# Comptes Rendus 

## Mathématique

Stéphane R. Louboutin
On the continued fraction expansions of $(1+\sqrt{p q}) / 2$ and $\sqrt{p q}$
Volume 359, issue 9 (2021), p. 1201-1205
Published online: 25 November 2021
https: //doi.org/10.5802/crmath. 266
$(\sigma)$ BY $\quad$ This article is licensed under the
Creative Commons Attribution 4.0 International License.
http://creativecommons.org/licenses/by/4.0/


MERSENNE
Les Comptes Rendus. Mathématique sont membres du
Centre Mersenne pour l'édition scientifique ouverte
www.centre-mersenne.org
e-ISSN : 1778-3569

# On the continued fraction expansions of $(1+\sqrt{p q}) / 2$ and $\sqrt{p q}$ 

Stéphane R. Louboutin ${ }^{a}$

${ }^{a}$ Aix Marseille Université, CNRS, Centrale Marseille, I2M, Marseille, France
E-mail: stephane.louboutin@univ-amu.fr


#### Abstract

The evenness and the values modulo 4 of the lengths of the periods of the continued fraction expansions of $\sqrt{p}$ and $\sqrt{2 p}$ for $p \equiv 3(\bmod 4)$ a prime are known. Here we prove similar results for the continued fraction expansion of $\sqrt{p q}$, where $p, q \equiv 3(\bmod 4)$ are distinct primes.


Mathematical subject classification (2010). 11A55, 11R11.
Manuscript received 21st June 2021, accepted 27th August 2021.

## 1. Introduction

Let $\alpha$ be a real quadratic irrational number. Its continued fraction expansion $\alpha=\left[a_{0}, a_{1}, a_{2}, \ldots\right]$ is periodic, i.e. there exists $k \geq 0$ and $l \geq 1$ such that $a_{i+l}=a_{i}$ for $i \geq k$. In that case we write $\alpha=\left[a_{0}, \ldots, a_{k-1}, \overline{a_{k}, \ldots, a_{k+l-1}}\right]$. The least such $l$ is called the length of the period of the periodic continued fraction expansion of $\alpha$. The evenness of the length of the period of the continued fraction expansion of $\sqrt{p}$ for $p \equiv 3(\bmod 4)$ a prime is well known. In [8] we determined its value modulo 4 and gave a similar result for $\sqrt{2 p}$ :

Theorem 1. Take $d=p$ or $d=2 p$, where $p \equiv 3(\bmod 4)$ is a prime integer. Let $l \geq 1$ be the length of the period of the periodic continued fraction expansion $\sqrt{d}=\left[a_{0}, \overline{a_{1}, \ldots, a_{l}}\right]$. Then,
(i) $a_{0}=\lfloor\sqrt{d}\rfloor, a_{l}=2 a_{0}$ and $a_{k}=a_{l-k}$ for $1 \leq k \leq l-1$,
(ii) $l=2 L$ is even and $L$ is even if and only if $p \equiv 7(\bmod 8)$,
(iii) $a_{l / 2}=a_{L}$ is the integer in $\left\{a_{0}-1, a_{0}\right\}$ of the same parity as $d$.

This behavior in the case of $d=p$ had already been proved in [3, Corollary 2 p. 2071]. Our proof was different and applied both to $d=p$ and $d=2 p$. It was based on the arithmetic of quadratic number fields and their ideal class groups in the narrow sense (as in [6] and [7]). Let $\mathscr{I}$ be an integral ideal of the ring of algebraic integers $\mathbb{Z}_{K}$ of a real quadratic number field $K$. Recall that $\mathscr{I}$ is principal if and only if there exists $\alpha \in \mathbb{Z}_{K}$ such that $\mathscr{I}=\alpha \mathbb{Z}_{K}$, whereas $\mathscr{I}$ is principal in the narrow sense if there exists a totally positive element $\alpha \in \mathbb{Z}_{K}$ such that $\mathscr{I}=\alpha \mathbb{Z}_{K}$. Here, bearing on a similar approach, we prove:

Theorem 2. Let $p, q$ be two prime integers equal to $3(\bmod 4)$, with $3 \leq p<q$. Let $l \geq 1$ be the length of the period of the periodic continued fraction expansion $(1+\sqrt{p q}) / 2=\left[a_{0}, \overline{a_{1}, \ldots, a_{l}}\right]$. Then,
(i) $a_{l}=2 a_{0}-1$ and $a_{k}=a_{l-k}$ for $1 \leq k \leq l-1$,
(ii) $l=2 L$ is even and $(-1)^{L}=\left(\frac{p}{q}\right)$ (Legendre's symbol),
(iii) $a_{l / 2}=a_{L}$ is the unique odd integer in $\{\lfloor\sqrt{q / p}\rfloor-1,\lfloor\sqrt{q / p}\rfloor\}$.

Theorem 3. Let $p, q$ be two prime integers equal to $3(\bmod 4)$, with $3 \leq p<q$. Let $l \geq 1$ be the length of the period of the periodic continued fraction expansion $\sqrt{p q}=\left[a_{0}, \overline{a_{1}, \ldots, a_{l}}\right]$. Then,
(i) $a_{0}=\lfloor\sqrt{p q}\rfloor, a_{l}=2 a_{0}$ and $a_{k}=a_{l-k}$ for $1 \leq k \leq l-1$,
(ii) $l=2 L$ is even and $(-1)^{L}=\left(\frac{p}{q}\right)$ (Legendre's symbol),
(iii) $a_{l / 2}=a_{L}=2\lfloor\sqrt{q / p}\rfloor$ is even.

Part of Theorem 3 was proved in [10, Corollary 1], [2, Theorem 2] and [1], but notice that point (iii) of Theorem 3 is much more precise than [1, Theorem 1.2].

## 2. On the continued fraction expansions of some real quadratic irrational numbers

(i). Let $\omega$ be a real quadratic irrational number. Hence $\omega=(P+\sqrt{d}) / Q$ for some non-square integer $d>1$, some $P \in \mathbb{Z}$ and some $Q \in \mathbb{Z} \backslash\{0\}$ dividing $d-P^{2}$. Then $\omega$ is called reduced if $\omega>1$ and $-1 / \omega^{\prime}>1$, where $\omega^{\prime}=(P-\sqrt{d}) / Q$ is the conjugate of $\omega$ in $\mathbb{Q}(\sqrt{d})$. Hence, $\omega$ is reduced if and only if $P+\sqrt{d} \geq Q>\sqrt{d}-P>0$, which implies $0<Q<2 \sqrt{d},|P|<\sqrt{d}, 2 \sqrt{d} / Q-1<\omega<2 \sqrt{d} / Q$ and $\lfloor\omega\rfloor \in\{\lfloor 2 \sqrt{d} / Q\rfloor-1,\lfloor 2 \sqrt{d} / Q\rfloor\}$.
(ii). The continued fraction expansion $\omega_{0}=\left[a_{0}, a_{1}, \ldots\right]$ of $\omega_{0}=\left(P_{0}+\sqrt{d}\right) / Q_{0}$ with $P_{0}, Q_{0} \in \mathbb{Z}$, and $Q_{0} \neq 0$ dividing $d-P_{0}^{2}$, can be computed inductively by writing $\omega_{k}=\left[a_{k}, \ldots\right]$ as $\omega_{k}=\left(P_{k}+\sqrt{d}\right) / Q_{k}$, where the $P_{k}, Q_{k} \in \mathbb{Z}$ with $Q_{k} \neq 0$ dividing $d-P_{k}^{2}$ are inductively computed, using $a_{k}=\left\lfloor\omega_{k}\right\rfloor$ and $\omega_{k}=a_{k}+1 / \omega_{k+1}$, by $P_{k+1}=a_{k} Q_{k}-P_{k}$ and $Q_{k+1}=\left(d-P_{k+1}^{2}\right) / Q_{k}=\left(d-P_{k}^{2}\right) / Q_{k}+2 a_{k} P_{k}-a_{k}^{2} Q_{k}$. (Hence $Q_{1}$ is a non-zero rational integer, $Q_{k+1}=Q_{k-1}+2 a_{k} P_{k}-a_{k}^{2} Q_{k}$ for $k \geq 1$ and the $Q_{k}$ 's are non-zero rational integers, by induction on $k$.)
(iii). Assume that $\omega_{0}=\left(P_{0}+\sqrt{d}\right) / Q_{0}$ is reduced. Using $\omega_{k}=a_{k}+1 / \omega_{k+1}$, we obtain that all the $\omega_{k}$ 's are reduced, by induction. Hence $0<Q_{k}<2 \sqrt{d}$ and $\left|P_{k}\right|<\sqrt{d}$ for $k \geq 0$ and there are only finitely many pairwise distinct $\omega_{k}$ 's. It follows that $\omega_{m}=\omega_{n}$ for some $m>n \geq 0$, which implies $\omega_{k+l}=\omega_{k}$ and $a_{k+l}=a_{k}$ for $k \geq b$, where $l:=m-n \geq 1$. Hence, the continued fraction expansion of $\omega_{0}$ is $l$-periodic. In fact is purely periodic, which we write $\omega_{0}=\left[\overline{a_{0}, \ldots, a_{l-1}}\right]$, i.e. $\omega_{k+l}=\omega_{k}$ and $a_{k+l}=a_{k}$ for $k \geq 0$, where $l:=m-n \geq 1$. (Notice that $\omega_{k+l}=\omega_{k}$ and $k \geq 1$ imply $\omega_{k-1}-a_{k-1}=1 / \omega_{k}=1 / \omega_{k+l}=\omega_{k+l-1}-a_{k+l-1}$, hence imply $\omega_{k+l-1}-\omega_{k-1}=a_{k+l-1}-a_{k-1} \in \mathbb{Z}$ and $\omega_{k+l-1}-\omega_{k-1}=\omega_{k+l-1}^{\prime}-\omega_{k-1}^{\prime} \in(-1,1) \cap \mathbb{Z}$, hence imply $\omega_{k+l-1}=\omega_{k-1}$.) The least such $l \geq 1$ is called the length of the purely periodic continued fraction expansion of the reduced quadratic irrational number $\omega_{0}$.

In that case $-1 / \omega_{0}^{\prime}=\left[\overline{a_{l-1}, \ldots, a_{0}}\right]$ (e.g. see [4, XV page 311]).
(iv). If $\omega_{0}=\left[\overline{a_{0}, a_{1}, \ldots, a_{l-1}}\right] \in \mathbb{Q}(\sqrt{d})$ is reduced, using $\omega_{k}=a_{k}+1 / \omega_{k+1}$ we obtain $\mathbb{M}_{k}:=$ $\mathbb{Z}+\mathbb{Z} \omega_{k}=\mathbb{Z}+\mathbb{Z} \omega_{k+1}^{-1}=\omega_{k+1}^{-1} \mathbb{M}_{k+1}$ and $\mathbb{M}_{0}=\omega_{1}^{-1} \mathbb{M}_{1}=\omega_{1}^{-1} \omega_{2}^{-1} \mathbb{M}_{2}=\cdots=\varepsilon^{-1} \mathbb{M}_{l}=\varepsilon^{-1} \mathbb{M}_{0}$, where $\varepsilon=\omega_{1} \omega_{2} \ldots \omega_{l}=\omega_{0} \omega_{1} \ldots \omega_{l-1}$. Therefore, $\varepsilon$ is a unit of norm $N(\varepsilon)=\prod_{k=0}^{l-1}\left(\omega_{k} \omega_{k}^{\prime}\right)=(-1)^{l}$ of the $\mathbb{Z}$-module $\mathbb{M}_{0}=\mathbb{Z}+\mathbb{Z} \omega_{0} \subseteq \mathbb{Q}(\sqrt{d})\left(\right.$ as $\omega_{k}>1$ and $\left.-1 / \omega_{k}^{\prime}>1\right)$.
(v). See [4, p. 305-322], [5, Chapter 10] and [9] for more information on continued fractions.

## 3. Proof of Theorem 2

Let $d \equiv 1(\bmod 4)$ be a non-square integer, with $d \geq 5$. Let $g^{\prime} \geq 1$ be the unique odd integer in $[\sqrt{d}-2, \sqrt{d})$. Then $\omega_{0}=\left(P_{0}+\sqrt{d}\right) / Q_{0}=\left(g^{\prime}+\sqrt{d}\right) / 2$ is reduced. Its continued fraction expansion $\omega_{0}=\left[\overline{g^{\prime}, a_{1}, \ldots, a_{l-1}}\right]$ is purely periodic and $\omega_{1}=\left[\overline{a_{1}, \ldots, a_{l-1}, g^{\prime}}\right]=1 /\left(\omega_{0}-g^{\prime}\right)=2 /\left(\sqrt{d}-g^{\prime}\right)=$ $-1 / \omega_{0}^{\prime}=\left[a_{l-1}, \ldots, a_{1}, g^{\prime}\right]$. Hence, $a_{k}=a_{l-k}$ for $1 \leq k \leq l-1$. Using $Q_{0}=2$, the oddness of $P_{0}=g^{\prime}$, the evenness of $Q_{1}=\left(d-P_{0}^{2}\right) / / Q_{0}=\left(d-g^{\prime 2}\right) / 2$ and the identities $Q_{k+1}=Q_{k-1}+2 a_{k} P_{k}-a_{k}^{2} Q_{k}$ for $k \geq 1$ and $P_{k+1}=a_{k} Q_{k}-P_{k}$ for $k \geq 0$, we obtain that the $Q_{k}$ 's are even and the $P_{k}$ 's are odd for $k \geq 0$. Consequently, if $d$ is square-free then $\mathbb{M}_{0}$ is equal to the ring of algebraic integers $\mathbb{Z}_{\mathbb{K}}$ of the real quadratic number field $\mathbb{K}=\mathbb{Q}(\sqrt{d})$ and the $\mathbb{Z}$-modules

$$
\mathscr{I}_{k}:=\left(Q_{k} / 2\right) \mathbb{M}_{k}=\left(Q_{k} / 2\right) \mathbb{Z}+\frac{P_{k}+\sqrt{d}}{2} \mathbb{Z}=\left(Q_{k} / 2\right) \omega_{1} \ldots \omega_{k} \mathbb{M}_{0}=\alpha_{k} \mathbb{Z}_{\mathbb{K}}
$$

are primitive, principal, integral ideals of norms $Q_{k} / 2$ of the real quadratic number field $\mathbb{Q}(\sqrt{d})$, where $\alpha_{k}=\left(Q_{k} / 2\right) \omega_{1} \ldots \omega_{k} \in \mathscr{I}_{k} \subseteq \mathbb{Z}_{\mathbb{K}}$ is an algebraic integer of norm $(-1)^{k}\left(Q_{k} / 2\right)$ (recall that $\omega_{k}>1$ and $-1 / \omega_{k}^{\prime}>1$ for $k \geq 0$ ). Hence, $\mathscr{I}_{k}$ is principal in the narrow sense if and only if $k$ is even.

Now, assume that $d$ is divisible by a prime $p \equiv 3(\bmod 4)$. Since the congruence $x^{2}-d y^{2} \equiv-4(\bmod p)$ has no solution in rational integers, any algebraic unit of $\mathbb{Q}(\sqrt{d})$ has norm +1 . The algebraic unit $\varepsilon=\omega_{0} \omega_{1} \ldots \omega_{l-1}:=\mathbb{Z}+\mathbb{Z} \omega_{0}$ being of norm $(-1)^{l}, l=2 L$ is even, $\omega_{0}=\left[\overline{g^{\prime}, a_{1}, \ldots, a_{L-1}, a_{L}, a_{L-1}, \ldots, a_{1}}\right], \omega_{L}=\left[\overline{a_{L}, \ldots, a_{1}, g^{\prime}, a_{1}, \ldots, a_{L-1}}\right]$ and $\omega_{L+1}=$ $\left[a_{L-1}, \ldots, a_{1}, g^{\prime}, a_{1}, \ldots, a_{L}\right]=-1 / \omega_{L}^{\prime}$. Hence, $-1=\omega_{L+1} \omega_{L}^{\prime}=\frac{P_{L+1}+\sqrt{d}}{Q_{L+1}} \frac{P_{L}-\sqrt{d}}{Q_{L}}$, which implies $P_{L+1}=P_{L}$. Since $P_{L+1}=a_{L} Q_{L}-P_{L}$, we have $P_{L+1}=a_{L}\left(Q_{L} / 2\right)$ and $a_{L}$ is odd. Moreover,

$$
d-P_{L+1}^{2}=d-a_{L}^{2}\left(Q_{L} / 2\right)^{2}=4\left(Q_{L} / 2\right)\left(Q_{L+1} / 2\right)
$$

Hence, $Q_{L} / 2$ divides $d$. Finally, $\omega_{L}=\left(P_{L}+\sqrt{d}\right) / Q_{L}$ being reduced, we have $1<Q_{L}<2 \sqrt{d}$ and $a_{L}=\left\lfloor\omega_{L}\right\rfloor \in\left\{\left\lfloor 2 \sqrt{d} / Q_{L}\right\rfloor,\left\lfloor 2 \sqrt{d} / Q_{L}\right\rfloor-1\right\}$, and we obtain the following Proposition and Corollary from which Theorem 2 follows:

Proposition 4. Let $d \equiv 1(\bmod 4)$ be a square-free integer, with $d \geq 5$ such that at least one prime $p \equiv 3(\bmod 4)$ divides $d$. Let $g^{\prime} \geq 1$ be the unique odd integer in the interval $[\sqrt{d}-2, \sqrt{d})$. Set $\omega_{0}=\left(g^{\prime}+\sqrt{d}\right) / 2 . l \geq 1$ be the length of the period of the purely periodic continued fraction expansion $\omega_{0}=\left[\overline{g^{\prime}, a_{1}, \ldots, a_{l-1}}\right]$. Then
(i) $a_{k}=a_{l-k}$ for $1 \leq k \leq l-1$;
(ii) $l=2 L$ is even;
(iii) $Q_{L} / 2$ divides $d$ and $1<Q_{L} / 2<\sqrt{d}$;
(iv) $a_{L}$ is odd and $a_{L}=\left\lfloor\omega_{L}\right\rfloor \in\left\{\left\lfloor 2 \sqrt{d} / Q_{L}\right\rfloor,\left\lfloor 2 \sqrt{d} / Q_{L}\right\rfloor-1\right\}$;
(v) The integral ideal $\mathscr{I}_{L}=\left(Q_{L} / 2\right) \mathbb{Z}+\frac{P_{L}+\sqrt{d}}{2} \mathbb{Z}$ of norm $Q_{L} / 2$ is principal and $L$ is even if and only $\mathscr{I}_{L}$ is principal in the narrow sense.
Corollary 5. Let $p, q$ be two prime integers equal to $3(\bmod 4)$, with $3 \leq p<q$. Take $d=p q \equiv 1$ $(\bmod 4)$. Then $Q_{L} / 2=p$. Hence, $\mathscr{I}_{L}$ is the prime ramified ideal $\mathscr{P}$ of norm $p$ of the ring of algebraic integers of the real quadratic field $\mathbb{Q}(\sqrt{d})$ and $a_{L}$ is the unique odd integer in $\{\lfloor\sqrt{q / p}\rfloor,\lfloor\sqrt{q / p}\rfloor-1\}$. Moreover, $\mathscr{P}$ is principal in the narrow sense if and only if $\left(\frac{p}{q}\right)=+1$.
Proof. Let $\mathscr{P}$ and $\mathscr{Q}$ be the prime ideals above $p$ and $q$, respectively. Hence $\mathscr{P}=\mathscr{I}=(\alpha)$ is principal and $\mathscr{P} \mathscr{Q}=(\sqrt{d})$ is also clearly principal. Since $\sqrt{d} \in \mathscr{P} \mathscr{Q} \subseteq \mathscr{P}=(\alpha)$, we have $\sqrt{d}=\alpha \beta$ for some algebraic integer $\beta$. Hence $\mathscr{Q}=(\beta)$ is also principal. Since $N(\alpha) N(\beta)=N(\alpha \beta)=N(\sqrt{d})=$ $-d<0$, only one of the two principal ideals $\mathscr{P}$ or $\mathscr{Q}$ is principal in the narrow sense. If $\mathscr{P}=(\alpha)$ is principal in the narrow sense, with $\alpha=(x+y \sqrt{d}) / 2$ such that $p=N(\alpha)=\left(x^{2}-p q y^{2}\right) / 4$, then $p$ divides $x=p X, 4=p X^{2}-q y^{2}$ and $\left(\frac{p}{q}\right)=+1$. If $\mathscr{P}$ is not principal in the narrow sense, then $\mathscr{Q}=(\beta)$ is principal in the narrow sense, with $\beta=(x+y \sqrt{d}) / 2$ such that $q=N(\beta)=\left(x^{2}-p q y^{2}\right) / 4$. Hence, $q$ divides $x=q X, 4=q X^{2}-p y^{2}$ and $\left(\frac{-p}{q}\right)=-\left(\frac{p}{q}\right)=+1$.

## 4. Proof of Theorem 3

Let $d \equiv 1(\bmod 4)$ be a non-square integer, with $d \geq 5$. Set $g=\lfloor\sqrt{d}\rfloor$. Then $\omega_{0}=\left(P_{0}+\sqrt{d}\right) / Q_{0}=$ $g+\sqrt{d}$ is reduced. Since $\mathbb{M}_{0}=\mathbb{Z}\left[\omega_{0}\right]=\mathbb{Z}[\sqrt{d}]$ is not the ring of algebraic integers of $\mathbb{Q}(\sqrt{d})$, the proof of Theorem 3 is a little more tricky than the one of Theorem 2. Here again, the continued fraction expansion $\omega_{0}=\left[\overline{2 g, a_{1}, \ldots, a_{l-1}}\right]$ is purely periodic and $\omega_{1}=\left[\overline{a_{1}, \ldots, a_{l-1}, 2 g}\right]=1 /\left(\omega_{0}-\right.$ $2 g)=1 /(\sqrt{d}-g)=-1 / \omega_{0}^{\prime}=\left[\overline{a_{l-1}, \ldots, a_{1}, 2 g}\right]$. Hence, $a_{k}=a_{l-k}$ for $1 \leq k \leq l-1$. Suppose that we had $Q_{n} \equiv 2(\bmod 4)$ for some $n \geq 0$. Then $P_{n+1}$ would be odd and $Q_{n+1}$ would be even, as $Q_{n} Q_{n+1}=d-P_{n+1}^{2}$. Therefore, all the $Q_{k}$ 's would be even for $k \geq n$, as $Q_{k+1}=Q_{k-1}+2 a_{k} P_{k}-a_{k}^{2} Q_{k}$ for $k \geq 1$, hence for $k \geq 0$, by pure periodicity of the continued fraction expansion of $\omega_{0}$. Since $Q_{0}$ is odd, we deduce that $Q_{k} \not \equiv 2(\bmod 4)$ for $k \geq 0$.

Now, assume that $d$ is divisible by a prime $p \equiv 3(\bmod 4)$. As above, $l=2 L$ is even and

$$
2 P_{L+1}=a_{L} Q_{L}, \quad \text { and } \quad 4 d-a_{L}^{2} Q_{L}^{2}=4 Q_{L} Q_{L+1} .
$$

Hence, $Q_{L}$ divides $4 d$ and 4 does not divide $Q_{L}$ and we obtain the following Proposition from which Theorem 3 follows, by Corollary 5 :

Proposition 6. Let $d \equiv 1(\bmod 4)$ be a square-free integer, with $d \geq 5$ such that at least one prime $p \equiv 3(\bmod 4)$ divides $d$.

Set $\omega_{0}=g+\sqrt{d}$, where $g=\lfloor\sqrt{d}\rfloor$. Let $l \geq 1$ be the length of the period of the purely periodic continued fraction expansion $\omega_{0}=\left[\overline{2 g, a_{1}, \ldots, a_{l-1}}\right]$. Then
(i) $a_{k}=a_{l-k}$ for $1 \leq k \leq l-1$;
(ii) $l=2 L$ is even;
(iii) $Q_{L}$ divides $2 d$ and $1<Q_{L}<2 \sqrt{d}$;
(iv) $a_{L}=\left\lfloor\omega_{L}\right\rfloor \in\left\{\left\lfloor 2 \sqrt{d} / Q_{L}\right\rfloor,\left\lfloor 2 \sqrt{d} / Q_{L}\right\rfloor-1\right\}$;
(v) if $d=p q$, where $p, q$ are prime numbers equal to 3 modulo 4 with $p<q$, then $a_{L}=$ $2\lfloor\sqrt{q / p}\rfloor, Q_{L}=p$, the prime ideal $\mathscr{P}$ of norm $p$ of the ring of algebraic integers of the real quadratic field $\mathbb{Q}(\sqrt{d})$ is principal and $L$ is even if and only if $\mathscr{P}$ is principal in the narrow sense.

Proof. It remains to prove point $(\nu)$. Since $Q_{L}$ divides $2 p q, Q_{L} \neq 2(\bmod 4)$ and $Q_{L}<2 \sqrt{p q}$, we have $Q_{L} \in\{p, q\}$. Since $Q_{L}=q$ would yield the contradiction $4 q Q_{L+1}=4 d-a_{L}^{2} Q_{L}^{2} \leq 4 p q-4 q^{2}<0$, we have $Q_{L}=p$. Hence, $a_{L}$ is even, as $2 P_{L}=a_{L} Q_{L}$, and $a_{L} \in\{\lfloor 2 x\rfloor,\lfloor 2 x\rfloor-1\}$, where $x=\sqrt{d} / Q_{L}$. Since $\lfloor 2 x\rfloor \in\{2\lfloor x\rfloor, 2\lfloor x\rfloor+1\}$ for $x$ real, we have that $a_{L}$ is even and $a_{L} \in\{2\lfloor x\rfloor-1,2\lfloor x\rfloor, 2\lfloor x\rfloor+1\}$. Therefore, $a_{L}=2\lfloor x\rfloor=2\left\lfloor\sqrt{d} / Q_{L}\right\rfloor=2\lfloor\sqrt{q / p}\rfloor$.

Finally, set $\beta_{L}=Q_{L} \omega_{1} \ldots \omega_{L}$. Then

$$
\mathscr{J}_{L}:=\beta_{L} \mathbb{Z}[\sqrt{d}]=\beta_{L} \mathbb{M}_{0}=Q_{L} \omega_{1} \ldots \omega_{L} \mathbb{M}_{0}=Q_{L} \mathbb{M}_{L}=Q_{L} \mathbb{Z}+\left(P_{L}+\sqrt{d}\right) \mathbb{Z} \subseteq \mathbb{Z}[\sqrt{d}]
$$

Hence, $\beta_{L}=x+y \sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ and $\left\{Q_{L}, P_{L}+\sqrt{d}\right\}$ and $\left\{\beta_{L}, \beta_{L} \sqrt{d}\right\}=\{x+y \sqrt{d}, d y+x \sqrt{d}\}$ are two $\mathbb{Z}$-bases of $\mathscr{J}_{L}$ and the change of basis matrix

$$
A=\left(\begin{array}{cc}
\frac{x-y P_{L}}{Q_{L}} & \frac{d y-x P_{L}}{Q_{L}} \\
y & x
\end{array}\right)
$$

is in $M_{2}(\mathbb{Z})$ and of determinant $\pm 1$, i.e. $\pm 1=\left(x^{2}-d y^{2}\right) / Q_{L}=N\left(\beta_{L}\right) / p$. Therefore, $N\left(\beta_{L}\right)=$ $(-1)^{L} p$, with $\beta_{L} \in \mathbb{Z}[\sqrt{d}]$. It follows that the prime ideal $\mathscr{P}$ of the ring of algebraic integers $\mathbb{Z}_{\mathbb{K}}=\mathbb{Z}[(1+\sqrt{d}) / 2]$ of $\mathbb{K}=\mathbb{Q}(\sqrt{d})$ lying above $p$ is principal and equal to $\left(\beta_{L}\right)$ and that $\mathscr{P}$ it is principal in the narrow sense if and only if $L$ is even.

## References

[1] S. Das, D. Chakraborty, A. Saikia, "On the period of the continued fraction of $\sqrt{p q} "$, Acta Arith. 196 (2020), no. 3, p. 291-302.
[2] C. Friesen, "Legendre symbols and continued fractions", Acta Arith. 59 (1991), no. 4, p. 365-379.
[3] E. P. Golubeva, "Quadratic irrationals with fixed period length in the continued fraction expansion", J. Math. Sci., New York 70 (1994), no. 6, p. 2059-2076.
[4] H. Hasse, Vorlesungen über Zahlentheorie, Grundlehren der Mathematischen Wissenschaften, vol. 59, Springer, 1964.
[5] L. K. Hua, Introduction to number theory, Springer, 1982, translated from the Chinese by Peter Shiu.
[6] S. R. Louboutin, "Continued fractions and real quadratic fields", J. Number Theory 30 (1988), no. 2, p. 167-176.
[7] -, "Groupes des classes d’idéaux triviaux", Acta Arith. 54 (1989), no. 1, p. 61-74.
[8] ——" "On the continued fraction expansions of $\sqrt{p}$ and $\sqrt{2 p}$ for primes $p \equiv 3(\bmod 4)$ ", in Class groups of Number fields and related topics, Springer, 2020, p. 175-178.
[9] O. Perron, Die Lehre von den Kettenbrüchen. Band I. 3. erweiterte und verbesserte Aufl., Teubner, 1954.
[10] A. J. van der Poorten, P. G. Walsh, "A note on Jacobi symbols and continued fractions", Am. Math. Mon. 106 (1999), no. 1, p. 52-56.

