



INSTITUT DE FRANCE  
Académie des sciences

# *Comptes Rendus*

---

# *Mathématique*


Stéphane R. Louboutin

**On the continued fraction expansions of  $(1 + \sqrt{pq})/2$  and  $\sqrt{pq}$**

Volume 359, issue 9 (2021), p. 1201-1205

<<https://doi.org/10.5802/crmath.266>>

© Académie des sciences, Paris and the authors, 2021.  
*Some rights reserved.*

 This article is licensed under the  
CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL LICENSE.  
<http://creativecommons.org/licenses/by/4.0/>



*Les Comptes Rendus. Mathématique* sont membres du  
Centre Mersenne pour l'édition scientifique ouverte  
[www.centre-mersenne.org](http://www.centre-mersenne.org)



Number theory / *Théorie des nombres*

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

Stéphane R. Louboutin<sup>a</sup>

<sup>a</sup> Aix Marseille Université, CNRS, Centrale Marseille, I2M, Marseille, France

E-mail: [stephane.louboutin@univ-amu.fr](mailto: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  $\sqrt{2p}$  for  $p \equiv 3 \pmod{4}$  a prime are known. Here we prove similar results for the continued fraction expansion of  $\sqrt{pq}$ , where  $p, q \equiv 3 \pmod{4}$  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  $\alpha = [a_0, a_1, a_2, \dots]$  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  $\alpha = [a_0, \dots, a_{k-1}, \overline{a_k, \dots, a_{k+l-1}}]$ . 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  $p \equiv 3 \pmod{4}$  a prime is well known. In [8] we determined its value modulo 4 and gave a similar result for  $\sqrt{2p}$ :

**Theorem 1.** *Take  $d = p$  or  $d = 2p$ , where  $p \equiv 3 \pmod{4}$  is a prime integer. Let  $l \geq 1$  be the length of the period of the periodic continued fraction expansion  $\sqrt{d} = [a_0, \overline{a_1, \dots, a_l}]$ . Then,*

- (i)  $a_0 = \lfloor \sqrt{d} \rfloor$ ,  $a_l = 2a_0$  and  $a_k = a_{l-k}$  for  $1 \leq k \leq l-1$ ,
- (ii)  $l = 2L$  is even and  $L$  is even if and only if  $p \equiv 7 \pmod{8}$ ,
- (iii)  $a_{l/2} = a_L$  is the integer in  $\{a_0 - 1, a_0\}$  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  $d = 2p$ . 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  $\mathcal{I}$  be an integral ideal of the ring of algebraic integers  $\mathbb{Z}_K$  of a real quadratic number field  $K$ . Recall that  $\mathcal{I}$  is principal if and only if there exists  $\alpha \in \mathbb{Z}_K$  such that  $\mathcal{I} = \alpha\mathbb{Z}_K$ , whereas  $\mathcal{I}$  is principal in the narrow sense if there exists a totally positive element  $\alpha \in \mathbb{Z}_K$  such that  $\mathcal{I} = \alpha\mathbb{Z}_K$ . Here, bearing on a similar approach, we prove:

**Theorem 2.** Let  $p, q$  be two prime integers equal to  $3 \pmod{4}$ , with  $3 \leq p < q$ . Let  $l \geq 1$  be the length of the period of the periodic continued fraction expansion  $(1 + \sqrt{pq})/2 = [a_0, \overline{a_1, \dots, a_l}]$ . Then,

- (i)  $a_l = 2a_0 - 1$  and  $a_k = a_{l-k}$  for  $1 \leq k \leq l - 1$ ,
- (ii)  $l = 2L$  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  $3 \pmod{4}$ , with  $3 \leq p < q$ . Let  $l \geq 1$  be the length of the period of the periodic continued fraction expansion  $\sqrt{pq} = [a_0, \overline{a_1, \dots, a_l}]$ . Then,

- (i)  $a_0 = \lfloor \sqrt{pq} \rfloor$ ,  $a_l = 2a_0$  and  $a_k = a_{l-k}$  for  $1 \leq k \leq l - 1$ ,
- (ii)  $l = 2L$  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  $Q \in \mathbb{Z} \setminus \{0\}$  dividing  $d - P^2$ . Then  $\omega$  is called *reduced* if  $\omega > 1$  and  $-1/\omega' > 1$ , where  $\omega' = (P - \sqrt{d})/Q$  is the conjugate of  $\omega$  in  $\mathbb{Q}(\sqrt{d})$ . Hence,  $\omega$  is reduced if and only if  $P + \sqrt{d} > Q > \sqrt{d} - P > 0$ , which implies  $0 < Q < 2\sqrt{d}$ ,  $|P| < \sqrt{d}$ ,  $2\sqrt{d}/Q - 1 < \omega < 2\sqrt{d}/Q$  and  $[\omega] \in \{[2\sqrt{d}/Q] - 1, [2\sqrt{d}/Q]\}$ .

(ii). The *continued fraction expansion*  $\omega_0 = [a_0, a_1, \dots]$  of  $\omega_0 = (P_0 + \sqrt{d})/Q_0$  with  $P_0, Q_0 \in \mathbb{Z}$ , and  $Q_0 \neq 0$  dividing  $d - P_0^2$ , can be computed inductively by writing  $\omega_k = [a_k, \dots]$  as  $\omega_k = (P_k + \sqrt{d})/Q_k$ , where the  $P_k, Q_k \in \mathbb{Z}$  with  $Q_k \neq 0$  dividing  $d - P_k^2$  are inductively computed, using  $a_k = [\omega_k]$  and  $\omega_k = a_k + 1/\omega_{k+1}$ , by  $P_{k+1} = a_k Q_k - P_k$  and  $Q_{k+1} = (d - P_{k+1}^2)/Q_k = (d - P_k^2)/Q_k + 2a_k P_k - a_k^2 Q_k$ . (Hence  $Q_1$  is a non-zero rational integer,  $Q_{k+1} = Q_{k-1} + 2a_k P_k - a_k^2 Q_k$  for  $k \geq 1$  and the  $Q_k$ 's are non-zero rational integers, by induction on  $k$ .)

(iii). Assume that  $\omega_0 = (P_0 + \sqrt{d})/Q_0$  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  $|P_k| < \sqrt{d}$  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  $\omega_0 = [\overline{a_0, \dots, a_{l-1}}]$ , 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  $\omega_{k+l-1} - \omega_{k-1} = \omega'_{k+l-1} - \omega'_{k-1} \in (-1, 1) \cap \mathbb{Z}$ , 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  $-1/\omega'_0 = [\overline{a_{l-1}, \dots, a_0}]$  (e.g. see [4, XV page 311]).

(iv). If  $\omega_0 = [\overline{a_0, a_1, \dots, a_{l-1}}] \in \mathbb{Q}(\sqrt{d})$  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  $\mathbb{M}_0 = \omega_1^{-1}\mathbb{M}_1 = \omega_1^{-1}\omega_2^{-1}\mathbb{M}_2 = \dots = \varepsilon^{-1}\mathbb{M}_l = \varepsilon^{-1}\mathbb{M}_0$ , where  $\varepsilon = \omega_1\omega_2 \dots \omega_l = \omega_0\omega_1 \dots \omega_{l-1}$ . Therefore,  $\varepsilon$  is a unit of norm  $N(\varepsilon) = \prod_{k=0}^{l-1} (\omega_k \omega'_k) = (-1)^l$  of the  $\mathbb{Z}$ -module  $\mathbb{M}_0 = \mathbb{Z} + \mathbb{Z}\omega_0 \subseteq \mathbb{Q}(\sqrt{d})$  (as  $\omega_k > 1$  and  $-1/\omega'_k > 1$ ).

(v). See [4, p. 305–322], [5, Chapter 10] and [9] for more information on continued fractions.

### 3. Proof of Theorem 2

Let  $d \equiv 1 \pmod{4}$  be a non-square integer, with  $d \geq 5$ . Let  $g' \geq 1$  be the unique odd integer in  $[\sqrt{d}-2, \sqrt{d}]$ . Then  $\omega_0 = (P_0 + \sqrt{d})/Q_0 = (g' + \sqrt{d})/2$  is reduced. Its continued fraction expansion  $\omega_0 = [g', a_1, \dots, a_{l-1}]$  is purely periodic and  $\omega_1 = [a_1, \dots, a_{l-1}, g'] = 1/(\omega_0 - g') = 2/(\sqrt{d} - g') = -1/\omega'_0 = [a_{l-1}, \dots, a_1, g']$ . Hence,  $a_k = a_{l-k}$  for  $1 \leq k \leq l-1$ . Using  $Q_0 = 2$ , the oddness of  $P_0 = g'$ , the evenness of  $Q_1 = (d - P_0^2)/Q_0 = (d - g'^2)/2$  and the identities  $Q_{k+1} = Q_{k-1} + 2a_k P_k - a_k^2 Q_k$  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

$$\mathcal{I}_k := (Q_k/2)\mathbb{M}_k = (Q_k/2)\mathbb{Z} + \frac{P_k + \sqrt{d}}{2}\mathbb{Z} = (Q_k/2)\omega_1 \dots \omega_k \mathbb{M}_0 = \alpha_k \mathbb{Z}_{\mathbb{K}}$$

are primitive, principal, integral ideals of norms  $Q_k/2$  of the real quadratic number field  $\mathbb{Q}(\sqrt{d})$ , where  $\alpha_k = (Q_k/2)\omega_1 \dots \omega_k \in \mathcal{I}_k \subseteq \mathbb{Z}_{\mathbb{K}}$  is an algebraic integer of norm  $(-1)^k(Q_k/2)$  (recall that  $\omega_k > 1$  and  $-1/\omega'_k > 1$  for  $k \geq 0$ ). Hence,  $\mathcal{I}_k$  is principal in the narrow sense if and only if  $k$  is even.

Now, assume that  $d$  is divisible by a prime  $p \equiv 3 \pmod{4}$ . Since the congruence  $x^2 - dy^2 \equiv -4 \pmod{p}$  has no solution in rational integers, any algebraic unit of  $\mathbb{Q}(\sqrt{d})$  has norm  $+1$ . The algebraic unit  $\varepsilon = \omega_0 \omega_1 \dots \omega_{l-1} := \mathbb{Z} + \mathbb{Z}\omega_0$  being of norm  $(-1)^l$ ,  $l = 2L$  is even,  $\omega_0 = [g', a_1, \dots, a_{L-1}, a_L, a_{L-1}, \dots, a_1]$ ,  $\omega_L = [a_L, \dots, a_1, g', a_1, \dots, a_{L-1}]$  and  $\omega_{L+1} = [a_{L-1}, \dots, a_1, g', a_1, \dots, a_L] = -1/\omega'_L$ . Hence,  $-1 = \omega_{L+1}\omega'_L = \frac{P_{L+1} + \sqrt{d}}{Q_{L+1}} \frac{P_L - \sqrt{d}}{Q_L}$ , which implies  $P_{L+1} = P_L$ . Since  $P_{L+1} = a_L Q_L - P_L$ , we have  $P_{L+1} = a_L(Q_L/2)$  and  $a_L$  is odd. Moreover,

$$d - P_{L+1}^2 = d - a_L^2(Q_L/2)^2 = 4(Q_L/2)(Q_{L+1}/2).$$

Hence,  $Q_L/2$  divides  $d$ . Finally,  $\omega_L = (P_L + \sqrt{d})/Q_L$  being reduced, we have  $1 < Q_L < 2\sqrt{d}$  and  $a_L = [\omega_L] \in \{[2\sqrt{d}/Q_L], [2\sqrt{d}/Q_L] - 1\}$ , and we obtain the following Proposition and Corollary from which Theorem 2 follows:

**Proposition 4.** *Let  $d \equiv 1 \pmod{4}$  be a square-free integer, with  $d \geq 5$  such that at least one prime  $p \equiv 3 \pmod{4}$  divides  $d$ . Let  $g' \geq 1$  be the unique odd integer in the interval  $[\sqrt{d}-2, \sqrt{d}]$ . Set  $\omega_0 = (g' + \sqrt{d})/2$ .  $l \geq 1$  be the length of the period of the purely periodic continued fraction expansion  $\omega_0 = [g', a_1, \dots, a_{l-1}]$ . Then*

- (i)  $a_k = a_{l-k}$  for  $1 \leq k \leq l-1$ ;
- (ii)  $l = 2L$  is even;
- (iii)  $Q_L/2$  divides  $d$  and  $1 < Q_L/2 < \sqrt{d}$ ;
- (iv)  $a_L$  is odd and  $a_L = [\omega_L] \in \{[2\sqrt{d}/Q_L], [2\sqrt{d}/Q_L] - 1\}$ ;
- (v) The integral ideal  $\mathcal{I}_L = (Q_L/2)\mathbb{Z} + \frac{P_L + \sqrt{d}}{2}\mathbb{Z}$  of norm  $Q_L/2$  is principal and  $L$  is even if and only  $\mathcal{I}_L$  is principal in the narrow sense.

**Corollary 5.** *Let  $p, q$  be two prime integers equal to  $3 \pmod{4}$ , with  $3 \leq p < q$ . Take  $d = pq \equiv 1 \pmod{4}$ . Then  $Q_L/2 = p$ . Hence,  $\mathcal{I}_L$  is the prime ramified ideal  $\mathcal{P}$  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  $\{[\sqrt{q/p}], [\sqrt{q/p}] - 1\}$ . Moreover,  $\mathcal{P}$  is principal in the narrow sense if and only if  $\left(\frac{p}{q}\right) = +1$ .*

**Proof.** Let  $\mathcal{P}$  and  $\mathcal{Q}$  be the prime ideals above  $p$  and  $q$ , respectively. Hence  $\mathcal{P} = \mathcal{I} = (\alpha)$  is principal and  $\mathcal{P}\mathcal{Q} = (\sqrt{d})$  is also clearly principal. Since  $\sqrt{d} \in \mathcal{P}\mathcal{Q} \subseteq \mathcal{P} = (\alpha)$ , we have  $\sqrt{d} = \alpha\beta$  for some algebraic integer  $\beta$ . Hence  $\mathcal{Q} = (\beta)$  is also principal. Since  $N(\alpha)N(\beta) = N(\alpha\beta) = N(\sqrt{d}) = -d < 0$ , only one of the two principal ideals  $\mathcal{P}$  or  $\mathcal{Q}$  is principal in the narrow sense. If  $\mathcal{P} = (\alpha)$  is principal in the narrow sense, with  $\alpha = (x + y\sqrt{d})/2$  such that  $p = N(\alpha) = (x^2 - pqy^2)/4$ , then  $p$  divides  $x = pX$ ,  $4 = pX^2 - qy^2$  and  $\left(\frac{p}{q}\right) = +1$ . If  $\mathcal{P}$  is not principal in the narrow sense, then  $\mathcal{Q} = (\beta)$  is principal in the narrow sense, with  $\beta = (x + y\sqrt{d})/2$  such that  $q = N(\beta) = (x^2 - pqy^2)/4$ . Hence,  $q$  divides  $x = qX$ ,  $4 = qX^2 - py^2$  and  $\left(\frac{-p}{q}\right) = -\left(\frac{p}{q}\right) = +1$ . □

**4. Proof of Theorem 3**

Let  $d \equiv 1 \pmod{4}$  be a non-square integer, with  $d \geq 5$ . Set  $g = \lfloor \sqrt{d} \rfloor$ . Then  $\omega_0 = (P_0 + \sqrt{d})/Q_0 = g + \sqrt{d}$  is reduced. Since  $\mathbb{M}_0 = \mathbb{Z}[\omega_0] = \mathbb{Z}[\sqrt{d}]$  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  $\omega_0 = [2g, \overline{a_1, \dots, a_{l-1}}]$  is purely periodic and  $\omega_1 = [\overline{a_1, \dots, a_{l-1}}, 2g] = 1/(\omega_0 - 2g) = 1/(\sqrt{d} - g) = -1/\omega'_0 = [\overline{a_{l-1}, \dots, a_1, 2g}]$ . Hence,  $a_k = a_{l-k}$  for  $1 \leq k \leq l-1$ . Suppose that we had  $Q_n \equiv 2 \pmod{4}$  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  $Q_{k+1} = Q_{k-1} + 2a_k P_k - a_k^2 Q_k$  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  $Q_k \not\equiv 2 \pmod{4}$  for  $k \geq 0$ .

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

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

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

**Proposition 6.** *Let  $d \equiv 1 \pmod{4}$  be a square-free integer, with  $d \geq 5$  such that at least one prime  $p \equiv 3 \pmod{4}$  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  $\omega_0 = [2g, \overline{a_1, \dots, a_{l-1}}]$ . Then*

- (i)  $a_k = a_{l-k}$  for  $1 \leq k \leq l-1$ ;
- (ii)  $l = 2L$  is even;
- (iii)  $Q_L$  divides  $2d$  and  $1 < Q_L < 2\sqrt{d}$ ;
- (iv)  $a_L = \lfloor \omega_L \rfloor \in \{ \lfloor 2\sqrt{d}/Q_L \rfloor, \lfloor 2\sqrt{d}/Q_L \rfloor - 1 \}$ ;
- (v) *if  $d = pq$ , 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  $\mathcal{P}$  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  $\mathcal{P}$  is principal in the narrow sense.*

**Proof.** It remains to prove point (v). Since  $Q_L$  divides  $2pq$ ,  $Q_L \not\equiv 2 \pmod{4}$  and  $Q_L < 2\sqrt{pq}$ , we have  $Q_L \in \{p, q\}$ . Since  $Q_L = q$  would yield the contradiction  $4qQ_{L+1} = 4d - a_L^2 Q_L^2 \leq 4pq - 4q^2 < 0$ , we have  $Q_L = p$ . Hence,  $a_L$  is even, as  $2P_L = a_L Q_L$ , and  $a_L \in \{ \lfloor 2x \rfloor, \lfloor 2x \rfloor - 1 \}$ , where  $x = \sqrt{d}/Q_L$ . Since  $\lfloor 2x \rfloor \in \{ \lfloor 2x \rfloor, \lfloor 2x \rfloor + 1 \}$  for  $x$  real, we have that  $a_L$  is even and  $a_L \in \{ \lfloor 2x \rfloor - 1, \lfloor 2x \rfloor, \lfloor 2x \rfloor + 1 \}$ . Therefore,  $a_L = 2\lfloor x \rfloor = 2\lfloor \sqrt{d}/Q_L \rfloor = 2\lfloor \sqrt{q/p} \rfloor$ .

Finally, set  $\beta_L = Q_L \omega_1 \dots \omega_L$ . Then

$$\mathcal{J}_L := \beta_L \mathbb{Z}[\sqrt{d}] = \beta_L \mathbb{M}_0 = Q_L \omega_1 \dots \omega_L \mathbb{M}_0 = Q_L \mathbb{M}_L = Q_L \mathbb{Z} + (P_L + \sqrt{d})\mathbb{Z} \subseteq \mathbb{Z}[\sqrt{d}].$$

Hence,  $\beta_L = x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$  and  $\{Q_L, P_L + \sqrt{d}\}$  and  $\{\beta_L, \beta_L \sqrt{d}\} = \{x + y\sqrt{d}, dy + x\sqrt{d}\}$  are two  $\mathbb{Z}$ -bases of  $\mathcal{J}_L$  and the change of basis matrix

$$A = \begin{pmatrix} \frac{x-yP_L}{Q_L} & \frac{dy-xP_L}{Q_L} \\ y & x \end{pmatrix}$$

is in  $M_2(\mathbb{Z})$  and of determinant  $\pm 1$ , i.e.  $\pm 1 = (x^2 - dy^2)/Q_L = N(\beta_L)/p$ . Therefore,  $N(\beta_L) = (-1)^L p$ , with  $\beta_L \in \mathbb{Z}[\sqrt{d}]$ . It follows that the prime ideal  $\mathcal{P}$  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  $(\beta_L)$  and that  $\mathcal{P}$  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  $\sqrt{pq}$ ”, *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  $\sqrt{2p}$  for primes  $p \equiv 3 \pmod{4}$ ”, 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.