ACTA ARITHMETICA
LXXXV.1 (1998)

Length of continued fractions in principal quadratic fields

by

Guillaume Grisel (Caen)

Let $d \ge 2$ be a square-free integer and for all $n \ge 0$, let $l(\sqrt{d}^{2n+1})$ be the length of the continued fraction expansion of $\sqrt{d}^{2n+1}$. If $\mathbb{Q}(\sqrt{d})$ is a principal quadratic field, then under a condition on the fundamental unit of $\mathbb{Z}[\sqrt{d}]$ we prove that there exist constants C_1 and C_2 such that $C_1\sqrt{d}^{2n+1} \ge l(\sqrt{d}^{2n+1}) \ge C_2\sqrt{d}^{2n+1}$ for all large n. This is a generalization of a theorem of S. Chowla and S. S. Pillai [2] and an improvement in a particular case of a theorem of [6].

1. Introduction and main result. Let α be a real quadratic irrationality and let $l(\alpha)$ be the length of the period of its continued fraction expansion. In [6], we investigated $l(\alpha^n)$, $n \ge 1$, and we proved that for a large class of quadratic irrationalities, we have

$$l(\alpha^n) \ge Ke^{kn}/n,$$

where K and k are strictly positive and explicit constants depending only on α (if $\alpha^2 \in \mathbb{Q}$, then n is an odd integer). In the particular case of $\alpha = \sqrt{d}$, with $d \ge 2$ a square-free integer, the above inequality holds and takes the form, for all $n \ge 1$,

$$l(\sqrt{d}^{2n+1}) \ge \frac{\log \varepsilon_0}{\log 4d} \cdot \frac{d^{n-r}}{n},$$

where $\varepsilon_0 > 1$ is the fundamental unit of the ring $\mathbb{Z}[\sqrt{d}]$ and r is a positive integer depending only on d. But this inequality is not the best possible, and can be improved for well chosen d. In 1931, S. Chowla and S. S. Pillai showed [2] that there exist constants C and C' (C' is non-effective) such that for all n large enough,

$$C\sqrt{5}^{2n+1} \ge l(\sqrt{5}^{2n+1}) \ge C'\sqrt{5}^{2n+1}.$$

1991 *Mathematics Subject Classification*: 11A55, 11J70.

The aim of this paper is to generalize these inequalities when $\mathbb{Q}(\sqrt{d})$ is a principal field.

Notation and property. Let a be a positive integer. We denote by $\nu(a)$ the index of the unit group of the ring $\mathbb{Z}[a\sqrt{d}]$ in the unit group of the ring $\mathbb{Z}[\sqrt{d}]$, i.e. $\nu(a)$ is the smallest integer m such that $\varepsilon_0^m \in \mathbb{Z}[a\sqrt{d}]$. Note that if b is another positive integer such that $\gcd(a,b) = 1$, then $\nu(ab) = \operatorname{lcm}(\nu(a), \nu(b))$.

THEOREM 1. *Let $d \geq 2$ be a square-free integer such that the following two conditions are satisfied*:

(i) $\mathbb{Q}(\sqrt{d})$ *is a principal field*;
(ii) $\nu(d) = d$.

Then there exist constants C_1 and C_2 such that for all large n (*the bound on n is not effective*),

$$C_1\sqrt{d}^{2n+1} \geq l(\sqrt{d}^{2n+1}) \geq C_2\sqrt{d}^{2n+1}.$$

The upper bound for $l(\sqrt{d}^{2n+1})$ does not depend on the conditions (i) and (ii). We show in Section 2 that it follows from a general result on quadratic irrationalities, and we give in Theorem 2 an explicit value for the constant C_1.

Section 3 is devoted to establishing a lower bound for $l(\sqrt{d}^{2n+1})$. For all $n \geq 0$, let δ_n be an infinite sequence of distinct positive integers such that there exists an integer $R > 1$ with $\operatorname{Rad}(\delta_n) = \prod_{p\mid\delta_n} p = R$. We first find a lower bound for the caliber of the order of conductor δ_n of the ring of integers of the field $\mathbb{Q}(\sqrt{d})$. Conditions (i) and (ii) suffice to prove that for all $n \geq 0$ either the order $\mathbb{Z}[\sqrt{d}^{2n+1}]$ or $\mathbb{Z}[(1+\sqrt{d}^{2n+1})/2]$ is principal. Hence, the reduced ideals of these orders are in bijection with the complete quotients of the period of the continued fraction expansion of $\sqrt{d}^{2n+1}$ or $(1+\sqrt{d}^{2n+1})/2$. Then the lower bound found before can be applied with $\delta_n = d^n$ or $2d^n$. In fact, we prove more than stated in Theorem 1, since we give in Theorem 3 an explicit lower bound for

$$\liminf_n \frac{l(\sqrt{d}^{2n+1})}{\sqrt{d}^{2n+1}}.$$

In Section 4 we discuss explicit computations relating to Theorem 1. We close the paper with a discussion of the method when $\mathbb{Q}(\sqrt{d})$ is not principal.

This work was intended as an attempt to develop original techniques for bounding from below the length of continued fractions. It becomes more interesting when compared with the results and methods presented in [6] and [7].

2. Upper bound for the period. Let α be a real quadratic irrationality and let α_i be the ith complete quotient of the continued fraction of α. It is well known that the fundamental unit $\varphi > 1$ of the ring of stabilizers of $\mathbb{Z} + \mathbb{Z}\alpha$ is equal to the product of all the α_i contained "in a period" of the continued fraction of α. Therefore, the smaller the α_i, the larger the length $l(\alpha)$ of the period. But we will show that they cannot all be too small. This property will provide an upper bound for $l(\alpha)$ in terms of the fundamental unit φ. Then it will remain to explicitly give this fundamental unit in the particular case $\alpha = \sqrt{d}^{2n+1}$.

THEOREM 2. *Let $d = d_1 \ldots d_s$ be a square-free integer, d_i prime. For all $i = 1, \ldots, s$, define $r(i) = \max\{m : \nu(d_i^m) = \nu(d_i)\}$. Then, for all $n \geq 0$,*

$$l(\sqrt{d}^{2n+1}) \leq \frac{\nu(d)\log\varepsilon_0}{\sqrt{d}\log\left(\frac{1+\sqrt{5}}{2}\right)\prod_{i=1}^{s} d_i^{r_i}}\sqrt{d}^{2n+1}.$$

This theorem follows directly from the next two lemmas.

LEMMA 1. *Let α be a real quadratic irrationality and let $\varphi > 1$ be the fundamental unit of the ring of stabilizers of the module $\mathbb{Z} + \mathbb{Z}\alpha$. Then*

$$l(\alpha) \leq \frac{\log\varphi}{\log\frac{1+\sqrt{5}}{2}}.$$

Proof. Let $\alpha = [a_0, \ldots, a_i, \ldots]$ be the continued fraction expansion. For all $i \geq 0$, denote by α_i the complete quotients of this expansion, i.e. $\alpha_i = a_i + 1/\alpha_{i+1}$. Suppose that there exists i such that $\alpha_i \leq (1+\sqrt{5})/2$.

If $a_i \neq 0$, then

$$\alpha_{i+1} = \frac{1}{\alpha_i - a_i} \geq \frac{1}{(1+\sqrt{5})/2 - 1} = \frac{1+\sqrt{5}}{2}$$

and

$$\alpha_{i+1}\alpha_i = a_i\alpha_{i+1} + 1 \geq \frac{1+\sqrt{5}}{2} + 1 = \left(\frac{1+\sqrt{5}}{2}\right)^2.$$

Let i_0 be the smallest index i such that α_i is reduced (i.e. $\alpha_i > 1$ and its quadratic conjugate satisfies $-1 < \overline{\alpha}_i < 0$). Hence $a_i \neq 0$ for all $i \geq i_0$. It is well known that

$$\varphi = \alpha_{i_0} \ldots \alpha_{i_0+l(\alpha)-1}.$$

Then, if $\alpha_{i_0+l(\alpha)-1} > (1+\sqrt{5})/2$, using the above properties, we have

$$\varphi = \alpha_{i_0} \ldots \alpha_{i_0+l(\alpha)-1} \geq \left(\frac{1+\sqrt{5}}{2}\right)^{l(\alpha)}.$$

On the other hand, if $\alpha_{i_0+l(\alpha)-1} \leq (1+\sqrt{5})/2$, then $\alpha_{i_0+l(\alpha)} \geq (1+\sqrt{5})/2$. Moreover, $\alpha_{i_0+l(\alpha)} = \alpha_{i_0}$ and $\varphi = \alpha_{i_0+1} \ldots \alpha_{i_0+l(\alpha)}$, which leads us to the same situation as before. ∎

For all $n \geq 0$, let $\varphi_n > 1$ be the fundamental unit of $\mathbb{Z}[\sqrt{d}^{2n+1}]$. Hence $\varphi_n = \varepsilon_0^{\nu(d^n)}$. We apply Lemma 1 with $\alpha = \sqrt{d}^{2n+1}$; then the determination of $\nu(d^n)$ suffices to prove Theorem 2.

LEMMA 2. *Let $d = d_1 \ldots d_s$ be a square-free integer, d_i prime. For all $i = 1, \ldots, s$, define $r(i) = \max\{m : \nu(d_i^m) = \nu(d_i)\}$. Then, for all $n \geq 0$,*

$$\nu(d^n) = \nu(d) \prod_{i=1}^{s} d_i^{n-r(i)}.$$

Proof. Fix $i = 1, \ldots, s$. Let $\gamma \geq 1$ and $m \geq 1$ be integers such that $\nu(d_i^m) = \gamma$ and $\nu(d_i^{m+1}) \neq \gamma$. We claim that $\nu(d_i^{m+1}) = d_i\gamma$. To prove this, write $\varepsilon_0^k = U_k + V_k\sqrt{d}$, for all $k \geq 1$, with U_k, V_k integers. For all $u \geq 1$, we have

$$U_{u\gamma} + V_{u\gamma}\sqrt{d} = (U_\gamma + V_\gamma\sqrt{d})^u.$$

Hence

$$V_{u\gamma} = \sum_{j=0}^{[(u-1)/2]} \binom{u}{2j+1} U_\gamma^{u-2j-1} V_\gamma^{2j+1} d^j.$$

But by the assumption and by the definition of $\nu(d_i^m)$, d_i^m divides exactly V_γ. Hence d_i^{2m} divides all the members of the sum except perhaps

$$\binom{u}{1} U_\gamma^{u-1} V_\gamma = u U_\gamma^{u-1} V_\gamma.$$

Now, it is easily seen that d_i is the smallest u such that d_i^{m+1} divides $uU_\gamma^{u-1}V_\gamma$, and the claim follows.

From the claim, by induction we have

$$\nu(d_i^n) = \nu(d_i) d_i^{n-r(i)}.$$

As all the d_i are prime and by the properties of ν, this leads to

$$\nu(d^n) = \operatorname{lcm}(\nu(d_i^n)) = \operatorname{lcm}(\nu(d_i)) \prod_{i=1}^{s} d_i^{n-r(i)} = \nu(d) \prod_{i=1}^{s} d_i^{n-r(i)}. \ \blacksquare$$

The following corollary will be useful in Section 3.

COROLLARY. *Let $d = d_1 \ldots d_s$ be a square-free integer, d_i prime. If $\nu(d) = d$ then $\nu(d^n) = d^n$.*

Proof. As $\nu(d) = \operatorname{lcm}(\nu(d_i)) = d$, by Lemma 2 it suffices to show that $r(i) = 1$ for all $i = 1, \ldots, s$. Each d_i is prime, and we know that $\nu(d_i) = 1$ or d_i (see [3], Théorème 5.3). Thus $\nu(d) = d$ implies $\nu(d_i) = d_i$. We just have to prove that $\nu(d_i^2) \neq \nu(d_i)$. Write again

$$\varepsilon_0^{d_i} = U_{d_i} + V_{d_i}\sqrt{d} = (U_1 + V_1\sqrt{d})^{d_i}.$$

Then

$$V_{d_i} = \sum_{j=0}^{[(d_i-1)/2]} \binom{d_i}{2j+1} U_1^{d_i-2j-1} V_1^{2j+1} d^j.$$

Let p be a prime number and $v_p(\cdot)$ the p-adic valuation. From $\nu(d_i) = d_i$, it follows that $v_{d_i}(V_1) = 0$. As $U_1^2 - V_1^2 d = \pm 1$, we have $v_{d_i}(U_1) = 0$. Hence $v_{d_i}(d_i U_1^{d_i-1} V_1) = 1$.

Thus, d_i^2 divides all the members of the sum except the first one and perhaps the second one $\binom{d_i}{3} U_1^{d_i-3} V_1^3 d$.

But $\binom{3}{3} = 1$ and if $d_i > 3$, we have $v_{d_i}\big(\binom{d_i}{3}\big) = 1$. Hence

$$v_{d_i}\left(\binom{d_i}{3} U_1^{d_i-3} V_1^3 d\right) = 2.$$

Finally, we have

$$v_{d_i}\left(d_i U_1^{d_i-1} V_1 + \binom{d_i}{3} U_1^{d_i-3} V_1^3 d\right) = 1,$$

and d_i^2 does not divide V_{d_i}, which implies $r(i) = 1$ and by Lemma 2,

$$\nu(d^n) = \nu(d) \prod_{i=1}^{s} d_i^{n-r(i)} = d^n. \ \blacksquare$$

3. Lower bound for the period. For all $n \ge 0$, let δ_n be a sequence of distinct positive integers such that there exists an integer $R > 1$ with

$$\mathrm{Rad}(\delta_n) = \prod_{p \mid \delta_n} p = R.$$

Then we are able to give, for n large enough, a lower bound for the caliber of the order of conductor δ_n of the ring of integers of the field $\mathbb{Q}(\sqrt{d})$. For that, Ikehara's theorem is used.

Let $\varepsilon > 1$ be the fundamental unit of $\mathbb{Q}(\sqrt{d})$. We prove that if $\nu(d) = d$ then the orders $\mathbb{Z}[\sqrt{d}^{2n+1}]$ if $d \not\equiv 5 \pmod 8$ or if $d \equiv 5 \pmod 8$ and $\varepsilon^3 = \varepsilon_0$, and the orders $\mathbb{Z}[(1+\sqrt{d}^{2n+1})/2]$ if $d \equiv 5 \pmod 8$ and $\varepsilon = \varepsilon_0$, have the same class number as the field $\mathbb{Q}(\sqrt{d})$. It is then easy to deduce the theorem:

THEOREM 3. *Let $d \ge 2$ be a square-free integer and D the discriminant of the field $\mathbb{Q}(\sqrt{d})$. Let $\varepsilon > 1$ and $\varepsilon_0 > 1$ be the fundamental unit of the field $\mathbb{Q}(\sqrt{d})$ and of the ring $\mathbb{Z}[\sqrt{d}]$ respectively. Denote by χ the character of the field $\mathbb{Q}(\sqrt{d})$ and by $L(1,\chi)$ the value of the Dirichlet L-function at $s = 1$. Suppose that d satisfies the following two conditions*:

(i) $\mathbb{Q}(\sqrt{d})$ *is a principal field*;
(ii) $\nu(d) = d$.

Then

$$\liminf_n \frac{l(\sqrt{d}^{2n+1})}{\sqrt{d}^{2n+1}} \geq \frac{fL(1,\chi)}{\pi^2 \prod_{p|D}(1+1/p)},$$

with $\pi = 3.14159\ldots$, *and where*

$$f = \begin{cases} 6 & \text{if } d \not\equiv 1 \pmod 4 \text{ or } d \equiv 5 \pmod 8 \text{ and } \varepsilon_0 = \varepsilon^3, \\ 2 & \text{if } d \equiv 1 \pmod 8, \\ 1 & \text{if } d \equiv 5 \pmod 8 \text{ and } \varepsilon_0 = \varepsilon. \end{cases}$$

The theory of ideals in an arbitrary order of a quadratic field is a little more complicated than that for the maximal order. In particular, a fractional ideal is not usually invertible. The invertible ideals I of an order O are exactly those which satisfy $\{\beta \in K : \beta I \subset I\} = O$. Hence, they form a group $I(O)$, which can be divided by the subgroup $P(O)$ of principal ideals to give a finite group $C(O)$, the *class group* of the order O. Its cardinality, denoted by $h(O)$, is the *class number* of the order O. If O is the order of conductor δ of the ring of integers O_K of a field K, we have the formula (see [4], Theorem 7.24, p. 146)

$$h(O) = h_K \frac{\delta}{[O_K^* : O^*]} \prod_{p|\delta} \left(1 - \frac{\chi(p)}{p}\right), \tag{1}$$

where h_K is the class number of K, $[O_K^* : O^*]$ the index of the unit group of O in the unit group of O_K, and χ the character of K.

As in the case of the maximal order, each ideal can be factorized into a product of prime ideals. But O is not integrally closed and thus is not a Dedekind ring. Hence, this factorization is usually not unique.

The quadratic field K is of the form $\mathbb{Q}(\sqrt{d})$ for a square-free integer $d \geq 2$. Let $\omega = \sqrt{d}$ if $d \not\equiv 1 \pmod 4$ and $\omega = (1+\sqrt{d})/2$ if $d \equiv 1 \pmod 4$. Then a primitive ideal of O is a $\mathbb{Z}$-module $I = c\mathbb{Z} + (a+\delta\omega)\mathbb{Z}$, with a and c integers, $c > 1$, a determined modulo c and $c \mid N(a+\delta\omega)$, where $N(a+\delta\omega)$ is the norm of the real number $a+\delta\omega$. Hence, we can associate with each primitive ideal a family of real numbers $x_a(I) = (a+\delta\omega)/c$. The ideal I is then called *reduced* if there exists an integer a modulo c such that $x_a(I)$ is reduced, i.e. $x_a(I) > 1$ and its quadratic conjugate satisfies $0 > \overline{x}_a(I) > -1$. There exist only a finite number of reduced ideals in O. This number is the *caliber* of O, denoted by $\mathrm{Cal}(O)$. Note that there is at least one reduced ideal in each class of $C(O)$.

PROPOSITION 1. *Let d be a square-free integer and D the discriminant of the field $\mathbb{Q}(\sqrt{d})$. Let also $(\delta_n)_{n\geq 0}$ be a sequence of distinct positive integers such that there exists an integer $R > 1$ with $\mathrm{Rad}(\delta_n) = \prod_{p|\delta_n} p = R$ for all $n \geq 0$. For all $n \geq 0$, denote by O_n the order of conductor δ_n of the ring of* *integers of the field* $\mathbb{Q}(\sqrt{d})$*. Then*

$$\liminf_n \frac{\mathrm{Cal}(O_n)}{\frac{1}{2}\delta_n\sqrt{D}} \geq \frac{6L(1,\chi)}{\pi^2 k(1)\prod_{p|D}(1+1/p)},$$

where

$$k(1) = \prod_{\substack{p|R \\ \chi(p)=1}} \frac{1+1/p}{1-1/p}.$$

Proof. Fix $n \geq 0$. For all $1 < m < \frac{1}{2}\delta_n\sqrt{D}$, we set

$$f(m) = \begin{cases} 1 & \text{if } \gcd(m,\delta_n) = 1 \text{ and all prime factors of } m \text{ split in } \mathbb{Q}(\sqrt{d}), \\ 0 & \text{otherwise.} \end{cases}$$

Note that because $\mathrm{Rad}(\delta_n) = R$ for all $n \geq 0$, the map $m \to f(m)$ does not depend on n.

Consider m such that $f(m) = 1$, and let $m = \prod_{i=1}^{i_m} p_i^{e_i}$, $p_i \geq 2$ prime and distinct, $e_i \geq 1$, be its decomposition into primes. As each p_i splits, we have $(p_i) = I_i\bar{I}_i$, where I_i is an ideal of the ring of integers $O_{\mathbb{Q}(\sqrt{d})}$ of $\mathbb{Q}(\sqrt{D})$ and $\bar{I}_i \neq I_i$. Moreover, the norm satisfies $N(I_i) = p_i$.

It is well known that the set of ideals of O_n with norm prime to δ_n is in bijection with the set of ideals of $O_{\mathbb{Q}(\sqrt{d})}$ with norm prime to δ_n (see [4], Proposition 7.20, p. 144), i.e. there exists an ideal $I_{i,n}$ of O_n such that $I_i \cap O_n = I_{i,n}$. Again, $\bar{I}_{i,n} \neq I_{i,n}$ and $N(I_{i,n}) = p_i$.

Consider the set of ideals

$$H_m = \Big\{ \prod_{i=1}^{i_m} J_{i,n}^{e_i} : J_{i,n} = I_{i,n} \text{ or } \bar{I}_{i,n} \Big\}.$$

Every ideal in H_m is primitive with norm m, and $\mathrm{card}(H_m) = 2^{i_m}$. Moreover, they are all distinct.

Lemma 3. *Let I be a primitive ideal of the order O of conductor δ of the quadratic field of discriminant D. If $N(I) \leq \delta\sqrt{D}/2$, then I is a reduced ideal of O.*

Proof. Let $x_a(I) = (a+\delta\omega)/c$ be a real number attached to I. As a is determined modulo c, it is possible to choose a such that $-c-\delta\overline{\omega} < a < -\delta\overline{\omega}$, i.e. $-1 < x_a(I) < 0$. But, by the assumption, we have $2N(I) \leq \delta\sqrt{D} = \delta(\omega - \overline{\omega})$, which leads to $c - \delta\overline{\omega} \leq -c - \delta\omega$. Hence, from the left hand side of the previous inequality, we obtain $a > c - \delta\omega$, which is $x_a(I) > 1$, and $x_a(I)$ is reduced. ■

Hence, by Lemma 3, all the ideals of H_m are reduced. In this way, for each integer $1 < m < \delta_n\sqrt{D}/2$ such that $f(m) = 1$, we are able to give 2^{i_m}

distincts reduced ideals of O_n. Thus, setting $f(1)=0$, we have the lower bound

$$\mathrm{Cal}(O_n)\ge \sum_{m=1}^{[\delta_n\sqrt{D}/2]} 2^{i_m} f(m). \tag{2}$$

To express this lower bound in an explicit way, we apply a deep result on Dirichlet series. The following lemma will allow us to verify that the assumptions of this result are all satisfied.

LEMMA 4. *Let s be a complex number*, $|s|>1$. *Set*

$$k(s)=\prod_{\substack{p\mid R\\ \chi(p)=1}} \frac{1+1/p^s}{1-1/p^s}.$$

Then

$$\sum_{m=1}^{\infty}\frac{2^{i_m}f(m)}{m^s}=\frac{\zeta(s)L(s,\chi)}{k(s)\zeta(2s)\prod_{p\mid D}(1+1/p^s)},$$

where $\zeta(s)$ and $L(s,\chi)$ are the zeta-function and the Dirichlet L-function respectively.

Proof. The result is obtained by writing each side of the equality as a product. $2^{i_m}f(m)$ is a multiplicative function (i.e. if n and m are coprime, then $2^{i_{nm}}f(nm)=2^{i_n}f(n)2^{i_m}f(m)$). As $|s|>1$, it is well known that

$$\sum_{m=1}^{\infty}\frac{2^{i_m}f(m)}{m^s}=\prod\nolimits^{*}\left(1+\frac{2}{p^s}+\frac{2}{p^{2s}}+\ldots\right),$$

where the product $\prod^*$ is taken over all the primes p which satisfy $\chi(p)=1$ and $\gcd(p,\delta_n)=1$, i.e. $\gcd(p,R)=1$. We can write

$$\begin{aligned}\sum_{m=1}^{\infty}\frac{2^{i_m}f(m)}{m^s}&=\prod\nolimits^{*}\left(2\left(1+\frac{1}{p^s}+\frac{1}{p^{2s}}+\ldots\right)-1\right)\\&=\prod\nolimits^{*}\left(2\left(\frac{1}{1-1/p^s}\right)-1\right)=\prod\nolimits^{*}\frac{1+1/p^s}{1-1/p^s}.\end{aligned}$$

On the other hand, for $|s|>1$ we have

$$\zeta(s)=\prod_{p=1}^{\infty}\frac{1}{1-1/p^s}\quad\text{and}\quad L(s,\chi)=\prod_{p=1}^{\infty}\frac{1}{1-\chi(p)/p^s},$$

and therefore

$$\begin{aligned}\frac{\zeta(s)L(s,\chi)}{\zeta(2s)}&=\prod_{p=1}^{\infty}\frac{1+1/p^s}{1-\chi(p)/p^s}=\prod_{p\mid D}\left(1+\frac{1}{p^s}\right)\prod_{\substack{p=1\\ \chi(p)=1}}^{\infty}\frac{1+1/p^s}{1-1/p^s}\\&=k(s)\prod_{p\mid D}\left(1+\frac{1}{p^s}\right)\prod\nolimits^{*}\frac{1+1/p^s}{1-1/p^s}. \ \blacksquare\end{aligned}$$

We are now able to finish the proof of Proposition 1. For all complex s, set

$$F(s) = \sum_{m=1}^{\infty} \frac{2^{i_m} f(m)}{m^s} \quad \text{and} \quad G(s) = \frac{\zeta(s)L(s,\chi)}{k(s)(1+1/d^s)\zeta(2s)}.$$

According to Lemma 4, the functions F and G coincide on the half plane defined by $\mathrm{Re}(s) > 1$. Moreover, G is a meromorphic function, whose poles, in this half plane, are the poles of $\zeta(s)$. The function $\zeta(s)$ admits for $s = 1$ a simple pole with residue 1. Then we apply Ikehara's theorem ([5], Théorème 8.7.1, p. 258) which states that if $F(s) = \sum a_n/n^s$ is a Dirichlet series which satisfies:

- $a_n \geq 0$ for all n;
- $F(s)$ converges in the half plane defined by $\mathrm{Re}(s) \geq 1$;
- $F(s)$ coincides in the half plane $\mathrm{Re}(s) > 1$ with a function G meromorphic in an open set Ω which contains the half plane $\mathrm{Re}(s) \geq 1$, and which has a unique pole in Ω, simple, localized at $s = 1$ and with residue ϱ;

then

$$\lim_{x\to\infty} \frac{\sum_{n=1}^{x} a_n}{x} = \varrho.$$

Hence, we obtain

$$\lim_{n\to\infty} \frac{\sum_{m=1}^{\delta_n\sqrt{D}/2} 2^{i_m} f(m)}{\delta_n\sqrt{D}/2} = \frac{6L(1,\chi)}{\pi^2 k(1)\prod_{p\mid D}(1+1/p)}.$$

Then Proposition 1 follows from inequality (2). ∎

Proof of Theorem 3. Theorem 3 is in fact a corollary to Proposition 1. It follows from the remark that the orders $\mathbb{Z}[\sqrt{d}^{2n+1}]$ if $d \not\equiv 5 \pmod 8$ or if $d \equiv 5 \pmod 8$ and $\varepsilon_0 = \varepsilon^3$, and the orders $\mathbb{Z}[(1+\sqrt{d}^{2n+1})/2]$ if $d \equiv 5 \pmod 8$ and $\varepsilon_0 = \varepsilon$, have, for all $n \geq 1$, class number equal to the class number of the field $\mathbb{Q}(\sqrt{d})$.

Lemma 5. *For all $n \geq 0$, set*

$$O_n = \mathbb{Z}[\sqrt{d}^{2n+1}] \quad \textit{and} \quad \widetilde{O}_n = \mathbb{Z}\left[\frac{1+\sqrt{d}^{2n+1}}{2}\right].$$

Suppose that $\nu(d) = d$. Then, for all $n \geq 0$,

$$h_{\mathbb{Q}(\sqrt{d})} = \begin{cases} h(O_n) & \textit{if } d \not\equiv 5 \pmod 8 \textit{ or if } d \equiv 5 \pmod 8 \textit{ and } \varepsilon_0 = \varepsilon^3, \\ h(\widetilde{O}_n) & \textit{if } d \equiv 5 \pmod 8 \textit{ and } \varepsilon_0 = \varepsilon. \end{cases}$$

Proof. As before, for all $n \geq 0$, let $\varphi_n > 1$ be the fundamental unit of $\mathbb{Z}[\sqrt{d}^{2n+1}]$. Then $\varphi_n = \varepsilon_0^{\nu(d^n)}$ for all $n \geq 0$. Hence

$$(3) \qquad [O^*_{\mathbb{Q}(\sqrt{d})} : O^*_n] = \begin{cases} \nu(d^n) & \text{if } d \not\equiv 5 \pmod 8, \\ 3\nu(d^n) & \text{if } d \equiv 5 \pmod 8 \text{ and } \varepsilon_0 = \varepsilon^3, \\ \nu(d^n) & \text{if } d \equiv 5 \pmod 8 \text{ and } \varepsilon_0 = \varepsilon. \end{cases}$$

Since $\nu(d) = d$, we have $\nu(d^n) = d^n$ by the corollary to Lemma 2. Moreover, the conductor of the order O_n is equal to

$$(4) \qquad \delta_n = \begin{cases} 2d^n & \text{if } d \equiv 1 \pmod 4, \\ d^n & \text{if } d \not\equiv 1 \pmod 4. \end{cases}$$

Suppose first that $d \not\equiv 5 \pmod 8$ or $d \equiv 5 \pmod 8$ and $\varepsilon_0 = \varepsilon^3$. Then using equalities (1), (3) and (4) we can write, for all $n \geq 0$,

$$h(O_n) = \begin{cases} h_{\mathbb{Q}(\sqrt{d})} \prod_{p \mid d^n} \left(1 - \frac{\chi(p)}{p}\right) & \text{if } d \not\equiv 1 \pmod 4, \\ 2h_{\mathbb{Q}(\sqrt{d})} \prod_{p \mid 2d^n} \left(1 - \frac{\chi(p)}{p}\right) & \text{if } d \equiv 1 \pmod 8, \\ \frac{2}{3} h_{\mathbb{Q}(\sqrt{d})} \prod_{p \mid 2d^n} \left(1 - \frac{\chi(p)}{p}\right) & \text{if } d \equiv 5 \pmod 8. \end{cases}$$

As $\chi(p) = 0$ if and only if p divides D, $\chi(2) = 1$ if and only if $d \equiv 1 \pmod 8$, and $\chi(2) = -1$ if and only if $d \equiv 5 \pmod 8$, the above equalities become

$$h(O_n) = h_{\mathbb{Q}(\sqrt{d})}.$$

Suppose now that $d \equiv 5 \pmod 8$ and $\varepsilon_0 = \varepsilon$. Let $\widetilde{O}^*_n$ be the unit group of $\widetilde{O}_n$. As $\varepsilon_0 = \varepsilon$, we have $\widetilde{O}^*_n = O^*_n$. Hence, from (3) and because $\nu(d^n) = d^n$, we obtain

$$[O^*_{\mathbb{Q}(\sqrt{d})} : \widetilde{O}^*_n] = [O^*_{\mathbb{Q}(\sqrt{d})} : O^*_n] = d^n.$$

Moreover, $\widetilde{O}_n$ is the order of conductor $\widetilde{\delta}_n = d^n$ of the ring $\mathbb{Z}[(1 + \sqrt{d})/2]$. Then we deduce from (1) that for all $n \geq 0$,

$$h(\widetilde{O}_n) = h_{\mathbb{Q}(\sqrt{d})} \prod_{p \mid d^n} \left(1 - \frac{\chi(p)}{p}\right) = h_{\mathbb{Q}(\sqrt{d})}. \ \blacksquare$$

It is well known that if α is a real quadratic irrationality of discriminant $\delta^2 D$, then the complete quotients of the period of its continued fraction expansion (i.e. using the notations of Lemma 1, the α_i with $i_0 + kl(\alpha) \leq i \leq i_0 + (k+1)l(\alpha) - 1$, $k \geq 0$) are in bijection with the reduced ideals of a class of ideals of the order O of conductor δ of the real quadratic field of discriminant D. It follows that if O has class number 1, then $l(\alpha) = \mathrm{Cal}(O)$.

Hence, as $\mathbb{Q}(\sqrt{d})$ is principal and $\nu(d)=d$, we have by Lemma 5, for all $n\ge 0$,

$$l(\sqrt{d}^{2n+1})=\mathrm{Cal}(O_n)\quad \text{if } d\not\equiv 5 \pmod 8 \text{ or } d\equiv 5 \pmod 8 \text{ and } \varepsilon_0=\varepsilon^3,$$

$$l\biggl(\frac{1+\sqrt{d}^{2n+1}}{2}\biggr)=\mathrm{Cal}(\widetilde{O}_n)\quad \text{if } d\equiv 5 \pmod 8 \text{ and } \varepsilon_0=\varepsilon.$$

Thus, Proposition 1 leads us to:

• If $d\not\equiv 5 \pmod 8$ or $d\equiv 5 \pmod 8$ and $\varepsilon_0=\varepsilon^3$ then

$$\liminf_n \frac{l(\sqrt{d}^{2n+1})}{\sqrt{d}^{2n+1}}\ge \frac{fL(1,\chi)}{\pi^2\prod_{p\mid D}(1+1/p)},$$

with $f=2$ if $d\equiv 1 \pmod 8$ and $f=6$ otherwise.

• If $d\equiv 5 \pmod 8$ and $\varepsilon_0=\varepsilon$ then

$$\liminf_n \frac{l((1+\sqrt{d}^{2n+1})/2)}{\frac12\sqrt{d}^{2n+1}}\ge \frac{6L(1,\chi)}{\pi^2\prod_{p\mid D}(1+1/p)}.$$

The theorem is then proved for $d\not\equiv 5 \pmod 8$, and for $d\equiv 5 \pmod 8$ and $\varepsilon_0=\varepsilon^3$. In the remaining case, it suffices to give a lower bound for $l(\sqrt{d}^{2n+1})$ in terms of $l((1+\sqrt{d}^{2n+1})/2)$.

For that, let π_n (resp. $\widetilde{\pi}_n$) and $P_s^{(n)}/Q_s^{(n)}$ (resp. $\widetilde{P}_s^{(n)}/\widetilde{Q}_s^{(n)}$) be respectively the length of the period and the sth convergent of the continued fraction expansion of $\sqrt{d}^{2n+1}$ (resp. $(1+\sqrt{d}^{2n+1})/2$). As by the assumption $\varepsilon_0=\varepsilon$, and using a well known fact of the theory of continued fractions, we have

$$\varphi_n=\widetilde{P}^{(n)}_{\widetilde{\pi}_n-1}+\widetilde{Q}^{(n)}_{\widetilde{\pi}_n-1}\biggl(\frac{-1+\sqrt{d}^{2n+1}}{2}\biggr)=P^{(n)}_{\pi_n-1}+Q^{(n)}_{\pi_n-1}\sqrt{d}^{2n+1},$$

which implies

$$\frac{\widetilde{P}^{(n)}_{\widetilde{\pi}_n-1}}{\widetilde{Q}^{(n)}_{\widetilde{\pi}_n-1}}=\frac12\cdot\frac{P^{(n)}_{\pi_n-1}}{Q^{(n)}_{\pi_n-1}}+1.$$

For β rational denote by $d(\beta)$ the number of partial quotients of its continued fraction expansion of even length. Hence

$$d\biggl(\frac{P^{(n)}_{\pi_n-1}}{Q^{(n)}_{\pi_n-1}}\biggr)=l(\sqrt{d}^{2n+1})+\gamma$$

and

$$d\biggl(\frac{\widetilde{P}^{(n)}_{\widetilde{\pi}_n-1}}{\widetilde{Q}^{(n)}_{\widetilde{\pi}_n-1}}\biggr)=l\biggl(\frac{1+\sqrt{d}^{2n+1}}{2}\biggr)+\gamma',$$

with γ and γ' equal to -1, 0 or 1. Then using a theorem of M. Mendès France [9] which gives a lower bound for the length of the continued fraction expansion of a homographic transformation of a rational number, we obtain

$$l(\sqrt{d}^{2n+1}) \geq \frac{1}{3} l\left(\frac{1+\sqrt{d}^{2n+1}}{2}\right) - 10. \qquad \blacksquare$$

4. Fields to which Theorem 1 applies. In Table 1 we give the set of all square-free numbers $250 \geq d \geq 2$ for which the field $\mathbb{Q}(\sqrt{d})$ is principal and we specify if d satisfies condition (ii) of Theorem 1 or not. 81 integers occur in this set, and for 59 of them, Theorem 1 can be applied.

Table 1

d	$\nu(d)=d$	d	$\nu(d)=d$	d	$\nu(d)=d$	d	$\nu(d)=d$	d	$\nu(d)=d$
2	yes	38	no	89	yes	141	yes	201	yes
3	yes	41	yes	93	no	149	yes	206	no
5	yes	43	yes	94	no	151	yes	209	yes
6	no	46	no	97	yes	157	yes	211	yes
7	yes	47	yes	101	yes	158	no	213	no
11	yes	53	yes	103	yes	161	yes	214	no
13	no	57	yes	107	yes	163	yes	217	yes
14	no	59	yes	109	yes	166	no	227	yes
17	yes	61	yes	113	yes	167	yes	233	yes
19	yes	62	no	118	no	173	yes	237	no
21	no	67	yes	127	yes	177	no	239	yes
22	no	69	no	129	yes	179	yes	241	yes
23	yes	71	yes	131	yes	181	yes	249	no
29	yes	73	yes	133	yes	191	yes		
31	yes	77	yes	134	no	193	yes		
33	yes	83	yes	137	yes	197	yes		
37	yes	86	no	139	yes	199	yes		

The principal difficulty in the applications of Theorem 1 comes from (ii). In fact, this condition can be rewritten in the following form: let $\varepsilon_0 = u + v\sqrt{d}$, u, v integers, be as before the fundamental unit of the ring $\mathbb{Z}[\sqrt{d}]$. Then condition (ii) is satisfied if and only if $\gcd(v, d) = 1$. Furthermore, if d is prime this condition is particularly simple, since $\nu(d) = 1$ or d ([3], Théorème 5.3). Moreover, it seems that in this case we always have $\nu(d) = d$.

Conjecture. *If d is a prime number, then d does not divide v (i.e. $\nu(d) = d$).*

This conjecture was proposed in 1952 by N. C. Ankeny, E. Artin and S. Chowla [1] for $d \equiv 1 \pmod 4$. It was proved by L. J. Mordell [10] for $d \equiv 1 \pmod 4$ regular prime, i.e. if the number of classes of ideals in the cyclotomic field $\mathbb{Q}(e^{2i\pi/d})$ is not divisible by d. In the same paper he has extended the conjecture to all primes $d \not\equiv 1 \pmod 4$.

In [8], p. 71, Gerry Myerson reports that this conjecture has been confirmed for $d \equiv 1 \pmod 4$, $d < 6270713$ and for $d \equiv 3 \pmod 4$, $d < 7679299$.

5. Some remarks on non-principal fields. It is natural to try to generalize Theorem 3 to non-principal fields. Indeed, Proposition 1 gives a lower bound for the number of reduced ideals in an order, and Lemma 1 an upper bound for the number of reduced ideal in each class of that order. Then we can hope to deduce a lower bound for this last number. Unfortunately, as shown below, this method is not successful. The reason is that the upper bound of Lemma 1 is too large. And it cannot be improved because of the possible irregular distribution of the reduced ideals in each class. In fact, this upper bound is the best possible.

For all $n \geq 0$, set $\omega_n = \sqrt{d}^{2n+1}$ if $d \not\equiv 5 \pmod 8$ or $d \equiv 5 \pmod 8$ and $\varepsilon_0 = \varepsilon^3$, and $\omega_n = (1 + \sqrt{d}^{2n+1})/2$ if $d \equiv 5 \pmod 8$ and $\varepsilon_0 = \varepsilon$. Then put $\Omega_n = \mathbb{Z}[\omega_n]$.

Set also

$$A = \frac{\gamma L(1, \chi)}{\pi^2 \prod_{p|D}(1 + 1/p)}$$

where

$$\gamma = \begin{cases} 3 & \text{if } d \equiv 5 \pmod 8 \text{ and } \varepsilon_0 = \varepsilon, \\ 2 & \text{if } d \equiv 1 \pmod 8, \\ 6 & \text{in the other cases.} \end{cases}$$

It is well known that $L(1, \chi) = 2h_k \frac{\log \varepsilon}{\sqrt{D}}$. Hence the constant A can be written as

$$A = \frac{2\gamma \log \varepsilon}{\pi^2 \sqrt{D} \prod_{p|D}(1 + 1/p)}.$$

Then Proposition 1 gives

$$\liminf_n \left(\frac{\mathrm{Cal}(\Omega_n)}{\sqrt{d}^{2n+1}} \right) \geq A.$$

Thus, for any $\eta > 0$ there exists n_0 such that for all $n \geq n_0$,

$$\mathrm{Cal}(\Omega_n) \geq (A - \eta)\sqrt{d}^{2n+1}. \tag{5}$$

Suppose that $\nu(d) = d$. Hence, Lemma 5 leads to $h(\Omega_n) = h_K$ for all $n \geq 0$. Next, choose h_{K-1} quadratic irrationals $\beta_2^{(n)}, \ldots, \beta_{h_K}^{(n)}$ of discriminant $\delta_n^2 D$ such that $\omega_n, \beta_2^{(n)}, \ldots, \beta_{h_K}^{(n)}$ is a system of representatives of each ideal class of Ω_n. Hence, for all $n \geq 0$,

$$l(\omega_n) + \sum_{i=2}^{h_K} l(\beta_i^{(n)}) = \mathrm{Cal}(\Omega_n). \tag{6}$$

But by Lemma 1, we have for all $i = 2, \ldots, h_K$,

$$l(\beta_i^{(n)}) \leq \frac{\log \varphi_n}{\log \frac{1+\sqrt{5}}{2}}, \tag{7}$$

where $\varphi_n > 1$ is the fundamental unit of Ω_n. Thus by Lemma 2,

$$\log \varphi_n = \begin{cases} d^n \log \varepsilon_0 & \text{if } \omega_n = \sqrt{d}^{2n+1}, \\ 3d^n \log \varepsilon & \text{if } \omega_n = (1+\sqrt{d}^{2n+1})/2. \end{cases} \tag{8}$$

Therefore by (5)–(8), we obtain $l(\omega_n) \geq H\sqrt{d}^{2n+1}$, where

$$H = \begin{cases} \dfrac{\log \varepsilon_0}{\sqrt{d}} \left(\dfrac{6h_K}{\pi^2 \prod_{p|D}(1+1/p)} - \dfrac{\eta\sqrt{d}}{\log \varepsilon_0} - \dfrac{h_K - 1}{\log \frac{1+\sqrt{5}}{2}} \right) \\ \qquad\qquad \text{if } d \not\equiv 1 \pmod 4 \text{ or } d \equiv 5 \pmod 8 \text{ and } \varepsilon_0 = \varepsilon, \\ \dfrac{\log \varepsilon_0}{\sqrt{d}} \left(\dfrac{4h_K}{\pi^2 \prod_{p|D}(1+1/p)} - \dfrac{\eta\sqrt{d}}{\log \varepsilon_0} - \dfrac{h_K - 1}{\log \frac{1+\sqrt{5}}{2}} \right) \\ \qquad\qquad \text{if } d \equiv 1 \pmod 8, \\ \dfrac{\log \varepsilon}{\sqrt{d}} \left(\dfrac{12h_K}{\pi^2 \prod_{p|D}(1+1/p)} - \dfrac{\eta\sqrt{d}}{\log \varepsilon} - \dfrac{3(h_K - 1)}{\log \frac{1+\sqrt{5}}{2}} \right) \\ \qquad\qquad \text{if } d \equiv 5 \pmod 8 \text{ and } \varepsilon_0 = \varepsilon^3. \end{cases}$$

The lower bound given for $l(\omega_n)$ is not trivial only if $H > 0$. But it is easy to see that $H > 0$ if and only if $h_K = 1$. Curiously, the determination of a lower bound for $l(\sqrt{d}^{2n+1})$ requires finding a more explicit upper bound for $l(\beta_i^{(n)})$.

References

[1] N. C. Ankeny, E. Artin and S. Chowla, *The class number of real quadratic number fields*, Ann. of Math. 56 (1952), 479–493.

[2] S. Chowla and S. S. Pillai, *Periodic simple continued fraction*, J. London Math. Soc. 6 (1931), 85–89.

[3] H. Cohen, *Multiplication par un entier d'une fraction continue périodique*, Acta Arith. 26 (1974), 129–148.

[4] D. A. Cox, *Primes of the Form $x^2 + ny^2$*, Wiley, 1989.

[5] R. Descombes, *Eléments de théorie des nombres*, Presses Univ. France, 1986.

[6] G. Grisel, *Sur la longueur de la fraction continue de* α^n, Acta Arith. 74 (1996), 161–176.
[7] —, *Length of the continued fraction of the powers of a rational fraction*, J. Number Theory 62 (1997), 322–337.
[8] R. K. Guy, *Unsolved Problems in Number Theory*, 2nd ed., Springer, 1994.
[9] M. Mendès France, *The depth of a rational number*, in: Topics in Number Theory (Debrecen, 1974), Colloq. Math. Soc. János Bolyai 13, North-Holland, 1976, 183–194.
[10] L. J. Mordell, *On a Pellian equation conjecture*, Acta Arith. 6 (1960), 137–144.

Département de Mathématiques
Université de Caen
Esplanade de la Paix
14032 Caen Cedex, France
E-mail: grisel@math.unicaen.fr

Received on 10.1.1997
and in revised form on 25.11.1997 (3110)