Monatshefte für Mathematik (2023) 202:507–514
https://doi.org/10.1007/s00605-023-01885-4

On the equivalence of certain quadratic irrationals

Kurt Girstmair[1]

Received: 30 August 2022 / Accepted: 26 June 2023 / Published online: 19 July 2023

Abstract
This paper deals with quadratic irrationals of the form $m/q + \sqrt{v}$ for fixed positive integers v and q, v not a square, and varying integers m, $(m, q) = 1$. Two numbers $m/q + \sqrt{v}$, $n/q + \sqrt{v}$ of this kind are equivalent (in a classical sense) if their continued fraction expansions can be written with the same period. We give a necessary and sufficient condition for the equivalence in terms of solutions of Pell's equation. Moreover, we determine the number of equivalence classes to which these quadratic irrationals belong.

Keywords Quadratic irrationals · Periodic continued fractions

Mathematics Subject Classification 11A55 · 11R11

1 Introduction and results

Let v and q be positive integers, v not a square. In this paper we study the equivalence between numbers

$$x = m/q + \sqrt{v},$$

where m is an integer, $(m, q) = 1$. Thus, v and q are fixed, whereas m may vary.

The equivalence of two numbers x, y of this kind means that the (regular) continued fractions of x and y can be written with the same period, say,

$$x = [a_0, \ldots, a_{j-1}, [b_1, \ldots, b_k]], \; y = [c_0, \ldots, c_{l-1}, [b_1, \ldots, b_k]], \qquad (1)$$

Communicated by Alberto Minguez.

✉ Kurt Girstmair
Kurt.Girstmair@uibk.ac.at

1 Institut für Mathematik, Universität Innsbruck, Technikerstr. 13/7, A-6020 Innsbruck, Austria

where $[b_1, \ldots, b_k]$ is the common period. Here the pre-periods $a_0, \ldots, a_{j-1}$ and $c_0, \ldots, c_{l-1}$ need not occur. In general, it is more likely that you find equivalent numbers x and y than inequivalent ones, for example,

$$x = \frac{1}{12} + \sqrt{7} = [2, [1, 2, 1, 2, 4, 5, 16, 47, 1, 1, 3, 1, 1, 4]],$$
$$y = \frac{5}{12} + \sqrt{7} = [3, [16, 47, 1, 1, 3, 1, 1, 4, 1, 2, 1, 2, 4, 5]]$$
$$= [3, 16, 47, 1, 1, 3, 1, 1, 4, [1, 2, 1, 2, 4, 5, 16, 47, 1, 1, 3, 1, 1, 4]].$$

We write $x \sim y$ if x and y are equivalent. It is a classical result of Serret that $x \sim y$ is the same as

$$y = \frac{ax + b}{cx + d}, \text{ where } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2, \mathbb{Z}), \tag{2}$$

i.e., $a, b, c, d \in \mathbb{Z}$ and $ad - bc = \pm 1$ (see [5, p. 54], [1, p. 38]).

Our first aim is the following theorem.

Theorem 1 *Let $x = m/q + \sqrt{v}$, $y = n/q + \sqrt{v}$, $(m, q) = (n, q) = 1$. Let $q_1 = (m - n, q)$. Then $x \sim y$ if, and only if, the equation*

$$r^2 - c^2 v = \pm 1 \tag{3}$$

has a solution $(r, c) \in \mathbb{Z}^2$ such that $(c, q^2) = qq_1$.

Of course, (3) is known as Pell's equation. Our next question concerns the number of equivalence classes to which our quadratic irrationals belong. Since $x + 1 \sim x$, we may restrict ourselves to numbers $x = m/q + \sqrt{v}$, $y = n/q + \sqrt{v}$ with $0 \le m, n \le q - 1$.

Theorem 2 *Let q_0 be the smallest divisor of q such that there is a solution (r, c) of (3) with $(c, q^2) = qq_0$. Then the numbers $x = m/q + \sqrt{v}$, $(m, q) = 1$, $0 \le m \le q - 1$, belong to exactly $\varphi(q_0)$ equivalence classes, each of which contains $\varphi(q)/\varphi(q_0)$ elements x.*

Remarks 1. Note that every equivalence class contains many elements different from the numbers x in question. For instance, $1/3 + \sqrt{2} \sim 9\sqrt{2}/2$, the latter not being of the appropriate form for $v = 2$ and $q = 3$. Equivalent numbers have the same discriminant (see [1, p. 41]). Since the discriminant of $x = m/q + \sqrt{v}$, $(m, q) = 1$, equals $4q^4 v$, x cannot be equivalent to a number $m'/q' + \sqrt{v}$, $(m', q') = 1, q' > 0$, $q' \ne q$.

2. The unit group $\mathbb{Z}[\sqrt{v}]^\times$ of the ring $\mathbb{Z}[\sqrt{v}]$ is isomorphic to $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and is generated by a fundamental unit $s + t\sqrt{v}$ together with -1. For $r + c\sqrt{v} \in \mathbb{Z}[\sqrt{v}]^\times$ we have $q \mid c$ if, and only if, $r + c\sqrt{v} \in \mathbb{Z}[q\sqrt{v}]^\times$, the unit group of the subring $\mathbb{Z}[q\sqrt{v}]$. This group has a finite index k in $\mathbb{Z}[\sqrt{v}]^\times$ (see [4, p. 296]). Accordingly, $(s + t\sqrt{v})^k$ is an element of $\mathbb{Z}[q\sqrt{v}]^\times$.
3. It may happen that $\mathbb{Z}[q\sqrt{v}]^\times$ coincides with $\mathbb{Z}[qq_1\sqrt{v}]^\times$ for some divisor q_1 of q, $q_1 > 2$. In this case c is divisible by qq_1 for each $r + c\sqrt{v} \in \mathbb{Z}[q\sqrt{v}]^\times$. In particular, $qq_1 \mid (c, q^2)$ for all these units. Let q_0 be the smallest divisor of q such that there

is a unit $r + c\sqrt{v} \in \mathbb{Z}[q\sqrt{v}]^\times$ with $(c, q^2) = qq_0$. Then $qq_1 \mid (c, q^2) = qq_0$, and, accordingly, $q_1 \mid q_0$. By Theorem 2, the numbers $m/q + \sqrt{v}$, $(m, q) = 1$, $0 \le m \le q - 1$, belong to $\varphi(q_0) \ge \varphi(q_1) > 1$ equivalence classes. In particular, not all of these numbers are equivalent.

Example Let $v = 979$ and $q = 12$. The fundamental unit in $\mathbb{Z}[\sqrt{v}]$ is $s + t\sqrt{v}$ with $s = 360449$ and $t = 11520 = q^2 \cdot 80$. Hence $\mathbb{Z}[\sqrt{v}]^\times = \mathbb{Z}[q^2\sqrt{v}]^\times$ and for every $r + c\sqrt{v} \in \mathbb{Z}[\sqrt{v}]^\times$ we have $q^2 \mid c$. Accordingly, the number q_0 of Theorem 2 equals $q = 12$, and the four numbers $m/12 + \sqrt{979}$, $m \in \{1, 5, 7, 12\}$ belong to four different equivalence classes. Indeed,

$$\frac{1}{12} + \sqrt{979} = [31, [2, 1, 2, 5, 2, 3, 6, 1, 4, 62]],$$
$$\frac{5}{12} + \sqrt{979} = [31, [1, 2, 2, 1, 1, 13, 1, 4, 1, 6, 1, 61]].$$

So these numbers have periods of different lengths. The numbers $7/12 + \sqrt{979}$ and $5/12 + \sqrt{979}$ have inverse periods, and $11/12 + \sqrt{979}$ and $1/12 + \sqrt{979}$, too. In general, we say that x and y have *inverse periods* if they can be written as in (1), the period of y being $[b_k, b_{k-1}, \dots, b_1]$, however.

Theorem 1 answers the question whether $x = m/q + \sqrt{v}$ and $y = n/q + \sqrt{v}$ have inverse periods. This happens if, and only if, $x \sim y' = n/q - \sqrt{v}$ (see [5, p. 77]). Since $y' \sim -y' = -n/q + \sqrt{v}$, we obtain the following corollary to Theorem 1.

Corollary 1 *Let $x = m/q + \sqrt{v}$, $y = n/q + \sqrt{v}$ be as above. Let $q_1' = (m + n, q)$. Then x and y have inverse periods if, and only if, the equation (3) has a solution $(r, c) \in \mathbb{Z}^2$ such that $(c, q^2) = qq_1'$.*

We say that x has a *self-inverse* period if x can be written with a period $[b_1, \dots, b_k]$ but also with the period $[b_k, \dots, b_1]$ (see [5, p. 78], [2]). From Corollary 1 we obtain

Corollary 2 *Let $x = m/q + \sqrt{v}$ be as above. Put $q_1' = 2$ if q is even, and $q_1' = 1$, otherwise. Then x has a self-inverse period if, and only if, the equation (3) has a solution $(r, c) \in \mathbb{Z}^2$ such that $(c, q^2) = qq_1'$.*

Remarks 1. The reader may consult [3], where quadratic irrationals with self-inverse periods are classified by certain equivalences.

2. Many examples show the following tendency, for which we have no precise mathematical formulation. Namely, if the numbers $m/q + \sqrt{v}$, $(m, q) = 1$, $0 \le m \le q - 1$, belong to many equivalence classes, then their periods are short. For instance, in the case $v = 979$, $q = 12$ of the above example we have the largest possible number of equivalence classes, which is 4. The corresponding period lengths of $m/q + \sqrt{v}$ are 10 or 12. If we choose $q = 9$ instead, then all numbers $m/q + \sqrt{v}$ belong to the same equivalence class, and the common period of the 6 elements m/q has length 78.

2 Proofs

Proof of Theorem 1 Let $x = m/q + \sqrt{v}$, $y = n/q + \sqrt{v}$, $(m, q) = (n, q) = 1$. First suppose $x \sim y$, i.e., there is a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2, \mathbb{Z})$ such that (2) holds. Then comparison of the coefficients with respect to the $\mathbb{Q}$-basis $(1, \sqrt{v})$ of $\mathbb{Q}[\sqrt{v}]$ shows that (2) is equivalent to the identities

$$a = \frac{c(m+n)}{q} + d \tag{4}$$

and

$$b = \frac{-d(m-n)}{q} - \frac{cm^2}{q^2} + cv. \tag{5}$$

Since $b \in \mathbb{Z}$, (5) implies

$$d(m-n)q + cm^2 \equiv 0 \mod q^2. \tag{6}$$

However, $(m, q) = 1$, so (6) requires $c \equiv 0 \mod q$. Then $a \in \mathbb{Z}$, by (4). Let $m - n = q_1 m_1$ with $q_1 = (m - n, q)$ and $(m_1, q/q_1) = 1$. Accordingly, (6) can be written

$$dm_1 q q_1 + cm^2 \equiv 0 \mod q^2. \tag{7}$$

If $q_1 = q$, this congruence yields $c \equiv 0 \equiv qq_1 \mod q^2$. If $q_1 < q$, we have $qq_1 \mid c$. In this case one easily checks that (c, q^2) must be qq_1 (observe that $(d, q) = 1$ since $q \mid c$ and the matrix in question has determinant ± 1).

Moreover, the condition $ad - bc = \pm 1$ is the same as saying

$$d = -\frac{cm}{q} + \sqrt{c^2 v \pm 1}, \tag{8}$$

where we do not fix a sign for the square root. Hence there is an integer r such that (3) holds.

Conversely, suppose that (r, c) is a solution of (3) and $c = qq_1c_1$ for some integer c_1 with $(c_1, q/q_1) = 1$ (observe $q^2/(qq_1) = q/q_1$). We define d in such a way that (8) is satisfied, i.e.,

$$d = -\frac{cm}{q} + r = -q_1 c_1 m + r. \tag{9}$$

Then condition (6) reads

$$(-q_1 c_1 m + r)(m-n)q + qq_1 c_1 m^2 \equiv 0 \mod q^2.$$

This congruence is equivalent to the congruence

$$c_1 mn + rm_1 \equiv 0 \mod q/q_1. \tag{10}$$

Here $(m, q) = (n, q) = (m_1, q/q_1) = 1$. Observe that $(c_1, q/q_1) = 1$. By (3), we have $(r, q) = 1$, since $q \mid c$. Of course, it may happen that our pair (r, c) does not satisfy (10). In this case we consider $r' + c'\sqrt{v} = (r + c\sqrt{v})^k$ for some positive integer k prime to q. Since $q \mid c$, we obtain

$$r' + c'\sqrt{v} \equiv r^k + kr^{k-1}c\sqrt{v} \mod q^2,$$

a congruence mod $\mathbb{Z}[\sqrt{v}]q^2$. It is easy to see that this congruence implies the congruences

$$r' \equiv r^k \mod q^2, \;\; c' \equiv kr^{k-1}c \mod q^2, \tag{11}$$

which are congruences mod $\mathbb{Z}q^2$. In particular, $(c', q^2) = (kc, q^2) = (c, q^2)$, since $(k, q) = 1$. The second of the congruences (11) shows that we may write $c' = qq_1c_1'$ with $c_1' \equiv kr^{k-1}c_1 \mod q/q_1$. The congruence (10), for r' and c' instead of r and c, reads

$$c_1'nm + r'm_1 \equiv 0 \mod q/q_1, \tag{12}$$

or

$$kr^{k-1}c_1nm + r^km_1 \equiv 0 \mod q/q_1.$$

Because $(r, q) = 1$, this is equivalent to

$$kc_1nm + rm_1 \equiv 0 \mod q/q_1. \tag{13}$$

Observe $(c_1, q/q_1) = (m_1, q/q_1) = (m, q) = (n, q) = 1$ and $q/q_1 \mid q$. Therefore, the number k (prime to q) can be chosen such that (13) holds. Then (12) holds, and, thus, the congruence (6).

We define d by (9) with r', c' instead of r, c. Finally, we define a, b by (4) and (5) with c' instead of c. Then a, b are integers, $ad - bc' = \pm 1$, and (2) also holds. □

Example Let $v = 7, q = 12, m = 1, n = 5$. Hence $x = 1/12 + \sqrt{7}$, $y = 5/12 + \sqrt{7}$, $m - n = -4 = q_1m_1$ with $q_1 = 4$, $m_1 = -1$ (see the example at the beginning of this paper). The fundamental unit of $\mathbb{Z}[\sqrt{7}]$ is $s + t\sqrt{7} = 8 + 3\sqrt{7}$. Since $(s + t\sqrt{7})^2 = 127 + 48\sqrt{7}$, we put $r = 127$, $c = 48$. In particular, $(c, q^2) = qq_1 = 48$. So x is equivalent to y (what we already know). We have $c_1 = 1$ and $q/q_1 = 3$. However, the congruence (10) does not hold, but (13) is true with $k = 5$, $(k, q) = 1$. This choice, however, leads to rather large numbers. But we may also choose $k = 2$ (which is not prime to q). Indeed, define r', c' by

$$r' + c'\sqrt{7} = (r + c\sqrt{7})^2 = 32257 + 12192\sqrt{7}.$$

Then $(c', q^2) = (12192, 144) = 48 = qq_1$, as required. As in the proof of Theorem 1 we obtain $d = 31241$, $a = 37337$, and $b = 95673$. In this way $ad - bc' = 1$ and $(ax + b)/(c'x + d) = y$.

The proof of Theorem 2 requires the following lemmas.

Lemma 1 *Let (r_1, c_1) and (r_2, c_2) be solutions of (3) such that $(c_1, q^2) = qq_1$ and $(c_2, q^2) = qq_2$ for divisors q_1, q_2 of q. Let $q' = (q_1, q_2)$. Then there is a solution (r', c') of (3) such that $(c', q^2) = q'$.*

Proof Let j_1, j_2 be positive integers. We have

$$(r_i + c_i\sqrt{v})^{j_i} \equiv r_i^{j_i} + j_i r_i^{j_i-1} c_i \sqrt{v} \mod q^2,$$

$i = 1, 2$. We define $r' + c'\sqrt{v}$ by

$$r' + c'\sqrt{v} = (r_1 + c_1\sqrt{v})^{j_1}(r_2 + c_2\sqrt{v})^{j_2}.$$

Since

$$(r_1 + c_1\sqrt{v})^{j_1}(r_2 + c_2\sqrt{v})^{j_2} \equiv r_1^{j_1} r_2^{j_2} + (j_1 r_1^{j_1-1} r_2^{j_2} c_1 + j_2 r_1^{j_1} r_2^{j_2-1} c_2)\sqrt{v} \mod q^2,$$

we obtain

$$c' \equiv r_1^{j_1-1} r_2^{j_2-1}(j_1 r_2 c_1 + j_2 r_1 c_2) \mod q^2. \tag{14}$$

Observe that $(r_1, q) = (r_2, q) = 1$, since $q \mid c_1, c_2$. We consider the ideal $\mathbb{Z}r_2c_1 + \mathbb{Z}q^2$ in $\mathbb{Z}$. We have $(r_2c_1, q^2) = qq_1$. This can be written as

$$\mathbb{Z}r_2c_1 + \mathbb{Z}q^2 = \mathbb{Z}qq_1.$$

In the same way, we obtain

$$\mathbb{Z}r_1c_2 + \mathbb{Z}q^2 = \mathbb{Z}qq_2.$$

However, $(qq_1, qq_2) = qq'$, and so $\mathbb{Z}qq_1 + \mathbb{Z}qq_2 = \mathbb{Z}qq'$. This yields

$$\mathbb{Z}r_2c_1 + \mathbb{Z}r_1c_2 + \mathbb{Z}q^2 = \mathbb{Z}qq'.$$

Accordingly, there are integers k_1, k_2 such that

$$k_1 r_2 c_1 + k_2 r_1 c_2 \equiv qq' \mod q^2. \tag{15}$$

We put $j_1 = k_1 + lq^2$ and $j_2 = k_2 + lq^2$, where l is chosen such that both j_1, j_2 are positive. Then (14) and (15) show that c' satisfies $(c', q^2) = qq'$. □

Lemma 2 *Let q_1 divide q. Let (r, c) be a solution of (3) such that $(c, q^2) = qq_1$. Let p be a prime dividing q/q_1. Define (r', c') by $r' + c'\sqrt{v} = (r + c\sqrt{v})^p$. Then (r', c') is a solution of (3) such that $(c', q^2) = qq_1p$.*

Proof Let l be a prime number. By $v_l(k)$ we denote the l-exponent of the integer k, i.e., $l^{v_l(k)} \mid k$, $l^{v_l(k)+1} \nmid k$. If l divides q, we have $v_l(c) = v_l(qq_1)$, since $qq_1 \mid q^2$ and $(c, q^2) = qq_1$.

First let $p = 2$. Then $c' = 2rc$ and $v_2(2rc) = v_2(c) + 1$, since $v_2(r) = 0$, by (3). If l is a prime divisor of q different from 2, we see $v_l(2rc) = v_l(c)$. Hence $(c', q^2) = qq_1p$.

If $p \geq 3$ we have

$$r' + c'\sqrt{v} \equiv r^p + pr^{p-1}c\sqrt{v} \mod c^2p, \tag{16}$$

since $c^j \equiv 0 \mod c^2p$ for $j \geq 3$ (recall $p \mid c$) and $\binom{p}{2}c^2 \equiv 0 \mod c^2p$. Thus, $v_p(c') = v_p(pr^{p-1}c) = v_p(c) + 1$, because $v_p(c^2p) > v_p(c) + 1$. For a prime divisor l of q different from p we have $v_l(c^2p) = 2v_l(c) > v_l(c)(\geq 1)$. From (16) we obtain $v_l(c') = v_l(pr^{p-1}c) = v_l(c)$. □

Proof of Theorem 2 Let q_0 be the smallest divisor of q such that there is a solution (r, c) of (3) with $(c, q^2) = qq_0$.

If q is even, then $m - n$ is even for all m, n with $(m, q) = (n, q) = 1$. Hence $(m - n, q)$ is even. Accordingly, q_0 cannot have the form $q_0 = (m - n, q)$ if q_0 is odd. Suppose that this holds. Then we replace q_0 by $2q_0$. Since $\varphi(2q_0) = \varphi(q_0)$, this does not change the assertion of Theorem 2. Moreover, by Lemma 2, we have a solution (r', c') of (3) such that $(c', q^2) = 2qq_0$.

Accordingly, we may assume that q_0 is even if q is even and suppose that (r, c) is a solution of (3) with $(c, q^2) = qq_0$.

Let $y = n/q + \sqrt{v}$, $(n, q) = 1$. We show that the sets

$$X_1 = \{m/q + \sqrt{v} : (m, q) = 1, m/q + \sqrt{v} \sim y\}$$

and

$$X_2 = \{m/q + \sqrt{v} : (m, q) = 1, q_0 \mid m - n\}$$

coincide. Indeed, if $m/q + \sqrt{v}$ is in X_1 and $(m - n, q) = q_1$, then there is a solution (r', c') of (3) such that $(c', q^2) = qq_1$. On the other hand, we have a solution (r, c) of (3) such that $(c, q^2) = qq_0$. By Lemma 1, there is a solution (r'', c'') such that $(c'', q^2) = q(q_0, q_1)$. If $(q_0, q_1) \neq q_0$, then $(q_0, q_1) < q_0$, which contradicts the minimality of q_0. Accordingly, $(q_0, q_1) = q_0$ and $q_0 \mid q_1 = (m - n, q)$. In particular, q_0 divides $m - n$ and $m/q + \sqrt{v} \in X_2$.

Conversely, if $m/q + \sqrt{v} \in X_2$, then $(m - n, q) = q_0k$ for some positive integer k. By Lemma 2, there exists a solution (r', c') of (3) such that $(c', q^2) = qq_0k$. This implies $m/q + \sqrt{v} \sim y$ and $m/q + \sqrt{v} \in X_1$.

We consider $X = \{m/q + \sqrt{v} : (m, q) = 1, 0 \leq m \leq q - 1\}$ and $X_1' = X_1 \cap X$. Now $m/q + \sqrt{v} \in X$ lies in X_1' if, and only if, $q_0 \mid m - n$, i.e., the canonical surjection

$$\pi : (\mathbb{Z}/q\mathbb{Z})^\times \to (\mathbb{Z}/q_0\mathbb{Z})^\times : \overline{k} \mapsto \overline{k}$$

maps $\overline{m}$ onto $\overline{n}$. Thereby, $|X_1'| = |\pi^{-1}(\overline{n})| = \varphi(q)/\varphi(q_0)$. Hence there are exactly $\varphi(q)/\varphi(q_0)$ elements of X that are equivalent to y. This, however, implies that there must be exactly $\varphi(q_0)$ equivalence classes whose intersections with X are not empty. □

Acknowledgements The author thanks the anonymous referee for valuable suggestions.

Funding Open access funding provided by University of Innsbruck and Medical University of Innsbruck.

Data availability The datasets generated and analysed during the current study are available from the author on reasonable request.

References

1. Borwein, J., van der Poorten, A., Shallit, J., Zudilin, W.: Neverending Fractions. An Introduction to Continued Fractions, Cambridge University Press, Cambridge (2014)
2. Burger, E.B.: A tail of two palindromes. Am. Math. Monthly **112**, 311–321 (2005)
3. German, O.N., Tlyustangelov, I.A.: Palindromes and periodic continued fractions. Mosc. J. Comb. Number Theory **6**, 233–252 (2016)
4. Hasse, H.: Vorlesungen über Zahlentheorie. Springer, Berlin (1950)
5. Perron, O.: Die Lehre von den Kettenbrüchen, vol. 1, 3rd edn. Teubner, Stuttgart (1954)