable, but we have only solvability of the equation $x^2 - dy^2 = 2U_1$, which follows already from $(U_1 + 1)^2 - dY_1^2 = 2U_1$. Consequently, in this case, and similarly in the case when $U$ is odd, we cannot exclude the possibility that $r^2 = s^2$ in the above proof. That possibility corresponds to the equations $X^2 - (U_1^2+1)Y^2 = 2U_1$ and $X^2 - (U^2+4)Y^2 = 4U$ which indeed have (infinitely many) solutions.

**Remark 2.3.** Biró [1, 2] determined all 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] obtained analogous results 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. There are families of polynomials for which Theorem 1.1 gives such results, like $g_c(k) = (2c^2+2c+1)^2(2k+4)^2 + 2(4c+2)(c^2+c+1)(2k+4) + 4c^2+4c+5$ (corresponding to quadratic irrationals with continued fraction expansion of period length 3) and

$$\begin{aligned} h_c(k) = {} & (256c^8 - 512c^7 + 1024c^6 - 1024c^5 + 960c^4 - 512c^3 + 256c^2 - 64c \\ & + 16)k^2 + (256c^9 - 1024c^8 + 2048c^7 - 3008c^6 + 2944c^5 - 2304c^4 \\ & + 1248c^3 - 544c^2 + 160c - 32)k + 64c^{10} - 384c^9 + 1024c^8 \\ & - 1760c^7 + 2192c^6 - 1984c^5 + 1396c^4 - 736c^3 + 304c^2 - 92c + 17, \end{aligned}$$

(corresponding to quadratic irrationals with continued fraction expansion of period length 7). However, it should be noted that the same results for these families of polynomials follow also from the results of [7]. Namely, if $d \equiv 1 \pmod 8$, then the prime 2 splits in the quadratic field $\mathbb{Q}(\sqrt{d})$. Hence, if $h_{\mathbb{K}} = 1$, then in the notation of [7], one of the $Q_i$'s must be equal to 4, which is not the case to the mentioned families. In fact, we were not be able to find an integer $d > 17$ such that $d \equiv 1 \pmod 8$, $U \equiv 0 \pmod 8$, $\varepsilon_{\mathbb{K}} \le (2d)^{2/3}$ and one of the $Q_i$'s is equal to 4 (in the notation of [7]).

## Acknowledgements

We thank Professor Yasuhiro Kishi for comments which improved the quality of the paper. We are very grateful to the referee for pointing out several important mistakes in previous versions of the 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, a project cofinanced by the Croatian Government and European Union through the European Regional Development Fund - the Competitiveness and Cohesion Operational Programme (Grant KK.01.1.1.01.0004). 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.

## References

[1] A. Biró, *Chowla's conjecture*, Acta Arith. **107** (2003), 179– 194.

[2] A. Biró, *Yokoi's conjecture*, Acta Arith. **106** (2003), 85–104.

[3] A. Biró and K. Lapkova, *The class number one problem for the real quadratic fields* $\mathbb{Q}(\sqrt{(an)^2+4a})$, Acta Arith. **172** (2016), 117–131.

[4] A. Dujella, *Continued fractions and RSA with small secret exponent*, Tatra Mt. Math. Publ. **29** (2004), 101–112.

[5] A. Dujella and B. Jadrijević, *A family of quartic Thue inequalities*, Acta Arith. **111** (2004), 61–76.

[6] H. Hasse, Number Theory, Springer-Verlag, 1980.

[7] S. Louboutin, *Continued fractions and real quadratic fields*, J. Number Theory **30** (1988), 167–176.

[8] R. T. Worley, *Estimating* $|\alpha - p/q|$, J. Austral. Math. Soc. **31** (1981), 202–206.

Andrej Dujella
Department of Mathematics, Faculty of Science, University of Zagreb
Bijenička cesta 30, 10000 Zagreb, Croatia

e-mail: duje@math.hr

Florian Luca
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: florian.luca@wits.ac.za