UNITS FROM SQUARE ROOTS OF RATIONAL NUMBERS

Kurt Girstmair
Institut für Mathematik, Universität Innsbruck, Innsbruck, Austria
Kurt.Girstmair@uibk.ac.at

Received: 11/30/22, Accepted: 1/11/23, Published: 1/27/23

Abstract

Let D, Q be natural numbers, $(D, Q) = 1$, such that $D/Q > 1$ and D/Q is not a square. Let q be the smallest divisor of Q such that $Q \mid q^2$. We show that the units greater than 1 of the ring $\mathbb{Z}[\sqrt{Dq^2/Q}]$ are connected with certain convergents of $\sqrt{D/Q}$. Among these units, the units of $\mathbb{Z}[\sqrt{DQ}]$ play a special role, inasmuch as they correspond to the convergents of $\sqrt{D/Q}$ that occur just before the end of each period. We also show that the last-mentioned units allow reading the (periodic) continued fraction expansion of certain quadratic irrationals from the (finite) continued fraction expansion of certain rational numbers.

1. Introduction and Results

Let $\mathbb{N} = \{1, 2, 3 \ldots\}$ denote the set of natural numbers. Let $D \in \mathbb{N}$, D not a square. In particular, $D > 1$. It is well-known how the units in the ring $\mathbb{Z}[\sqrt{D}]$ can be found, see [2, p. 93]; see also [1, p. 296], [3, p. 64]. Indeed, $\sqrt{D}$ has a periodic continued fraction expansion

$$[b_0, \{b_1, \ldots, b_m, 2b_0\}], \tag{1}$$

where $b_0, \ldots, b_m$ are natural numbers and $\{b_1, \ldots, b_m, 2b_0\}$ is the period. It is also known that the sequence $b_1, \ldots, b_m$ is symmetric, i.e., identical with the sequence $b_m, \ldots, b_1$. Suppose that m has been chosen smallest possible. Let r_k/s_k, $k = 0, 1, 2 \ldots$ denote the kth convergent of $\sqrt{D}$. As usual, $(r_k, s_k) = 1$. Now the units of $\mathbb{Z}[\sqrt{D}]$ are given by

$$r_k + s_k\sqrt{D}, \ \ k = l(m+1) - 1, \ \ l \in \mathbb{N}.$$

In other words, the convergents occurring just before the end of each period supply these units.

DOI: 10.5281/zenodo.7569232

In this note we study numbers D/Q, where $D, Q \in \mathbb{N}$ are such that $(D, Q) = 1$, D/Q is not a square, and $D/Q > 1$, i.e., $Q < D$. The continued fraction expansion of $\sqrt{D/Q}$ also has the form (1), and $b_1, \ldots, b_m$ have the same symmetry property. The following theorem describes the units obtained from convergents of the continued fraction expansion (1) of $\sqrt{D/Q}$. To this end let q be the smallest divisor of Q such that $Q \mid q^2$. Then $D_1 = Dq^2/Q$ is a natural number not less than D/Q and not a square. For the time being, we do not assume that m is smallest possible.

Theorem 1. *In the above setting, let $r + s\sqrt{D_1}$ be a unit in $\mathbb{Z}[\sqrt{D_1}]$. Let $t = (r, q)$. Then $(r/t, sq/t)$ is a convergent of $\sqrt{D/Q}$. Moreover, if $(r/t, sq/t) = (r_k, s_k)$, then (r_{k+m+1}, s_{k+m+1}) also has the form $(r'/t, s'q/t)$ for another unit $r' + s'\sqrt{D_1}$ of $\mathbb{Z}[\sqrt{D_1}]$. Here $(r', q) = t$ for the same number t.*

So the units of $\mathbb{Z}[\sqrt{D_1}]$ are closely connected with certain convergents of $\sqrt{D/Q}$. Let $D_2 = DQ$. Since $D_2 = D_1(Q/q)^2$, the ring $\mathbb{Z}[\sqrt{D_2}]$ is contained in $\mathbb{Z}[\sqrt{D_1}]$. Its units play a special role in the continued fraction expansion of $\sqrt{D/Q}$.

Theorem 2. *In the above setting, let m be smallest possible. Then the units of $\mathbb{Z}[\sqrt{D_2}]$ have the form $r + s\sqrt{D_1}$, where $r = r_k, sq = s_k$, $k = l(m+1) - 1, l \in \mathbb{N}$; i.e., the numbers r_k/s_k are the convergents of $\sqrt{D/Q}$ occurring just before the end of each period of this quadratic irrational.*

The above theorems suggest the following notation. A unit of $\mathbb{Z}[\sqrt{D_1}]$ that lies in $\mathbb{Z}[\sqrt{D_2}]$ is called a *regular* unit, whereas a unit of $\mathbb{Z}[\sqrt{D_1}]$ that is not in $\mathbb{Z}[\sqrt{D_2}]$ is called an *irregular unit*.

Irregular units are only possible if $q^2 \neq Q$. Moreover, they can only occur if the unit group of $\mathbb{Z}[\sqrt{D_1}]$ is larger than that of $\mathbb{Z}[\sqrt{D_2}]$.

Example. Let $D = 157$, a prime, and $Q = 45$. Then $q = 15$. Here $D_1 = 5 \cdot 157 = 785$ and $D_2 = 9 \cdot 785$. So we have $\mathbb{Z}[\sqrt{D_1}] = \mathbb{Z}[\sqrt{785}] \neq \mathbb{Z}[\sqrt{D_2}] = \mathbb{Z}[3\sqrt{785}]$. The fundamental unit of $\mathbb{Z}[\sqrt{D_1}]$ is $\varepsilon = 28 + \sqrt{785}$. Since $\varepsilon \notin \mathbb{Z}[\sqrt{D_2}]$, ε is an irregular unit.

Now $\sqrt{D/Q} = \sqrt{157/45}$ has the smallest possible period length 16 and $r_{15} = 4923521$, $s_{15} = 2635920$. Here $\varepsilon^4 = 4923521 + 175728\sqrt{785} = r + s\sqrt{D_1}$, and $r_{15} = r$, $s_{15} = sq = 175728 \cdot 15$. Theorem 2 says that $r + s\sqrt{D_1}$ is a regular unit. Indeed, we have $r + s\sqrt{D_1} = 4923521 + 58576\sqrt{D_2}$. Of course, $r + s\sqrt{D_1}$ is the fundamental unit of $\mathbb{Z}[\sqrt{D_2}]$.

We have $r_4 = 28$ and $s_4 = 15$, whose connection with ε is obvious. We obtain $\varepsilon^2 = 1569 + 56\sqrt{D_1}$. Here $t = (1569, q) = 3$. This gives $r_7 = 1569/3 = 523$ and $s_7 = 56 \cdot 15/3 = 280$. Finally, $\varepsilon^3 = 87892 + 3137\sqrt{D_1}$ and $r_{10} = 87892, s_{10} = 47055 = 3137 \cdot 15$. Hence we have irregular units connected with the convergents of indices $2, 7, 10$ and $2 + l \cdot 16$, $7 + l \cdot 16$, $10 + l \cdot 16$, $l \in \mathbb{N}$. The regular units are connected with the convergents of indices 15 and $15 + l \cdot 16$, $l \in \mathbb{N}$.

Of course, the regular units can also be found by the continued fraction expansion of $\sqrt{D_2}$. Observing the monotonous growth of the numerators and denominators of convergents, we obtain the following corollary.

Corollary 1. *In the above setting, let m be smallest possible such that $\sqrt{D/Q} = [b_0, \{b_1, \ldots, b_m, 2b_0\}]$. Let n be smallest possible such that $\sqrt{D_2} = [b'_0, \{b'_1, \ldots, b'_n, 2b'_0\}]$. Let r_k/s_k be the kth convergent of $\sqrt{D/Q}$ and r'_k/s'_k the kth convergent of $\sqrt{D_2}$. Then*

$$r_{l(m+1)-1} = r'_{l(n+1)-1}, \quad s_{l(m+1)-1} = s'_{l(n+1)-1}Q$$

for all $l \in \mathbb{N}$.

In the above example, $m = 16$ and $\sqrt{D_2}$ has the smallest possible period length $n = 8$. So we have $r'_7 = r_{15} = 4923521$ and $s'_7 = 58576$, $s'_7Q = s_{15} = 2635920$.

Theorems 1 and 2 exhibit the structure of the units greater than 1 in $\mathbb{Z}[\sqrt{D_1}]$. To this end let m be smallest possible. If $k = m$, then the convergent r_k/s_k of $\sqrt{D/Q}$ defines the fundamental unit η of $\mathbb{Z}[\sqrt{D_2}]$, by Theorem 2. Suppose that the fundamental unit ε of $\sqrt{D_1}$ is different from η. Then $\eta = \varepsilon^j$ for some $j > 1$. By Theorem 1, the units $\varepsilon, \varepsilon^2, \ldots, \varepsilon^{j-1}$ are connected with convergents $r_{k_1}/s_{k_1}, \ldots, r_{k_{j-1}}/s_{k_{j-1}}$ of $\sqrt{D/Q}$, and, due to the strictly monotonic growth of $r_k + s_k\sqrt{D/Q}$ for $k \to \infty$, we have $k_1 < \ldots < k_{j-1} < m$. By Theorem 1, the convergents $r_{k_{1+m+1}}/s_{k_{1+m+1}}, \ldots, r_{k_{j-1+m+1}}/s_{k_{j-1+m+1}}$ define units in $\mathbb{Z}[\sqrt{D_1}]$ larger than η but smaller than η^2, the latter being defined by r_{2m+1}/s_{2m+1}. Hence there is only one possibility, namely, the aforesaid convergents define the units $\varepsilon^{j+1}, \ldots, \varepsilon^{2j-1}$, which are the only units of $\mathbb{Z}[\sqrt{D_1}]$ that are larger than η but smaller than η^2. In the same way one can proceed for higher powers of ε.

Altogether, we see that the continued fraction expansion of $\sqrt{D/Q}$, i.e., the square root of the *fractional* number D/Q, yields the units of the ring of algebraic integers $\mathbb{Z}[\sqrt{D_1}]$. This fact is a bit surprising. But we have seen even more: Namely, the units of the subring $\mathbb{Z}[\sqrt{D_2}]$ are given by very special convergents of $\sqrt{D/Q}$ (those occurring just before the end of each period of $\sqrt{D/Q}$). We think that these properties of periodic continued fractions deserve some attention.

In what follows we also consider the continued fraction expansion of a *rational* number x, so

$$x = [c_0, \ldots, c_n]. \tag{2}$$

Here c_n need not be at least 2. Depending on the situation, we require, instead, that n is even or odd. This can be obtained on replacing c_n by the sequence $c_n - 1, 1$ at the end of the identity (2).

Theorem 3. *Let $r_k + s_k\sqrt{D/Q}$ be a regular unit, i.e., $k = l(m+1) - 1$ if m is smallest possible. Let t be a divisor of s_k. Let*

$$r_k/t = [c_0, \ldots, c_n],$$

where $n \equiv k \mod 2$. *Then* $(s_k/t)\sqrt{D/Q} = [c_0, \{c_1, \dots, c_n, 2c_0\}]$.

In other words, we may read the continued fraction expansion of the quadratic irrational $(s_k/t)\sqrt{D/Q}$ from the continued fraction expansion of the rational number r_k/t.

Example. In the above example, we have $r_{15} = 4923521$, $s_{15} = 2635920 = 16 \cdot 9 \cdot 5 \cdot 7 \cdot 523$. We choose $t = 16 \cdot 9 \cdot 7$ and obtain $r_{15}/t = [4884, 2, 4, 12, 4, 2]$. This yields

$$(s_{15}/t)\sqrt{D/Q} = 523\sqrt{785}/3 = [4884, \{2, 4, 12, 4, 2, 9768\}].$$

2. Proofs

Proof of Theorem 1. The number $r + s\sqrt{D_1}$ is a unit, if, and only if,

$$r^2 - s^2 D_1 = \pm 1. \tag{3}$$

Since $D_1 = Dq^2/Q$ and $t = (r, q)$, this is the same as saying

$$(r/t)^2 - (sq/t)^2 D/Q = \pm(1/t)^2. \tag{4}$$

Since $1/t \le 1$ and $D/Q > 1$, we see that $r/t = r_k$, $sq/t = s_k$ defines a convergent of $\sqrt{D/Q}$; see [2, p. 39].

For the next step we need the kth complete quotient x_k of $x_0 = \sqrt{D/Q}$. By [2, p. 80],

$$x_k = (\sqrt{D_2} + P_k)/Q_k \tag{5}$$

with $P_k \in \mathbb{Z}$ and $Q_k \in \mathbb{N}$. In particular, $x_0 = \sqrt{D/Q} = (\sqrt{D_2} + P_0)/Q_0$, with $P_0 = 0$ and $Q_0 = Q$. From [2, p. 71] we obtain

$$r_k^2 - s_k^2 D/Q = \pm Q_{k+1}/Q. \tag{6}$$

Suppose now that $r_k = r/t$, $s_k = sq/t$. Comparing the identities (4) and (6), we see that

$$Q_{k+1}/Q = 1/t^2, \text{ i.e. }, Q_{k+1} = Q/t^2.$$

In particular, $t^2 \mid Q$. Now the complete quotient $x_{k+1+m+1}$ is the same as x_{k+1}, whence we obtain

$$r_{k+m+1}^2 - s_{k+m+1}^2 D/Q = \pm Q_{k+1}/Q = \pm(1/t)^2.$$

This gives

$$(r_{k+m+1}t)^2 - (s_{k+m+1}t)^2 D/Q = \pm 1.$$

Therefore, however, Q divides $(s_{k+m+1}t)^2$, which, by the minimal property of q, implies $q \mid s_{k+m+1}t$. Accordingly, we may define $r', s' \in \mathbb{Z}$ by $r' = r_{k+m+1}t$, $s' = s_{k+m+1}t/q$ and obtain

$$r'^2 - s'^2 Dq^2/Q = r'^2 - s'^2 D_1 = \pm 1.$$

This is the desired result. □

Proof of Theorem 2. Let $r + s\sqrt{D_1}$ be a unit in $\mathbb{Z}[\sqrt{D_1}]$. It is easy to see that this unit lies in $\mathbb{Z}[\sqrt{D_2}]$ if, and only if, $Q \mid sq$.

Suppose that this holds. Then the identity (3) implies $(r, Q) = 1$. By the argument used in the proof of Theorem 1, $r_k = r, s_k = sq$ is a convergent of $\sqrt{D/Q}$. From the identity (6) we obtain

$$r_k^2 - s_k^2 D/Q = \pm Q_{k+1}/Q = \pm 1.$$

Therefore, the complete quotient x_{k+1} has the form

$$x_{k+1} = (\sqrt{D_2} + P)/Q, \tag{7}$$

for some integer P (see the identity (5)).

We show that $Q \mid P$. Since $x_0 = \sqrt{D/Q} = [b_0, \ldots, b_k, x_{k+1}]$, we obtain

$$x_0 = \frac{r_k x_{k+1} + r_{k-1}}{s_k x_{k+1} + s_{k-1}}.$$

Let

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} r_k & r_{k-1} \\ s_k & s_{k-1} \end{pmatrix},$$

a matrix whose determinant $ad - bc = \pm 1$. In particular, $c = s_k$. We use $x_0 = \sqrt{D_2}/Q$ and the identity (7) in order to compare the coefficients in the relation

$$x_0(cx_{k+1} + d) = ax_{k+1} + b.$$

This yields

$$b = -aP/Q + cD_2/Q^2 = -aP/Q + cD/Q. \tag{8}$$

Now we know $Q \mid c$. Then $cD/Q \in \mathbb{Z}$ and, by the identity (8), $-aP/Q \in \mathbb{Z}$. But $(a, Q) = 1$, since, otherwise, we have a contradiction to $ad - bc = \pm 1$. Therefore, $Q \mid P$ and $x_{k+1} = x_0 + C$, $C \in \mathbb{Z}$. But then $x_{k+2} = x_1$, which means that $k + 1$ marks the end of a period. Thus, $k = l(m + 1) - 1$, $l \in \mathbb{N}$.

Conversely, let $k = l(m+1) - 1$, $l \in \mathbb{N}$. Since $x_{k+2} = x_1$, we have $x_{k+1} = x_0 + C$, $C \in \mathbb{Z}$. On the other hand, x_{k+1} has the form given in the identity (7), by [2, p. 81]. This yields $Q \mid P$. Then $-aP/Q \in \mathbb{Z}$ and, by the identity (8), $cD/Q \in \mathbb{Z}$. Since $(D, Q) = 1$, $Q \mid c$, and $c = s_k$. Again, we have the identity (6) with $Q_{k+1} = Q$. Accordingly, r_k/s_k belongs to a unit in $\mathbb{Z}[\sqrt{D_2}]$. □

Proof of Theorem 3. The regular unit $r_k + s_k\sqrt{D/Q}$ can be written

$$r_k + s_k\sqrt{D/Q} = r_k + t\sqrt{(s_k/t)^2 D/Q}.$$

If we write $(s_k/t)^2 D/Q$ in the form D'/Q', $(D', Q') = 1$, then

$$t\sqrt{D'/Q'} = a\sqrt{D'Q'} \tag{9}$$

for some natural number a. This identity will be proved below. It says that $r_k + t\sqrt{D'/Q'}$ is a regular unit (with respect to D' and Q'). Accordingly, Theorem 2 yields $r_k/t = [c_0, \ldots, c_n]$, where

$$(s_k/t)\sqrt{D/Q} = \sqrt{D'/Q'} = [c_0, \{c_1, \ldots, c_n, 2c_0\}]$$

(n not necessarily smallest possible). Here $n \equiv k \mod 2$ since the sign of $r_k^2 - t^2 D'/Q' = r_k^2 - s_k^2 D/Q$ $(= \pm 1)$ defines the parity of k and n.

In order to prove the identity (9), we consider the p-exponent $v_p(a)$ of a rational number a. Because $Q' \mid Q$, only prime divisors p of Q are relevant. Let $v_p(Q) = e_p$, $v_p(t) = f_p$, and $v_p(s_k/t) = g_p$. Since $Q \mid s_k$, we have $f_p + g_p \geq e_p$. Now $v_p((s_k/t^2)D/Q) = 2g_p - e_p = v_p(D'/Q')$. Hence

$$v_p(D') = \begin{cases} 2g_p - e_p, & \text{if } e_p \leq 2g_p; \\ 0, & \text{if } e_p > 2g_p. \end{cases}$$

Further,

$$v_p(Q') = \begin{cases} 0, & \text{if } e_p \leq 2g_p; \\ e_p - 2g_p, & \text{if } e_p > 2g_p. \end{cases}$$

Accordingly,

$$v_p(D'Q')) = \begin{cases} 2g_p - e_p, & \text{if } e_p \leq 2g_p; \\ e_p - 2g_p, & \text{if } e_p > 2g_p. \end{cases} \tag{10}$$

Now

$$v_p(t^2 D'/Q') = v_p(t^2 (s_k/t)^2 D/Q) = 2f_p + 2g_p - e_p. \tag{11}$$

We obtain, from the identities (10) and (11),

$$v_p\left(\frac{t^2 D'/Q'}{D'Q'}\right) = \begin{cases} 2f_p, & \text{if } e_p \leq 2g_p; \\ 2f_p + 4g_p - 2e_p, & \text{if } e_p > 2g_p. \end{cases}$$

Because $f_p + g_p \geq e_p$, this exponent is always nonnegative and even. This implies the identity (9). □

References

[1] H. Hasse, *Vorlesungen über Zahlentheorie*, Springer, Berlin, 1950.

[2] O. Perron, *Die Lehre von den Kettenbrüchen*, vol. I (3d ed.), Teubner, Stuttgart, 1954.

[3] A. M. Rockett, P. Szüsz,*Continued Fractions*, World Scientific, Singapore, 1992.