NONPERIODIC p-ADIC CONTINUED FRACTIONS OF QUADRATIC IRRATIONALS

TOMISLAV PEJKOVIĆ

ABSTRACT. For every prime $p \geq 7$, we consider two classes of p-adic continued fraction algorithms. We prove that every algorithm in these classes admits infinitely many quadratic irrationals in $\mathbb{Q}_p$ whose expansions are not eventually periodic. The first class includes Ruban's algorithm and Browkin's first algorithm, and the second includes Schneider's algorithm and its balanced version. In all cases the representatives in $\mathbb{Z}[1/p]$ modulo $p\mathbb{Z}_p$ may be chosen arbitrarily. The proof uses finite sets of quadratic irrationals that are independent of the choice of representatives. The required quadratic irrationals are constructed using Dirichlet's theorem for Gaussian integers.

1. INTRODUCTION

The analogue of Lagrange's theorem for p-adic continued fractions depends on the algorithm chosen (see [15] for a survey). De Weger [9] and Ooto [12] gave nonperiodicity criteria for Schneider's algorithm [17] and Ruban's algorithm [16], respectively. For every prime p, these criteria yield quadratic irrationals whose expansions are not eventually periodic. Capuano, Veneziano and Zannier [8] also gave an effective criterion for eventual periodicity of quadratic Ruban continued fractions. Browkin's first algorithm [4] is obtained from Ruban's algorithm by choosing balanced residue representatives. The analogous modification of Schneider's algorithm gives the balanced version, mentioned in [5, p. 1285] and studied in [13]. For Browkin's first algorithm, explicit nonperiodic quadratic irrationals were obtained in [14], and periodicity criteria and constructions with prescribed periods are given in [2, 7]. In this paper, we consider two classes that include all four algorithms and allow arbitrary choices of residue representatives. We prove that, for every prime $p \geq 7$ and every algorithm in either class, there are infinitely many quadratic irrationals $x \in \mathbb{Q}_p$ whose expansions are not eventually periodic. These numbers can be chosen so that the fields $\mathbb{Q}(x)$ are pairwise distinct and each admits an embedding into $\mathbb{R}$.

Let p be an odd prime and put $R = \mathbb{Z}[1/p]$. We consider any map $a\colon \mathbb{Q}_p \to R$ satisfying

$$x - a(x) \in p\mathbb{Z}_p, \qquad \text{and} \qquad a(x) = a(y) \quad \text{whenever } x - y \in p\mathbb{Z}_p. \tag{1}$$

Thus a chooses an arbitrary representative in R of each coset modulo $p\mathbb{Z}_p$. In particular, we do not require the normalization $a(0) = 0$ used in [4, §1] and [6, Definition 3.1].

The first algorithm defines the complete quotients x_n by

$$x_{n+1} = T_0(x_n), \qquad T_0(x) = \frac{1}{x - a(x)}. \tag{2}$$

Choosing the representatives in $[0, p)$ gives Ruban's algorithm, and choosing them in $[-p/2, p/2)$ gives Browkin's first algorithm.

2020 *Mathematics Subject Classification.* 11J70, 11A55, 11R11.

Key words and phrases. p-adic continued fraction, quadratic irrationality, periodicity, Schneider's algorithm, Browkin's algorithm, Gaussian primes.

Department of Mathematics, Faculty of Science, University of Zagreb, Bijenička cesta 30, 10000 Zagreb, Croatia.
Corresponding author: pejkovic@math.hr.

The second algorithm is defined by

$$x_{n+1} = T_1(x_n), \qquad T_1(x) = \frac{p^{h(x)}}{x - a(x)}, \qquad h(x) = v_p(x - a(x)), \tag{3}$$

where v_p is the p-adic valuation normalized by $v_p(p) = 1$. After the first step of this algorithm all complete quotients are p-adic units. Choosing $1, \dots, p-1$ as representatives of the nonzero residue classes modulo p gives Schneider's algorithm, while choosing $\pm 1, \dots, \pm(p-1)/2$ gives its balanced version.

An expansion is (eventually) periodic if the partial quotients $a(x_n)$ in (2), or the pairs $(a(x_n), h(x_n))$ in (3), form an (eventually) periodic sequence. For a quadratic irrational, both algorithms are defined at every step, and $h(x_n) \geq 1$ for the second algorithm. Algorithms that alternate different residue conditions, including Browkin's second algorithm [5] and those in [11], are not covered.

Two numbers are $\mathrm{GL}_2(R)$-equivalent if one is obtained from the other by a fractional linear transformation with matrix in $\mathrm{GL}_2(R)$. For either algorithm, if the expansions of two numbers reach a common complete quotient, they have a common tail and the two numbers are $\mathrm{GL}_2(R)$-equivalent.

Theorem 1. *For every prime $p \geq 7$ and every map a satisfying* (1)*, each of the algorithms* (2) *and* (3) *admits infinitely many quadratic irrationals $x \in \mathbb{Q}_p$ whose expansions are not eventually periodic. These numbers can be chosen so that the fields $\mathbb{Q}(x)$ are pairwise distinct and each admits an embedding into $\mathbb{R}$. In particular, these numbers are pairwise $\mathrm{GL}_2(\mathbb{Q})$-inequivalent, and hence pairwise $\mathrm{GL}_2(R)$-inequivalent.*

For each algorithm, we consider a finite set of quadratic irrationals of negative norm in a fixed $\mathrm{GL}_2(R)$-orbit. These sets are independent of a. We prove that if every matrix in $\mathrm{GL}_2(R)$ fixing the initial quadratic irrational has positive determinant, then eventual periodicity for all elements of either set would force its cardinality to be divisible by 4. We then choose the initial quadratic irrational so that every matrix in $\mathrm{GL}_2(R)$ fixing it has positive determinant. Using two involutions, we partition all but two elements of each finite set into subsets of size four. Each finite set therefore has cardinality congruent to 2 modulo 4, so at least one of its elements has an expansion that is not eventually periodic. The required arithmetic conditions are obtained using Dirichlet's theorem for Gaussian integers. The quadratic irrationals in the theorem are selected from these finite sets and may depend on a and on the algorithm.

2. A nonperiodicity criterion

Let K be a quadratic extension of $\mathbb{Q}$ with fixed embeddings into $\mathbb{Q}_p$ and $\mathbb{R}$. We use the same notation for elements of K and their images under these embeddings. For $x \in K$, write x' for its conjugate and $\mathrm{N}(x) = xx'$ for its norm.

Fix $z \in K \setminus \mathbb{Q}$. For a matrix

$$G = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GL}_2(R),$$

write

$$Gz = \frac{\alpha z + \beta}{\gamma z + \delta}.$$

Let $\mathcal{O}$ be the $\mathrm{GL}_2(R)$-orbit of z, i.e.

$$\mathcal{O} = \{Gz : G \in \mathrm{GL}_2(R)\}.$$

For the two algorithms, we consider the sets

$$\mathcal{Y}_0 = \{x \in \mathcal{O} : |x|_p > 1 > |x'|_p\},$$
$$\mathcal{Y}_1 = \{x \in \mathcal{O} : |x|_p = 1 > |x'|_p\}.$$

These conditions play a role analogous to reducedness for regular real continued fractions. As shown in the proof of Proposition 3, an eventually periodic expansion for the corresponding algorithm is purely periodic under these conditions. For Browkin's first algorithm, this implication was proved by Bedocchi [3, Proposition 3.2].

For $\varepsilon \in \{0, 1\}$, put

$$\mathcal{Y}_\varepsilon^- = \{x \in \mathcal{Y}_\varepsilon : \mathrm{N}(x) < 0\}.$$

For fixed z, these sets are independent of the choice of a.

The discriminant of a quadratic irrational is that of its primitive quadratic polynomial in $\mathbb{Z}[X]$.

Lemma 2. *The discriminants of any two elements of $\mathcal{O}$ differ by a factor p^{2n}, where $n \in \mathbb{Z}$. If $x \in \mathcal{Y}_0 \cup \mathcal{Y}_1$, then the discriminant of x is not divisible by p. Consequently, any two elements of $\mathcal{Y}_0 \cup \mathcal{Y}_1$ have the same discriminant.*

Proof. Let $f \in \mathbb{Z}[X]$ be the primitive quadratic polynomial of z, and write $x = Gz$. Multiplying G by a sufficiently large power of p does not change Gz, so we may assume that its entries are integers. Since the units of R are precisely the numbers $\pm p^j$, $j \in \mathbb{Z}$, the determinant of this integer matrix is $\pm p^k$ for some $k \geq 0$. Solving $x = (\alpha z + \beta)/(\gamma z + \delta)$ for z and substituting into $f(z) = 0$ shows that x is a root of

$$g(X) = (\alpha - \gamma X)^2 f\left(\frac{\delta X - \beta}{\alpha - \gamma X}\right) \in \mathbb{Z}[X].$$

Expanding the coefficients gives

$$\operatorname{disc}(g) = (\det G)^2 \operatorname{disc}(f) = p^{2k} \operatorname{disc}(f).$$

Reversing the substitution gives the polynomial identity

$$(\gamma X + \delta)^2 g\left(\frac{\alpha X + \beta}{\gamma X + \delta}\right) = p^{2k} f(X).$$

The coefficients on the left are integer linear combinations of the coefficients of g. Hence the greatest common divisor of the coefficients of g divides every coefficient of $p^{2k} f$. Since f is primitive, this greatest common divisor divides p^{2k}, so it equals p^j for some $j \geq 0$. Dividing g by p^j gives a primitive polynomial of x, whose discriminant is

$$p^{-2j} \operatorname{disc}(g) = p^{2(k-j)} \operatorname{disc}(f).$$

Thus discriminants in a $\mathrm{GL}_2(R)$-orbit differ by factors p^{2n}, where $n \in \mathbb{Z}$.

Now let $AX^2 + BX + C$ be the primitive polynomial of $x \in \mathcal{Y}_0 \cup \mathcal{Y}_1$. Since $x' \in p\mathbb{Z}_p$, the equation $A(x')^2 + Bx' + C = 0$ gives $p \mid C$. If $p \mid B$, the equation satisfied by x gives

$$A = -\frac{B}{x} - \frac{C}{x^2} \in p\mathbb{Z}_p,$$

because $1/x \in \mathbb{Z}_p$. Then p would divide all three coefficients, contrary to primitivity. Hence $p \nmid B$, and the discriminant $B^2 - 4AC$ is prime to p. Any two such discriminants have ratio p^{2n}, so they must be equal. □

Proposition 3. *The sets $\mathcal{Y}_0^-$ and $\mathcal{Y}_1^-$ are finite. Suppose that every matrix in $\mathrm{GL}_2(R)$ fixing z has positive determinant. Let $\varepsilon \in \{0, 1\}$ and assume that $\#\mathcal{Y}_\varepsilon^- \equiv 2 \pmod 4$. Then for every map a satisfying (1), some element of $\mathcal{Y}_\varepsilon^-$ has a T_ε-expansion that is not eventually periodic.*

Proof. For $x \in \mathcal{Y}_0^- \cup \mathcal{Y}_1^-$, let AX^2+BX+C be the primitive polynomial of x. By Lemma 2, its discriminant Δ is independent of x. Since $\mathrm{N}(x) = C/A < 0$, we have $AC < 0$ and $B^2 < \Delta$, leaving only finitely many possible integers B. For each such B, the product $AC = (B^2 - \Delta)/4$ is a fixed nonzero integer, so it has only finitely many integer factor pairs. There are therefore finitely many possible primitive polynomials, each with two roots. Hence $\mathcal{Y}_0^-$ and $\mathcal{Y}_1^-$ are finite. A similar finiteness argument for complete quotients of negative norm appears in [7, Proposition 4.1 and Corollary 4.2].

For the remaining assertion, fix a map a satisfying (1) and an index $\varepsilon \in \{0, 1\}$ with $\#\mathcal{Y}_\varepsilon^- \equiv 2 \pmod 4$. We first show that T_ε preserves $\mathcal{Y}_\varepsilon$. For $x \in \mathcal{Y}_\varepsilon$, we have $v_p(x) \le 0$, whereas $v_p(x - a(x)) \ge 1$ and $v_p(x') \ge 1$. The equality $a(x) = x - (x - a(x))$ therefore gives $v_p(a(x)) = v_p(x)$, and then $v_p(x' - a(x)) = v_p(x)$.

Since $a(x)$ is rational, and the numerator $p^{h(x)}$ in the second algorithm is rational as well, conjugating the defining formulas gives

$$(T_0 x)' = \frac{1}{x' - a(x)}, \qquad (T_1 x)' = \frac{p^{h(x)}}{x' - a(x)}.$$

For $x \in \mathcal{Y}_0$, we therefore obtain

$$v_p(T_0 x) = -v_p(x - a(x)) \le -1, \qquad v_p((T_0 x)') = -v_p(x) > 0.$$

For $x \in \mathcal{Y}_1$, we have $v_p(x) = 0$ and $h(x) = v_p(x - a(x)) \ge 1$, so

$$v_p(T_1 x) = 0, \qquad v_p((T_1 x)') = h(x) \ge 1.$$

For each x, the matrices

$$\begin{pmatrix} 0 & 1 \\ 1 & -a(x) \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} 0 & p^{h(x)} \\ 1 & -a(x) \end{pmatrix}$$

represent fractional linear transformations sending x to $T_0 x$ and $T_1 x$, respectively. Their determinants are -1 and $-p^{h(x)}$, so both matrices belong to $\mathrm{GL}_2(R)$. Thus both algorithms preserve $\mathcal{O}$, and the valuation conditions just proved show that each preserves the corresponding set $\mathcal{Y}_\varepsilon$.

We next prove injectivity. Suppose $T_\varepsilon x = T_\varepsilon y$, where $x, y \in \mathcal{Y}_\varepsilon$. If $\varepsilon = 1$, their conjugate images are equal as well. Since $v_p((T_1 x)') = h(x)$, we have $h(x) = h(y)$. Thus, for either value of ε, equality of the images implies

$$x - a(x) = y - a(y).$$

In particular, $x - y = a(x) - a(y)$ is rational, so conjugation fixes this difference. Hence

$$x - y = x' - y' \in p\mathbb{Z}_p.$$

Condition (1) gives $a(x) = a(y)$, and consequently $x = y$.

We use the usual contraction argument to show that an infinite expansion uniquely determines its initial value for the algorithms considered here. Suppose that $x_0, y_0 \in \mathcal{Y}_\varepsilon$ have the same T_ε-expansion, and let (x_n) and (y_n) be their respective sequences of complete quotients. Thus $a(x_n) = a(y_n)$ for every $n \ge 0$, and for T_1 we also have $h(x_n) = h(y_n)$.

For T_0, subtracting the equalities $x_n = a(x_n) + 1/x_{n+1}$ and $y_n = a(y_n) + 1/y_{n+1}$, and using $a(x_n) = a(y_n)$, gives

$$|x_n - y_n|_p = \frac{|x_{n+1} - y_{n+1}|_p}{|x_{n+1}|_p \, |y_{n+1}|_p} \le p^{-2} |x_{n+1} - y_{n+1}|_p,$$

since both factors in the denominator are at least p. For T_1, we have $x_n = a(x_n) + p^{h(x_n)}/x_{n+1}$ and $y_n = a(y_n) + p^{h(y_n)}/y_{n+1}$. Using $a(x_n) = a(y_n)$, $h(x_n) = h(y_n)$ and

$|x_{n+1}|_p = |y_{n+1}|_p = 1$, we obtain

$$|x_n - y_n|_p = p^{-h(x_n)}|x_{n+1} - y_{n+1}|_p \le p^{-1}|x_{n+1} - y_{n+1}|_p.$$

At any depth N, the equality $a(x_N) = a(y_N)$ and condition (1) give $|x_N - y_N|_p \le p^{-1}$. Iterating the corresponding inequality N times, with contraction factor at most p^{-1} in either case, therefore yields

$$|x_0 - y_0|_p \le p^{-N-1}.$$

Since this holds for every N, we obtain $x_0 = y_0$.

We next show that any eventually periodic expansion arising from an orbit in $\mathcal{Y}_\varepsilon$ is purely periodic. Suppose that the expansion is periodic with period r from index N onwards. The expansions starting at x_N and x_{N+r} coincide, so the uniqueness just proved gives $x_N = x_{N+r}$. Applying injectivity N times yields $x_0 = x_r$, and the expansion is therefore purely periodic.

For $x = Gz \in \mathcal{O}$, define

$$\sigma(x) = \operatorname{sgn}(\det G)\operatorname{sgn}(x - x'),$$

where signs are taken in the fixed real embedding. If $G_1 z = G_2 z$, then $G_2^{-1}G_1$ fixes z and therefore has positive determinant by assumption. Hence $\det G_1$ and $\det G_2$ have the same sign, so $\sigma(x)$ is well defined. The matrix

$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(R)$$

represents the map $x \mapsto -x$, which preserves $\mathcal{Y}_\varepsilon^-$. Its determinant is negative, and $(-x) - (-x') = -(x - x')$, so $\sigma(-x) = \sigma(x)$.

Subtracting the expressions for $T_0 x$ and $(T_0 x)'$, and likewise for T_1, gives

$$T_0 x - (T_0 x)' = -\frac{x - x'}{\mathrm{N}(x - a(x))}, \qquad T_1 x - (T_1 x)' = -\frac{p^{h(x)}(x - x')}{\mathrm{N}(x - a(x))}.$$

Since both matrices representing the algorithms have negative determinants, these identities give

$$\sigma(T_\varepsilon x) = \sigma(x)\operatorname{sgn}\mathrm{N}(x - a(x)) = \sigma(x)\operatorname{sgn}\mathrm{N}(T_\varepsilon x). \tag{4}$$

The last equality follows by taking norms in the defining formulas for T_0 and T_1, whose numerators have positive norm.

Suppose, for a contradiction, that every element of $\mathcal{Y}_\varepsilon^-$ has an eventually periodic expansion. Each such element then lies on a cycle of T_ε in $\mathcal{Y}_\varepsilon$. By (4), the sign changes precisely when the next complete quotient has negative norm. Hence the signs at successive visits to $\mathcal{Y}_\varepsilon^-$ alternate, including the passage from the last such visit in a cycle to the first. Each cycle therefore contains equally many elements of $\mathcal{Y}_\varepsilon^-$ with sign 1 and with sign -1. Distinct cycles are disjoint, and their intersections with $\mathcal{Y}_\varepsilon^-$ partition this finite set. Thus $\mathcal{Y}_\varepsilon^-$ itself contains equally many elements of each sign. Since negation preserves the sign and has no fixed points, the number of elements of each sign is even. Consequently, $\#\mathcal{Y}_\varepsilon^-$ is divisible by 4, contrary to the assumption. □

3. Counting modulo 4

We now give arithmetic conditions that ensure the hypotheses of Proposition 3 for both algorithms.

The following proposition is closely related to [14, Proposition 4].

Proposition 4. *Let $D > 1$ be a squarefree integer not divisible by p. Suppose that*

(i) *there is exactly one pair of positive integers* (u, A) *such that*
$$D = u^2 + A^2, \qquad p \mid A, \qquad \gcd(A, 2u) = 1,$$
(ii) *the equation* $X^2 - DY^2 = -1$ *has no solution* $X, Y \in R$,
(iii) D *has a prime divisor* ℓ *such that* $\ell \equiv 1 \pmod 4$ *and the Legendre symbol* $\left(\frac{p}{\ell}\right)$ *equals* -1.

Choose $s \in \mathbb{Q}_p$ *with* $s^2 = D$ *and* $s \equiv u \pmod p$, *and choose the real embedding of* $K = \mathbb{Q}(s)$ *with* $s > 0$. *Put*
$$z = \frac{u + s}{A}.$$
Then every matrix in $\mathrm{GL}_2(R)$ *fixing* z *has positive determinant. For the orbit* $\mathcal{O}$ *defined by* z, *we have* $\#\mathcal{Y}_0^- \equiv \#\mathcal{Y}_1^- \equiv 2 \pmod 4$.

Proof. Since p divides A but does not divide $D = u^2 + A^2$, it cannot divide u. Hensel's lemma therefore gives the specified root s. The polynomial $AX^2 - 2uX - A$ is primitive and has z as a root, so z has discriminant $4D$ and $\mathrm{N}(z) = -1$. Put $k = v_p(A) \geq 1$. The congruence $s \equiv u \pmod p$ gives $v_p(u + s) = 0$, and $(u + s)(u - s) = -A^2$ then gives
$$v_p(z) = -k, \qquad v_p(z') = k.$$
Thus $z \in \mathcal{Y}_0^-$ and $p^k z \in \mathcal{Y}_1^-$. By Lemma 2, every element of $\mathcal{Y}_0 \cup \mathcal{Y}_1$ has discriminant $4D$.

We first show that every matrix in $\mathrm{GL}_2(R)$ fixing z has positive determinant. Suppose that $H = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{GL}_2(R)$ fixes z. Then $\gamma z^2 + (\delta - \alpha)z - \beta = 0$. Comparison with the primitive polynomial of z gives $\gamma = A\theta$, $\beta = A\theta$ and $\delta - \alpha = -2u\theta$ for some $\theta \in \mathbb{Q}$. Since $\gcd(A, 2u) = 1$, an integer linear combination of $A\theta$ and $2u\theta$ equals θ, so $\theta \in R$. Thus
$$H = \begin{pmatrix} \delta + 2u\theta & A\theta \\ A\theta & \delta \end{pmatrix}, \qquad \det H = (\delta + u\theta)^2 - D\theta^2.$$
A negative determinant would have the form $-p^j$ with $j \in \mathbb{Z}$. If j is even, multiplying $\delta + u\theta$ and θ by $p^{-j/2}$ gives a solution of $X^2 - DY^2 = -1$ in R, contrary to (ii). If j is odd, reduction modulo ℓ gives $(\delta + u\theta)^2 \equiv -p^j \pmod \ell$, which is impossible because $-p^j$ is a quadratic nonresidue modulo ℓ by (iii). Reduction is valid for elements of R since $\ell \neq p$. Thus every matrix fixing z has positive determinant.

It remains to count $\mathcal{Y}_0^-$ and $\mathcal{Y}_1^-$ modulo 4. We use the map
$$\rho(x) = -\frac{1}{x'}.$$
To see that it preserves $\mathcal{O}$, put $J = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and note that $z' = J^{-1}z$ because $\mathrm{N}(z) = -1$. If $x = Gz$, rationality of the entries of G gives $x' = Gz'$, so
$$\rho(x) = JGJ^{-1}z. \tag{5}$$
The matrix on the right belongs to $\mathrm{GL}_2(R)$. Also $\mathrm{N}(\rho(x)) = 1/\mathrm{N}(x)$, so negative norm is preserved.

The set $\mathcal{Y}_0^-$. The map ρ preserves $\mathcal{Y}_0^-$ because $|\rho(x)|_p = |x'|_p^{-1} > 1$ and $|\rho(x)'|_p = |x|_p^{-1} < 1$. It is an involution and commutes with the map $x \mapsto -x$. These two maps partition $\mathcal{Y}_0^-$ into sets
$$\{x, -x, \rho(x), -\rho(x)\}.$$
Here $x \neq -x$, while $\rho(x) = -x$ would give $\mathrm{N}(x) = 1$, contrary to $\mathrm{N}(x) < 0$. Thus a set has four elements unless $\rho(x) = x$, which is equivalent to $\mathrm{N}(x) = -1$.

For such a fixed point, the primitive polynomial with positive leading coefficient has the form $BX^2 - 2vX - B$, with $B > 0$ and $v \in \mathbb{Z}$. The middle coefficient is even because the discriminant is $4D$. Comparing discriminants gives $D = v^2 + B^2$, and $v \neq 0$ because D

is not a square. Substitution of $x' \in p\mathbb{Z}_p$ into the polynomial gives $p \mid B$, and primitivity gives $\gcd(B, 2v) = 1$. Condition (i) therefore yields $|v| = u$ and $B = A$. The possible roots are $z, z', -z, -z'$, of which only $z, -z$ satisfy the valuation inequalities defining $\mathcal{Y}_0^-$. Hence there is one two-element set $\{z, -z\}$ and all remaining sets have four elements. This proves $\#\mathcal{Y}_0^- \equiv 2 \pmod 4$.

The set $\mathcal{Y}_1^-$. For $x \in \mathcal{Y}_1^-$, put $t = v_p(\mathrm{N}(x)) = v_p(x') > 0$ and define

$$\psi(x) = -\frac{p^t}{x'}.$$

Equation (5) and multiplication by p^t show that $\psi(x) \in \mathcal{O}$. For $y = \psi(x)$, we have

$$v_p(y) = 0, \qquad v_p(y') = t, \qquad \mathrm{N}(y) = \frac{p^{2t}}{\mathrm{N}(x)} < 0.$$

Thus $y \in \mathcal{Y}_1^-$, and $v_p(\mathrm{N}(y)) = t$. Since $y' = -p^t/x$, we have $\psi(y) = x$. The maps ψ and $x \mapsto -x$ commute. As above, the sets $\{x, -x, \psi(x), -\psi(x)\}$ have four elements unless $\psi(x) = x$, because $\psi(x) = -x$ would give $\mathrm{N}(x) = p^t > 0$.

A fixed point x of ψ has norm $-p^t$ and primitive polynomial $BX^2 - 2vX - Bp^t$, where $B > 0$ and $v \in \mathbb{Z}$. Its discriminant gives $D = v^2 + p^t B^2$. If t is odd, then $-p^t$ is a quadratic nonresidue modulo ℓ. Reducing this equality modulo ℓ forces $\ell \mid B$ and $\ell \mid v$, contrary to primitivity. Hence $t = 2j$ for some $j \geq 1$. Put $\xi = p^{-j}x$, so $v_p(\xi) = -j$, $v_p(\xi') = j$ and $\mathrm{N}(\xi) = -1$. Multiplication by p^{-j} preserves $\mathcal{O}$, hence $\xi \in \mathcal{Y}_0^-$. The preceding calculation of the fixed points of ρ gives $\xi = \pm z$. Comparing valuations yields $j = k$, so $x = \pm p^k z$. Both numbers belong to $\mathcal{Y}_1^-$ and are fixed by ψ, so they form the only two-element set in its partition. Hence $\#\mathcal{Y}_1^- \equiv 2 \pmod 4$. □

4. Construction using Gaussian primes

We use Dirichlet's theorem for Gaussian integers [10], which is stated in modern notation in [1, Theorem 5.15]. If $m, \tau \in \mathbb{Z}[i]$ are relatively prime and $m \neq 0$, then there are infinitely many Gaussian primes π with $\pi \equiv \tau \pmod{m\mathbb{Z}[i]}$. A bar denotes Gaussian conjugation, also on residue classes, and the norm of a Gaussian integer π is $\pi\overline{\pi}$.

4.1. **A negative Pell equation.**

Lemma 5. *Let $\pi_j = \alpha_j + \beta_j i \in \mathbb{Z}[i]$ for $j = 0, 1, 2$, where α_j is odd and β_j is even. Suppose that $q_j = \pi_j\overline{\pi}_j$ are distinct rational primes, all different from p, and that*

$$\left(\frac{p}{q_0}\right) = 1, \qquad q_0 \mid \beta_1, \quad q_0 \mid \beta_2, \qquad \left(\frac{\alpha_0\alpha_1\alpha_2}{q_0}\right) = -1.$$

Then $X^2 - q_0q_1q_2Y^2 = -1$ has no solution $X, Y \in R$.

Proof. A solution in R would, after clearing a minimal common power of p from the denominators, give integers X, Y and $k \geq 0$ satisfying

$$X^2 + p^{2k} = q_0q_1q_2Y^2. \tag{6}$$

If $k > 0$ and $p \mid X$, reduction modulo p gives $p \mid Y$, contrary to the minimality of k. Thus X and p^k are relatively prime for all $k \geq 0$. Since each $q_j = \alpha_j^2 + \beta_j^2$ is congruent to 1 modulo 4, reduction of (6) modulo 4 shows that X is even and Y is odd. The Gaussian integers $X + ip^k$ and $X - ip^k$ are relatively prime. Indeed, a common Gaussian prime divisor would divide both $2X$ and $2ip^k$, and hence would divide 2 because X and p^k are relatively prime. The factor $1 + i$ is excluded by the opposite parities of X and p^k.

Unique factorization in $\mathbb{Z}[i]$ applied to (6) therefore gives

$$X + ip^k = \zeta(\alpha_0 + \eta_0\beta_0 i)(\alpha_1 + \eta_1\beta_1 i)(\alpha_2 + \eta_2\beta_2 i)(v + wi)^2,$$

where $\eta_j \in \{1,-1\}$, $v,w \in \mathbb{Z}$, and $\zeta \in \{1,-1,i,-i\}$. A rational prime that remains prime in $\mathbb{Z}[i]$ cannot divide $X+ip^k$, since it would also divide its conjugate $X-ip^k$. For each q_j, exactly one of its two conjugate Gaussian prime factors occurs on the left. Its exponent is odd, and all remaining prime exponents are even, which explains the displayed factorization. Taking norms gives $v^2+w^2=|Y|$, so v,w have opposite parity. The product on the right without ζ has odd real part and even imaginary part. Comparison with the left side yields $\zeta \in \{i,-i\}$.

Since $\zeta = \pm i$, taking imaginary parts expresses p^k, up to sign, as the real part of the product on the right without ζ. Using $q_0 \mid \beta_1, \beta_2$, we therefore obtain

$$\begin{aligned} p^k &\equiv \pm\alpha_1\alpha_2\Big(\alpha_0(v^2-w^2) - 2\eta_0\beta_0 vw\Big) \\ &\equiv \pm\alpha_0\alpha_1\alpha_2\Big(v - \eta_0\beta_0\alpha_0^{-1}w\Big)^2 \pmod{q_0}. \end{aligned} \tag{7}$$

Here α_0^{-1} denotes its inverse modulo q_0, and the second congruence follows from $\beta_0^2 \equiv -\alpha_0^2 \pmod{q_0}$. The factor in parentheses is nonzero modulo q_0 because $p \neq q_0$. Since $\left(\frac{-1}{q_0}\right) = 1$, the hypothesis on $\alpha_0\alpha_1\alpha_2$ shows that the right side of (7) is a quadratic nonresidue modulo q_0. The left side is a nonzero square by $\left(\frac{p}{q_0}\right) = 1$, a contradiction. □

4.2. **The construction.** We now choose three Gaussian primes so that their product gives the unique representation in Proposition 4(i). The congruence conditions imposed on these primes will also ensure (ii) and (iii).

Proposition 6. *For every prime $p \geq 7$, there are infinitely many positive odd squarefree integers D not divisible by p that satisfy all three conditions of Proposition 4.*

Proof. Let n be the least positive quadratic nonresidue modulo p. Then $n-1$ is a nonzero square modulo p, so we can choose an integer t such that $t^2 \equiv n-1 \pmod{p}$. The Gaussian integers

$$3+4i, \qquad 1+ti, \qquad (4+3i)(1-ti)$$

have norms congruent modulo p to $25, n, 25n$, respectively, so all three are invertible modulo p. Both coordinates of $3+4i$ are nonzero modulo p because $p \geq 7$. The same is true for each of the other two Gaussian integers. A coordinate divisible by p would make the norm a square modulo p, whereas their norms are quadratic nonresidues. A Gaussian prime congruent modulo p to any of these three numbers therefore has nonzero real and imaginary parts, and its norm is a rational prime.

Since $3+4i$ is relatively prime to $2p$, Dirichlet's theorem gives a Gaussian prime $\pi_0 = \alpha_0 + \beta_0 i$ satisfying

$$\pi_0 \equiv 3+4i \pmod{2p}.$$

Put $q_0 = \pi_0\overline{\pi}_0$ and choose a quadratic nonresidue g modulo q_0. Next consider the two systems of congruences

$$\begin{aligned} &\pi_1 \equiv 1+ti \pmod{p}, && \pi_1 \equiv \alpha_0 g \pmod{q_0}, && \pi_1 \equiv 1 \pmod{2}, \\ &\pi_2 \equiv (4+3i)(1-ti) \pmod{p}, && \pi_2 \equiv 1 \pmod{q_0}, && \pi_2 \equiv 1 \pmod{2}. \end{aligned}$$

All congruences here are in $\mathbb{Z}[i]$. The prescribed values modulo p are invertible by the norm calculations above. The values $\alpha_0 g$ and 1 prescribed modulo q_0 are invertible because $q_0 \nmid \alpha_0 g$, and both systems prescribe 1 modulo 2. Here $q_0 \nmid \alpha_0$ because $q_0 = \alpha_0^2+\beta_0^2$ is prime. Since the integers $2, p, q_0$ are pairwise relatively prime, the Chinese remainder theorem applies separately to the real and imaginary parts. Each system therefore determines a single invertible residue class modulo $2pq_0$. Dirichlet's theorem gives infinitely many Gaussian primes in each class, so we can choose π_1 and π_2 satisfying the respective systems. We may require the rational prime norms $q_j = \pi_j\overline{\pi}_j$ to be distinct, since only finitely

many Gaussian primes have any one prescribed norm. They are all different from p and congruent to 1 modulo 4. Taking norms modulo p gives $q_0 \equiv 25$, $q_1 \equiv n$ and $q_2 \equiv 25n \pmod p$. Hence

$$\left(\frac{q_0}{p}\right) = 1, \qquad \left(\frac{q_1}{p}\right) = \left(\frac{q_2}{p}\right) = -1. \tag{8}$$

Put $D = q_0q_1q_2$ and $\Pi = \pi_0\pi_1\pi_2$, and set $A = |\operatorname{Re}\Pi|$ and $u = |\operatorname{Im}\Pi|$. We have

$$\Pi \equiv (3+4i)(1+ti)(4+3i)(1-ti) \equiv 25ni \pmod p.$$

Also $\Pi \equiv 1 \pmod 2$. Thus $p \mid A$, $p \nmid u$, A is odd and u is even. Taking norms gives $D = u^2 + A^2$. Since D is squarefree and greater than 1, neither A nor u is zero, and $\gcd(A, 2u) = 1$.

We verify uniqueness in condition (i). In any representation $D = v^2 + B^2$ with $\gcd(B, 2v) = 1$, the integer B is odd and v is even. Unique factorization in $\mathbb{Z}[i]$ shows that $B + vi$ is a unit multiple of a product obtained by choosing either π_j or $\overline{\pi}_j$ for each j. The unit is 1 or -1, since i and $-i$ would interchange the parities of the two coordinates. Up to conjugating the whole product, it is enough to consider Π and the three products obtained by conjugating just one factor. Indeed, conjugating two of the three factors is equivalent to conjugating the remaining factor and then the whole product.

Suppose that replacing π_j by $\overline{\pi}_j$ also gave a product with real part divisible by p. Both products would then be nonzero scalar multiples of i modulo p. All factors are invertible modulo p, so dividing the two products and cancelling the unchanged factors would give

$$\overline{\pi}_j \equiv \lambda\pi_j \pmod p$$

for some integer λ not divisible by p. Both coordinates of π_j are nonzero modulo p, so comparison of the real coordinates gives $\lambda \equiv 1 \pmod p$, while comparison of the imaginary coordinates gives $\lambda \equiv -1 \pmod p$. This is impossible because p is odd. Thus only Π and its conjugate, up to sign, have real part divisible by p, proving that (u, A) is the unique positive pair in (i).

Write $\pi_j = \alpha_j + \beta_j i$ for $j = 1, 2$. The congruences modulo 2 give the parities required in Lemma 5, while those modulo q_0 give $q_0 \mid \beta_1, \beta_2$ and

$$\alpha_0\alpha_1\alpha_2 \equiv \alpha_0^2 g \pmod{q_0}.$$

Since $q_0 \nmid \alpha_0$ and g is a quadratic nonresidue, this gives $\left(\frac{\alpha_0\alpha_1\alpha_2}{q_0}\right) = -1$. Quadratic reciprocity and (8) give

$$\left(\frac{p}{q_0}\right) = \left(\frac{q_0}{p}\right) = 1.$$

Lemma 5 proves condition (ii). Finally, we may take $\ell = q_1$ in (iii), because $q_1 \equiv 1 \pmod 4$ and $\left(\frac{p}{q_1}\right) = \left(\frac{q_1}{p}\right) = -1$. Keeping π_0, π_1 fixed and varying π_2 gives infinitely many distinct prime norms q_2, and hence infinitely many such D. □

Proof of Theorem 1. Fix $p \geq 7$ and a map a satisfying (1). For each D supplied by Proposition 6, choose s, z as in Proposition 4. The hypotheses of Proposition 3 hold for both algorithms, so it provides, for each algorithm, a quadratic irrational in $\mathbb{Q}(s)$ whose expansion is not eventually periodic. By Lemma 2, all elements of $\mathcal{Y}_0^- \cup \mathcal{Y}_1^-$ have the same discriminant $4D$ as z. A primitive polynomial of discriminant $4D$ has even middle coefficient and can be written as $cX^2 - 2bX + (b^2 - D)/c$, with $b, c \in \mathbb{Z}$. Since the constant coefficient is an integer, we have $c \mid D - b^2$, and primitivity means that the three coefficients have greatest common divisor 1. The roots are $(b \pm s)/c$. Changing the

signs of both b and c if necessary, we can express either root as $(b+s)/c$. Their norm is $(b^2-D)/c^2$, so it is negative precisely when $b^2 < D$. Thus both sets are contained in

$$\left\{ \frac{b+s}{c} : \begin{array}{c} b,c \in \mathbb{Z}, \quad b^2 < D, \quad c \mid D-b^2, \\ \gcd\left(c, 2b, \dfrac{D-b^2}{c}\right) = 1 \end{array} \right\}.$$

The set is finite because there are finitely many possible b and, for each of them, finitely many signed divisors c of $D-b^2$. It is independent of a, although the selected nonperiodic number may depend on a and on the algorithm.

For every selected number $x = (b+s)/c$, the identity $s = cx - b$ gives $\mathbb{Q}(x) = \mathbb{Q}(s)$. Since $D > 0$, this field admits an embedding into $\mathbb{R}$. Distinct squarefree values of D give distinct quadratic fields. A rational fractional linear transformation with nonzero determinant preserves the field generated by an irrational number, since its inverse is again a rational fractional linear transformation. Thus the quadratic irrationals obtained from different values of D are pairwise $\mathrm{GL}_2(\mathbb{Q})$-inequivalent, and hence pairwise $\mathrm{GL}_2(R)$-inequivalent. □

The construction requires a residue class for π_0 whose coordinates are nonzero modulo p and whose norm is a nonzero square modulo p. The class of $3+4i$ has these properties for every prime $p \geq 7$. No such class exists for $p = 3$ or $p = 5$. We leave open whether the conclusion of Theorem 1 extends to $p = 2, 3, 5$ for arbitrary choices of residue representatives.

Statements and declarations

Funding. The author was supported by the Croatian Science Foundation under project no. IP-2022-10-5008 (TEBAG). The author acknowledges support from the project "Implementation of cutting-edge research and its application as part of the Scientific Center of Excellence for Quantum and Complex Systems, and Representations of Lie Algebras", Grant No. PK.1.1.10.0004, co-financed by the European Union through the European Regional Development Fund – Competitiveness and Cohesion Programme 2021–2027. This research was funded by the European Union's NextGenerationEU through the institutional grant to the Faculty of Science of the University of Zagreb under the National Recovery and Resilience Plan 2021–2026 (IK IA 1.1.3. Impact4Math).

Competing interests. The author has no relevant financial or non-financial interests to disclose.

Author contributions. The author carried out the research and prepared the manuscript.

Use of artificial intelligence. The author used ChatGPT 6 (OpenAI) and Claude Opus 5.5 (Anthropic) as interactive research and writing tools in the preparation of this paper. Their use included developing proof strategies, deriving mathematical arguments, constructing examples and counterexamples, writing code for exact computations, and drafting and revising the manuscript. The author reviewed and revised the mathematical arguments throughout the preparation of the manuscript. The author takes full responsibility for the content of the paper.

Data availability. No datasets were generated or analysed during the current study.

References

[1] A. Abiad, W. Castryck, M. De Boeck, J. H. Koolen and S. Zeijlemaker, *An infinite class of Neumaier graphs and non-existence results*, J. Combin. Theory Ser. A **193** (2023), Paper No. 105684. https://doi.org/10.1016/j.jcta.2022.105684

[2] S. Barbero, N. Murru and M. Urani, *Periodicity and period-length bounds for Browkin p-adic continued fractions*, preprint (2026). https://doi.org/10.48550/arXiv.2609.15531

[3] E. Bedocchi, *Nota sulle frazioni continue p-adiche*, Ann. Mat. Pura Appl. (4) **152** (1988), 197–207. https://doi.org/10.1007/BF01766149

[4] J. Browkin, *Continued fractions in local fields, I*, Demonstr. Math. **11** (1978), no. 1, 67–82. https://doi.org/10.1515/dema-1978-0108

[5] J. Browkin, *Continued fractions in local fields, II*, Math. Comp. **70** (2001), no. 235, 1281–1292. https://doi.org/10.1090/S0025-5718-00-01296-5

[6] L. Capuano, N. Murru and L. Terracini, *On the finiteness of $\mathfrak{P}$-adic continued fractions for number fields*, Bull. Soc. Math. France **150** (2022), no. 4, 743–772. https://doi.org/10.24033/bsmf.2860

[7] L. Capuano, N. Murru and L. Terracini, *On periodicity of p-adic Browkin continued fractions*, Math. Z. **305** (2023), Paper No. 17. https://doi.org/10.1007/s00209-023-03333-3

[8] L. Capuano, F. Veneziano and U. Zannier, *An effective criterion for periodicity of ℓ-adic continued fractions*, Math. Comp. **88** (2019), 1851–1882. https://doi.org/10.1090/mcom/3385

[9] B. M. M. de Weger, *Periodicity of p-adic continued fractions*, Elem. Math. **43** (1988), no. 4, 112–116. https://math.deweger.net/papers/[5]dW-PerContFr-ElemMat[1988].pdf

[10] P. G. L. Dirichlet, *Untersuchungen über die Theorie der complexen Zahlen*, Abh. Königl. Preuss. Akad. Wiss. (1841), 141–161. Reprinted in *G. Lejeune Dirichlet's Werke*, Vol. I, Reimer, Berlin, 1889, 509–532. https://www.e-rara.ch/download/pdf/5688065.pdf

[11] N. Murru, G. Romeo and G. Santilli, *Convergence conditions for p-adic continued fractions*, Res. Number Theory **9** (2023), Paper No. 66. https://doi.org/10.1007/s40993-023-00470-w

[12] T. Ooto, *Transcendental p-adic continued fractions*, Math. Z. **287** (2017), no. 3–4, 1053–1064. https://doi.org/10.1007/s00209-017-1859-2

[13] T. Pejković, *Balanced Schneider's p-adic continued fractions*, preprint (2026). https://web.math.pmf.unizg.hr/~pejkovic/papers/balanced2.pdf

[14] T. Pejković, *Nonperiodic quadratic Browkin continued fractions*, preprint (2026). https://web.math.pmf.unizg.hr/~pejkovic/papers/browkin7a.pdf

[15] G. Romeo, *Continued fractions in the field of p-adic numbers*, Bull. Amer. Math. Soc. **61** (2024), no. 2, 343–371. https://doi.org/10.1090/bull/1819

[16] A. A. Ruban, *Some metric properties of p-adic numbers*, Siberian Math. J. **11** (1970), 176–180. https://doi.org/10.1007/BF00970247

[17] Th. Schneider, *Über p-adische Kettenbrüche*, in: Symposia Mathematica, Vol. IV (INDAM, Rome, 1968/69), Academic Press, London, 1970, 181–189.