ON SEVERAL CONJECTURES CONCERNING p-ADIC CONTINUED FRACTIONS

ABSTRACT. Let p be an odd prime and let $h \geq 2$ be even. If $(p,h) \neq (3,2)$, infinitely many real and infinitely many imaginary quadratic fields have the form $\mathbb{Q}(\sqrt{D})$, where D is an integer whose p-adic square roots have least period h under Browkin's second algorithm. For $(p,h) = (3,2)$, we give two radicands and bound all such radicands in terms of their preperiods. We prove eventual periodicity for quadratic inputs to the fourth algorithm of Wang and Deng at $p = 5$ and to Yasutomi's simultaneous algorithm for real quadratic fields at $p = 3$. The real approximation error after n digits is $O(n^{-3})$ for Ruban's expansion of a quadratic irrational and for Schneider's expansion of a quadratic p-adic unit. For both Browkin algorithms and the alternating algorithm of Murru and Romeo, we determine the real and p-adic approximation exponents in terms of the reduced denominator for Haar-almost every input. The real limit is transcendental and has finite irrationality exponent.

In each cubic field embedded in $\mathbb{Q}_p$, a suitable generator gives eventual periodicity for every basis $1, x, y$ in a variant of the algorithm of Saito, Tamura and Yasutomi that computes the translation after inversion and row reduction. Computing the translation from the input gives nonperiodic expansions on a dense set of bases in every degree at least two. For the p-adic Jacobi–Perron algorithm we construct pairs of Liouville numbers on a rational line with infinite expansions that are not eventually periodic. We also prove an irreducibility conjecture for a sequence of polynomials arising from a Pell equation.

hexagon:2611.00743v1

Use of artificial intelligence. The research was carried out under human direction from the choice of topic and research questions to the selection of results for the paper. OpenAI's ChatGPT 6 and Anthropic's Claude Opus 5.5 assisted in developing arguments, checking examples and drafting the manuscript. OpenAI's ChatGPT 6.2 Astra developed further constructions and proofs, checked the computations and references, and revised the manuscript. Anthropic's Claude subsequently reviewed the full manuscript and suggested improvements to the proofs and exposition. The human review did not include an independent check of every proof.

1. INTRODUCTION

Several continued fraction algorithms expand quadratic irrationals in $\mathbb{Q}_p$. The choice of partial quotients affects periodicity and the behavior of the rational convergents in $\mathbb{R}$. Romeo surveys these algorithms and their history [24].

Section 3 concerns Browkin's second algorithm. Murru, Romeo and Santilli [15, Conjecture 20] ask whether, for every odd prime p and every positive even integer h, infinitely many nonsquare integers have a square root with least period h. Theorems 3.1 and 3.17 give infinitely many distinct real quadratic fields and infinitely many distinct imaginary quadratic fields for every pair except $(3,2)$. Browkin [4, Lemma 2] had constructed examples of period two for $p \geq 5$. The period-four construction of Murru, Romeo and Santilli [15, Theorem 18 and Corollary 19] works for $p \geq 5$. At $p = 3$ the odd-step correction changes their word. Proposition 3.8 gives a family valid at every odd prime. Our

2020 *Mathematics Subject Classification.* Primary 11J70, Secondary 11B39, 11J61, 11K50, 11R11.

Key words and phrases. p-adic continued fractions, quadratic irrationals, periodicity, real convergence, Jacobi–Perron algorithm.

Tomislav Pejković proposed the topic and guided the research presented in this paper. Department of Mathematics, Faculty of Science, University of Zagreb, Bijenička cesta 30, 10000 Zagreb, Croatia (pejkovic@math.hr).

construction adapts the palindromes of Capuano, Murru and Terracini [6] to Browkin's correction at the odd steps. At $p = 3$ the square roots of 171 and 13851 have period two, with least preperiods 10 and 40. A bound for the radicand in terms of the preperiod restricts any further examples. Infinitude in this case remains open.

Section 4 treats periodicity for quadratic inputs. Wang and Deng use the half-trace of each complete quotient to choose its partial quotient. Yasutomi uses a chosen real embedding in his simultaneous algorithm. For the fourth algorithm of Wang and Deng the complete quotients of every quadratic irrational are eventually periodic at $p = 5$. We determine the sharp eventual bound on their denominators and give sufficient conditions for periodicity of the fifth algorithm. For Yasutomi's simultaneous algorithm we prove periodicity at $p = 3$ and show that the real convergents tend to the image of the input under the chosen embedding. For each $p \geq 5$, inputs of period two in every admissible real quadratic field can converge to the other real conjugate. For Yasutomi's separate algorithm with a choice of sign we describe periodic orbits and the accuracy of their convergents.

Capuano, Veneziano and Zannier [7, Proposition 4.5] proved real convergence for every quadratic Ruban expansion. In Section 5 we bound the error after n digits by $O(n^{-3})$. Corollary 5.3 gives the same bound for Schneider's expansions of quadratic p-adic units, improving the exponent in [22, Theorem 2.3]. Section 6 treats Browkin's two algorithms and the alternating algorithm of Murru and Romeo [14]. For these algorithms, convergence to a real conjugate at a rate faster than every inverse power, even along a subsequence, forces eventual periodicity. Romeo asks whether convergence to a real conjugate alone forces eventual periodicity [25, Conjectures 2 and 17]. Section 7 treats the same three algorithms with respect to additive Haar measure on $\mathbb{Q}_p$. For almost every input the real limit is transcendental with finite irrationality exponent. Theorem 7.1 gives the exponential rate of convergence, and Corollary 7.5 gives the real and p-adic exponents in terms of the reduced denominator.

In dimension two, Section 8 studies a version of the algorithm of Saito, Tamura and Yasutomi in which the rational constants are reduced after inversion and row reduction. We prove periodicity for all cubic bases in the stated domain. For the translation evaluated on the input in formula (4) of the arXiv version of [27], Corollary 8.3 gives, in every degree at least two, a dense set of bases whose expansions are not eventually periodic. The same bases reach the fixed power basis in one step when the constants are reduced after inversion. Section 9 constructs pairs of Liouville numbers on a rational line with infinite, nonperiodic p-adic Jacobi–Perron expansions, answering a question of Murru and Terracini [17, Conjecture 1]. In Section 10, Theorem 10.1 proves an irreducibility conjecture of Capuano, Mula, Terracini and Veneziano [5, Conjecture 4.29]. We also relate their prime-value conjecture to two classical sequences and bound the common divisors of terms at a fixed distance.

2. Preliminaries

Unless otherwise stated, p is an odd prime. We write v_p for the valuation normalized by $v_p(p) = 1$, put $v_p(0) = +\infty$, and write $|x|_p = p^{-v_p(x)}$. An absolute value without a subscript is the usual real or complex absolute value, and x' denotes the other conjugate of a quadratic irrational x. The sign of a nonzero rational number refers to its real sign. The prime-to-p part of $\pm p^k m \in \mathbb{Z}[1/p] \setminus \{0\}$, where $m > 0$ and $p \nmid m$, is m.

Put $\Sigma_p = \{-(p-1)/2, \ldots, (p-1)/2\}$. Browkin's balanced truncations [3, 4] are the unique representatives satisfying

$$s(x) \in \mathbb{Z}[1/p] \cap (-p/2, p/2), \qquad x - s(x) \in p\mathbb{Z}_p, \tag{2.1}$$

$$t(x) \in \mathbb{Z}[1/p] \cap (-1/2, 1/2), \qquad x - t(x) \in \mathbb{Z}_p. \tag{2.2}$$

For a p-adic unit, $s(x)$ is the nonzero element of Σ_p congruent to x modulo p.

In the one-dimensional algorithms with partial numerators equal to one, the complete quotients α_n and partial quotients a_n satisfy

$$\alpha_{n+1} = \frac{1}{\alpha_n - a_n}. \tag{2.3}$$

We write $[a_0; a_1, a_2, \ldots]$ for the expansion and use an overline for a repeated word. Period length always means minimal eventual period. The minimal preperiod is the least index at which a periodic tail begins. For a parity-dependent algorithm, complete quotients are compared only at indices of the same parity.

Put $M(a) = \left(\begin{smallmatrix} a & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Matrices act by Möbius transformations, so

$$[a_0; a_1, \ldots, a_m, z] = M(a_0) \cdots M(a_m) \cdot z.$$

Finite words are interpreted projectively by these products. We use continuants $K() = 1$, $K(a_1) = a_1$ and

$$K(a_1, \ldots, a_m) = a_m K(a_1, \ldots, a_{m-1}) + K(a_1, \ldots, a_{m-2}).$$

For $m \geq 2$ these continuants give

$$M(a_1) \cdots M(a_m) = \begin{pmatrix} K(a_1, \ldots, a_m) & K(a_1, \ldots, a_{m-1}) \\ K(a_2, \ldots, a_m) & K(a_2, \ldots, a_{m-1}) \end{pmatrix}.$$

The determinant is $(-1)^m$, and reversing a word leaves its continuant unchanged.

3. Prescribed period lengths for Browkin's second algorithm

Murru, Romeo and Santilli asked whether every even period occurs for infinitely many square roots of integers under Browkin's second algorithm [15, Conjecture 20]. We adapt the palindromic construction of Capuano, Murru and Terracini for Browkin's first algorithm [6, Theorem 5.6] to the alternating truncations and the sign correction in Browkin II.

Theorem 3.1. *Let p be an odd prime and let $h \geq 2$ be even. There is a nonsquare integer D such that a square root of D in $\mathbb{Q}_p$ has a Browkin II expansion of minimal period h. If $(p, h) \neq (3, 2)$, there are infinitely many such integers D.*

3.1. **Admissible expansions.** Browkin's second algorithm [4, 15] starts at $\alpha_0 = \alpha$ and uses (2.3) with

$$a_n = \begin{cases} s(\alpha_n), & n \text{ even}, \\ t(\alpha_n), & n \text{ odd and } |\alpha_n - t(\alpha_n)|_p = 1, \\ t(\alpha_n) - \operatorname{sgn} t(\alpha_n), & n \text{ odd and } |\alpha_n - t(\alpha_n)|_p < 1. \end{cases} \tag{3.1}$$

For $n \geq 1$, odd complete quotients have norm greater than 1 and even complete quotients have norm 1. Indeed, an even remainder belongs to $p\mathbb{Z}_p$, while the correction at an odd step makes the remainder a unit. Thus even partial quotients from index 2 on are nonzero elements of Σ_p, and odd partial quotients are nonintegral. Every eventual period is consequently even. Negating the input negates all partial quotients, so the period length of a square root does not depend on its sign.

Definition 3.2. A finite or infinite sequence (b_n) with consecutive indices is *admissible* if $b_n \in \Sigma_p \setminus \{0\}$ for even n, and $b_n \in \mathbb{Z}[1/p]$ with $|b_n|_p > 1$ for odd n, subject to the following condition. An odd entry is either *uncorrected*, with $|b_n| < 1/2$, or *corrected*, with $1/2 < |b_n| < 1$. In the latter case its next entry, when present, must be $-\operatorname{sgn} b_n$.

Lemma 3.3. *Let $(b_n)_{n_0\le n\le N}$ be admissible.*

(1) *If $N<\infty$, let $Z\in\mathbb{Q}_p$ satisfy $|Z|_p=1$ when $N+1$ is even and $|Z|_p>1$ when $N+1$ is odd. If b_N is corrected, assume also $Z\equiv-\operatorname{sgn} b_N \pmod p$. Then $[b_{n_0};\dots,b_N,Z]$ is defined and the algorithm, started at index n_0, produces the displayed partial quotients and the complete quotient Z.*

(2) *If $N=\infty$, the continued fraction converges in $\mathbb{Q}_p$ and is the expansion of its limit under the algorithm started at index n_0.*

In both cases the complete quotients satisfy $|\xi_n|_p=1$ and $\xi_n\equiv b_n \pmod p$ at even indices, and $|\xi_n|_p=|b_n|_p$ at odd indices.

Proof. For a finite word, backwards evaluation by $\xi_n=b_n+1/\xi_{n+1}$ gives the stated norms and congruences, so no complete quotient vanishes. At even indices these identify $s(\xi_n)=b_n$. At an uncorrected odd entry, $t(\xi_n)=b_n$ and $\xi_n-b_n=1/\xi_{n+1}$ is a unit. At a corrected entry put $\tau=b_n-\operatorname{sgn} b_n$. Then $|\tau|<1/2$, $\operatorname{sgn}\tau=-\operatorname{sgn} b_n$ and

$$\xi_n-\tau=\operatorname{sgn} b_n+1/\xi_{n+1}\in p\mathbb{Z}_p,$$

because $\xi_{n+1}\equiv-\operatorname{sgn} b_n \pmod p$. Thus $t(\xi_n)=\tau$ and its correction is b_n.

For a tail beginning at index i, its continuant denominators satisfy $|B_j|_p=\prod_{n=i+1}^{j}|b_n|_p$ for $j\ge i$, with $B_i=1$. Indeed, $B_{i+1}=b_{i+1}$, and $|b_jb_{j-1}|_p>1$ gives $|b_jB_{j-1}|_p>|B_{j-2}|_p$ in each subsequent recurrence. Hence $|B_j|_p\to\infty$. The determinant identity gives convergence of this tail, as in [4, Lemma 1]. Apply the finite case to truncations ending at an even index, taking the final even digit as the terminal complete quotient Z. Their complete quotients have the stated norms and congruences, which pass to the limits since the corresponding spheres and residue classes are closed. The limits are nonzero, and the preceding verification of the algorithm applies to each tail. □

We shall repeatedly use the following observation. If a periodic word contains an entry whose p-adic norm is strictly greater than that of every other entry, its length is the minimal period. Indeed, a shorter minimal period would divide the displayed length and repeat that entry within the word.

3.2. **A palindromic construction.**

Lemma 3.4. *Let $c_0,\dots,c_j,\mu\in\mathbb{Q}$, put $\Gamma=M(c_0)\cdots M(c_j)=(g_{ik})$ and $\delta=\det\Gamma=(-1)^{j+1}$, and define*

$$\Phi(\mu)=\frac{g_{11}(g_{11}\mu+2g_{12})}{g_{21}(g_{21}\mu+2g_{22})}$$

when the denominator is nonzero. If $\Phi(\mu)$ is defined and $\xi\ne0$ satisfies

$$\xi=[c_0;c_1,\dots,c_j,\mu,c_j,\dots,c_1,\xi+c_0], \tag{3.2}$$

then $\xi^2=\Phi(\mu)$. If $g_{11}g_{21}\ne0$, put $A=g_{11}/g_{21}$ and $B=g_{21}/g_{11}$. Then

$$\Phi(\mu)=A^2-\frac{2\delta A}{g_{21}(g_{21}\mu+2g_{22})}, \tag{3.3}$$

$$\frac{1}{\Phi(\mu)}=B^2+\frac{2\delta B}{g_{11}(g_{11}\mu+2g_{12})}, \tag{3.4}$$

wherever the expressions are defined.

Proof. The matrices $M(a)$ are symmetric and the translation $z\mapsto z+c_0$ is $M(c_0)M(0)$. Hence the right side of (3.2) is $S\cdot(1/\xi)$, where

$$S=\Gamma M(\mu)\Gamma^T=\begin{pmatrix}s_1&s_2\\s_2&s_3\end{pmatrix},\qquad s_1=g_{11}(g_{11}\mu+2g_{12}),\quad s_3=g_{21}(g_{21}\mu+2g_{22}).$$

Thus $\xi = (s_1 + s_2\xi)/(s_2 + s_3\xi)$ implies $s_3\xi^2 = s_1$. The other two identities follow from $g_{11}g_{22} - g_{12}g_{21} = \delta$. □

We use two settings for the prefix $(c_0, \dots, c_j)$, with every odd-position entry uncorrected.

(E) The integer $j \geq 0$ is even and the prefix is admissible from index 0. Put

$$A = \frac{g_{11}}{g_{21}}, \qquad \mu_\infty = -\frac{2g_{22}}{g_{21}}.$$

Here A is a p-adic unit congruent to c_0 modulo p. For $j \geq 2$ we have $\mu_\infty = -2/[c_j; c_{j-1}, \dots, c_1]$, and for $j = 0$ we have $\mu_\infty = 0$.

(O) The integer $j \geq 1$ is odd and the prefix is admissible from index 1, so c_i stands at position $i + 1$. Assume $|c_0| < 1/4$ and put

$$B = \frac{g_{21}}{g_{11}}, \qquad \mu_\infty = -\frac{2g_{12}}{g_{11}} = -\frac{2}{[c_j; c_{j-1}, \dots, c_0]}.$$

Here $B \in p\mathbb{Z}_p \setminus \{0\}$, since $[c_0; \dots, c_j]$ has norm $|c_0|_p > 1$.

These valuation statements follow by backwards evaluation. In particular, $g_{11}g_{21} \neq 0$ in both settings. The middle entry μ stands at an odd position in either case.

Proposition 3.5. *Let μ be uncorrected.*

(1) *In setting (E), assume $2c_0 \in \Sigma_p$ and $D = \Phi(\mu) \in \mathbb{Z}$. Then the square root $\xi \equiv c_0 \pmod p$ of D has the expansion*

$$\xi = [c_0; \overline{c_1, \dots, c_j, \mu, c_j, \dots, c_1, 2c_0}\,].$$

(2) *In setting (O), assume $D = 1/\Phi(\mu) \in \mathbb{Z}$, with $\Phi(\mu)$ defined and nonzero. Then a square root $\eta \in p\mathbb{Z}_p$ of D has the expansion*

$$\eta = [0; c_0, \overline{c_1, \dots, c_j, \mu, c_j, \dots, c_1, 2c_0}\,].$$

In either case, if $|\mu|_p > |c_i|_p$ for all $0 \leq i \leq j$, the minimal period is $2j + 2$.

Proof. The word starting at c_0 is admissible at the prescribed starting index. Reversal preserves the parity of the entries, and the closing entry $2c_0$ is allowed by $2c_0 \in \Sigma_p$ in (E) and $|2c_0| < 1/2$ in (O). By Lemma 3.3, this word is the expansion of its limit γ. Let γ_1 be the complete quotient immediately following c_0. The complete quotient at the closing entry is $2c_0 + 1/\gamma_1 = \gamma + c_0$. Thus (3.2) holds and $\gamma^2 = \Phi(\mu)$. In (E) we take $\xi = \gamma$. In (O), $|\gamma|_p = |c_0|_p > 1$, so $\eta = 1/\gamma \in p\mathbb{Z}_p$ has initial partial quotient 0 and the asserted expansion. The unique entry of largest p-adic norm proves minimality. □

For $p = 3$, the closing entry $2c_0$ in setting (E) is not a digit. We replace it using the identity

$$M(0)\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} M(1)M(\tfrac{1}{3})M(-1)M(-\tfrac{1}{3}) = M(-\tfrac{1}{3})M(1)M(\tfrac{2}{3}). \tag{3.5}$$

Proposition 3.6. *Let $p = 3$ and assume setting (E), with $c_0 = 1$, $j \geq 4$ and $(c_1, c_2, c_3, c_4) = (1/3, -1, -1/3, -1)$. Let μ be uncorrected and $D = \Phi(\mu) \in \mathbb{Z}$. Then the square root $\xi \equiv 1 \pmod 3$ of D has the expansion*

$$\xi = \left[1; \frac{1}{3}, -1, -\frac{1}{3}, \overline{-1, c_5, \dots, c_j, \mu, c_j, \dots, c_1, -1, -\frac{1}{3}, 1, \frac{2}{3}}\right].$$

If $|\mu|_3 > |c_i|_3$ for all $0 \leq i \leq j$, its minimal period is $2j + 2$.

Proof. The displayed word is admissible. In particular, the corrected entry $2/3$ is followed by -1. Let its limit be ξ, with complete quotients ξ_n. The periodic tail begins at index 4, so $\xi_{2j+6} = \xi_4$. Since $\xi = [1; 1/3, -1, -1/3, \xi_4]$, identity (3.5) gives

$$\xi_{2j+3} = [-1/3; 1, 2/3, \xi_4] = \frac{1}{\xi + 2}.$$

Consequently $\xi_{2j+2} = -1 + 1/\xi_{2j+3} = \xi + 1$, which proves (3.2). Lemma 3.4 yields $\xi^2 = D$. The periodic word has length $2j + 2$ and contains μ once, proving minimality under the stated norm condition. □

The value μ_∞ is the pole of Φ in (E) and of $1/\Phi$ in (O). The following deformation preserves integrality while making the middle entry small in the real absolute value and large in the p-adic one.

Proposition 3.7. *Assume setting (E) or (O), with $|\mu_\infty| < 1/2$. Suppose that $\mu_0 \in \mathbb{Z}[1/p]$ gives an integer $D_0 = \Phi(\mu_0)$ in (E), or $D_0 = 1/\Phi(\mu_0)$ in (O), with $\Phi(\mu_0)$ defined and nonzero in the latter case. Write $n/d = A$ in (E) and $n/d = B$ in (O), in lowest terms with $d > 0$. Let o be the order of p modulo d^2, with $o = 1$ if $d = 1$, and put*

$$D_t = \frac{n^2 + p^{to}(d^2 D_0 - n^2)}{d^2}, \qquad \mu_t = \mu_\infty + p^{-to}(\mu_0 - \mu_\infty), \qquad t \geq 1. \tag{3.6}$$

For all sufficiently large t, the D_t are distinct nonsquare integers, μ_t is uncorrected, and $|\mu_t|_p \to \infty$. Moreover, $\Phi(\mu_t) = D_t$ in (E) and $\Phi(\mu_t) = 1/D_t$ in (O).

Proof. In (E), write $g_{21} = dw$ and $g_{11} = nw$, with $w \in \mathbb{Z}[1/p]$. Since

$$\delta = w(ng_{22} - dg_{12}),$$

w is a unit of $\mathbb{Z}[1/p]$, and $d\mu_\infty = -2g_{22}/w \in \mathbb{Z}[1/p]$. The same argument in (O), after exchanging the rows of Γ, gives $g_{11} = dw$ and $d\mu_\infty \in \mathbb{Z}[1/p]$. Also $p \nmid d$, because $A \in \mathbb{Z}_p^\times$ and $B \in p\mathbb{Z}_p$.

The congruence $p^{to} \equiv 1 \pmod{d^2}$ makes D_t integral and gives

$$p^{to}\mu_t = \mu_0 + (p^{to} - 1)\mu_\infty \in \mathbb{Z}[1/p].$$

Identities (3.3)–(3.4) prove the claimed relations between D_t and μ_t. They also show that $C = d^2 D_0 - n^2 \neq 0$ and $\mu_0 \neq \mu_\infty$. Thus the D_t are distinct, $\mu_t \to \mu_\infty$ in $\mathbb{R}$, and $|\mu_t|_p \to \infty$. A possible value $D_t = 0$ in (O) is discarded.

If $D_t = y^2$ for an integer y, then $(dy - n)(dy + n) = Cp^{to}$. The two factors differ by $2n \neq 0$. Put $r = v_p(2n)$. Once $v_p(C) + to > 2r$, their valuations differ and the smaller one is r. The corresponding factor is therefore $\pm p^r$ times a divisor of the fixed prime-to-p part of C. There are only finitely many possibilities for that factor and hence for the other one. Since $|Cp^{to}| \to \infty$, only finitely many D_t are squares. □

3.3. **Infinite families with prescribed period length.**

3.3.1. *The case $p \geq 5$ and $h \equiv 2 \pmod 4$.* Fix $\varepsilon \in \{-1, 1\}$ and choose $r \geq 1$ with $p^r > 8$. When $j = 0$ and $c_0 = 1$, we have $\Phi(\mu) = 1 + 2/\mu$. With $\lambda = 2\varepsilon p^{-r}$, Proposition 3.5(1) gives

$$\sqrt{1 + \varepsilon p^r} = [1; \overline{\lambda, 2}\,]$$

for the root congruent to 1 modulo p. The period is two. For $\varepsilon = 1$, an integral square root $z > 0$ would be even, and the coprime positive odd factors $z - 1, z + 1$ of p^r would force $z = 2$ and $p^r = 3$. For $\varepsilon = -1$ the radicand is negative. The positive family is a special case of [4, Lemma 2], where Browkin attributes the sufficiency of the conditions to de Weger. The corresponding family of convergent periodic words also appears in [5, Example 4.16(a)].

For fixed $k \geq 1$, take the prefix $c_0 = 1$, $c_{2i-1} = \lambda$, $c_{2i} = 2$ for $1 \leq i \leq k$. The displayed expansion satisfies (3.2) for this prefix with $\mu_0 = \lambda$. Its entries from positions 1 to $4k+1$ form the required palindrome, and its complete quotient at position $4k+2$ is $\sqrt{1+\varepsilon p^r}+1$. Thus $D_0 = 1 + \varepsilon p^r$ is an initial integer for Proposition 3.7. As $r \to \infty$,

$$\Gamma = M(1)\Big(M(\lambda)M(2)\Big)^k \longrightarrow \begin{pmatrix} 2k+1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Hence $A \to 2k+1$ and $\mu_\infty \to 0$. Choose r large enough that $|\mu_\infty| < 1/2$ and $D_0 - A^2$ has sign ε. Then $D_t = A^2 + p^{to}(D_0 - A^2)$ has the same sign for all large t. Propositions 3.7 and 3.5(1) give infinitely many nonsquare integers of each sign with minimal period $4k+2$.

3.3.2. *The case $h \equiv 0 \pmod 4$.* Let p be any odd prime. Fix $e \geq 1$ with $p^e > 4$, put $x = p^{-e}$ and $d = p^e + 1$, and let o be the order of p modulo d^2.

Proposition 3.8. *For all sufficiently large integers u, put*

$$D_u = \frac{p^{2e}(1-p^{uo})}{(p^e+1)^2}, \qquad \mu_u = -\frac{2(p^{uo}+p^e)}{(p^e+1)p^{uo}}.$$

Then D_u is a negative integer, μ_u is uncorrected, and a square root of D_u has the expansion

$$[0; x, \overline{1, \mu_u, 1, 2x}\,]$$

with minimal period four.

Proof. The congruence $p^{uo} \equiv 1 \pmod{d^2}$ makes D_u integral. Since $p^{uo} + p^e \equiv 0 \pmod d$, we also have $\mu_u \in \mathbb{Z}[1/p]$. As $u \to \infty$,

$$\mu_u \longrightarrow -\frac{2}{p^e+1}, \qquad |\mu_u|_p = p^{uo-e} \longrightarrow \infty,$$

so μ_u is uncorrected for large u. In setting (O), take $j = 1$ and $(c_0, c_1) = (x, 1)$. Then $\Gamma = \left(\begin{smallmatrix} 1+x & x \\ 1 & 1 \end{smallmatrix}\right)$, and direct substitution gives $1/\Phi(\mu_u) = D_u$. Proposition 3.5(2) gives the expansion and its minimal period. □

Murru, Romeo and Santilli gave a family of period four in [15, Theorem 18 and Corollary 19]. Their displayed word is admissible for $p \geq 5$. At $p = 3$ its odd entry $-1 + 3^{1-t}$, $t \geq 2$, is corrected and must be followed by 1. The next entry in their word is -1. Taking $p^e > 4$ in Proposition 3.8 gives a family at this prime as well.

Proposition 3.9. *For every $m, e \geq 1$ with $p^e > 4$, infinitely many negative integers D with $v_p(D) = 2e$ have a square root whose Browkin II expansion has least preperiod two and least period $4m$.*

Proof. The case $m = 1$ is Proposition 3.8. Let $m \geq 2$ and let $\gamma_u = 1/\sqrt{D_u}$, with the root chosen there. Its expansion from index 1 has entries $a_1 = x$, $a_n = 1$ for even n, $a_n = \mu_u$ for $n \equiv 3 \pmod 4$, and $a_n = 2x$ for $n \equiv 1 \pmod 4$, $n \geq 5$. Use $(a_1, \ldots, a_{2m})$ as the prefix in setting (O), so $j = 2m-1$.

For $1 \leq i \leq 2m-1$, the entries a_{2m+1+i} and a_{2m+1-i} coincide. If i is odd both positions are even, and if i is even they are congruent modulo four and exceed one. The complete quotient at position $4m+1$ equals $\gamma_u + x$. Thus (3.2) holds with middle entry $a_{2m+1} \in \{\mu_u, 2x\}$, and $D_0 = D_u$ is an initial integer for Proposition 3.7.

Put $r_i = [a_i; a_{i-1}, \ldots, a_1]$, so $\mu_\infty = -2/r_{2m}$. Replacing μ_u by its real limit $-2x/(1+x)$ gives a sequence of period four,

$$r_1^\infty = x, \quad r_2^\infty = \frac{1+x}{x}, \quad r_3^\infty = -\frac{x}{1+x}, \quad r_4^\infty = -\frac{1}{x}.$$

None of these values is zero, and $|2/r_{2m}^{\infty}| \le 2x < 1/2$. Each r_i depends continuously on μ_u near its limit, so $|\mu_\infty| < 1/2$ for sufficiently large u. Fix such a u. Propositions 3.7 and 3.5(2) give infinitely many expansions of minimal period $2j+2 = 4m$. In (3.6) we have $D_t = B^2 + p^{to}(D_u - B^2) < 0$, since $D_u < 0$. The first two digits $0, x$ give the root valuation e, and $x \neq 2x$ gives least preperiod two. The same valuation and preperiod follow from the displayed expansion in Proposition 3.8 when $m = 1$. □

3.3.3. *The case $p = 3$ and $h = 6$.*

Proposition 3.10. *Let $p = 3$, $k \ge 1$, $q = (-3)^k$ and $D_k = (1 - 9q)/4$. Then D_k is a nonsquare integer, and its square root $\xi \equiv 1 \pmod 3$ has the expansion*

$$\xi = [1; \overline{1/3, -1, 1/q, 1, -1/3, -1}\,]$$

with minimal period six.

Proof. Since $q \equiv 1 \pmod 4$, $D_k \in \mathbb{Z}$. It is negative for even k. For odd k, the equation $D_k = y^2$ would give $(2y-1)(2y+1) = 3^{k+2}$ with coprime positive factors, which is impossible. The displayed word is admissible, so it is the expansion of its limit $\xi \equiv 1 \pmod 3$. Its complete quotient at position 6 is $\xi - 2$, and direct substitution in

$$\xi = [1; 1/3, -1, 1/q, 1, -1/3, \xi - 2]$$

gives $4\xi^2 = 1 - 9q$. For $k \ge 2$, the entry $1/q$ has uniquely largest 3-adic norm. For $k = 1$, the minimal period is even, divides six, and is not two because $a_1 = 1/3 \neq -1/3 = a_3$. □

3.3.4. *The case $p = 3$, $h \equiv 2 \pmod 4$ and $h \ge 10$.* For a prefix $(1; c_1, \dots, c_j)$ in setting (E), put $K_i = K(c_1, \dots, c_i)$ and $R_i = K_i/K_{i-1} = [c_i; c_{i-1}, \dots, c_1]$. Thus $g_{21} = K_j$, $g_{22} = K_{j-1}$ and $\mu_\infty = -2/R_j$. By the determinant argument in Proposition 3.7, the denominator of A in lowest terms is the prime-to-3 part of K_j.

Lemma 3.11. *For every even $j \ge 4$, the prefix*

$$(1; 1/3, -1, -1/3, -1, c_5, \dots, c_j)$$

can be chosen in setting (E) *with all odd entries uncorrected, $K_j > 0$, $R_j \ge 5$, and the prime-to-3 part d_j of K_j a positive power of 5 or 7.*

Proof. For $j = 4$ the continuants are $1/3, 2/3, 1/9, 5/9$, so $d_4 = R_4 = 5$. Suppose the prefix has been chosen through j. Let q be the prime in $\{5, 7\}$ that does not divide d_j. We seek positive integers a, σ for which $H = q^a/3^\sigma$ satisfies

$$H \equiv K_{j-1} \pmod{d_j\mathbb{Z}[1/3]}, \qquad K_j < H < 5K_j/4.$$

The determinant identity for consecutive continuants shows that K_{j-1} is a unit modulo d_j. The orders of 3 modulo 5 and 7 are 4 and 6, and $v_5(3^4 - 1) = v_7(3^6 - 1) = 1$. Hence 3 generates the units modulo every power of either prime. Put $o = \varphi(d_j)$ and choose σ_0 with $3^{-\sigma_0} \equiv K_{j-1} \pmod{d_j\mathbb{Z}[1/3]}$. The congruence for H holds whenever $o \mid a$ and $\sigma \equiv \sigma_0 \pmod o$. Since $\log 3/\log q$ is irrational, the numbers $\sigma \log 3$ for σ in this progression are dense modulo $o \log q$, even after deletion of any finite initial segment. We can therefore satisfy the inequalities as well, with σ arbitrarily large.

Set $y = H/K_j - 1$, $c_{j+1} = y - 1/R_j$ and $c_{j+2} = 1$. Then $0 < y < 1/4$. Since K_j is d_j times a unit of $\mathbb{Z}[1/3]$, the congruence for H gives

$$c_{j+1} = \frac{H - K_j - K_{j-1}}{K_j} \in \mathbb{Z}[1/3].$$

For large σ this digit has negative 3-adic valuation. Its real absolute value is less than $1/4$, so it is uncorrected. The recurrences give $K_{j+1} = yK_j$, $K_{j+2} = H$ and $R_{j+2} = 1 + 1/y > 5$. Thus $d_{j+2} = q^a$, which completes the induction. □

Fix $\varepsilon \in \{-1, 1\}$ and take a prefix from Lemma 3.11, with $A = n/d$ in lowest terms. As 3 generates the units modulo d^2, there are arbitrarily large r with $3^r \equiv -\varepsilon n^2 \pmod{d^2}$. Put

$$D_0 = \frac{n^2 + \varepsilon 3^r}{d^2}.$$

Write $g_{11} = nw$, $g_{21} = dw$, where w is a unit of $\mathbb{Z}[1/3]$, as in Proposition 3.7. Solving $\Phi(\mu_0) = D_0$ gives

$$\mu_0 = \frac{2(D_0 g_{21} g_{22} - g_{11} g_{12})}{g_{11}^2 - D_0 g_{21}^2} = \frac{2(D_0 d g_{22} - n g_{12})}{-\varepsilon w 3^r} \in \mathbb{Z}[1/3].$$

Indeed $g_{21}\mu_0 + 2g_{22} = 2\delta g_{11}/(g_{11}^2 - D_0 g_{21}^2) \neq 0$. Now $|\mu_\infty| = 2/R_j \leq 2/5$. By Propositions 3.7 and 3.6, the integers $D_t = (n^2 + \varepsilon 3^{r+to})/d^2$ are nonsquares of sign ε and give minimal period $2j + 2$ for all sufficiently large t, where o is the order of 3 modulo d^2.

The displayed preperiods are minimal. In settings (E) and (O), extension one place to the left would identify c_0 with $2c_0$. In Proposition 3.6, the entries at positions 3 and $h + 3$ are $-1/3$ and $2/3$, so the minimal preperiod is four. For period six, the initial entry 1 differs from the last entry -1 of the period.

3.4. **Period two at $p = 3$.**

Proposition 3.12. *Let $\rho \in \mathbb{Q}_3$ satisfy $\rho^2 = 19$ and $\rho \equiv 1 \pmod 3$. The Browkin II expansion of 3ρ is*

$$3\rho = \left[0; -\frac{2}{3}, 1, \frac{1}{3}, -1, \frac{4}{9}, 1, \frac{2}{3}, -1, -\frac{7}{9}, \overline{1, \frac{2}{9}}\right]$$

with minimal preperiod ten and minimal period two.

Proof. The admissible periodic tail $z = \overline{[1, 2/9]}$, started at an even index, satisfies

$$z = 1 + \frac{1}{2/9 + 1/z}, \qquad 2z^2 - 2z - 9 = 0, \qquad z \equiv 1 \pmod 3.$$

Thus $z = (1 + \rho)/2$. The finite word at indices $1, \ldots, 9$ in the displayed expansion is admissible. Its corrected entries $-2/3$, $2/3$ and $-7/9$ are followed respectively by 1, -1 and $z \equiv 1 \pmod 3$. Lemma 3.3(1) therefore realizes this prefix followed by z. Its value has norm greater than one, so taking its reciprocal supplies the initial partial quotient zero. Multiplication of the ten prefix matrices gives

$$[0; -2/3, 1, 1/3, -1, 4/9, 1, 2/3, -1, -7/9, z] = \frac{3(1789z - 657)}{25z + 882} = 6z - 3 = 3\rho,$$

where the second equality uses $2z^2 - 2z - 9 = 0$. The period has length two, and $a_9 = -7/9 \neq 2/9 = a_{11}$ proves minimality of the preperiod. □

This completes the proof of Theorem 3.1. The following results give restrictions for $(p, h) = (3, 2)$ and distinguish the fields in the other cases.

3.4.1. *Restrictions on the exceptional period.* Let L denote the minimal preperiod and let $F_0 = 0$, $F_1 = 1$, $F_{i+2} = F_{i+1} + F_i$.

Proposition 3.13. *Suppose that a square root of a nonsquare integer D has period two for Browkin II at $p = 3$. Then $D > 0$, L is even, and, after changing the sign of the root if necessary, its period is $(1, x)$, where*

$$x = \frac{2u}{3^k}, \qquad D = 3^{2e} D_*, \qquad D_* = u(u + 2 \cdot 3^k), \qquad e \geq 0, \quad 3 \nmid u, \quad 0 < u < 3^k/4.$$

Moreover,

$$3^e D_* \leq 3^k F_{L+2}^2.$$

Proof. For a complete quotient z write z' for its conjugate. Call an even state regular when $v_3(z) = 0 < v_3(z')$, and an odd state regular when $v_3(z) < 0 = v_3(z')$. To see that the next state is regular, observe that at an even step $z' - a$ is a unit, and at an odd step $v_3(z' - a) = v_3(a) < 0$. For a unit initial square root, $z_1' = 1/(-z_0 - a_0)$ is a unit, since $z_0 \equiv a_0 = \pm 1 \pmod 3$. If $v_3(z_0) > 0$, then $a_0 = 0$ and $z_1' = -z_1$, so $v_3(z_1' - a_1) = v_3(-2a_1 - (z_1 - a_1)) = v_3(a_1) < 0$. Thus the first regular state occurs at index 1 for a unit square root and at index 2 otherwise. Every later state is regular, including both states on the cycle.

Negate the input if required to make the even periodic digit 1. Write $\alpha = 1 + 1/\beta$ and $\beta = x + 1/\alpha$ for the even and odd cycle states. The only regular predecessor of β is α, because its even digit $b = \pm 1$ must satisfy $b \equiv -1/\beta' \equiv 1 \pmod 3$. A regular odd predecessor of α has the form $y = a + 1/\alpha$. Then $a - x = y' - \beta' \in \mathbb{Z}[1/3] \cap \mathbb{Z}_3 = \mathbb{Z}$, and $|a|, |x| < 1$. Since $\beta' \equiv -1 \pmod 3$, regularity excludes $a - x = 1$. The only possible external digit is therefore $a = x - 1$, which requires $x > 0$. As a corrected positive digit must be followed by -1, this x is uncorrected and $0 < x < 1/2$.

Direct entry from the nonregular initial part is impossible. If the first regular state is $z_1 = \beta$, then $1/\beta = \alpha - 1$ has trace -1 since $\alpha^2 - \alpha - 1/x = 0$. Trace zero for $z_0 = a_0 + 1/\beta$ would require $a_0 = 1/2$. If the first regular state is $z_2 = \alpha$, then $1/\alpha$ has trace $-x$, so $z_1 = 1/z_0 = a_1 + 1/\alpha$ requires $a_1 = x/2$ and $D = 4/[x(x+4)]$. Writing $x = m/T$ in lowest terms with $T = 3^k$, $k \geq 1$, integrality would force $m(m+4T) \mid 4$, since $3 \nmid m$. But $|m| < T$ gives $|m + 4T| > 3T > 4$. This argument applies to both signs of x. Thus first entry is at the even state α from the external regular predecessor, so L is even and $x > 0$. The even cycle state satisfies $\alpha^2 - \alpha - 1/x = 0$. Its discriminant $1 + 4/x$ is positive. As the prefix matrix is invertible over $\mathbb{Q}$, we have $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\alpha)$ and hence $D > 0$.

Put $R = \mathbb{Z}[1/3]$. The form $Q(X, Y) = mX^2 - mXY - TY^2$ is primitive over R. For $\Gamma = M(a_0) \cdots M(a_{L-1})$, the form $Q \circ \Gamma^{-1}$ vanishes at $(\sqrt{D}, 1)$ and is therefore $c(X^2 - DY^2)$. Unimodularity over R preserves the ideal generated by the coefficients, giving $c \in R^\times$. The discriminants give $4c^2 D = m(m+4T)$, a 3-adic unit, whence $c = \pm 3^{-e}$ and $e = v_3(D)/2 \geq 0$. Thus $4D = 3^{2e} m(m+4T)$, which gives $m \equiv 0 \pmod 2$. Writing $m = 2u$ yields the asserted formula for D.

Every initial digit has real absolute value at most one, including the corrected odd digits. Each inverse step $(v, w) \mapsto (w, v - a_i w)$ has its two absolute coordinates bounded componentwise by applying $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ to $(|v|, |w|)$. Hence the sum of the absolute coordinates of the second column of Γ^{-1} is at most F_{L+2}. The matrix of Q has coefficients bounded by T. Evaluating on that column gives $3^e D_* = |cD| \leq T F_{L+2}^2$. □

Proposition 3.14. *With the notation of Proposition 3.13, $x > 1/9$. If $k \geq 5$, then also $x < 5/18$.*

Proof. Represent a regular state by its integral form $AZ^2 - 2BZ + C$ with $B^2 - AC = D_*$. At the even and odd cycle states these triples are $(2u, u, -T)$ and $(T, u, -2u)$, respectively. They may be multiplied by -1. Under a backward step with digit a the new triple is

$$(C, B + Ca, A + 2Ba + Ca^2). \tag{3.7}$$

Since $A^2(z - z')^2 = 4d$ is a 3-adic unit, the valuations of z, z' determine those of A and $C = Azz'$. At an odd target, $3 \mid A$ and both B and C are units. Its sole regular predecessor has even digit $b = \pm 1$ congruent to $B/C \pmod 3$, since the new constant coefficient must vanish modulo 3. At an even target, A, B are units, $C = 3^v c$ with $v > 0$ and $3 \nmid c$, and $z \equiv q \pmod 3$, where $q \in \{-1, 1\}$ represents $2B/A$. Any regular predecessor requires $a \equiv -2B/C \pmod{\mathbb{Z}_3}$ by $1/z + 1/z' = 2B/C$ and $a + 1/z' \in \mathbb{Z}_3$. Thus $a = r/3^v$, where $r \equiv -2B/c \pmod{3^v}$. Keep the candidates with $0 < |a| < 1/2$ or $1/2 < |a| < 1$ and

$\operatorname{sgn} a = -q$, and require the last entry in (3.7) to be a 3-adic unit. They also suffice because z has digit q, its inverse is a unit, and the odd correction rule is exactly the sign test above. The new coefficients are integers, since Ca and $a(2B + Ca)$ are integral. For an odd predecessor $y = a + 1/z$ we have $v_3(y) = -v$ and the new constant coefficient is Cyy'. It is a unit precisely when y' is a unit. For an even predecessor the new even root is a unit and the congruence for b gives positive valuation for its conjugate.

There are two possible initial boundaries. At an odd state reached as z_1 from a unit square root, trace zero forces $a_0 = -B/C = \pm 1$. The coefficient of Z^2 in the resulting form is C, so the discriminant calculation in Proposition 3.13 gives $|B| = |C| = 1$. At an even state reached as z_2 from a square root with $e > 0$, trace zero similarly forces $a_1 = -B/C$. Taking a reciprocal interchanges the two diagonal coefficients of $(C, 0, -D_*/C)$. Comparing them gives $|C| = 3^e D_*$. In particular the prime-to-3 part of $|C|$ is D_*.

We give the complete lists needed in the stated ranges. Set $t = T/9$, $w = 9x = 2u/t$. If $x < 1/9$, then $k \geq 3$. For the upper range we assume $k \geq 5$. Besides the two cycle states, the backward path begins by the four digits $x - 1, -1, -1/3, 1$. The following rows are consecutive triples after these digits.

i	A	B	C
1	$-9t$	$9t - u$	$-9t + 4u$
2	$-9t + 4u$	$18t - 5u$	$-6(6t - u)$
3	$-6(6t - u)$	$30t - 7u$	$-25t + 8u$
4	$-25t + 8u$	$5t + u$	$-t$

At row 2 the alternative $2/3$ gives new constant coefficient $-t$ and is excluded. At row 4 one has $q = 1$ and $-2B/C = w + 10$. The candidates are $a = w - j$, $j \in \mathbb{Z}$, with $-1 < w - j < 1/2$. The new constant coefficient is $-(j + 5)^2 t + 2(j + 14)u$, which is a unit exactly when $j \not\equiv 1 \pmod 3$.

For $0 < w < 1/2$ only $j = 0$ survives. The path continues by $w, -1$, giving rows $(-t, 5t - u, -25t + 28u)$ and $(-25t + 28u, 30t - 29u, -6(6t - 5u))$. Here $q = -1$ and the uncorrected candidate $1/3$ gives new constant $-3(3t - 4u)$. The corrected candidate $-2/3$ has the wrong sign. For $1/2 < w < 1$ no candidate survives at row 4. At the odd rows $1, 3, 5$ the displayed $|B|$ exceeds one, since $0 < u < t/2$ (at row 5, $u < t/4$). The odd cycle state has $|C| = 2u > 1$. At even rows $2, 4, 6$ the prime-to-3 parts of $|C|$ are respectively $2(6t - u), 1, 2(6t - 5u)$, all strictly less than $D_* \geq 2T$. The even cycle state likewise has prime-to-3 part one. Thus there is no initial boundary. The endpoints $x = 1/18$ and $x = 1/9$ are excluded by the reduced even numerator of x.

For $5/2 < w < 7/2$ only $j = 3$ survives at row 4. There is no candidate for $7/2 < w < 4$, and only $j = 5$ survives for $4 < w < 9/2$. The internal thresholds are impossible in reduced denominator 3^k for $k \geq 5$. The remaining backward digits, starting at row 4, and the corresponding last coefficients are

j	digits	successive constant coefficients
3	$(w - 3, -1, 4/9, -1)$	$-2(32t - 17u),\ -9(9t - 4u),\ -2(8t - 5u),\ -169t + 84u$
5	$(w - 5, 1, -5/9, 1)$	$-2(50t - 19u),\ -9(9t - 4u),\ -25t + 8u,\ -2(98t - 39u)$

For verification, at row 6 in both branches the uncorrected candidate is $4/9$. In the first branch $-5/9$ has the wrong sign. In the second branch $4/9$ gives the nonunit $-2(98t - 39u)$ and $-5/9$ is legal. At row 8 the only sign-compatible candidates are respectively $1/3, -1/3$, both yielding $-t/9$, a nonunit because $27 \mid t$. These modular tests follow directly from (3.7).

Inspection of the displayed constant coefficients gives $|C| < 42T$ throughout, as $t = T/9$ and $u < T/4$. The same bound holds for $|A|$ since a new leading coefficient is the old constant coefficient. But $D_* > 5T^2/18 > 42T + 1$ for $T \geq 243$. This excludes the

boundary $|C| = 3^e D_*$. It also excludes the unit boundary $|C| = |B| = 1$, which would give $|A| = D_* - 1$. The endpoint $5/18$ has even reduced denominator. This proves the claim. □

Corollary 3.15. *At $p = 3$ only finitely many nonsquare integer radicands with period two have preperiod bounded by any prescribed integer. More precisely, every such radicand satisfies*

$$3^{e+k} < 9F_{L+2}^2, \qquad D < 9F_{L+2}^4.$$

Proof. Write $T = 3^k$. The lower bound for x gives $u > T/18$ and $D_* > 2Tu > T^2/9$. Apply Proposition 3.13. This bounds e and k in terms of L. Multiplying the height bound by 3^e gives $D \le 3^e T F_{L+2}^2 < 9F_{L+2}^4$. □

Proposition 3.16. *For $k \le 6$ in Proposition 3.13, the only radicands are* 171 *and* 13851*, both with $x = 2/9$. Their minimal preperiods are* 10 *and* 40*, respectively. In particular, $1/9 < x < 5/18$ for all k, and any further radicand is at least* 548512*.*

Computer-assisted proof. For each $k = 1, \dots, 6$ and each u with $0 < 4u < 3^k$ and $3 \nmid u$, put $T = 3^k$ and $D_* = u(u + 2T)$. Discard D_* if it is a square. Start a breadth-first search with the even and odd cycle triples $(2u, u, -T)$ and $(T, u, -2u)$, both at distance zero. Store each triple together with its parity, changing its common sign if necessary to make $A > 0$. For fixed D_*, two proportional triples have proportionality factor ± 1, and the parity distinguishes the root by its valuation.

For odd m write $\langle v \rangle_m$ for the integer in $(-m/2, m/2)$ representing v modulo m. At each vertex (A, B, C) form the following list of predecessor digits r/m.

(1) At an odd vertex take $m = 1$ and $r = \langle BC \rangle_3$.
(2) At an even vertex put $m = 3^{v_3(C)}$, $c = C/m$ and $q = \langle 2BA \rangle_3$. Take $r_0 = \langle -2Bc^{-1} \rangle_m$. Use $r = r_0$ and also $r = r_0 - m \operatorname{sgn} r_0$ if this second numerator satisfies $rq < 0$.

For each candidate compute

$$B_1 = B + (C/m)r, \qquad C_1 = (B_1^2 - D_*)/C.$$

These integers give the triple (C, B_1, C_1) in (3.7). At an even vertex discard the candidate if $3 \mid C_1$. Normalize the remaining triples and add each unseen vertex of the opposite parity to the queue at distance one greater than the current distance. Continue until the queue is empty.

Test each vertex for an initial square root. At an odd vertex the condition $|B| = |C| = 1$ is sufficient as well as necessary, since $a_0 = -B/C = \pm 1$ gives a square root of D_*. At an even vertex use m, c, q as above. When $|c| = D_*$ and $c \mid B$, put $r = -B/c$. A boundary occurs precisely when $0 < |r| < m$ and either $2|r| < m$ or $rq < 0$. Then $a_1 = r/m = -B/C$ is an admissible odd digit before the given state z, and $[0; a_1, z]^2 = m^2 d$. The forward algorithm determines the path to the cycle uniquely. A boundary at distance n therefore gives minimal preperiod $n + 1$ at an odd vertex and $n + 2$ at an even one.

The resulting counts, summed over u for each k, are

k	2	3	4	5	6
parameters	2	4	14	40	122
regular states	94	926	1042	1732	14342
maximum distance	40	206	116	144	624

There are no parameters at $k = 1$. The only boundaries occur for $(k, u) = (2, 1)$, for which the graph has 88 vertices. Both are even vertices. The normalized triples are $(25, 38, 57)$ at distance 8 and $(254, -361, 513)$ at distance 38. They have $m = 3$ and $m = 27$, respectively. As $D_* = 19$, this gives 171 and 13851 with the stated preperiods. The range for x follows

from Proposition 3.14 and the finite enumeration. For every further radicand we have $k \geq 7$ and $u > 3^k/18$, whence $u \geq 122$ and $D \geq 122(122 + 2 \cdot 2187) = 548512$. □

The necessary conditions for period two do not by themselves guarantee that period. For instance, the root ρ of Proposition 3.12 has the expansion

$$\rho = [1; 1/9, -1, 1/3, -1, -1/3, \overline{-1, -1/3, 1, 2/3}].$$

The word satisfies the truncation rules in Lemma 3.3, and multiplication of its prefix and period matrices gives a square root of 19 congruent to 1 modulo 3. Its least preperiod is six and its least period is four.

3.5. **Real and imaginary quadratic fields.**

Theorem 3.17. *Let p be an odd prime and h a positive even integer, with $(p, h) \neq (3, 2)$. For each prescribed sign there are infinitely many nonsquare integers D of that sign whose square roots in $\mathbb{Q}_p$ have minimal Browkin II period h. For either sign the quadratic fields $\mathbb{Q}(\sqrt{D})$ can be chosen pairwise distinct.*

Proof. Fix $\varepsilon \in \{1, -1\}$. First suppose $4 \mid h$. Choose $r \geq 1$ with $y = p^r \geq 5$, and put

$$P = y^2, \qquad d = y^2 - y + 1, \qquad x = d/P - 1 = -(y-1)/y^2.$$

Then $0 < |x| < 1/5$, $|x|_p = P$ and $|2x| < 1/2$. As d is odd and $p^{3r} = (y+1)d - 1$, the binomial theorem gives $p^{3rd} \equiv -1 \pmod{d^2}$. Thus there are arbitrarily large N with $p^N \equiv -\varepsilon \pmod{d^2}$. Put

$$D_N = \frac{P^2(1 + \varepsilon p^N)}{d^2}, \qquad \mu_N = -2 + \frac{2P}{d}(1 + \varepsilon p^{-N}).$$

Then $D_N \in \mathbb{Z}$ and $\mu_N \in \mathbb{Z}[1/p]$, since $d \mid p^N + \varepsilon$. For $N > 2r$ we have $|\mu_N|_p = p^{N-2r}$, while $\mu_N \to -2x/(1+x)$ in $\mathbb{R}$. The limit has absolute value less than $1/2$, so μ_N is uncorrected for large N.

For the prefix $(x, 1)$ in setting (O), put $B = 1/(1+x) = P/d$. Identity (3.4) gives

$$\frac{1}{\Phi(\mu)} = B^2 + \frac{2B^3}{\mu + 2x/(1+x)}.$$

In particular $1/\Phi(\mu_N) = D_N$, with $\Phi(\mu_N)$ finite and nonzero for large N. Proposition 3.5 gives a square root $[0; x, \overline{1, \mu_N, 1, 2x}]$ of D_N with minimal period four. A negative D_N is nonsquare. For $\varepsilon = 1$, if $1 + p^N$ were a square, its square root z would be an even integer and the coprime positive factors $(z-1)(z+1) = p^N$ would give $p^N = 3$. Thus D_N is also nonsquare in this case.

For $h = 4m$, $m \geq 2$, take the first $2m$ digits after the initial zero as in the proof of Proposition 3.9. The same reflection gives the palindrome with seed D_N, and the reversed continuant ratios have the same four nonzero limits $x, (1+x)/x, -x/(1+x), -1/x$. Here $|x| < 1/5$ also gives $|x/(1+x)| < 1/4$, so $|\mu_\infty| < 1/2$ for large N. Moreover, $g_{11} = \prod_{i=1}^{2m} r_i$ has nonzero limit and g_{21} is a continuant in digits with finite limits. Thus $B' = g_{21}/g_{11}$ stays bounded. Fix N sufficiently large that $D_N - (B')^2$ has sign ε. Equation (3.6) and Proposition 3.5(2) now give infinitely many radicands of this sign with minimal period $4m$.

For $h \equiv 2 \pmod 4$ the preceding constructions already give both signs. At $p = 3$, $h = 6$, they correspond to the two parities of k in $(1 - 9(-3)^k)/4$.

Finally, every constructed family has the form $D = (n^2 + Cp^s)/d^2$ for fixed nonzero integers n, C, d and infinitely many distinct positive exponents s. Fix a squarefree integer f of the chosen sign. If $D = fz^2$, choose $j \in \{0, 1, 2\}$ with $s \equiv j \pmod 3$ and put

$X = p^{(s-j)/3}$, $A = Cp^j$, $H = fd^2$. Here $z \in \mathbb{Z}$, since D is an integer and f is its squarefree part. Thus $Hz^2 = AX^3 + n^2$, and the integers $(U, V) = (HAX, H^2Az)$ satisfy

$$V^2 = U^3 + H^3A^2n^2.$$

For fixed f and j the constant term is a nonzero integer, so the cubic is nonsingular. By Siegel's theorem [30, Corollary IX.3.2.1] the curve has only finitely many integral points. Distinct s in the same residue class give distinct $U = HAp^{(s-j)/3}$. Thus only finitely many radicands in the family have squarefree part f. □

4. Periodicity and approximation for quadratic irrationals

4.1. **Wang and Deng's fourth algorithm at $p = 5$.** Wang and Deng proved eventual periodicity for their fourth and fifth algorithms at $p = 2, 3$ and conjectured it at $p = 5$ [31, Section 3.3]. We prove their conjecture for the fourth algorithm and give a sharp bound for the denominators of its complete quotients.

A quadratic irrational in $\mathbb{Q}_5$ can be written as

$$\alpha = \frac{P + \sqrt{D}}{Q}, \qquad P, Q, D \in \mathbb{Z}, \quad Q \neq 0, \quad Q \mid D - P^2,$$

with D nonsquare and $\sqrt{D} \in \mathbb{Z}_5$. Indeed, after clearing denominators and scaling the radical, the substitution $(P, Q, \sqrt{D}) \mapsto (PQ, Q^2, Q\sqrt{D})$ ensures the divisibility. If $a \in \mathbb{Z}[1/5]$ and $\alpha - a \in \mathbb{Z}_5$, then the next complete quotient has integral coordinates

$$P_1 = aQ - P, \qquad Q_1 = \frac{D - P_1^2}{Q}, \qquad \frac{1}{\alpha - a} = \frac{P_1 + \sqrt{D}}{Q_1}. \tag{4.1}$$

To see this, $aQ = P + \sqrt{D} - Q(\alpha - a)$ lies in both $\mathbb{Z}[1/5]$ and $\mathbb{Z}_5$, and hence is integral. Expanding Q_1 gives membership in $\mathbb{Z}[1/5]$, while $Q_1 = (\alpha - a)(\sqrt{D} + P_1)$ gives membership in $\mathbb{Z}_5$. Nonsquareness excludes $Q_1 = 0$, and $Q_1 \mid D - P_1^2$ follows from $D - P_1^2 = QQ_1$.

For a quadratic irrational $\alpha = (P + \sqrt{D})/Q \in \mathbb{Q}_5$, Wang and Deng [31, Section 3] choose $\bar{s}(\alpha)$ from $s(\alpha) + 5\mathbb{Z}$ and $\bar{t}(\alpha)$ from $t(\alpha) + \mathbb{Z}$, in each case closest to the half-trace P/Q. Fix a deterministic rule in case of a tie. Thus

$$\begin{aligned} &\alpha - \bar{s}(\alpha) \in 5\mathbb{Z}_5, && |P/Q - \bar{s}(\alpha)| \leq 5/2, \\ &\alpha - \bar{t}(\alpha) \in \mathbb{Z}_5, && |P/Q - \bar{t}(\alpha)| \leq 1/2. \end{aligned} \tag{4.2}$$

Algorithm 4 starts with $b_0 = \bar{s}(\alpha_0)$ and then uses

$$b_n = \begin{cases} \bar{s}(\alpha_n), & |\alpha_n|_5 = 1, \\ \bar{t}(\alpha_n), & |\alpha_n|_5 > 1, \end{cases} \quad (n \geq 1), \qquad \alpha_{n+1} = \frac{1}{\alpha_n - b_n} \quad (n \geq 0).$$

After the first step $|\alpha_n|_5 \geq 1$. Every $\bar{s}$-step is followed by a $\bar{t}$-step.

Theorem 4.1. *Every quadratic irrational in $\mathbb{Q}_5$ has an eventually periodic expansion under Wang and Deng's Algorithm 4. In the integral normalization* (4.1)*, put $d = |D|$ and $H = \max\{|Q_0|, |Q_1|, 4d + 1\}$. Then*

$$|Q_n| \leq H \quad (n \geq 0), \qquad |P_n| \leq \sqrt{d + H^2} \quad (n \geq 1).$$

For all sufficiently large n, we have $|Q_n| \leq 4d + 1$. Equality in this last bound occurs on a periodic orbit for infinitely many d.

Proof. At a $\bar{t}$-index $n \geq 1$, write $M = |Q_n|$, $A = |P_{n+1}|$ and $N = |Q_{n+1}|$. Since $|\alpha_n|_5 > 1$ and $P_n, \sqrt{D}$ are 5-adically integral, $5 \mid Q_n$. In particular $M \geq 5$. From the recurrence and the nearest-integer rule,

$$2A \leq M, \qquad MN = |A^2 - D|, \qquad N \leq M/4 + d/M.$$

If the next index is a $\bar{t}$-index, the next return has denominator of absolute value N. Otherwise α_{n+1} is a unit. Its $\bar{s}$-coset is a nonzero integer class modulo five. Put $B = |P_{n+2}|$ and $R = |Q_{n+2}|$. We have $NR = |B^2 - D|$ and $B \le 5N/2$.

Suppose first that $M > 2d$. Then $N \le M/4 + d/M < M$. Since $MN > d$ and $D - A^2 \le d$, we have $A^2 - D = MN$. It follows that

$$M(2N - A) = -A(M - 2A) - 2D \le 2d < M.$$

Thus $2N \le A$ by integrality. Set $x = P_{n+1}/Q_{n+1}$, so $|x| = A/N \ge 2$. The $\bar{s}$-coset contains an integer k with the sign of x and $1 \le |k| \le 4$. Hence $|x - k| \le |x|$, strictly if $|x| > 2$. The choice of the nearest representative gives $B \le A$, strictly if $2N < A$. Since $A^2 - D > d$, it follows that $|B^2 - D| \le A^2 - D$, with strict inequality when $B < A$. In particular $R \le M$. Equality can only occur if $2N = A$, in which case $A(M - 2A) = -2D = 2d$. Both factors are positive integers, and $2u + v \le 2uv + 1$ for $u, v \ge 1$. Taking $u = A$ and $v = M - 2A$ yields $M \le 4d + 1$. Thus every return to a $\bar{t}$-index decreases the denominator strictly when $M > 4d + 1$.

Suppose now that $5 \le M \le 2d$. Then $d \ge 4$, since neither 3 nor -3 is a square modulo five. By convexity on $[2, 2d]$, $N \le M/4 + d/M \le (d + 1)/2$. If $N = 1$, the half-trace at the intermediate step is an integer, so $B \le 2$ and $R \le d + 4 \le 4d + 1$. If $N \ge 2$, then

$$R \le \frac{25N}{4} + \frac{d}{N} \le \frac{29d + 25}{8} < 4d + 2.$$

Thus $R \le 4d + 1$ by integrality. All estimates for B, R apply whenever that intermediate $\bar{s}$-step occurs.

Index one is a $\bar{t}$-index, and at most one $\bar{s}$-step lies between consecutive $\bar{t}$-indices. The preceding bounds show that the absolute values of the denominators at these indices eventually enter $[1, 4d+1]$ and stay there. They also bound every intermediate denominator. The claimed estimate for P_n follows from $P_n^2 = D - Q_{n-1}Q_n$. The bounded integral pairs form a finite set, so the deterministic orbit is eventually periodic.

For sharpness let $k \ge 1$, $M = 5^k$ and $d = (M - 1)/4$. Choose $\rho \in \mathbb{Z}_5$ with $\rho^2 = -d$ and $\rho \equiv 2 \pmod 5$. Such a root exists since $d \equiv 1 \pmod 5$. For $\alpha = (2d + \rho)/d$ the first digit is 4, since $\alpha \equiv 4 \pmod 5$ and its half-trace is 2. Equation (4.1) gives $\alpha_1 = (2d+\rho)/(-M)$. The factorization $(2d - \rho)(2d + \rho) = dM$ gives $v_5(2d - \rho) = k$, as $2d + \rho$ is a unit. Thus $b = -4d/M = -1+5^{-k}$ is in the $\bar{t}$-coset of α_1, its distance to the half-trace is $2d/M < 1/2$, and $1/(\alpha_1 - b) = \alpha$. The expansion is purely periodic of minimal period two, with digits $4, b$ and denominators $d, -M$. It is also an Algorithm 5 expansion. The primitive polynomial $dX^2 - 4dX + M$ has discriminant $-4d$, so these examples use the stated normalization without a common scaling factor. □

4.2. **Two sufficient conditions for the fifth algorithm.** Wang and Deng's Algorithm 5 takes $\bar{s}$ at even indices and $\bar{t}$ at odd indices, regardless of the valuation of the input to a step. Its full periodicity assertion at $p = 5$ remains open.

Corollary 4.2. *If the odd remainders $\alpha_{2j+1} - \bar{t}(\alpha_{2j+1})$ are 5-adic units for all sufficiently large j, the Algorithm 5 expansion of a quadratic irrational in $\mathbb{Q}_5$ is eventually periodic.*

Proof. Every following even complete quotient is a unit. Starting at one of these even indices, Algorithms 4 and 5 therefore make the same choices when given the same deterministic tie rule. Apply Theorem 4.1. □

For a different criterion, write $e_n = |b_n - P_n/Q_n|$ for the real distance of the selected digit from the half-trace. For a set S of nonnegative integers write $\overline{d}(S) = \limsup_{m\to\infty} |S \cap [0, m)|/m$.

Proposition 4.3. *Let $p \geq 5$ be an odd prime and consider a quadratic Algorithm 5 expansion in $\mathbb{Q}_p$. If the expansion is not eventually periodic, then for every $0 < c < 1$,*

$$\overline{d}\big(\{j \geq 0 : e_{2j+1}e_{2j+2} \leq c\}\big) \leq \frac{\log(p/4)}{\log((p/4)/c)}.$$

In particular, for $p = 5$, the expansion is eventually periodic if the upper density of $\{j \geq 0 : e_{2j+1} \leq 1/4\}$ is greater than $\log(5/4)/\log 2$.

Proof. The normalization (4.1) and its proof apply to every odd prime. If $|Q_n| \leq H$ at infinitely many indices, then $|P_{n+1}| \leq pH/2$, since $e_n \leq p/2$. The next denominator is bounded by $|D| + (pH/2)^2$. Two of the resulting integral states (P_{n+1}, Q_{n+1}) coincide at indices of the same parity, forcing eventual periodicity. Hence a nonperiodic orbit satisfies $|Q_n| \to \infty$ and $|P_{n+1}| \to \infty$, the latter by $P_{n+1}^2 = D - Q_nQ_{n+1}$. After deleting a finite prefix we may take logarithms in

$$\frac{|Q_{n+1}|}{|Q_n|} = e_n^2 \left|1 - \frac{D}{P_{n+1}^2}\right|.$$

The logarithm of the last factor tends to zero. Summing over successive odd–even pairs therefore shows that the lower limit of the mean of $\log(e_{2j+1}e_{2j+2})$ is nonnegative. Here and below a finite initial segment on which a logarithm is undefined is omitted. Each pair product is at most $p/4$. If a fraction f_m of the first m pairs has product at most c, the mean over the retained tail is at most $\log(p/4) - f_m \log((p/4)/c) + o(1)$. Taking the subsequence along which f_m attains its upper limit proves the inequality. For $p = 5$ an odd distance at most $1/4$ gives a pair product at most $5/8$. Use $c = 5/8$. □

4.3. **Growing blocks for the fifth algorithm.**

Proposition 4.4. *Let $p \geq 5$ be prime. Put $h = 1$ if $p = 5$, and $h = 0$ otherwise, and set $a = p^{-h}$ and $D = 1 + 4p^{2h+1}$. For every $L \geq 1$ there are infinitely many quadratic inputs of primitive polynomial discriminant $4D$ whose Algorithm 5 expansions begin with exactly L full repetitions of $(-a, -a/p)$. With the fixed radical $\sqrt{D}$ their initial denominators can be arbitrarily large, and*

$$|Q_{n+2}| > \left(1 + \frac{a(2+a)}{p}\right)^2 |Q_n| \qquad (0 \leq n \leq 2L-1).$$

For $p \geq 7$ the same conclusions hold for Algorithm 4.

Proof. Choose $\rho^2 = D$ in $\mathbb{Z}_p$ with $\rho \equiv -1 \pmod p$. For $p = 5$, $22^2 < 501 < 23^2$. For $p \geq 7$, $D = (2t+1)^2$ with $t \geq 0$ would give $p = t(t+1)$. Thus D is nonsquare. Set $w = (\rho - 1)/(2p^h)$ and $z = w/p$. The relation $w(w+a) = p$ gives $1/(w+a) = z$ and $1/(z + a/p) = w$. The two residual valuations are $h+1$ and h, respectively.

Put $\mu = \rho + 1/(w-2)$. We have $v_p(w-2) = -h$. When $h = 0$ this follows from $w \equiv -1 \pmod p$ and $p \geq 7$. Choose arbitrarily large positive integers m with $v_p(m - \mu) = (4h+2)L + 2h + 1$ and put

$$x = 2 + \frac{1}{m - \rho} = \frac{2q + m + \rho}{q}, \qquad q = m^2 - D.$$

Since $w = 2 + 1/(\mu - \rho)$ and both $m - \rho$ and $\mu - \rho$ have valuation h, we get $v_p(x - w) = (4h+2)L + 1$. The primitive polynomial $qX^2 - 2(2q+m)X + 4q + 4m + 1$ has discriminant $4D$. It is primitive because a common divisor of its coefficients divides both $2m$ and $4m + 1$.

Both real conjugates of x lie in $I = (2, p/2 - a)$ for large m. The two-step map $F(y) = (y + a)/(1 + a(y + a)/p)$ is increasing and preserves I. Indeed $F(2) > 2$ and $F(p/2 - a) = p/(2 + a) < p/2 - a$, both by $p > 4 + 2a$. For $y \in I$ one has

$$y + a < p/2, \qquad \frac{1}{y+a} + \frac{a}{p} < \frac{1}{2+a} + \frac{a}{p} < \tfrac{1}{2}.$$

Thus the desired digits are strictly nearest to each half-trace provided they have the required p-adic residues.

At the beginning of pair $j < L$ the discrepancy from w has valuation $(4h+2)(L-j)+1$. Inversion after $-a$ lowers this valuation by $2h+2$, since both residuals have valuation $h+1$. The odd discrepancy still has valuation at least $2h + 1 > h$. Inversion after $-a/p$ therefore lowers it by $2h$, the two residuals having valuation h. This proves the digit congruences and the induction. For $h = 0$ the even states are units and the odd ones have valuation -1, so Algorithm 4 makes the same choices. At index $2L$ the discrepancy from w has valuation one and the next digit is still $-a$. At the ensuing odd index the discrepancy from z has valuation $1 - v_p(x_{2L} + a) - (h + 1) < 0$. Hence $-a/p$ is outside its $\bar{t}$-coset, and the run ends.

A determinant-one map $(Ay + B)/(Cy + E)$ multiplies a fixed-radical denominator by $(Cy + E)(Cy' + E)$, by the identity for the difference of its two real conjugates. The bottom row of F is $(a/p, 1 + a^2/p)$, and its even arguments exceed 2. The odd two-step map is $(y + a/p)/(ay + 1 + a^2/p)$ and its odd arguments exceed $2/p$. In both cases every factor exceeds $1 + a(2 + a)/p$, giving the claim. □

In particular, a bound of the form $|Q_{n+k}| < |Q_n|$ whenever $|Q_n|$ exceeds a fixed threshold fails for every fixed $k \geq 1$. For even k this follows from the proposition. For odd k one also uses $|Q_1|/|Q_0| = (x + a)(x' + a) > (2 + a)^2$ at the first step. This applies to Algorithm 5 at $p = 5$ and to both algorithms at larger primes.

Growth is also possible with a fixed imaginary quadratic field. Choose $s^2 = -6$ with $s \equiv 13 \pmod{25}$, put $m = 98 + 125k$ for $k \geq 0$ and set

$$q = m^2 + 6, \quad P = 2q + m, \quad M = 4q + 4m + 1,$$
$$x = (P + s)/q, \quad y = 1/5 + 1/x, \quad z = 1 + 1/y.$$

At $p = 5$ the first three Algorithm 5 digits of z are $1, 1/5, -2/5$. Indeed, $1/x = (P - s)/M$, $2/5 < P/M < 1/2$, and x has 5-adic norm 5, since $v_5(q) = 1$ and $P + s \equiv 1 \pmod 5$. Thus $y - 1/5 \in \mathbb{Z}_5$ and its half-trace differs from $1/5$ by less than $1/2$. The half-trace of $1/y$ lies between 0 and $5/3$, by $1/5 + P/M > 3/5$ and the nonreal conjugate pair. Also $1/y \in 5\mathbb{Z}_5$. To see that $x + 2/5 \in 5\mathbb{Z}_5$, observe that its numerator $12q + 5m + 5s$ is divisible by 125, while $v_5(5q) = 2$. Its real half-trace is $12/5 + m/q < 5/2$. Applying (4.1) with radical $-25s$ gives absolute denominators $25M$ and $144q + 120m + 25$ at indices one and three. Their ratio tends to $36/25 > 1$ as $k \to \infty$.

4.4. **Yasutomi's simultaneous algorithm at $p = 3$.** Let K be a real quadratic field with chosen embeddings into $\mathbb{R}$ and $\mathbb{Q}_p$. Write α_∞ for the real image of $\alpha \in K$. Yasutomi's algorithm [34, Definitions 1.1 and 1.2] chooses the $a_n \in \mathbb{Z}[1/p]$ closest to $(\alpha_n)_\infty$ subject to

$$\alpha_n - a_n \in p\mathbb{Z}_p \quad (n \text{ even}), \qquad \alpha_n - a_n \in \mathbb{Z}_p \quad (n \text{ odd}),$$

and then uses (2.3). For odd p these two sets of admissible digits are $s(\alpha_n) + p\mathbb{Z}$ and $t(\alpha_n) + \mathbb{Z}$. The congruence formulation also applies at $p = 2$. The midpoint of two consecutive representatives is rational, so the nearest representative is unique. Yasutomi proved periodicity and real convergence at $p = 2$ and conjectured eventual periodicity for the primes $3 \leq p \leq 23$ [34, Corollaries 3.14 and 3.20, Conjecture 5.2].

Theorem 4.5. *For $p = 3$, the above algorithm is eventually periodic for every $\alpha \in K \setminus \mathbb{Q}$. The real limit of its convergents is α_∞.*

Proof. For $n \geq 1$, put $r_n = 1/\alpha_n$, and let x_n, y_n be its two real conjugates, with x_n corresponding to the chosen embedding. The recurrence is

$$r_{n+1} = \frac{1}{r_n} - a_n. \tag{4.3}$$

The nearest-representative rule gives

$$|x_n| < \begin{cases} 1/2, & n \text{ even}, \\ 3/2, & n \text{ odd}, \end{cases} \qquad |r_n|_3 \leq \begin{cases} 1, & n \text{ even}, \\ 1/3, & n \text{ odd}. \end{cases}$$

First we bound the real separation $\delta_n = |x_n - y_n|$ away from zero. By (4.3),

$$\delta_{n+1} = \frac{\delta_n}{|x_n y_n|}.$$

If $|x_n| \leq A$, then $|y_n| \leq A + \delta_n$, and hence

$$\delta_{n+1} \geq f_A(\delta_n), \qquad f_A(t) = \frac{t}{A(A+t)}.$$

These functions are increasing on $t > 0$. For even n, composition yields

$$\delta_{n+2} \geq \frac{16\delta_n}{3(14\delta_n + 3)} \geq \min(\delta_n, 1/6).$$

For odd n, it similarly gives

$$\delta_{n+2} \geq \frac{16\delta_n}{14\delta_n + 9} \geq \min(\delta_n, 1/2).$$

Consequently

$$\delta_n \geq \delta_* := \min(\delta_1, \delta_2, 1/6) > 0 \qquad (n \geq 1). \tag{4.4}$$

Next let u_n, v_n be the two 3-adic conjugates of r_n, with $u_n = r_n$. We show that eventually

$$|v_n|_3 > 1 \quad (n \text{ even}), \qquad |v_n|_3 \geq 1 \quad (n \text{ odd}). \tag{4.5}$$

Once this pattern holds at one index, it persists. At an odd index, $|a_n|_3 = |1/u_n|_3 > 1$, while $|1/v_n|_3 \leq 1$, so the next conjugate has norm greater than one. At an even index, $|a_n|_3 = |1/u_n|_3 \geq 1$, while $|1/v_n|_3 < 1$, so the next conjugate has norm at least one.

If the pattern never occurred, both u_n and v_n would have norm at most $1/3$ at odd indices and at most one at even indices. Iterating

$$u_n - v_n = -u_n v_n (u_{n+1} - v_{n+1})$$

would give $|u_1 - v_1|_3 \leq 3^{-N}$ after N steps, since the terminal difference is bounded by one. This contradicts $u_1 \neq v_1$. Thus (4.5) holds eventually. In particular $|u_n - v_n|_3 \geq 1$ from some index onwards.

Choose an integral quadratic polynomial F_1 for r_1, and define $F_n(X) = A_n X^2 + B_n X + C_n$ recursively by

$$F_{n+1}(X) = (X + a_n)^2 F_n\Big(\frac{1}{X + a_n}\Big).$$

The coefficients of every F_n lie in $\mathbb{Z}[1/3]$. Its roots are the conjugates of r_n, and the substitutions preserve the discriminant $\Delta > 0$. Also $A_{n+1} = C_n$. By (4.4),

$$|A_n| = \frac{\sqrt{\Delta}}{\delta_n} \leq \frac{\sqrt{\Delta}}{\delta_*}.$$

By eventual 3-adic separation,

$$v_3(A_n) = \frac{1}{2}v_3(\Delta) - v_3(u_n - v_n) \geq \frac{1}{2}v_3(\Delta).$$

Since Δ is a positive integer, the last inequality and $A_n \in \mathbb{Z}[1/3]$ imply $A_n \in \mathbb{Z}$ for all sufficiently large n. The real bound therefore leaves only finitely many possible values of A_n. The same holds for $C_n = A_{n+1}$ and then for B_n, since $B_n^2 = \Delta + 4A_nC_n$. There are only finitely many transported polynomials and hence finitely many possible r_n. Repetition at indices of the same parity gives periodicity, and taking reciprocals gives the same conclusion for the original complete quotients.

For real convergence, choose $n \geq 1$ and an even integer h such that $\alpha_{k+h} = \alpha_k$ for all $k \geq n$, and put $T = M(a_n) \cdots M(a_{n+h-1})$. Then $((\alpha_n)_\infty, 1)^T$ is an eigenvector with eigenvalue

$$\lambda = \prod_{j=1}^{h} (\alpha_{n+j})_\infty, \qquad |\lambda| > (4/3)^{h/2} > 1,$$

by the real bounds on $x_{n+j} = 1/(\alpha_{n+j})_\infty$. Since $\det T = 1$, the other eigenvalue is λ^{-1}, with eigenvector $((\alpha_n')_\infty, 1)^T$. For each residue class of indices modulo h, the numerator–denominator vectors of the convergents of the periodic tail have the form $T^k v$ with a fixed nonzero rational vector v. Such a vector cannot lie in the second eigenspace, whose slope is irrational. The first eigencomponent therefore dominates as $k \to \infty$, and the ratios converge to $(\alpha_n)_\infty$. Applying the fixed matrix of the preperiod gives convergence to α_∞. Its denominator is nonzero at the irrational point $(\alpha_n)_\infty$. □

Corollary 4.6. *Let Δ be the discriminant of an integral quadratic polynomial for r_1 in the proof of Theorem 4.5, and put $D = \Delta/3^{v_3(\Delta)}$. The least even period h of the complete quotients satisfies*

$$h \leq 8 \sum_{\substack{B \in \mathbb{Z},\ |B| < 7\sqrt{D} \\ B^2 \equiv D \pmod 4}} \tau\left(\frac{|B^2 - D|}{4}\right) \ll_\epsilon D^{1/2+\epsilon} \qquad (\epsilon > 0),$$

where τ denotes the divisor function.

Proof. The integer $v_3(\Delta) = 2d$ is even since the two roots lie in $\mathbb{Q}_3$. The integer D is nonsquare, since $\Delta = 3^{2d}D$ is the discriminant of an irreducible quadratic. In the eventually periodic part of the orbit, the minimum real conjugate separation at even indices exceeds $1/6$. Indeed, the even two-step bound in the proof of Theorem 4.5 is strict and its increasing right-hand side is at least its argument for arguments at most $1/6$. Applying it to a predecessor of a point of minimum separation proves the assertion. At odd indices the corresponding minimum exceeds $1/2$.

For sufficiently large n, the same proof gives $v_3(A_n), v_3(C_n) \geq d$, and $B_n^2 = \Delta + 4A_nC_n$ then gives $v_3(B_n) \geq d$. Dividing each of these polynomials by 3^d gives integral coefficients of discriminant D. At even indices in the period, write these coefficients as A, B, C. The separation estimates and $C_n = A_{n+1}$ give

$$|A| < 6\sqrt{D}, \qquad |C| < 2\sqrt{D}, \qquad |B| < 7\sqrt{D}.$$

For each B in the sum there are at most $2\tau(|B^2 - D|/4)$ signed factorizations $AC = (B^2 - D)/4$, and each polynomial has two roots. The even positions in a minimal even cycle are distinct. Multiplying their number by two proves the displayed bound. In that sum $|B^2 - D|/4 < 12D$ for the terms arising from the orbit, and all terms displayed are $O(D)$. The standard divisor bound $\tau(m) \ll_\epsilon m^\epsilon$ finishes the proof. □

4.4.1. *The real conjugate at larger primes.*

Lemma 4.7. *Let K be a real quadratic field with fixed embeddings into $\mathbb{R}$ and $\mathbb{Q}_p$. Every open interval in $\mathbb{R}_{>0}$ contains real images of norm-one units $u \in \mathcal{O}_K[1/p]^\times$ with $v_p(u)$ arbitrarily negative.*

Proof. The chosen p-adic embedding determines one of the two distinct primes $\mathfrak{p}, \mathfrak{p}'$ above p. By finiteness of the ideal class group, take $m > 0$ and π with $(\pi) = \mathfrak{p}^m$. Writing primes for field conjugation, $\eta = (\pi'/\pi)^2$ is a positive norm-one unit in $\mathcal{O}_K[1/p]$ with $v_p(\eta) = -2m$. Choose an ordinary norm-one unit ϵ with $\epsilon_\infty > 1$ by the real quadratic unit theorem. The ratio $\log \eta_\infty / \log \epsilon_\infty$ is irrational, since otherwise a nonzero power of η would equal a power of ϵ, contradicting their valuations. The positive iterates of the corresponding irrational rotation are dense, as is every tail. Thus $\eta^j \epsilon^k$ lies in the prescribed real interval for arbitrarily large $j > 0$ and suitable integers k. □

Theorem 4.8. *For each prime $p \geq 5$ and each real quadratic field K with chosen real and p-adic embeddings, Yasutomi's alternating algorithm admits infinitely many $\alpha \in K$ with a purely periodic expansion of least period two whose convergents tend in $\mathbb{R}$ to the other real conjugate of α.*

Proof. Choose a unit u as in Lemma 4.7 with

$$\frac{2p}{2p+1} < u_\infty < 1 - \frac{2}{p^2}, \qquad v_p(u) < -2.$$

The interval is nonempty because $p^2 > 4p + 2$. Put

$$x = p^2(1-u), \quad y = u/x, \quad b = -p^{-2}, \quad a = -p^2(u + u^{-1} - 2).$$

The trace $u + u^{-1}$ belongs to $\mathbb{Z}[1/p]$. Direct substitution gives

$$x = a + 1/y, \qquad y = b + 1/x, \qquad v_p(x) = 2 + v_p(u) < 0, \qquad v_p(y) = -2.$$

Our interval gives $x_\infty > 2$ and $y_\infty > 2/p$. At the even step $x - a = 1/y$ belongs to $p\mathbb{Z}_p$ and has real absolute value $< p/2$. At the odd step $y - b = 1/x$ belongs to $\mathbb{Z}_p$ and has real absolute value $< 1/2$. These two strict inequalities characterize the required nearest representatives, so the complete quotients alternate between x and y. They are distinct because $y_\infty = u_\infty / x_\infty < 1/2$. The digits are distinct because $a = b$ would give $x = y$ from $x = (u-1)/b$, $y = (u-1)/a$.

The eigenvalue of $M(a)M(b)$ on $(x, 1)^T$ is $xy = u$. Its absolute value is < 1 in the chosen real embedding and > 1 in the selected p-adic embedding. The attracting real slope is therefore the conjugate $x' = p^2(1 - u^{-1})$, which is negative. Both projective subsequences of convergents approach x', since their initial vectors have rational slope and the repelling slope is irrational. Taking $v_p(u)$ arbitrarily negative makes the inputs x distinct. □

For example, let $p \geq 5$. The positive root x of $X^2 + p^{-1}X - p = 0$, embedded p-adically as the root of valuation -1, has successive complete quotients $x, x/p$ and digits $-1/p, -1/p^2$. Indeed, $x + 1/p = p/x$, $x > 2$, and $x/p + 1/p^2 = 1/x$. The period matrix has eigenvalue $x^2/p = 1 - x/p^2 < 1$ at the positive real root, so the convergents tend to the other real root. The integer $1 + 4p^3$ is nonsquare, since a square would give two consecutive coprime positive integers with product p^3, forcing that product to be 2. The polynomial $pX^2 + X - p^2$ has a root of valuation 2 by Hensel's lemma and the other has valuation -1. Together with the $p = 2$ convergence theorem of [34, Corollary 3.14], the preceding examples show that $p = 3$ is the largest prime for which convergence to the selected real embedding holds for every real quadratic input. The eventual periodicity in [34, Conjecture 5.2] remains open at $p = 5, 7, 11, 13, 17, 19, 23$.

4.5. **Yasutomi's sign algorithm.** In a separate algorithm [33, formula (1.1)], Yasutomi uses the ordinary, nonnegative truncation $\lfloor\cdot\rfloor_p$. Here $\lfloor u\rfloor_p$ is the unique $c \in \mathbb{Z}[1/p] \cap [0,p)$ for which $u - c \in p\mathbb{Z}_p$. With chosen embeddings of a real quadratic field K into $\mathbb{R}$ and $\mathbb{Q}_p$, put

$$\varepsilon_n = \operatorname{sgn}((\alpha_n)_\infty), \qquad b_n = \varepsilon_n \lfloor \varepsilon_n \alpha_n \rfloor_p, \qquad \alpha_{n+1} = 1/(\alpha_n - b_n).$$

Write $\beta_n = \varepsilon_n \alpha_n$, $x_n = (\beta_n)_\infty$ and $c_n = \lfloor \beta_n \rfloor_p$. For $n \geq 1$ we have $v_p(\beta_n) = v_p(c_n) < 0$ and $0 < c_n < p$. A change of sign occurs precisely when $x_n < c_n$ and then $\beta_{n+1} = 1/(c_n - \beta_n)$. Yasutomi conjectures eventual periodicity for every real quadratic input at $p = 2, 3$, with real convergence to one of its two conjugates. His numerical tables give examples of both limits at each prime [33, Tables 1 and 2 and Conjecture 3.1(1),(2)].

Theorem 4.9. *For a quadratic irrational input, if the signs ε_n alternate at every sufficiently late step, then $c_n > 2$ at infinitely many indices. At $p = 2$ every quadratic irrational has infinitely many indices with $\varepsilon_{n+1} = \varepsilon_n$.*

Proof. Suppose that all late steps change sign and have $c_n \leq 2$. Equality is impossible since $v_p(c_n) < 0$. On this tail $0 < x_n < c_n < 2$ and $x_{n+1} > 1/(2 - x_n)$. All x_n on the tail lie below one. Indeed, $x_n = 1$ would give $x_{n+1} > 1$, and as long as $1 < x_n < 2$ the positive quantities $1/(x_n - 1)$ would decrease by more than one at every step. Put $e_n = 1 - x_n$ and $g_n = 2 - c_n$. Since $x_{n+1} < 1$, we have $0 < g_n < e_n$ and

$$e_{n+1} = \frac{e_n - g_n}{1 + e_n - g_n} < \frac{e_n}{1 + e_n}.$$

It follows that $e_n \to 0$, hence $c_n \to 2$ from below. The digits in $(0, 2)$ of bounded p-power denominator form a finite set, so $-v_p(\beta_n) \to \infty$.

Write $\beta_n = (B_n + s)/K_n$ with $s^2 = D > 0$ a fixed nonsquare integer and $B_n, K_n \in \mathbb{Z}$, $K_n \mid D - B_n^2$. Such initial coordinates are obtained from $(B + s)/K$ by replacing (B, K, s) with (BK, K^2, Ks). On our tail the recurrence is

$$B_{n+1} = c_n K_n - B_n, \qquad K_{n+1} = (B_{n+1}^2 - D)/K_n.$$

The first new coordinate is integral since $c_n K_n = B_n + s - K_n(\beta_n - c_n)$ belongs to $\mathbb{Z}[1/p] \cap \mathbb{Z}_p$. The second belongs to $\mathbb{Z}[1/p]$ by expansion and equals $(c_n - \beta_n)(s + B_{n+1}) \in \mathbb{Z}_p$. It again divides $D - B_{n+1}^2$. Since $v_p(K_n) \geq -v_p(\beta_n)$, we have $|K_n| \to \infty$. From $x_n \to 1$ it follows that $|B_n| \to \infty$. Since $K_n K_{n+1} = B_{n+1}^2 - D > 0$ eventually, the sign of K_n is eventually constant, and we may choose $K_n > 0$ by changing the signs of B_n, K_n, s together.

For either $z_n = K_n - B_n$ or $z_n = B_{n+1} - K_n$, we have $K_n \mid z_n^2 - D$. Both quantities exceed s_∞ by $x_n < 1$ and $c_n - x_n = 1/x_{n+1} > 1$, respectively. Each z_n tends to $+\infty$. Indeed, a bounded subsequence would contain a fixed integer z and force $K_n \mid z^2 - D \neq 0$ on that subsequence. Thus eventually both real images of $1 - \beta_n$ and of $c_n - 1 - \beta_n$ are positive. In both embeddings the latter is strictly smaller because $c_n < 2$. With N the field norm, the quantities

$$H_n = K_n N(1 - \beta_n) = \frac{(K_n - B_n)^2 - D}{K_n}$$

are then positive integers. The identity $K_{n+1} = K_n N(c_n - \beta_n)$ gives

$$H_{n+1} = K_n N(c_n - 1 - \beta_n) < K_n N(1 - \beta_n) = H_n.$$

This contradiction proves the theorem. □

Proposition 4.10. *For every odd p and every real quadratic field K embedded in $\mathbb{Q}_p$, there are infinitely many inputs in K for which the sign algorithm gives a pure period $c, -c$ with $2 < c < p$. The values of c can approach 2. Either real conjugate can occur as the limit of the convergents.*

Proof. Choose u from Lemma 4.7 with $v_p(u) < 0$ and $u_\infty > 0$ arbitrarily close to one. Then $c = u+u^{-1} \in \mathbb{Z}[1/p]$ satisfies $2 < c < p$. Since $u-c = -1/u \in p\mathbb{Z}_p$, its ordinary digit is c. The complete quotients are $u, -u, u, \ldots$, and the digits are $c, -c, c, \ldots$. The period matrix on $(u,1)^T$ has eigenvalue $-u^2$. The attracting real slope is u_∞ if $u_\infty > 1$ and u_∞^{-1} if $u_\infty < 1$. The unit lemma allows either choice with arbitrarily negative valuation. □

Proposition 4.11. *In every real quadratic field embedded in $\mathbb{Q}_2$, each of the two alternatives for the real limit of Yasutomi's sign algorithm is attained by infinitely many inputs of least period six.*

Proof. Take a unit u as in Lemma 4.7 with $99/100 < u_\infty < 101/100$, $u_\infty \neq 1$ and $v_2(u) < -4$. Put

$$b = 3/2, \quad c = 5/8, \quad a = 34-16(u+u^{-1}), \qquad x = 24-16u, \quad z = c+1/x, \quad y = b-1/z.$$

The trace of u belongs to $\mathbb{Z}[1/2]$ and $3/2 < a < 2$. We have $7 < x_\infty < 9$, hence $z_\infty > 5/8 + 1/9 > 2/3$ and $y_\infty > 0$. As $bc - 1 = -1/16$, the relations

$$(bc-1)x + b = u, \qquad xyz = u, \qquad x - 1/y = (u + u^{-1} - b - c)/(bc-1) = a$$

follow directly. Also $v_2(x) = 4 + v_2(u) < 0$, $v_2(z) = -3$ and $v_2(y) = -1$. Thus $x - a = 1/y$, $y - b = -1/z$ and $z - c = 1/x$ belong to $2\mathbb{Z}_2$. Their real signs give the successive complete quotients $x, y, -z, -x, -y, z, x$. The corresponding digits $a, b, -c, -a, -b, c$ are distinct, so their least period is six. The period eigenvalue on $(x,1)^T$ is $-u^2$. The attracting real slope is x_∞ for $u_\infty > 1$ and the other conjugate $(24 - 16u^{-1})_\infty$ for $u_\infty < 1$. In either interval the valuation of u may be chosen arbitrarily negative. □

There is no uniform bound on the length of consecutive sign changes at $p = 2$, even within a fixed quadratic field.

Proposition 4.12. *For every real quadratic $K \subset \mathbb{Q}_2$ and every $L \geq 1$, some irrational input has L initial sign changes with a single common normalized digit.*

Proof. Write $K = \mathbb{Q}(\sqrt{d})$ with squarefree $d > 0$ and choose the sign of $\sqrt{d}$ positive at the real place. Take an integer $M > L + 4$ sufficiently large that $\epsilon\sqrt{d} < 2^{-M-1}$, where $\epsilon = 2^M/(2^{3M}+1)$. Put $g = 2^{-M}$, $c = 2 - g$, $\beta_L = 1 - g + \epsilon\sqrt{d}$, and recursively set $\beta_j = c - 1/\beta_{j+1}$. For $e_j = 1 - (\beta_j)_\infty$ we have $g/2 < e_L < g$ and $e_j = g + e_{j+1}/(1 - e_{j+1})$. Backward induction gives $0 < e_j \leq (2^{L-j+1} - 1)g < 1/2$. Thus all real β_j are positive and less than one. At the other place $v_2(\beta_L) = -M$ and induction gives $v_2(\beta_j) = -M$, $\beta_j - c = -1/\beta_{j+1} \in 2\mathbb{Z}_2$. These identities select c at every indicated step. Invertibility of the rational fractional linear transformations ensures that β_0 is irrational in K. □

There is a simple necessary condition for a nonperiodic orbit in Yasutomi's Conjecture 3.1(3). In addition to the selected real embedding, fix the p-adic square root s throughout. Write $\beta_n = (B_n + s)/K_n$ in the integral coordinates used in the proof of Theorem 4.9 and let $\eta_n = \varepsilon_n\varepsilon_{n+1}$. At an arbitrary step,

$$B_{n+1} = c_nK_n - B_n, \qquad K_{n+1} = \eta_n(D - B_{n+1}^2)/K_n.$$

The same argument proves integrality for either sign. Bounded B_n implies bounded K_n by $|K_{n-1}K_n| = |D - B_n^2|$, and bounded K_n implies bounded B_n by the same equality. In either case some $(B_n, K_n, \varepsilon_n)$ repeats. Conversely a periodic orbit has bounded coordinates, since the coordinate of the fixed irrational s determines K_n uniquely. In particular a nonperiodic orbit has unbounded $|K_n|$, equivalently its two real images approach each other along a subsequence. If there are only finitely many sign changes, its normalized tail is a Ruban expansion whose chosen real image is positive at every step. The tail is therefore periodic by the sufficient condition in [7, Theorem 6.5]. Constructing a nonperiodic orbit in every admissible field for $p > 3$ remains open.

4.5.1. *Approximation on a periodic orbit.* Yasutomi obtained upper bounds with exponents adding to two for his alternating algorithm at $p = 2$ [34, Corollary 3.25]. For another family of periodic continued fractions, Barbero, Cerruti and Murru [1] express the p-adic convergence rate in terms of the eigenvalues of a period matrix. For each of Yasutomi's two algorithms, the two eigenvalues determine the orders of both approximation errors.

Proposition 4.13. *For either of Yasutomi's algorithms, suppose that the complete quotients of a real quadratic irrational $\alpha \in \mathbb{Q}_p$ are eventually periodic. In the alternating algorithm take a period of even length. If p_n/q_n are the convergents in lowest integer terms, there is a $\xi \in \{\alpha_\infty, (\alpha')_\infty\}$ and there are $\gamma_\infty, \gamma_p > 0$ with $\gamma_\infty + \gamma_p = 2$ such that*

$$|\xi - p_n/q_n| \asymp |q_n|^{-\gamma_\infty}, \qquad |\alpha - p_n/q_n|_p \asymp |q_n|^{-\gamma_p}.$$

At $p = 3$ in Theorem 4.5, ξ is the selected real image. The implied constants depend on the orbit.

Proof. Let T be the product of the matrices $M(a)$ over one period, starting after the first complete quotient. The periodic complete quotient and its conjugate give two eigenlines of quadratic irrational slope, and $\det T = \pm 1$. On the selected p-adic eigenline its eigenvalue is the product of the complete quotients following the successive digits. Write P for its p-adic norm. We have $P > 1$. For the sign algorithm every factor has norm > 1. For the alternating algorithm the factors have norm at least one and every second factor has norm > 1. The two real eigenvalues have distinct absolute values. Otherwise their ratio would be 1 or -1, as their eigenlines are real and distinct, and T^2 would be scalar, contradicting the p-adic eigenvalue norms. Let $R > 1$ be the larger real eigenvalue modulus.

Write the unscaled continuants as (A_n, B_n). On each residue class modulo the period h, their column equals $UT^k w$ for $n = n_0 + kh$, a fixed rational matrix U of determinant ± 1 and a nonzero rational vector w. Both eigencomponents of w are nonzero. The two eigenlines transported by U have finite, irrational slopes, so their second coordinates are nonzero. Diagonalization at the real and p-adic places therefore gives, for all sufficiently large k,

$$|B_n| \asymp R^k, \quad |B_n|_p \asymp P^k, \quad |\xi - A_n/B_n| \asymp R^{-2k}, \quad |\alpha - A_n/B_n|_p \asymp P^{-2k},$$

where ξ is the real slope of the transported expanding eigenline. The two error estimates follow by taking a determinant with the expanding eigenvector and dividing by the second coordinate. The unimodular continuant identity shows that the column (A_n, B_n) generates the unit ideal of $\mathbb{Z}[1/p]$. Multiplication by $\max(|A_n|_p, |B_n|_p)$ thus gives a primitive integral column. Since $A_n/B_n \to \alpha \neq 0$ in $\mathbb{Q}_p$, this factor eventually equals $|B_n|_p \max(1, |\alpha|_p)$. Consequently $|q_n| \asymp (RP)^k$. Choosing

$$\gamma_\infty = \frac{2 \log R}{\log R + \log P}, \qquad \gamma_p = \frac{2 \log P}{\log R + \log P}$$

proves the assertion on each of the finitely many residue classes. □

Proposition 4.14. *Let K be a real quadratic field embedded in $\mathbb{Q}_p$ such that $\mathcal{O}_K[1/p]^\times$ contains a unit of norm -1. For every $C > 0$ the sign algorithm has a fixed point $\alpha \in K$ whose convergents p_n/q_n in lowest terms satisfy*

$$\lim_{n \to \infty} q_n^2 \, |\alpha_\infty - p_n/q_n| \, |\alpha - p_n/q_n|_p > C.$$

Such a field exists for every prime p. Even with K and p fixed, the product of the two constants in the upper bounds of Proposition 4.13 is unbounded as the fixed point varies.

Proof. Choose a unit $\theta \in \mathcal{O}_K[1/p]^\times$ of norm -1, changing its sign if necessary so that $\theta_\infty > 0$. By Lemma 4.7 there are norm-one units v for which $\alpha = \theta v$ satisfies $1 < \lambda :=$

$\alpha_\infty < 3/2$ and $M := |\alpha|_p$ is arbitrarily large. Take $M > 1$. Since $\alpha' = -1/\alpha$, the trace $c = \alpha - 1/\alpha$ belongs to $\mathbb{Z}[1/p]$, with $0 < c = \lambda - \lambda^{-1} < 1$ and $|c|_p = M$. Thus c is the ordinary p-adic digit of α and $1/(\alpha - c) = \alpha$. In particular the sign algorithm fixes α.

Put $S_0 = 0$, $S_1 = 1$ and $S_{m+1} = cS_m + S_{m-1}$. The convergent with $m \geq 1$ digits is $r_m = S_{m+1}/S_m$. Induction gives $|S_m|_p = M^{m-1}$, so multiplying the two entries by M^m gives an integral column whose first entry is prime to p. The unimodular continuant identity rules out a common prime divisor different from p. The reduced denominator is therefore $q_m = M^m S_m$. For either root z of $X^2 - cX - 1$ we have $S_{m+1} - zS_m = (-1/z)^m$. Hence

$$|r_m - \lambda| = \frac{\lambda^{-m}}{S_m}, \qquad |r_m - \alpha|_p = M^{-(2m-1)}.$$

The formula $S_m = (\lambda^m - (-1/\lambda)^m)/(\lambda + \lambda^{-1})$ now gives

$$\lim_{m\to\infty} q_m^2 \, |r_m - \lambda| \, |r_m - \alpha|_p = \frac{M}{\lambda + \lambda^{-1}} > \frac{2M}{5}.$$

Since the two exponents in Proposition 4.13 sum to two, the product of the two upper-bound constants is at least this limit.

For each p one may take $K = \mathbb{Q}(\sqrt{1 + 4p^2})$ and take θ to be the positive root of $X^2 - p^{-1}X - 1$. The integer $1 + 4p^2$ lies strictly between $(2p)^2$ and $(2p+1)^2$, and Hensel's lemma at $Y = 1$ for $Y^2 - Y - p^2$, with $Y = p\theta$, gives an embedding in $\mathbb{Q}_p$. The polynomial for θ shows that it is a unit of norm -1 in $\mathcal{O}_K[1/p]$. □

Universal eventual periodicity for the sign algorithm at $p = 2, 3$ remains open. Proposition 4.13 gives the real convergence asserted in [33, Conjecture 3.1(1),(2)] whenever the orbit is eventually periodic.

5. Real approximation for Ruban's and Schneider's algorithms

This section allows $p = 2$. In Ruban's algorithm [26], the partial quotient at x is the unique $a \in \mathbb{Z}[1/p] \cap [0, p)$ such that $x - a \in p\mathbb{Z}_p$. Capuano, Veneziano and Zannier proved that the Ruban expansion of every quadratic irrational has a finite real limit [7, Proposition 4.5]. They conjectured that this limit is transcendental whenever the expansion is nonperiodic [7, Section 4.2]. For Schneider's expansions [29] of quadratic p-adic units, Pejković proved a real error bound of order n^{-2} [22, Theorem 2.3]. As in that argument, a quadratic form controls the lengths of the intervals between consecutive convergents. For Ruban expansions, counting its possible middle coefficients gives the following bound.

Theorem 5.1. *Let $\alpha \in \mathbb{Q}_p$ be quadratic over $\mathbb{Q}$, let $r_n = [a_0; \ldots, a_{n-1}]$, and let ξ be the real limit of its Ruban expansion. For all $n \geq 2$,*

$$|r_n - \xi| \ll_{\alpha,p} n^{-3}.$$

If ξ is a zero of the minimal polynomial of α, the bound can be replaced by $O_{\alpha,p}(\theta^n)$ for some $0 < \theta < 1$.

Proof. Use the indexing of [7], with $w_0 = (1, 0)$, $w_1 = (a_0, 1)$, $w_n = (p_n, q_n)$ and $w_{n+1} = a_n w_n + w_{n-1}$. Thus $r_n = p_n/q_n$, and $|\det(w_n, w_{n-1})| = 1$. Put $e_0 = \max(0, -v_p(\alpha))$, $e_j = -v_p(a_j) \geq 1$ for $j \geq 1$, and $s_n = \sum_{j=0}^{n-1} e_j$. If $a_0 \neq 0$, then $e_0 = -v_p(a_0)$. The recurrence gives $v_p(q_n) = e_0 - s_n$ for $n \geq 1$. It also gives $v_p(p_n) = -s_n$ when $a_0 \neq 0$. When $a_0 = 0$ we have $e_0 = 0$, $p_1 = 0$, $p_2 = 1$ and $v_p(p_n) = e_1 - s_n$ for $n \geq 2$. In either recurrence the term containing the newest digit has strictly smaller valuation once both preceding terms are nonzero. The complete-quotient identity gives

$$v_p(p_n - \alpha q_n) = s_{n+1} - e_0.$$

In its denominator $q_n\alpha_n + q_{n-1}$, the first term dominates because $v_p(\alpha_n) = -e_n$.

Let $f(X) = aX^2 + bX + c$ be the primitive integral minimal polynomial, $F(X,Y) = aX^2 + bXY + cY^2$, $\Delta = b^2 - 4ac$, and $d = v_p(a(\alpha - \alpha')) = v_p(\Delta)/2$. The discriminant is a nonzero nonsquare integer with a square root $s = a(\alpha - \alpha')$ in $\mathbb{Z}_p$. Put $U_n = F(w_n)$ and $V_n = F(w_n + w_{n-1}) - U_n - U_{n-1}$. Since $r_n \to \alpha$ in $\mathbb{Q}_p$, we have $v_p(p_n - \alpha' q_n) = e_0 - s_n + v_p(\alpha - \alpha')$ for large n. Factoring F gives

$$v_p(U_n) = e_n + d, \qquad V_n^2 - \Delta = 4U_nU_{n-1}, \qquad V_{n+1} - V_n = 2a_nU_n. \tag{5.1}$$

The second identity is invariance of the discriminant under the basis (w_n, w_{n-1}). The last follows by bilinearity. The numbers U_n belong to $\mathbb{Z}[1/p]$ and are eventually nonzero integers. For all large n, V_n is integral since it is rational and V_n^2 is integral.

Put $T_n = q_nq_{n-1}$ and $L_n = T_{n+1} - T_n = a_nq_n^2$. The intervals with endpoints r_n, r_{n+1} are nested and have lengths $1/T_{n+1}$. Their endpoints stay bounded, and $|r_n - \xi| \le 1/T_{n+1}$. Since $p^{e_n}a_n$ is a positive integer,

$$L_n|f(r_n)| = a_n|U_n| \ge p^d \tag{5.2}$$

for all large n. Since f is bounded on these intervals, $T_n \gg n$. If $f(\xi) = 0$, then $|f(r_n)| \ll 1/T_{n+1}$, so $L_n \gg T_{n+1}$ and T_n grows at least exponentially.

Suppose $f(\xi) \ne 0$. The U_n eventually have one sign, and the integers V_n are then strictly monotone by (5.1). Also $|V_n| \ll T_n$ by bilinearity and boundedness of the r_n. In particular, $v_p(V_n^2 - \Delta) = v_p(4) + 2d + e_n + e_{n-1}$ for large n. Fix a dyadic interval $H \le T_n < 2H$, $H \ge 2$, and put $k = \lfloor (2/3)\log_p H \rfloor$. For indices in this interval with $v_p(V_n^2 - \Delta) \le k$,

$$L_nL_{n-1} = a_na_{n-1}T_n^2 \ge p^{-e_n - e_{n-1}}T_n^2 \gg H^{4/3}.$$

Their two adjacent increments have sum $\gg H^{2/3}$. Apart from the first and last index in the interval, the total of these sums is at most $2H$, since every increment is counted at most twice. This accounts for $O(H^{1/3})$ indices.

For each of the remaining indices, one of $V_n - s, V_n + s$ has valuation at most $v_p(2s)$. The other has valuation at least $k + 1 - v_p(2s)$. Thus all the integers V_n in question lie in at most two residue classes modulo $p^{k+1-v_p(2s)}$ for H sufficiently large. Each class contributes $O(1 + Hp^{-k}) = O(H^{1/3})$ integers of size $O(H)$. Strict monotonicity counts each at most once. Summing the bound for the dyadic intervals through T_n gives $n \ll T_n^{1/3}$. This proves the theorem. □

The condition that ξ be a real image of α is equivalent to eventual periodicity. An eventually periodic expansion converges to a real image of α by [7, Theorem 6.5]. Conversely, suppose $\xi = \sigma(\alpha)$ for a real embedding σ. For $j \ge 1$ the Ruban convergents of α_j have a finite real limit $\xi_j \ge a_j > 0$ by [7, Proposition 4.5]. Put $\xi_0 = \xi$. Taking limits gives $\xi_j = a_j + 1/\xi_{j+1}$ for $j \ge 0$. Thus $\xi_j = \sigma(\alpha_j)$ for every j, and $\xi_0 > 0$ as well. The positivity criterion in [7, Theorem 6.5] gives eventual periodicity.

Proposition 5.2. *With the preceding notation, let $Q_n = p^{s_n}q_n$ be the reduced positive denominator of r_n. The following two conditions are equivalent. If they hold, then ξ is transcendental.*

$$\limsup_{n\to\infty} \frac{\log Q_{n+1}}{\log Q_n} > 1, \qquad \limsup_{n\to\infty} \frac{e_n}{s_n} > 0.$$

Proof. The integers $P_n = p^{s_n}p_n$ and Q_n are coprime. Any common prime divides the determinant of the two scaled consecutive columns, whose absolute value is a power of p. If $a_0 \ne 0$, then P_n is a p-adic unit. If $a_0 = 0$, then Q_n is a p-adic unit. The interval bound and $v_p(Q_n) = e_0$ give

$$|P_n - \xi Q_n|\, Q_n\, |P_n - \alpha Q_n|_p\, |Q_n|_p \le Q_n/Q_{n+1}.$$

Indeed $v_p(P_n-\alpha Q_n) = s_n+s_{n+1}-e_0$ and $|P_n-\xi Q_n|Q_n \le Q_n^2/(q_nq_{n+1})$. If ξ were algebraic, the p-adic Subspace Theorem [28], with the forms $X-\xi Y, Y$ at infinity and $X-\alpha Y, Y$ at p, would exclude any fixed power saving in Q_n along infinitely many indices. Indeed the height of (P_n, Q_n) is comparable to Q_n, and finitely many rational lines contain only finitely many primitive vectors. Thus the first condition implies transcendence.

The integers Q_n increase strictly from index two. Boundedness of the positive digits gives $q_n \ll (p+1)^n$, while the two parity subsequences of q_n are bounded below. Hence $\log Q_n \asymp s_n$. Writing $b_n = p^{e_n}a_n$ gives

$$Q_{n+1} = b_nQ_n + p^{e_n+e_{n-1}}Q_{n-1}, \qquad 1 \le b_n < p^{e_n+1}.$$

If $e_n = o(s_n)$, then $\log(Q_{n+1}/Q_n) \le (e_n+e_{n-1}+1)\log p + \log 2 = o(s_n)$. Conversely, if $\log Q_{n+1}/\log Q_n \to 1$, the second term in the recurrence gives $(e_n+e_{n-1})\log p \le \log Q_{n+1} - \log Q_{n-1} = o(\log Q_n)$. This proves the equivalence. □

There is no known implication here from nonperiodicity to either growth condition. For instance, (5.1) gives $p^{e_n+d} \le q_n^2|f(r_n)|$. Thus if $\log q_n = o(n)$, then $e_n = o(s_n)$ even on a nonperiodic orbit.

The same counting argument improves the real error bound of Pejković for Schneider's algorithm.

Corollary 5.3. *Let p be a prime and let $\alpha \in \mathbb{Z}_p^\times$ be quadratic over $\mathbb{Q}$. If R_n/S_n is its nth Schneider convergent and L is the real limit, then $|R_n/S_n - L| \ll_{\alpha,p} n^{-3}$ for $n \ge 1$.*

Proof. Use the integral polynomials $F_n(X) = A_nX^2 + B_nX + C_n$ from the proof of [22, Theorem 2.3]. If $F_0(L) = 0$, that proof gives exponential decay. Otherwise choose the common sign so that $A_n > 0$ eventually. Write $1 \le b_n < p$ for the partial denominators and p^{a_n}, $a_n \ge 1$, for the partial numerators. The common discriminant is $D = s^2$ with $s = 2A_0\alpha + B_0 \in \mathbb{Z}_p \setminus \{0\}$. With $J_n = B_{n+1} - B_n = 2b_nA_n$, the identity $B_n^2 - D = 4p^{a_n}A_nA_{n-1}$ gives, for large n,

$$J_nJ_{n-1} = b_nb_{n-1}p^{-a_n}(B_n^2 - D) \ge p^{-v_p(B_n^2-D)}(B_n^2 - D).$$

The integers B_n eventually increase strictly to infinity. For $H \le B_n < 2H$, put $k = \lfloor (2/3)\log_p H \rfloor$. If $v_p(B_n^2-D) \le k$, then $J_n + J_{n-1} \gg H^{2/3}$. The remaining B_n lie in at most two residue classes modulo $p^{k+1-v_p(2s)}$ for large H. As in Theorem 5.1, summing the adjacent increments gives $O(H^{1/3})$ indices of the first kind, and strict increase gives $O(1+Hp^{-k})$ of the second. Dyadic summation yields $B_n \gg n^3$. Put $\Delta_n = |R_n/S_n - R_{n-1}/S_{n-1}|$. By [22, (2.10)], $\Delta_n^{-1} - \Delta_{n-1}^{-1} \gg b_nA_n = J_n/2$ for all large n. Summing gives $\Delta_n^{-1} \gg B_{n+1} \gg n^3$. Since all partial numerators and denominators are positive, L lies between R_{n-1}/S_{n-1} and R_n/S_n. Hence $|L - R_n/S_n| \le \Delta_n$. □

6. Real conjugates and the rate of convergence

Fix an odd prime p and use Browkin I, Browkin II or the alternating algorithm of Murru and Romeo [14, (5)], numbered (12) in [25]. Here and in the next section, $[a_0; \dots, a_n] = A_n/B_n$ denotes the convergent with its continuant denominator, so that $B_{-1} = 0$, $B_0 = 1$, and $B_n = a_nB_{n-1} + B_{n-2}$. The three algorithms use, respectively, s at every step, s, t alternately with Browkin's correction at the odd steps, and s, t alternately without the correction.

Theorem 6.1. *Let $x \in \mathbb{Q}_p$ be real quadratic, and let z_+, z_- be its two real images. For each of the three algorithms, eventual periodicity is equivalent to exponential real convergence of*

A_n/B_n to one of z_+, z_-. More precisely, on every nonperiodic orbit there are constants $c_x, C_x > 0$ such that, for all sufficiently large n and both signs,

$$|A_n/B_n - z_\pm| \geq c_x(n+2)^{-C_x}.$$

In particular, suppose that for one real conjugate z there is a subsequence $n_k \to \infty$ such that $n_k^M |A_{n_k}/B_{n_k} - z| \to 0$ for every $M > 0$. Then the expansion is eventually periodic. On a nonperiodic orbit for which $A_n/B_n \to z$ for one of the two conjugates, the ratio of successive errors tends to one.

Romeo proved that an eventually periodic expansion converges to a real conjugate and conjectured the converse [25, Proposition 1 and Conjectures 2 and 17]. Explicit nonperiodic Browkin I examples are known for $p = 7, 11$ [21, Theorem 1], and such examples occur in infinitely many distinct real quadratic fields for every $p \geq 7$ [20, Theorem 1]. We prove the lower bound by counting the integral quadratic forms visited by the orbit.

Lemma 6.2. *There are a fixed nonsquare integer $D > 0$, a choice $s_0^2 = D$ in $\mathbb{Q}_p$, and, for all sufficiently large n, integers u_n, v_n with $v_n \neq 0$ such that the complete quotient $x_n = (u_n + s_0)/v_n$ satisfies*

$$u_{n+1} = a_n v_n - u_n, \qquad v_{n+1} = (D - u_{n+1}^2)/v_n, \qquad v_n \mid D - u_n^2.$$

If the orbit is nonperiodic, each pair (u_n, v_n) occurs at most twice and $|u_n| \to \infty$.

Proof. For Browkin I the recurrences and the periodicity criterion in terms of u_n appear in [6, (9) and Proposition 4.1]. We give an argument that also covers the two alternating algorithms. Start with an integral quadratic form $F_0(X, Y)$ having root x and discriminant D. Transport it by $F_{n+1}(X, Y) = -F_n(a_n X + Y, X)$. Its coefficients h_n, k_n, l_n lie in $\mathbb{Z}[1/p]$, its discriminant remains D, and its roots are x_n and its field conjugate x_n'. All three algorithms have $|a_j|_p \geq 1$ for $j \geq 1$, $|a_1|_p > 1$, and $|a_j a_{j+1}|_p > 1$ for $j \geq 1$. The truncations also give $|x_j|_p = |a_j|_p$ for $j \geq 1$. Thus the continuant recurrence gives $|B_j|_p = \prod_{i=1}^{j} |a_i|_p$ by strict ultrametric dominance. In particular $|B_j|_p \to \infty$. The complete-quotient identity gives $|x - A_j/B_j|_p = (|B_j|_p^2 |x_{j+1}|_p)^{-1}$ for $j \geq 1$, so the convergents tend to x in $\mathbb{Q}_p$. Inverting the prefix at x' gives

$$x_n' = -\frac{A_{n-2} - x' B_{n-2}}{A_{n-1} - x' B_{n-1}}.$$

Since $A_j/B_j \to x \neq x'$ in $\mathbb{Q}_p$, for all large n this shows $|x_n'|_p = |a_{n-1}|_p^{-1} \leq 1$ and $|x_n'|_p < |x_n|_p$. Consequently $|x_n - x_n'|_p = |x_n|_p \geq 1$. The discriminant identity gives $|h_n|_p = |s_0|_p/|x_n|_p$. The sum and product of the roots then give $|k_n|_p, |l_n|_p \leq |s_0|_p \leq 1$. Thus all three coefficients are integers from this point on.

Set $u_n = -k_n$ and $v_n = 2h_n$, choosing the sign of s_0 so that $x_n = (u_n + s_0)/v_n$ at the first index under consideration. Indeed $u_{n+1} = a_n v_n - u_n$ and $v_n v_{n+1} = D - u_{n+1}^2$ by the transformation of forms. Thus $1/(x_n - a_n) = (u_{n+1} + s_0)/v_{n+1}$, which preserves the choice of s_0, while $D - u_n^2 = -4h_n l_n$ gives the divisibility. A repeated triple $(u_n, v_n, n \bmod 2)$ gives the same complete quotient at the same phase and hence an eventual period. For a fixed u the integer v is a signed divisor of $D - u^2 \neq 0$. This proves the final assertions. □

Proposition 6.3. *Suppose the orbit is nonperiodic, and label z_+, z_- so that s_0 has real images $\sqrt{D}, -\sqrt{D}$, respectively. With $q_n = A_n/B_n$ and $R_n = (q_n - z_+)/(q_n - z_-)$, there is N such that R_n has constant sign for $n \geq N$ and*

$$\log|R_n| + 2\sqrt{D} \sum_{j=N}^{n+1} u_j^{-1} \quad \textit{has a finite limit.}$$

Thus q_n tends to z_+ or z_- precisely when the partial sums of the displayed series tend to $+\infty$ or $-\infty$, respectively. The convergents have a projective real limit precisely when these sums have a limit in $[-\infty,+\infty]$. In the finite-sum case the limit differs from both conjugates and is finite unless $R_n \to 1$.

Proof. Write the finite-tail identity at the two real embeddings as $(A_n - z_\pm B_n)x_{n+1}^{\pm} = -(A_{n-1} - z_\pm B_{n-1})$. Division yields, for all sufficiently large n,

$$\frac{R_n}{R_{n-1}} = \frac{u_{n+1} - \sqrt{D}}{u_{n+1} + \sqrt{D}}.$$

The factors are eventually positive. The number of indices for any fixed u is at most $4\tau(|u^2 - D|)$, with τ the divisor function. As $\tau(m) \le 2\sqrt{m}$, we have $\sum_{j\ge N} |u_j|^{-3} < \infty$. The assertion follows on summing $\log|(u - \sqrt{D})/(u + \sqrt{D})| = -2\sqrt{D}/u + O_D(|u|^{-3})$ and inverting the fractional linear map $q \mapsto (q - z_+)/(q - z_-)$. □

Proof of Theorem 6.1. Write $A = \max(1, \sup_j |a_j|)$, which is finite for each algorithm. We show that

$$\left|\sum_{j=N}^{n+1} \frac{1}{u_j}\right| \ll_{D,A} \log(n+2) \tag{6.1}$$

after increasing N so that $u_j^2 > 2D$ throughout the tail. Let $\theta = 1/(4(A+1))$. Mark the edge $(j, j+1)$ if $|v_j| \le \theta \min(|u_j|, |u_{j+1}|)$. No two marked edges share a vertex, since $|v_{j-1}v_j| = u_j^2 - D > u_j^2/2$. At a marked edge the recurrence gives $|u_j + u_{j+1}| \le A|v_j|$ and $|u_j| \le (1 + A\theta)|u_{j+1}|$. Therefore

$$\left|\frac{1}{u_j} + \frac{1}{u_{j+1}}\right| \le A(1 + A\theta)\frac{|v_j|}{u_j^2}.$$

At a vertex j belonging to no marked edge both $|v_{j-1}|$ and $|v_j|$ exceed $\theta|u_j|/2$. Indeed a smaller $|v_j|$ would give $|u_{j+1}| \ge (1 - A\theta/2)|u_j| \ge |u_j|/2$ and mark the right edge. The same argument with $u_{j-1} = a_{j-1}v_{j-1} - u_j$ marks the left edge if $|v_{j-1}|$ is too small. The product formula then gives $|v_j| \asymp_A |u_j|$ at every unmatched vertex.

Let $\rho(d) = \#\{r \bmod d : r^2 \equiv D \pmod d\}$. We recall the estimate $\sum_{d\le X} \rho(d) \ll_D X$ from the divisor problem for quadratic polynomials [12, Lemma 2]. To see it directly, let χ be the nonprincipal quadratic character of $\mathbb{Q}(\sqrt{D})$. For $\gcd(d, 2D) = 1$, $\rho(d) \le (1 * \chi)(d)$ by the prime-power formulas. The nonnegative function $1 * \chi$ has partial sums $O_D(X)$, since $\sum_{b\le X} \chi(b)\lfloor X/b\rfloor = X\sum_{b\le X} \chi(b)/b + O(X)$, and χ has bounded partial sums. At each prime $l \mid 2D$ the numbers $\rho(l^k)$ are bounded in k. For $k > v_l(D)$ the valuation of a root is forced to be $v_l(D)/2$ whenever a root exists. After dividing out this fixed power, the unit congruence has at most two roots for odd l, or four for $l = 2$. The sum of the reciprocals of integers supported on the finitely many primes dividing $2D$ is finite. Multiplicativity now gives the estimate.

For $H \le |u_j| < 2H$ count visits by the state (u_j, v_j), whose multiplicity is at most two. For fixed $d = |v_j|$ there are $O(\rho(d)(H/d + 1))$ such visits. At unmatched vertices $d \asymp_A H$, so there are $O_{D,A}(H)$ of them and their absolute contribution to (6.1) is $O_{D,A}(1)$ per dyadic range. At marked edges with $H \le |u_j| < 2H$ the sum of the absolute values of the paired contributions is at most a constant times

$$\frac{1}{H^2}\sum_{d\le 2\theta H} d\,\rho(d)(H/d + 1) \ll_{D,A} 1.$$

A finite interval cuts at most two marked edges, giving bounded endpoint contributions. Sum over the $O(\log(n+2))$ dyadic ranges with $H \le n + 2$. In the remaining ranges each

singleton or pair contributes $O_A(1/(n+2))$, and there are at most $n+2$ terms. This proves (6.1).

Proposition 6.3 now gives $|\log|R_n|| \ll_x \log(n+2)$. Since $q_n - z_+ = (z_+ - z_-)R_n/(1-R_n)$ and $q_n - z_- = (z_+ - z_-)/(1-R_n)$, this gives the claimed lower bounds after increasing the constant. When $q_n \to z_+$, the quotient of successive errors tends to one by the recurrence for R_n and $q_n - z_- \to z_+ - z_-$. Interchanging the roots gives the other case.

For an eventually periodic word, let H be the period matrix after a prefix, doubling the period if necessary to make its determinant one. Its two real fixed points are the two irrational conjugates of the complete quotient, unless H is scalar. The scalar case would make all convergents along a residue class of the period equal to one rational projective point, contrary to their p-adic convergence to the irrational input. Thus H has distinct real eigenlines and, since $\det H = 1$, distinct eigenvalue moduli. The powers of H send every rational line exponentially to the attracting eigenline, as the repelling line is irrational. This applies to each of the finitely many positions in a period. Reinserting a rational prefix preserves the rate at these irrational real points. □

The same count gives a lower bound for the sum of the absolute values of the digits. For every real quadratic orbit of any of the three algorithms there is a constant C_x such that

$$\sum_{j=1}^{n} |a_j| \geq \log(n+1) - C_x \qquad (n \geq 1).$$

On a periodic tail this sum grows linearly. Otherwise put $s_n = \sum_{i=0}^{n-1} |a_i|$. In Euclidean operator norm, $\|M(a)\| = \exp(\operatorname{arsinh}(|a|/2)) \leq e^{|a|/2}$. The leading coefficient of the transported form F_j in Lemma 6.2 is, up to sign, the value of F_0 at the first column of $M(a_0)\cdots M(a_{j-1})$. Hence $|v_j| \leq H = Ce^{s_n}$ for $j \leq n$, with $C \geq 1$ depending only on F_0. For a sufficiently large $j \leq n$ put $d = |v_j|$. Then $u_j^2 \equiv D \pmod d$ and $|u_j| \leq \sqrt{D + Hd}$, since $D - u_j^2 = v_j v_{j-1}$. Each pair (u_j, v_j) occurs at most twice. Counting the $\rho(d)$ residue classes and summing over d gives

$$n \ll_x 1 + \sum_{d \leq H} \rho(d)(1 + \sqrt{H/d}) \ll_x H.$$

The last bound follows by partial summation from $\sum_{d \leq t} \rho(d) \ll_D t$. Taking logarithms proves the assertion.

Corollary 6.4. *If the digits of a real quadratic orbit of any of the three algorithms eventually have one sign, its convergents have a projective real limit, with error $O(n^{-3})$ in projective distance. In the nonperiodic case this limit differs from both real conjugates. If all digits from a_1 on have one sign, the limit is finite.*

Proof. Choose $N \geq 1$ so that a_{N+j} has a fixed sign σ for $j \geq 0$. The positive continued fraction with digits $c_j = |a_{N+j}|$ has quadratic p-adic value σx_N. Its consecutive real convergents determine nested intervals in $[c_0, c_0 + 1/c_1]$. Since $|x_{N+j}|_p = |c_j|_p \geq 1$ and $|c_j c_{j+1}|_p > 1$, the valuation computation in Theorem 5.1 applies with $e_j = -v_p(c_j) \geq 0$. In its notation, (5.2) gives $T_{j+1} - T_j \gg 1$, since f is bounded on the displayed interval. Thus the interval lengths $1/T_{j+1}$ tend to zero. The rest of the proof of Theorem 5.1 gives $1/T_{j+1} = O(j^{-3})$.

Restoring the sign gives a finite real limit η for the original tail, with $|\eta| \geq c_0 > 0$. The fixed prefix is Lipschitz in angular distance on the real projective line. Its image of η is finite unless $B_{N-1}\eta + B_{N-2} = 0$. For $N = 1$ this denominator is η.

For a nonperiodic orbit $|u_n| \to \infty$ and the recurrence for v_{n+1} shows that v_n eventually alternates in sign. As in the proof of [2, Proposition 26] for Browkin I, $g_n = (-1)^n u_n$ has increments $(-1)^{n+1} a_n v_n$ of constant sign. It is eventually monotone, of constant sign,

and $|g_n| \to \infty$. The alternating-series test gives convergence of $\sum 1/u_n = \sum(-1)^n/g_n$. Proposition 6.3 now excludes both conjugates. □

Corollary 6.5. *Write $e_n = -v_p(a_n)$, and fix $\epsilon > 0$. Along every nonperiodic real quadratic orbit of the three algorithms,*

$$|\log|R_n|| \ll_{x,\epsilon} 1 + \sum_{j=N}^{n+1} p^{-(e_j+e_{j-1})/(1+\epsilon)}.$$

If the series on the right converges, the convergents have a projective real limit distinct from both conjugates. A sufficient digit condition is $e_j + e_{j-1} \geq (1+\delta)\log_p j$ eventually for some $\delta > 0$.

Proof. For the fixed p-adic root s_0 of D and all integers m,

$$p^{v_p(m^2-D)} \ll_{D,p,\epsilon} (1+|m|)^{1+\epsilon}.$$

Indeed the two-place Subspace Theorem [28], applied to $(m,1)$ with forms X, Y at infinity and $X - s_0Y, Y$ at p, bounds $|m - s_0|_p$ below by a constant times $(1+|m|)^{-1-\epsilon}$. Each exceptional rational line contains at most one $(m,1)$, and s_0 is irrational. Applying the bound also to $-s_0$ and using $\min\{v_p(m-s_0), v_p(m+s_0)\} \leq v_p(2s_0)$ gives the displayed estimate.

In Lemma 6.2, $v_p(v_j) = v_p(2s_0)+e_j$ eventually, since $|x_j - x_j'|_p = p^{e_j}$. Substituting $m = u_j$ in the preceding estimate and using $D - u_j^2 = v_j v_{j-1}$ gives $|u_j|^{-1} \ll_{x,\epsilon} p^{-(e_j+e_{j-1})/(1+\epsilon)}$ for large j. Proposition 6.3 proves the claims, taking $0 < \epsilon < \delta$ in the last assertion. □

7. Almost-sure real convergence

Romeo [25, Conjecture 4] asks whether $|B_n|$ tends to infinity with probability one for the three algorithms when $p \geq 5$. We use additive Haar measure on $\mathbb{Q}_p$. The quadratic inputs considered in [25, Assumption 3] form a countable set of Haar measure zero.

Theorem 7.1. *For each odd prime p and each of Browkin I, Browkin II and the alternating algorithm of Murru and Romeo* [14, Algorithm (5)]*, there is a constant $\lambda > 0$ such that, for Haar-almost every $x \in \mathbb{Q}_p$, the convergents $q_n = A_n/B_n$ have a finite transcendental real limit L and*

$$\lim_{n\to\infty} \frac{\log|B_n|}{n} = \lambda, \qquad \lim_{n\to\infty} \frac{\log|q_n - L|}{n} = -2\lambda.$$

The irrationality exponent of L is finite.

For $k \geq 0$, let S_k be the set of m/p^k with $m \in \mathbb{Z}$, $p \nmid m$ and $|m| < p^{k+1}/2$. For $k \geq 1$, let T_k be the corresponding set with $|m| < p^k/2$. Write $S = \bigcup_{k\geq 1} S_k$ and $T = \bigcup_{k\geq 1} T_k$. In particular, $S_0 = \Sigma_p \setminus \{0\}$.

Lemma 7.2. *Under normalized Haar measure on any coset $a_0 + p\mathbb{Z}_p$ with $s(a_0) = a_0$, the pairs (a_{2j+1}, a_{2j+2}), $j \geq 0$, are independent and identically distributed. Each allowed pair (u,v) has probability $|u|_p^{-2}|v|_p^{-2}$. The sets of allowed pairs are*

Browkin I	$S \times S$,
Browkin II	$(T \times S_0) \ \cup \ \{(b - \operatorname{sgn} b, \operatorname{sgn} b) : b \in T\}$,
Murru–Romeo	$T \times (S_0 \cup S)$.

Proof. Put $y_j = \alpha_{2j} - a_{2j} \in p\mathbb{Z}_p$. The inverse branch for the next pair (u,v) sends $z = y_{j+1}$ to

$$y_j = \frac{1}{u + 1/(v+z)}, \qquad z \in p\mathbb{Z}_p.$$

Here $\alpha_{2j+2} = v + z$, so $s(\alpha_{2j+2}) = v$. In Browkin I, $|v|_p > 1$ gives $1/(v+z) \in p\mathbb{Z}_p$, and the preceding digit is u. The Browkin I branches $y \mapsto 1/y - u$ are fractional linear maps of the type considered by Rao and Yasutomi [23]. The cylinder argument of Choudhuri and Makadiya [8] for Ruban's representatives (Lemmas 13 and 15 of the preprint) also applies to balanced representatives. For Murru–Romeo, $|v|_p \geq 1$ gives $1/(v+z) \in \mathbb{Z}_p$, so the preceding odd truncation is $u \in T$.

In Browkin II the next even quotient is a unit. If the odd truncation $b \in T$ is uncorrected, its remainder $1/(v+z)$ is a unit and every $v \in S_0$ is possible. If it is corrected, the odd digit is $u = b - \operatorname{sgn} b$, and its remainder is congruent to $\operatorname{sgn} b$ modulo p. Thus $v = \operatorname{sgn} b$. Conversely, with this value of v we have $u + 1/(v+z) \in b + p\mathbb{Z}_p$, which activates the correction. These conditions exhaust the possibilities. Indeed, an odd complete quotient has norm greater than one. Its remainder belongs to $p\mathbb{Z}_p$ in Browkin I, to $\mathbb{Z}_p^\times$ in Browkin II and to $\mathbb{Z}_p$ in Murru–Romeo.

On each branch $|v+z|_p = |v|_p \geq 1$ and $|u + 1/(v+z)|_p = |u|_p > 1$. Inversion sends a ball $c + r\mathbb{Z}_p$ with $|r|_p < |c|_p$ onto $c^{-1} + (r/c^2)\mathbb{Z}_p$ and scales distances by $|c|_p^{-2}$. Each branch therefore maps $p\mathbb{Z}_p$ onto a ball with relative Haar measure $|u|_p^{-2}|v|_p^{-2}$. Conditional on this branch, the new remainder y_{j+1} is again uniform on $p\mathbb{Z}_p$. The branch balls are disjoint and cover $p\mathbb{Z}_p$ up to the countable set of terminating inputs. Since y_0 is uniform on $p\mathbb{Z}_p$, iteration gives the asserted pair law. □

Proof of Theorem 7.1. Fix the initial coset. Write $G_j = M(a_{2j-1})M(a_{2j})$ for $j \geq 1$. These matrices are independent and identically distributed in $\mathrm{SL}_2(\mathbb{R})$. All digit matrices and their inverses have uniformly bounded real norm, since the digits lie in a bounded real interval. In particular, the law μ of G_j has a finite exponential moment. Put $h = 1/p$ and take $e = h$ for Browkin I and $e = 1$ for the other two algorithms. By Lemma 7.2, the support contains $Q_+ = M(h)M(e)$ and $Q_- = M(-h)M(e)$. The trace of Q_+ is $2 + he > 2$. A finite invariant set on $\mathbb{P}^1(\mathbb{R})$ would be invariant under the group generated by the support. The translation

$$Q_+ Q_-^{-1} = \begin{pmatrix} 1 & 2h \\ 0 & 1 \end{pmatrix}$$

would force it to lie in $\{\infty\}$, whereas $Q_+\infty = h + 1/e$ is finite. The semigroup is therefore strongly irreducible and contains a proximal element. Its top Lyapunov exponent γ is positive by Furstenberg's theorem [11, Theorem 8.6].

Put $H_m = G_1 \cdots G_m$ and equip the projective line with the distance

$$d([v],[w]) = \frac{|\det(v,w)|}{\|v\|\,\|w\|}.$$

For every $\epsilon > 0$ there are $c, C > 0$ such that, uniformly in nonzero rows f and columns v,

$$\mathbb{P}\left(\left|\log \frac{|fH_m v|}{\|f\|\,\|v\|} - m\gamma\right| > m\epsilon\right) \leq Ce^{-cm}, \qquad \log 0 = -\infty.$$

Indeed, the logarithm of the coefficient ratio equals $\log(\|H_m v\|/\|v\|) + \log d(H_m[v], \ker f)$. The two bounds of [9, Proposition 2.1] apply with $\epsilon/2$. Reversing the order of an iid sample preserves its law.

Put $w = (1,0)^{\mathsf{T}}$. Apply the estimate with $v = w$ and with $v = M(a_{2m+1})w$. The latter vector is independent of H_m and has norm between 1 and a fixed constant. Applying Borel–Cantelli with $\epsilon = 1/k$, $k \geq 1$, shows that for each fixed $f \neq 0$, almost surely

$$\lim_{n\to\infty} \frac{1}{n} \log |fM(a_1)\cdots M(a_n)w| = \lambda, \qquad \lambda = \frac{\gamma}{2}.$$

Taking $f = (0,1)M(a_0) = (1,0)$ gives the assertion for B_n. Almost surely all sufficiently late denominators are nonzero, and

$$|q_n - q_{n-1}| = |B_n B_{n-1}|^{-1} = \exp(-2\lambda n + o(n)).$$

Summation gives a finite limit L and $\limsup_{n\to\infty} n^{-1} \log|q_n - L| \le -2\lambda$.

With $f = (0,1)$ the same argument gives, simultaneously for all $j \ge 0$, a real limit Z_{2j+1} of the tail beginning at a_{2j+1}. These limits have a common law ν. The identity $Z_1 = G_1 Z_3$ and the independence of Z_3 from G_1 make ν the stationary measure of μ. By [9, Proposition 2.2], there are $C, \delta > 0$ such that $\nu\{z : d(z,t) < r\} \le Cr^\delta$ for every projective point t and $0 < r < 1$. Thus ν gives mass zero to each point. Since the real algebraic numbers are countable, the Z_{2j+1} are all almost surely transcendental. The identities $Z_{2j} = a_{2j} + 1/Z_{2j+1}$ for $j \ge 1$ and $L = a_0 + 1/Z_1$ give the same conclusion for the even tails and for L.

On the fixed initial coset, the law of L is the image of ν under the projective transformation $z \mapsto a_0 + 1/z$. Its inverse is Lipschitz for d, so an interval of real length $r \le 1$ has probability $O_{a_0}(r^\delta)$. Fix an integer $K \ge 1$ and $\tau > 2/\delta$. For each $b \ge 1$ there are $O_K(b)$ integers a with $|a/b| \le K+1$. Since $\sum_{b\ge1} b^{1-\tau\delta} < \infty$, Borel–Cantelli gives probability zero to the event that $|L| \le K$ and $|L - a/b| < b^{-\tau}$ for infinitely many rationals a/b in lowest terms. Taking all K proves the assertion about the irrationality exponent.

Taking $t = 0, \infty$ gives $\nu\{|z| > R\} + \nu\{|z| < R^{-1}\} \ll R^{-\delta}$ for $R \ge 2$. With $R = \exp(\epsilon j)$, Borel–Cantelli gives $\left|\log|Z_{2j+1}|\right| = o(j)$ almost surely. Since all digits are bounded, the even-tail identity gives $\log^+|Z_j| = o(j)$ over both parities. The complete-tail formula now yields

$$|q_n - L| = \frac{1}{|B_n|\,|B_n Z_{n+1} + B_{n-1}|} \ge \exp(-2\lambda n - o(n)).$$

This proves the error exponent. The pair law is the same on every initial coset. These cosets form a countable partition of $\mathbb{Q}_p$, giving the conclusion for additive Haar measure. □

Proposition 7.3. *For any Browkin I digit $a = a_n$ with $n \ge 1$, under the Haar law of Lemma 7.2,*

$$\mathbb{P}(v_p(a) = -k) = (p-1)p^{-k}, \qquad \mathbb{E}(|a| \mid v_p(a) = -k) = \frac{p}{4} + \frac{1}{4p^{2k}} \quad (k \ge 1).$$

Consequently $\mathbb{E}|a| = p/4 + 1/(4(p^2+p+1))$ and $\mathbb{E}v_p(a) = -p/(p-1)$.

Proof. The set S_k has $(p-1)p^k$ elements. Since $\sum_{k\ge1} |S_k| p^{-2k} = 1$, the product formula in Lemma 7.2 gives each digit in S_k probability p^{-2k}. Given $v_p(a) = -k$, put $H = (p^{k+1}-1)/2$ and $J = (p^k-1)/2$. Summing $|m|$ for $|m| \le H$ and removing multiples of p gives

$$\mathbb{E}(|a| \mid v_p(a) = -k) = \frac{H(H+1) - pJ(J+1)}{(p-1)p^{2k}} = \frac{p}{4} + \frac{1}{4p^{2k}}.$$

Geometric summation gives the remaining formulas. The calculation in [25, Theorem 26] includes numerators divisible by p in the conditional mean. The positive quantity in [25, Proposition 24] is the mean of $-v_p(a)$. □

Remark 7.4. There are quadratic inputs with bounded real denominators for every odd prime. For Browkin I, take $a = c/p$, $1 \le c \le (p-1)/2$. By Hensel's lemma $Y^2 - cY + p^2$ has a root $Y \equiv c \pmod{p^2}$. Then $x = Y/p$ satisfies $x^2 - ax + 1 = 0$ and $s(x) = a$. As $1/(x-a) = -x$, the period is $(a, -a)$. For Browkin II and Murru–Romeo, let y be the root of $Y^2 - Y + p$ congruent to 1 modulo p. The even digit is 1 and $1/(y-1) = -y/p$. Since $(-y/p) - (-1/p) = (1-y)/p = 1/y$ is a unit, $t(-y/p) = -1/p$ and the next even quotient is again y. The period matrices have determinant one and traces $2 - a^2$ and

$2 - 1/p$, respectively. Both traces have absolute value less than two, so the matrix powers and all continuant denominators are bounded. Both quadratic fields are imaginary.

The continuant B_n is a rational number. Let D_n denote the positive denominator of the convergent q_n in lowest terms.

Corollary 7.5. *For Browkin I, Browkin II and the alternating algorithm of Murru and Romeo, respectively, let κ have the values*

$$\frac{p}{p-1}, \qquad \frac{p}{2(p-1)}, \qquad \frac{p+1}{2(p-1)}.$$

In the notation of Theorem 7.1, for Haar-almost every $x \in \mathbb{Q}_p$ we have $n^{-1} \log D_n \to \lambda + \kappa \log p$ and

$$\lim_{n\to\infty} \frac{-\log|L - q_n|}{\log D_n} = \frac{2\lambda}{\lambda + \kappa \log p} < 1, \qquad \lim_{n\to\infty} \frac{-\log|x - q_n|_p}{\log D_n} = \frac{2\kappa \log p}{\lambda + \kappa \log p} > 1.$$

In particular, $D_n|L - q_n| \to \infty$ almost surely.

Proof. Write $k_j = -v_p(a_j)$ for $j \geq 1$. Every odd digit has $\mathbb{P}(k_j = k) = (p-1)p^{-k}$ for $k \geq 1$, by Lemma 7.2. At even indices Browkin I has the same law, Browkin II has $k_j = 0$, and Murru–Romeo has $\mathbb{P}(k_j = k) = (p-1)p^{-k-1}$ for $k \geq 0$. Thus κ is half the mean of $k_1 + k_2$. The value $p/(p-1)$ also occurs for Ruban's representatives over $\mathbb{Q}_p$ in Choudhuri and Makadiya [8], Proposition 23 of the preprint. The strong law for the independent digit pairs and Borel–Cantelli for their geometric tails give $n^{-1} \sum_{j=1}^{n} k_j \to \kappa$ and $k_{n+1}/n \to 0$ almost surely.

The continuant recurrence gives $|B_n|_p = p^{\sum_{j=1}^{n} k_j}$, since $|a_j a_{j+1}|_p > 1$. The determinant identity implies that A_n and B_n have no common prime factor different from p in $\mathbb{Z}[1/p]$. Hence

$$D_n = |B_n|\,|B_n|_p \max(1, |q_n|_p).$$

The last factor is bounded since $q_n \to x$ in $\mathbb{Q}_p$. Moreover $|x - q_n|_p = (|B_n|_p^2 |\alpha_{n+1}|_p)^{-1}$ and $|\alpha_{n+1}|_p = p^{k_{n+1}}$. These identities and Theorem 7.1 give the three limits.

It remains to show $\lambda < \kappa \log p$. For Browkin I the absolute values of the entries of each $M(a_j)$ are bounded by the corresponding entries of $M(p/2)$, whose spectral radius is less than p. For the other two algorithms the absolute values of the entries of each digit-pair matrix are bounded by those of $M(U)M(V)$, with $(U, V) = (1, (p-1)/2)$ for Browkin II and $(U, V) = (1/2, p/2)$ for Murru–Romeo. Both comparison matrices have determinant one and trace $2 + UV < p + p^{-1}$, so their spectral radii are less than p. The same entrywise bounds hold for products. It follows that $\lambda < \log p$ for Browkin I and $2\lambda < \log p$ for the other two algorithms, as required. □

8. The cubic case of the multidimensional periodicity problem

We use the inversion and row reduction of Saito, Tamura and Yasutomi and evaluate the rational translation on the resulting coordinates. Formula (4) of arXiv:1705.06122v3, the version of [27] used for the numbered results below, evaluates the translation on the input. An earlier affine map $\Phi_{3A}^{[\varepsilon,z]}$ in arXiv:1705.06122v1, Sect. 5, also reduces the constants after the row operations. It uses the first coordinate as pivot and orders the nonconstant columns by increasing powers of z. Throughout this section p is any prime. Write $v = v_p$, put $v(0) = +\infty$, and let $R = \mathbb{Q} \cap \mathbb{Z}_p$. For $x \in \mathbb{Q}_p$, take its digits in $\{0, \ldots, p-1\}$. Write $[x]_p$ for its terms of degree at most zero and $\langle x \rangle_p = x - [x]_p$. The possible values of $[x]_p$ form $\mathcal{D} = \mathbb{Z}[1/p] \cap [0, p)$, a set of representatives modulo $p\mathbb{Z}_p$.

Let $K = \mathbb{Q}(z) \subset \mathbb{Q}_p$ have degree three, where $z \in p\mathbb{Z}_p$ satisfies Condition H of Saito, Tamura and Yasutomi. Thus its monic minimal polynomial is

$$f(X) = X^3 + aX^2 + bX + cp^k, \qquad a \in R, \quad b, c \in R^\times, \quad k = v(z) > 0.$$

Every cubic field contained in $\mathbb{Q}_p$ has such a generator by [27, Proposition 2.3]. For a $\mathbb{Q}$-basis $1, x, y$ of K, set $m_y = v(y)$ and $j = \max(m_y - v(x), 0)$. First take $p^j x/y$ and p^{m_y}/y and subtract from each its digit of degree zero. Both resulting elements belong to $p\mathbb{Z}_p$. Write them in the basis $z^2, z, 1$ and reduce their first two columns by row operations in $\mathrm{GL}_2(R)$ as in [27, Sect. 4.4]. Apply the same operations to the constant column. Finally subtract $\langle c_0 \rangle_p$ from each coordinate with rational constant c_0. Denote this map by T. If $G_2(\alpha)$ is the vector after inversion and subtraction of the digits of degree zero, then our translation is $\gamma'(G_2(\alpha))$ in the notation of [27, Sect. 4.4]. We take the sign in the inversion to be $+1$. An initial basis may be any basis in K. After one step the two coordinates belong to $p\mathbb{Z}_p$. We use periodicity in the sense of [27, Sect. 3], namely equality of two remainders at distinct indices.

Theorem 8.1. *For every prime p, every cubic generator z satisfying Condition H and every basis $1, x, y$ of $\mathbb{Q}(z)$, the sequence $T^n(x, y)$ is eventually periodic.*

Proof. We show that only finitely many reduced coefficient matrices occur along each orbit. After one step the pair has the form

$$x = p^d z^2 + uz + C, \qquad y = p^e z + D,$$

where $d, e \in \mathbb{Z}$, u contains only digits of degree less than e, and $C, D \in \mathcal{D}$. Indeed, multiplication by the pivot y sends $1, x/y, 1/y$ to the basis $y, x, 1$. Scaling the inverted coordinates by nonzero rationals, adding rational constants and performing invertible row operations preserve independence with 1. Thus both diagonal pivots are nonzero. Since $x, y \in p\mathbb{Z}_p$, the constants are $C = [-p^d z^2 - uz]_p$ and $D = [-p^e z]_p$.

Write $y = p^e(z + t)$. If $e + k > 0$, then $D = t = 0$. Otherwise $v(D) = e + k$ and $v(t) = k$. In both cases $v(z + t) = v(y) - e$. Since $f(z) = 0$, we have

$$\frac{1}{z+t} = -\frac{z^2 + (a-t)z + b - at + t^2}{f(-t)}.$$

The numerator evaluated at z is a p-adic unit, whence $v(f(-t)) = v(z + t)$.

Put $P(X) = p^d X^2 + uX + C$, $r = P(-t)$ and $j = \max(v(y) - v(x), 0)$. The rows of nonconstant coefficients after inversion generate over R a lattice with basis

$$V = (1, a - t), \qquad \rho V + p^h(0, 1), \qquad h = d + j - e, \quad v(\rho) = v(r) + j - v(y). \tag{8.1}$$

Indeed the row from $p^{v(y)}/y$ is $-p^{v(y)-e}V/f(-t)$, a unit multiple of V. Division of $P(X)$ by $X + t$ gives the other row with $\rho = -p^{j-e}r/f(-t)$. Write d', e', u' for the next reduced entries. The first column and the determinant give

$$d' = \min(0, v(\rho)), \qquad e' = h - d'.$$

If $d' = 0$, subtract the term ρV in (8.1). It follows that u' is the representative of $a - t$ modulo $p^{e'}R$ with digits of degree less than e'. In particular $u' \in R$. After two steps every lattice under consideration has a primitive vector $(1, A)$ with $A \in R$, by (8.1). Here primitive means that it is a member of an R-basis of the lattice. In particular $d \leq 0$ from the second step onward.

For a reduced matrix with rows $(p^d, u), (0, p^e)$, put

$$m = \min(d, e, v(u)), \qquad B = d + e - 2m.$$

The minimum valuation amongst all entries and the determinant valuation are unchanged by invertible row operations over R. Hence m and B can be read from any basis of the

lattice. Suppose first that $e \geq 0$, so $t = 0$ and $v(y) = e + k$. We have $v(C) \geq m + k$ and $v(x) \geq m + k$. Indeed $p^d z^2 + uz$ has valuation at least $m + k$. If its valuation is positive then $C = 0$. Otherwise its valuation equals $v(C)$ and $v(x) \geq 1$. Consequently $j \leq e - m$, and both $v(\rho)$ and h are at least $m + j - e$. Equation (8.1) now gives $m' \geq m + j - e$ and

$$B' = h - 2m' \leq B - j.$$

Suppose next that $e < 0$ and $d < 0$, at a step where the primitive vector $(1, A)$ is available. Its basis coefficients in the reduced rows are p^{-d} and $(A - p^{-d}u)/p^e$. The first is in pR, so the second is a unit. Since $A \in R$ and $e < 0$, this implies $v(u) = d + e$. Now

$$x - r = (z + t)\{p^d(z - t) + u\}, \qquad v(x - r) = v(y) + d.$$

To see the last equality, use $v(z-t) \geq k$ and $v(u) = d+e < d+k$. Put $l = \min(v(x), v(y))$. Since $v(x) \geq l$, the valuations of r and $x - r$ coincide whenever either is less than l. Hence

$$d' = \min(0, v(r) - l) = \min(0, v(y) + d - l) = \min(0, d + j).$$

If $d' < 0$, then $e' = -e > 0$. By the primitive vector at the next step, $p^{-d'}u' \in R$, since its difference from an element of R belongs to $p^{e'}R$. Thus $m' = d'$ and again $B' = B - j$.

It follows that an orbit with $d < 0$ at every step from the second onward has bounded B. Here $m \leq d < 0$. If $e \geq 0$, then $B = (d - m) + (e - m) \geq -m$. If $e < 0$, we found that $v(u) = d + e$, so $m = d + e$ and $B = -m$. Thus both d and e lie between $m \geq -B$ and $m + B \leq B$. All nonzero digits of u have degrees between m and $e - 1$. This gives finitely many possible reduced matrices, and the rational constants are uniquely determined. The orbit is eventually periodic.

It remains to consider an orbit reaching $d = 0$ from the second step onward. We have shown that $u \in R$, so $C = 0$. For $e \geq 0$ one has $t = 0$ and $r = 0$. For $e < 0$ the digit condition gives $u = 0$, so $x = z^2$ and $r = t^2$. Since $v(t) \geq k$, we have $v(r) \geq 2k = v(x)$, including $t = 0$. In either case (8.1) gives $d' = 0$, so d stays zero.

For $e \geq 0$ the recurrence is

$$e' = -\min(e, v(z + u)) \leq 0.$$

For $e = -s < 0$ it gives $e' = s + \max(v(y) - 2k, 0) > 0$ and $u' \equiv a - t \pmod{p^{e'}R}$. At the following step,

$$|e''| = \min(e', v(z + a - t)).$$

Set $L = v(2z + a)$, a finite nonnegative integer. If $s \geq L$, then $v(z + t) = s + v(y) > L$, so $v(z + a - t) = L$. There are only finitely many positive $s < L$, and each determines t uniquely from the second coordinate. Hence the magnitudes of all negative exponents in this part of the orbit are bounded. Each negative exponent also determines the following positive one. If $e = 0$, then $u = 0$ and the pair (z^2, z) is fixed. Thus only finitely many exponents occur. The coefficient u is integral with digits of degree less than e, so it too takes only finitely many values. This proves the result. □

8.1. **The two translations in arbitrary degree.** Now let $K = \mathbb{Q}(z) \subset \mathbb{Q}_p$ have degree $s + 1 \geq 2$, and assume that z satisfies Condition H. Define T as above, using the last coordinate as pivot and the column order $z^s, z^{s-1}, \ldots, z, 1$. Write the equation of z as

$$z^{s+1} + a_1 z^s + \cdots + a_s z + cp^k = 0, \qquad a_1, \ldots, a_s, c \in R, \quad a_s, c \in R^\times, \quad v(z) = k > 0.$$

Write $G_{s,\varepsilon}(\alpha)$ for the last-coordinate inversion with sign $\varepsilon \in \{-1, 1\}$ followed by subtraction of the digits of degree zero, and put $G_s = G_{s,1}$. In formula (4) of [27, Sect. 4.4] the row operation is computed from $G_s(\alpha)$ for either sign and the translation is evaluated on α. If A_α is the matrix of the nonconstant coefficients in the ordered basis $z^s, \ldots, z, 1$ and C_α

is the column of constants, write $U_\alpha \in \mathrm{GL}_s(R)$ for the row operation reducing A_α. Then $\gamma'(\alpha) = -\langle U_\alpha C_\alpha \rangle_p$, with the brackets taken coordinatewise. The resulting map is

$$T_{0,\varepsilon}(\alpha) = U_{G_s(\alpha)} G_{s,\varepsilon}(\alpha) + \gamma'(\alpha).$$

Proposition 8.2. *Let $\ell > p$ be a prime at which the coefficients of the monic minimal polynomial of z are integral, and put $S = \mathbb{Q} \cap \mathbb{Z}_\ell$. Write $\alpha = A(z^s, \dots, z)^t + C$, where $A \in \mathrm{GL}_s(S)$ has last row $(0, \dots, 0, q)$ and $C = (C_1, \dots, C_s)^t \in \mathbb{Q}^s$. Suppose $|C_i|_\ell \le M = |C_s|_\ell > 1$ for all i, with $|\ell|_\ell = 1/\ell$. After n steps of $T_{0,\varepsilon}$, the rational constant in the last coordinate has ℓ-adic absolute value M^{2^n}, even if the signs vary from step to step. In particular the expansion for either fixed sign is not eventually periodic.*

Proof. Every invertible p-reduced matrix has diagonal entries which are powers of p and entries above the diagonal in $\mathbb{Z}[1/p]$. It therefore belongs to $\mathrm{GL}_s(S)$. The nonconstant matrix of $G_{s,\varepsilon}(\alpha)$ is ε times that of $G_s(\alpha)$. Thus after one step the nonconstant matrix is εH with H p-reduced. The translation changes only the constants. The current nonconstant matrix A therefore lies in $\mathrm{GL}_s(S)$ at every step, including the first by hypothesis. Its row operation $U_\alpha = (U_\alpha A)A^{-1}$ also lies in $\mathrm{GL}_s(S)$.

At the current step write $y = \alpha_s = qz + D$, where $D = C_s$ and q is an ℓ-adic unit. This holds initially because A has the stated last row and unit determinant over S. At each later step $q = \pm p^e$ for some integer e. Assume that $|C_i|_\ell \le M = |D|_\ell > 1$ for all i. The inverted coordinates before row reduction are $g_i = a_i \alpha_i / y - \delta_i$ for $i < s$ and $g_s = b/y - \delta_s$, where $b = \varepsilon p^{v_p(y)}$ and $a_i = \varepsilon p^{\max(v_p(y) - v_p(\alpha_i), 0)}$. The δ_i lie between 0 and $p-1$, and $\delta_s \neq 0$ because b/y is a p-adic unit. Define a $\mathbb{Q}$-linear functional μ on the current basis by

$$\mu(1) = \delta_s / b, \qquad \mu(y) = 1, \qquad \mu(\alpha_i) = \delta_i / a_i \quad (i < s).$$

Since $\ell > p$, the first value is an ℓ-adic unit and the others are integral at ℓ. The functional $\lambda(w) = \mu(yw)$ satisfies $\lambda(1) = 1$ and $\lambda(g_i) = 0$ for every i.

From $\alpha = A(z^s, \dots, z)^t + (C_1, \dots, C_s)^t$ and the integrality of A^{-1} we obtain $|\mu(z^j)|_\ell \le M$ for $1 \le j \le s$. The minimal polynomial gives this bound also for $j = s+1$. Moreover $q\mu(z) = 1 - D\mu(1)$ gives $|\mu(z)|_\ell = M$. Consequently

$$|\lambda(z^j)|_\ell = |q\mu(z^{j+1}) + D\mu(z^j)|_\ell \le M^2 \quad (1 \le j \le s), \qquad |\lambda(z)|_\ell = M^2.$$

After the row operations all inverted coordinates are still annihilated by λ. Thus their new constants are the entries of $-A'(\lambda(z^s), \dots, \lambda(z))^t$, where $A' = \varepsilon H$ is the new nonconstant matrix. They have absolute value at most M^2, and the last has absolute value exactly M^2 because the only nonzero entry in the last row of A' is an ℓ-adic unit. All entries of $U_\alpha C$ have absolute value at most M. Since the truncation $[c_0]_p$ of a rational number belongs to $\mathbb{Z}[1/p]$, the entries of the input translation $-\langle U_\alpha C \rangle_p$ also have absolute value at most M. Thus the new constants satisfy the same inequalities with M^2 in place of M, independently of the sign at this step. Induction proves the formula and shows that no two remainders are equal. For either fixed sign, the branch data also fail to be eventually periodic. Indeed, from the first iterate onward the current nonconstant matrix is a p-reduced matrix multiplied by ε, so $U_\alpha = \varepsilon I$. The last entry of $\gamma'(\alpha)$ then has absolute value $|D|_\ell$. □

Corollary 8.3. *For each prime ℓ as in Proposition 8.2, there is a dense set of $\alpha \in \mathbb{Q}_p^s$ with $1, \alpha_1, \dots, \alpha_s$ a $\mathbb{Q}$-basis of K for which $T(\alpha) = (z^s, \dots, z)$ is fixed by T. For the same α and either sign ε, the rational constant in the last coordinate of $T_{0,\varepsilon}^n(\alpha)$ has ℓ-adic absolute value ℓ^{2^n} for every $n \ge 0$.*

Proof. If the nonconstant coefficient matrix of $G_s(\alpha)$ belongs to $\mathrm{GL}_s(R)$, its p-reduced form is the identity. Each output coordinate of T lies in $p\mathbb{Z}_p$ and its nonconstant part

is a positive power of z. Its normalized constant must therefore be zero. This gives $T(\alpha) = (z^s, \dots, z)$. For the power basis the nonpivot ratios are $z^{s-1}, \dots, z$, and

$$p^k/z = -(z^s + a_1 z^{s-1} + \cdots + a_s)/c$$

has integral coefficients at p with leading coefficient a unit. The matrix is thus unimodular and the power basis is fixed. This unimodular-matrix argument for a family with last coordinate z appears in the proof of [27, Theorem 6.2].

Take a target $(x_1, \dots, x_s)$ with all coordinates nonzero. Choose $q \in 1 + \ell\mathbb{Z}[1/p]$ so that qz is arbitrarily close to x_s and has the same valuation. For $i < s$, put $j_i = \max(v(x_s) - v(x_i), 0)$. Choose $r_i \in \mathbb{Z}[1/p]$ so that

$$\beta_i = qp^{-j_i} z(z^{s-i} + r_i)$$

is arbitrarily close to x_i with the same valuation, and set $\beta_s = qz$. These choices are possible by density of $\mathbb{Z}[1/p]$ in $\mathbb{Q}_p$. The nonconstant matrix of β is upper triangular with entries in S and diagonal entries $qp^{-j_1}, \dots, qp^{-j_{s-1}}, q$, all units at ℓ. In particular $1, \beta_1, \dots, \beta_s$ is a basis. The scaled nonpivot ratios are $z^{s-i} + r_i$, and the scaled pivot reciprocal is $(p^{v(q)}/q)(p^k/z)$. Thus the nonconstant coefficient matrix of $G_s(\beta)$ belongs to $\mathrm{GL}_s(R)$.

Replace the last coordinate qz by $qz + t$, leaving the others fixed. For rational t sufficiently close to zero in $\mathbb{Q}_p$, the valuations determining the inversion exponents do not change. The coefficients of $(qz + t)^{-1}$ in the power basis are rational functions of t regular at zero. Indeed the determinant of multiplication by $qz + t$ is nonzero at $t = 0$. Consequently the nonconstant coefficient matrix after inversion varies continuously at zero. Since $\mathrm{GL}_s(\mathbb{Z}_p)$ is open in the space of p-adic matrices, a sufficiently small rational t keeps this matrix in $\mathrm{GL}_s(R)$.

Now take $t = p^N/\ell$ for a sufficiently large integer N. For the resulting vector α we have $T(\alpha) = (z^s, \dots, z)$. Its input coefficient matrix is the same as that of β, its last coordinate is $qz + t$, and its rational constants are zero except for t, with $|t|_\ell = \ell$. Proposition 8.2 gives the claimed growth. Taking the initial approximations sufficiently close and then N sufficiently large places α in any prescribed neighborhood of the target. Such targets are dense in $\mathbb{Q}_p^s$. □

Taking $A = I$ and $C = (0, \dots, 0, p/\ell)^t$ in Proposition 8.2 gives an explicit basis whose expansion is not eventually periodic for every z satisfying Condition H. Thus formula (4) of arXiv:1705.06122v3 gives counterexamples to [27, Conjecture 1] for both signs. In degree two they also contradict [27, Theorem 5.5] for that formula. For example, let $p = 3$, $\ell = 5$ and let $z \in 3\mathbb{Z}_3$ be the root of $X^2 + X + 3$. This polynomial is irreducible over $\mathbb{Q}$ and has a simple root at zero modulo 3. Starting from $z + 3/5$, the first three rational constants for the positive sign, including the initial one, are $3/5$, $18/25$ and $891/625$. For the negative sign they are $3/5$, $21/25$ and $-1572/625$.

For the cubic example take the root $z \in 3\mathbb{Z}_3$ of $X^3 + X + 3$. The polynomial has no rational root and its derivative at zero is a 3-adic unit. For $(z^2, z + 3/5)$ the powers of 5 in the denominators are unbounded under $T_{0,\varepsilon}$ for either sign. The orbit under T is eventually periodic by Theorem 8.1.

The 2018 exposition [35, pp. 69–70, Theorem 7 and Proposition 8] uses the same descending order of powers and writes $\gamma'(\alpha)$. It announces cubic periodicity for generators satisfying $a \in pR$ or $a + c \in pR$, and the existence of such a generator in each embedded cubic field. Both statements are attributed there to a manuscript by Yasutomi then in preparation. The cubic example above has $a = 0$, so the announced periodicity fails for the displayed input translation at either sign. Yasutomi also announced periodicity for every basis in every embedded cubic field in a conference abstract [32]. That abstract does

not specify the transformation. Theorem 8.1 uses the output translation and covers every generator satisfying Condition H.

8.2. **A single pivot rule on a dense set of cubic bases.** In [27, Conjecture 2] the row matrix is the identity and the pivot may be either coordinate. Fix $\varepsilon \in \{-1, 1\}$. For pivot y and other coordinate x, take $\varepsilon p^{v(y)}/y$ and $\varepsilon p^{\max(v(y)-v(x),0)}x/y$ in their respective positions. Subtract their digits of degree zero, then subtract the positive-degree part of each rational constant in the basis $1, z, z^2$. If the nonconstant part of a resulting expression belongs to $p\mathbb{Z}_p$, these subtractions leave its constant term zero.

The calculation for (z, z^2) in [27, Theorem 6.1], with its cyclic permutation of the coordinates, suggests the following choice of pivot for the identity row matrix.

Proposition 8.4. *For every cubic generator z satisfying Condition H there are a pivot rule and a dense set of pairs $(x, y) \in \mathbb{Q}_p^2$ with $1, x, y$ a basis of K such that, for either sign, every pair in this set has preperiod one and least period six.*

Proof. Whenever exactly one coordinate is a rational multiple of z, choose it as pivot. Extend this rule arbitrarily to the other states. Put $W = z^2 + az$. Take

$$(x, y) = (qz, rz^2 + sz), \qquad q, r \in \mathbb{Q}^\times, \quad s \in \mathbb{Q}, \quad v(r) = \min\{v(q), v(rz + s)\}.$$

The three elements $1, x, y$ form a basis since $qr \neq 0$. For $h = \max(v(q) - v(rz + s), 0)$ the first transition gives

$$(R_0W, Q_0z), \qquad R_0 = -\frac{\varepsilon p^{v(q)}}{cq}, \qquad Q_0 = \frac{\varepsilon p^h r}{q}.$$

Both coefficients are units. Here we used $p^k/z = -(z^2 + az + b)/c$. Thereafter write the coordinates in the order (Qz, RW), recording their actual positions separately. Since $v(W) = k + v(z + a) \geq k$, the scaling exponent of the nonpivot ratio is zero. The pivot always lies on Qz and the two positions interchange at each step. In this order the parameters become

$$(Q, R) \longmapsto \left(\frac{\varepsilon R}{Q}, -\frac{\varepsilon}{cQ}\right).$$

Two applications give $(-\varepsilon/(cR), -Q/(cR))$, and the third returns (Q, R). The coordinate positions alternate, since the lines $\mathbb{Q}z$ and $\mathbb{Q}W$ are distinct. Thus the least period is six unless the parameter pair is fixed, in which case it is two. A fixed pair satisfies $Q^3 = -1/c$ and $R = \varepsilon Q^2$.

For density it suffices to approximate a pair (x_0, y_0) of nonzero p-adic numbers. Choose a nonzero rational q arbitrarily close to x_0/z, with the same valuation. If $Q^3 = -1/c$ has a rational solution Q_*, also require $-p^{v(q)}/(cq) \neq Q_*^2$. This excludes at most one q at the prescribed valuation and ensures that (Q_0, R_0) is not fixed for either sign. Put $r = p^{\min(v(x_0/z), v(y_0/z))}$ and choose a rational $s \neq ar$ arbitrarily close to $y_0/z - rz$. Then $v(rz + s) = v(y_0/z)$, and the displayed basis approximates (x_0, y_0) as closely as desired. Its second coordinate does not lie in $\mathbb{Q}W$, so the initial pair is outside the cycle for either sign. □

A directed graph gives a criterion for the existence of one pivot rule that works for all bases. Fix the field, generator and sign. Form the directed graph of ordered bases, with one edge for each legal pivot. A single pivot rule gives eventual periodicity for every basis if and only if each vertex reaches a finite directed cycle. The forward implication follows by following the rule. For the converse, enumerate the simple directed cycles, which is possible since K is countable. Retain each cycle disjoint from all those already retained. Every cycle meets their union, so every vertex has finite directed distance to it. On each

retained cycle follow its edges. Elsewhere choose an edge that decreases the distance to the union. This gives one rule on the whole graph. It extends arbitrarily to the remaining points of K^2, since the iterates of a basis are bases. It remains open whether every basis can reach a cycle.

9. Counterexamples to a conjecture of Murru and Terracini

Murru and Terracini [17, Conjecture 1] asked whether the p-adic Jacobi–Perron algorithm terminates or becomes periodic whenever the input coordinates and 1 are linearly dependent over $\mathbb{Q}$. They later studied the simultaneous rational approximations attached to linearly dependent inputs [18, Section 4.2]. Romeo lists the conjecture in his survey [24, Conjecture 9.5]. In dimension two the algorithm [16] takes $a = s(x)$ and $b = s(y)$ and sends (x, y) to $(1/(y-b), (x-a)/(y-b))$ when $y \neq b$. Thus the predecessor of (X, Y) with digits (a, b) is $(a + Y/X, b + 1/X)$.

Theorem 9.1. *For every odd prime p, the rational line*

$$p(p-1)\alpha + p\beta + p - 1 = 0$$

contains uncountably many pairs of p-adic Liouville numbers whose Jacobi–Perron expansions are infinite and not eventually periodic. On the same line, uncountably many pairs have bounded partial quotients in the p-adic absolute value and expansions that are infinite and not eventually periodic.

For a rational number m/n in lowest terms, put $H(m/n) = \max(|m|, |n|)$. The p-adic irrationality exponent of x is the supremum of the real numbers μ for which $0 < |x - r|_p < H(r)^{-\mu}$ has infinitely many solutions $r \in \mathbb{Q}$. A p-adic Liouville number has infinite irrationality exponent.

Proof. Put $h = (p-1)/p$, $q = h - p/(p-1)$ and $B = h + p\mathbb{Z}_p$. Then $q \in B$. For each $k \geq 1$ put

$$b_k = \frac{p-1}{2} + p^{-k}, \qquad a_k = \frac{p^2-3}{2p} - (p-1)p^{-k-1}.$$

Both digits belong to $\mathbb{Z}[1/p] \cap (0, p/2)$, and

$$|b_k|_p = p^k, \qquad |a_k|_p = p^{k+1}, \qquad pa_k + (p-1)b_k = p^2 - p - 1.$$

For $x \in B$ set $y = -(p-1)x - h$. Then $|x|_p = p$ and $y \in 1 + p\mathbb{Z}_p$. The pair $(X, Y) = (a_k + y/x, b_k + 1/x)$ has digits (a_k, b_k) since $y/x, 1/x \in p\mathbb{Z}_p$. In particular $|X|_p = p^{k+1}$ and $|Y|_p = p^k$, so $(h + Y/X, 1 + 1/X)$ has digits $(h, 1)$. The identity $pX + (p-1)Y = -1$ puts this last pair back on the original line. Its first coordinate is

$$F_k(x) = q - \frac{x}{(p-1)((a_k - p + 1)x - h)}.$$

The factor $(a_k - p + 1)x - h = xX$ has norm p^{k+2}, and $|h/(p-1)|_p = p$. Subtraction gives, for $x, z \in B$,

$$|F_k(x) - q|_p = p^{-k-1}, \qquad |F_k(x) - F_k(z)|_p = p^{-2k-3}|x - z|_p. \tag{9.1}$$

In particular $F_k(B) \subset B$. For every sequence $k_1, k_2, \ldots$, the nested compact sets $F_{k_1} \cdots F_{k_m}(B)$ have diameters tending to zero. Their intersection consists of one point α. Applying the predecessor calculation to each tail shows that the expansion of $(\alpha, -(p-1)\alpha - h)$ consists of the successive blocks $((h, 1), (a_{k_j}, b_{k_j}))$. Both steps of every block are defined. Different sequences give different points since the digits recover each k_j. Restricting to $k_j \in \{1, 2\}$ bounds the partial quotients. An eventually periodic digit sequence has an eventually periodic subsequence at the odd indices, and hence an

eventually periodic sequence of k_j. Only countably many words over $\{1,2\}$ are eventually periodic.

For the Liouville pairs let k_j equal $j!$ or $j!+1$ independently at each j. The pair on the line with first coordinate $r_m = F_{k_1}\cdots F_{k_m}(q)$ reaches $(q,1)$ after exactly m blocks, where the algorithm terminates. The r_m are therefore distinct. Writing $A_k = a_k - p + 1$, we have $F_k(x) = h + (b_k x + 1)/(A_k x - h)$. A matrix for this map is

$$\begin{pmatrix} hA_k + b_k & 1 - h^2 \\ A_k & -h \end{pmatrix}.$$

Since $-p+1 < A_k < 0$, $0 < b_k < p/2$ and $0 < h < 1$, the sum of the absolute values in either row is less than p. Multiplying by p^{k+2} makes this matrix integral. The height bound for a product of these matrices and (9.1) applied to the tail after m blocks give

$$H(r_m) \le C_p^{m+1} p^{\sum_{j=1}^{m} k_j}, \qquad |\alpha - r_m|_p = p^{-k_{m+1}-1-\sum_{j=1}^{m}(2k_j+3)}$$

for a constant C_p depending only on p. Since $k_{m+1}/(m + \sum_{j\le m} k_j) \to \infty$, these approximations satisfy the Liouville inequalities. The map $x \mapsto -(p-1)x - h$ preserves p-adic distances and increases rational heights by at most a constant factor, so its value at α is also Liouville. The norms p^{k_j+1} of the partial quotients a_{k_j} are unbounded. For each of the uncountably many choices, the expansion therefore fails to be eventually periodic. □

At $p = 3$ and $p = 5$ the line in Theorem 9.1 has equation $6\alpha + 3\beta + 2 = 0$ and $20\alpha + 5\beta + 4 = 0$, respectively. Murru and Terracini give period-two examples on both lines [17, Example 1]. The question for algebraic inputs remains open.

Proposition 9.2. *For every $\varepsilon > 0$, the line in Theorem 9.1 contains a set of Hausdorff dimension greater than $1/2$ consisting of points whose Jacobi–Perron expansions are infinite and not eventually periodic. The p-adic absolute values of their partial quotients are bounded in terms of p and ε. For either coordinate x of every point in this set,*

$$|x - r|_p \gg_{p,\varepsilon} H(r)^{-2-\varepsilon} \qquad (r \in \mathbb{Q}).$$

In particular, both irrationality exponents are at most $2 + \varepsilon$.

Proof. For $k \ge 1$, replace p^{-k} in the digit formulas by jp^{-k}, where $1 \le j < p^k/2$ and $p \nmid j$. Thus

$$b_{k,j} = \frac{p-1}{2} + \frac{j}{p^k}, \qquad a_{k,j} = \frac{p^2-3}{2p} - \frac{(p-1)j}{p^{k+1}}.$$

Both digits still lie in $(0, p/2)$ and have their previous norms. The two-step maps $F_{k,j}$ are similarities on B of ratio $r_k = p^{-2k-3}$. Their images are pairwise disjoint since the second pair of digits recovers $b_{k,j}$ and hence k, j. There are $N_k = (p-1)p^{k-1}/2$ choices of j because the units modulo p^k occur in pairs $j, p^k - j$.

Choose integers $k_0 \ge \max(1, 3/\varepsilon)$ and $K \ge k_0$ with $K - k_0 + 1 > 2p^{5/2}/(p-1)$, taking the least possible values. Restrict to $k_0 \le k \le K$. Since

$$\sum_{k=k_0}^{K} N_k r_k^{1/2} = \frac{(K - k_0 + 1)(p-1)}{2p^{5/2}} > 1,$$

there is a unique $s > 1/2$ with $\sum_{k=k_0}^{K} N_k r_k^s = 1$. Assign probability r_k^s to each symbol (k,j) independently at every position. The induced measure on the set of infinite expansions gives mass R^s to each cylinder of ratio R. Let $\delta > 0$ be the minimum distance between distinct first images, which are finitely many disjoint compact sets. In a cylinder of ratio R, distinct children are separated by at least $R\delta$. A ball of radius $u < \delta$ meeting the support therefore meets only one successive child as long as $u < R\delta$. At the first prefix with $R\delta \le u$, the ball has mass at most $R^s \le (u/\delta)^s$. The mass bound gives Hausdorff

dimension at least s. Removing the countably many eventually periodic words preserves this lower bound, and $x \mapsto (x, -(p-1)x - h)$ is an isometry for the maximum metric on $\mathbb{Q}_p^2$.

All partial quotients have p-adic absolute value at most p^{K+1}. The integral matrix in the proof of Theorem 9.1, with the digits $a_{k,j}, b_{k,j}$, still has maximum absolute row sum at most p^{k+3}. Write $S_m = \sum_{i=1}^{m} k_i$ and $T_m = 2S_m + 3m$. For a first coordinate α in our set the first m branches send q to distinct rational endpoints r_m, as in that proof. Hence

$$H(r_m) \le H(q)p^{T_m - S_m}, \qquad |\alpha - r_m|_p \le p^{-T_m}.$$

Given $r \in \mathbb{Q}$, take the least $m \ge 1$ with $p^{S_m} > 2H(r)H(q)$, increasing m by one if $r = r_m$. Clearing denominators gives

$$|r - r_m|_p \ge \frac{1}{2H(r)H(r_m)} > p^{-T_m} \ge |\alpha - r_m|_p.$$

It follows that $|\alpha - r|_p = |r_m - r|_p > p^{-T_m}$. Our choice of m gives $S_m \le \log_p(2H(r)H(q)) + 2K$, and $T_m \le (2 + 3/k_0)S_m \le (2+\varepsilon)S_m$. The claimed bound follows. It also holds for $-(p-1)\alpha - h$, since this affine map preserves p-adic distances and changes rational heights by at most a constant factor in either direction. □

10. Irreducibility and prime values of a polynomial sequence

Capuano, Mula, Terracini and Veneziano [5, Section 4.6.3] study period-three continued fractions attached to the Pell equation with $d = a^2 + 1$. For a positive integer a write

$$(a + \sqrt{d})^{2n} = u_n + v_n\sqrt{d}. \tag{10.1}$$

For every n we have $u_n^2 - dv_n^2 = 1$ and $u_n - dv_n = f_n(a)$, where the polynomials f_n are defined by

$$\begin{aligned} f_0(X) &= 1, \qquad f_1(X) = -2X^3 + 2X^2 - 2X + 1, \\ f_{n+2}(X) &= (4X^2 + 2)f_{n+1}(X) - f_n(X). \end{aligned} \tag{10.2}$$

Indeed, $(a+\sqrt{d})^2$ and $(a-\sqrt{d})^2$ have sum $4a^2+2$ and product 1. By [5, Proposition 4.26], if $|f_n(a)| = p^s$ for a prime p and $s \ge 1$, then

$$[\overline{au_n,\ a/f_n(a),\ av_n}] \tag{10.3}$$

converges in $\mathbb{Q}_p$ to a square root of d. Indeed, putting $D = u_n - v_n$, the identity $(u_n + v_n)f_n(a) = 1 - a^2u_nv_n$ gives the period matrix

$$\frac{1}{f_n(a)}\begin{pmatrix} a & dD \\ D & a \end{pmatrix}.$$

It has determinant -1. Since $f_n(a) \equiv 1 \pmod{2a}$ by (10.2), the trace has p-adic norm $p^s > 1$, and Hensel's lemma gives two eigenvalues in $\mathbb{Q}_p$ of distinct norms. Its fixed points are $\pm\sqrt{d}$, both irrational over $\mathbb{Q}$. Each of the three subsequences of convergents starts at a rational projective point and therefore tends to the attracting fixed point.

Conjecture 4.29 of [5] asserts that f_n is irreducible for every $n \ge 1$. Their Conjecture 4.30 asks whether, for each fixed positive integer a, infinitely many values $|f_n(a)|$ are prime.

Theorem 10.1. *For every $n \ge 1$, the polynomial $f_n(X)$ is irreducible in $\mathbb{Z}[X]$.*

Proof. Consider

$$P_n(Z) = Z^{2n+1} - Z^{2n} - Z - 1.$$

Ljunggren's criterion for quadrinomials with coefficients ± 1 [13, Theorem 1], also stated in [10, Theorem 1], gives irreducibility over $\mathbb{Q}$ if P_n has no root of unity. If $P_n(\zeta) = 0$ and

$|\zeta| = 1$, then $\zeta^{2n}(\zeta - 1) = \zeta + 1$. Equality of the absolute values of $\zeta - 1$ and $\zeta + 1$ gives $\zeta = \pm i$. For these two values $(\zeta + 1)/(\zeta - 1) = -\zeta$ is imaginary, whereas ζ^{2n} is real. It follows that P_n is irreducible.

Write $x = (Z - Z^{-1})/2$ and $y = (Z + Z^{-1})/2$, so that $y^2 = x^2 + 1$ and $x + y = Z$. Adding and subtracting $(x+y)^{2n}$ and $(x-y)^{2n}$ as in (10.1) gives $2f_n(x) = (1-y)Z^{2n} + (1+y)Z^{-2n}$. Hence

$$\begin{aligned} 4Z^{2n+1} f_n\left(\frac{Z - Z^{-1}}{2}\right) &= (Z+1)^2 - Z^{4n}(Z-1)^2 \\ &= -P_n(Z)\Big(Z^{2n+1} - Z^{2n} + Z + 1\Big). \end{aligned}$$

If z is a root of P_n, then $x = (z - z^{-1})/2$ satisfies $f_n(x) = 0$, and $z^2 - 2xz - 1 = 0$. The degree $[\mathbb{Q}(z) : \mathbb{Q}(x)]$ is at most 2 and divides the odd integer $[\mathbb{Q}(z) : \mathbb{Q}] = 2n + 1$, so it is 1. Thus $[\mathbb{Q}(x) : \mathbb{Q}] = 2n + 1 = \deg f_n$, the last equality following from (10.2). Finally, $f_n(0) = 1$ by the recurrence, so f_n is primitive. Gauss's lemma gives the assertion over $\mathbb{Z}$. □

10.1. **Prime divisors and two specializations.** Fix $a \geq 1$, put $d = a^2 + 1$, and write $\varepsilon = a + \sqrt{d}$ and $\eta = (1 + \sqrt{d})/a$. Since $a\eta = 1 + \sqrt{d}$ and $a\eta^{-1} = \sqrt{d} - 1$, equation (10.1) gives

$$f_n(a) = \frac{a}{2}\left(\eta\varepsilon^{-2n} - \eta^{-1}\varepsilon^{2n}\right). \tag{10.4}$$

In particular $|f_n(a)| \to \infty$.

Proposition 10.2. *Suppose that a prime ℓ divides $f_n(a)$. Then d is a nonzero square modulo ℓ. For either square root t of d modulo ℓ, put $e = a + t$ and let r be the multiplicative order of e^4 in $\mathbb{F}_\ell^\times$. For every $m \geq 0$,*

$$\ell \mid f_m(a) \quad \Longleftrightarrow \quad m \equiv n \pmod{r}, \qquad r \mid \frac{\ell - 1}{\gcd(4, \ell - 1)}, \qquad r \nmid 2n.$$

Consequently, $\ell - 1 \mid 8n$ excludes ℓ as a prime divisor of $f_n(a)$ for every a. In particular 3 and 5 divide none of these values.

Proof. We have $\ell \nmid 2a$. The congruence $u_n \equiv dv_n \pmod{\ell}$ and $u_n^2 - dv_n^2 = 1$ give $a^2 dv_n^2 \equiv 1 \pmod{\ell}$, so $d = (av_n)^{-2}$ in $\mathbb{F}_\ell$. Put $w = (1 + t)/a$ in that field. Both e and w are nonzero since $t^2 - a^2 = 1$ and $t^2 - 1 = a^2$. Substituting $\sqrt{d} = t$ in (10.4) gives $\ell \mid f_m(a)$ precisely when $e^{4m} = w^2$. The solutions form the residue class of n modulo r. The group of fourth powers in $\mathbb{F}_\ell^\times$ has order $(\ell - 1)/\gcd(4, \ell - 1)$. Moreover, $w - w^{-1} = 2/a$ and $w + w^{-1} = 2t/a$ are nonzero, so $w^2 \neq \pm 1$. Thus $e^{8n} = w^4 \neq 1$, giving $r \nmid 2n$ and, by Fermat's theorem, $\ell - 1 \nmid 8n$. □

Given $B \geq 2$, take n to be a positive multiple of all $\ell - 1$ for primes $\ell \leq B$. Then no prime at most B divides any $f_n(a)$, simultaneously for all $a \geq 1$. For each fixed a there is therefore an infinite subsequence of pairwise coprime values with absolute value greater than 1. At each step choose B larger than every prime divisor already used and take n sufficiently large.

Let $S_0 = S_1 = 1$ and $S_{m+2} = 2S_{m+1} + S_m$. The odd-indexed S_m are the Newman–Shanks–Williams numbers [19]. Let L_m denote the Lucas numbers with $L_0 = 2$, $L_1 = 1$. For $d = 5$, Capuano, Mula, Terracini and Veneziano related prime powers in the period-three problem to Lucas numbers and gave explicit examples for $a = 2$ [5, Examples 4.25 and 4.28].

Proposition 10.3. *For $n \geq 1$ one has*

$$f_n(1) = -S_{2n-1}, \qquad f_n(2) = -L_{6n-1}.$$

At $a = 1$, Conjecture 4.30 of [5] *is equivalent to the infinitude of Newman–Shanks–Williams primes, Question (D) of* [19, p. 130]. *At $a = 2$, it is equivalent to the existence of infinitely many primes $q \equiv 5 \pmod 6$ for which L_q is prime.*

Proof. For $a = 1$ we have $\eta = \varepsilon = 1 + \sqrt{2}$. For $a = 2$, putting $\varphi = (1 + \sqrt{5})/2$ gives $\eta = \varphi$ and $\varepsilon = \varphi^3$. The two identities follow from (10.4) and the usual formulas for S_m and L_m. For odd $r, s > 1$, let A, B be the rth powers of the two conjugate units in the relevant formula. Then $(A^s + B^s)/(A + B)$ is a rational algebraic integer, so $S_r \mid S_{rs}$ and $L_r \mid L_{rs}$. The inequalities $1 < S_r < S_{rs}$ and $1 < L_r < L_{rs}$ exclude every composite odd index. Every prime congruent to 5 modulo 6 is of the form $6n - 1$ with $n \geq 1$, giving the stated equivalence. □

For $a \geq 3$ the numbers η and ε are multiplicatively independent. Indeed, $\varepsilon > 1$ is an algebraic unit. A nontrivial relation would make a positive power of η integral, hence η itself integral, whereas its trace is $2/a$. The question of infinitely many prime terms for fixed a remains open.

Proposition 10.4. *For every $h \geq 1$ there is a least positive integer C_h for which*

$$\gcd\Big(f_m(a), f_{m+h}(a)\Big) \mid C_h \qquad (m \geq 0,\ a \geq 1).$$

It is effectively computable, and $C_1 = 1$, $C_2 = 1$, $C_3 = 91$, $C_4 = 17$.

Proof. Write $T = 4X^2 + 2$, $U_0 = 0$, $U_1 = 1$ and $U_{j+1} = TU_j - U_{j-1}$. Fix a and evaluate the polynomials at a. The recurrence and $f_0 = 1$ give $\gcd(f_j, f_{j+1}) = 1$ for every j. Since $f_{m+h} = U_h f_{m+1} - U_{h-1} f_m$, the required gcd is $\gcd(f_m, U_h)$. Similarly $\gcd(U_h, U_{h-1}) = 1$. Reducing the same identity modulo U_h and iterating therefore gives $\gcd(f_m, U_h) = \gcd(f_b, U_h)$ for $b \equiv m \pmod h$, $0 \leq b < h$.

For $b \geq 1$, $f_b(0) = 1$ and $f_b(1) = -S_{2b-1} < 0$, so f_b has a positive real root. For every real X, the inequality $T \geq 2$ gives $U_j(X) > U_{j-1}(X)$ for $j \geq 1$ by induction. Hence U_h cannot be divisible by the irreducible polynomial f_b, and $\operatorname{Res}(f_b, U_h) \neq 0$. The specialized gcd divides this resultant by the integral Bézout identity for the resultant. The case $b = 0$ contributes 1. Let B_h be the odd part of the least common multiple of the absolute resultants for $0 \leq b < h$. Since $f_m(a)$ is odd, the required gcd equals $\gcd(B_h, f_b(a), U_h(a))$. It therefore depends only on m mod h and a mod B_h. Taking the least common multiple over these residue classes gives C_h.

For $h = 1$ use $U_1 = 1$. Substituting $U_2 = T$, $U_3 = T^2 - 1$ and $U_4 = T(T^2 - 2)$ gives odd parts $(1, 1)$, $(1, 91, 91)$ and $(1, 17, 1, 17)$, respectively, in order of increasing b. The bounds for $h = 3, 4$ are attained, since (10.2) gives $91 \mid \gcd(f_1(48), f_4(48))$ and $17 \mid \gcd(f_1(10), f_5(10))$. □

For example, if every prime divisor of $C_1 \cdots C_H$ divides a, then every $H + 1$ consecutive terms of $(f_m(a))_{m \geq 0}$ are pairwise coprime, since $f_m(a) \equiv 1 \pmod a$ for every m.

Funding. T. P. acknowledges support from the Croatian Science Foundation under project IP-2022-10-5008 (TEBAG). He also 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 under the Competitiveness and Cohesion Programme 2021–2027. This research was funded by the European Union through NextGenerationEU under the National Recovery and Resilience Plan 2021–2026 (institutional grant of the Faculty of Science, University of Zagreb, IK IA 1.1.3. Impact4Math).

References

[1] S. Barbero, U. Cerruti and N. Murru, Periodic representations for quadratic irrationals in the field of p-adic numbers. Math. Comp. **90**, 2267–2280 (2021). 10.1090/mcom/3640

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

[3] J. Browkin, Continued fractions in local fields, I. Demonstratio Math. **11**, 67–82 (1978). 10.1515/dema-1978-0108

[4] J. Browkin, Continued fractions in local fields, II. Math. Comp. **70**, 1281–1292 (2001). 10.1090/S0025-5718-00-01296-5

[5] L. Capuano, M. Mula, L. Terracini and F. Veneziano, p-adically convergent loci in varieties arising from periodic continued fractions. Res. Number Theory **12**, Article 86 (2026). 10.1007/s40993-026-00770-x

[6] L. Capuano, N. Murru and L. Terracini, On periodicity of p-adic Browkin continued fractions. Math. Z. **305**, Article 17 (2023). 10.1007/s00209-023-03333-3

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

[8] M. Choudhuri and P.J. Makadiya, On a continued fraction algorithm in finite extensions of $\mathbb{Q}_p$ and its metrical theory. Period. Math. Hungar. **91**, 124–146 (2025). 10.1007/s10998-025-00634-4. Preprint version, arXiv:2407.04276.

[9] T.-C. Dinh, L. Kaufmann and H. Wu, Berry–Esseen bound and local limit theorem for the coefficients of products of random matrices. J. Inst. Math. Jussieu **23**, 705–735 (2024). 10.1017/S1474748022000561

[10] C. Finch and L. Jones, On the irreducibility of $\{-1, 0, 1\}$-quadrinomials. Integers **6**, A16 (2006). Journal PDF.

[11] H. Furstenberg, Noncommuting random products. Trans. Amer. Math. Soc. **108**, 377–428 (1963). 10.1090/S0002-9947-1963-0163345-0

[12] C. Hooley, On the number of divisors of quadratic polynomials. Acta Math. **110**, 97–114 (1963). 10.1007/BF02391856

[13] W. Ljunggren, On the irreducibility of certain trinomials and quadrinomials. Math. Scand. **8**, 65–70 (1960). 10.7146/math.scand.a-10593

[14] N. Murru and G. Romeo, A new algorithm for p-adic continued fractions. Math. Comp. **93**, 1309–1331 (2024). 10.1090/mcom/3890

[15] N. Murru, G. Romeo and G. Santilli, On the periodicity of an algorithm for p-adic continued fractions. Ann. Mat. Pura Appl. **202**, 2971–2984 (2023). 10.1007/s10231-023-01347-6

[16] N. Murru and L. Terracini, On p-adic multidimensional continued fractions. Math. Comp. **88**, 2913–2934 (2019). 10.1090/mcom/3450. Preprint version, arXiv:1805.00072.

[17] N. Murru and L. Terracini, On the finiteness and periodicity of the p-adic Jacobi–Perron algorithm. Math. Comp. **89**, 2913–2930 (2020). 10.1090/mcom/3540. Preprint version, arXiv:1901.04922.

[18] N. Murru and L. Terracini, Simultaneous approximations to p-adic numbers and algebraic dependence via multidimensional continued fractions. Ramanujan J. **56**, 67–86 (2021). 10.1007/s11139-021-00466-z

[19] M. Newman, D. Shanks and H.C. Williams, Simple groups of square order and an interesting sequence of primes. Acta Arith. **38**, 129–140 (1980). 10.4064/aa-38-2-129-140

[20] T. Pejković, Nonperiodic p-adic continued fractions of quadratic irrationals. Preprint.

[21] T. Pejković, Nonperiodic quadratic Browkin continued fractions. Preprint.

[22] T. Pejković, Real limits and period lengths of Schneider's p-adic continued fractions. Preprint.

[23] H. Rao and S. Yasutomi, Ergodicity for p-adic continued fraction algorithms. Indag. Math. (N.S.) **32**, 759–776 (2021). 10.1016/j.indag.2021.04.001

[24] G. Romeo, Continued fractions in the field of p-adic numbers. Bull. Amer. Math. Soc. (N.S.) **61**, 343–371 (2024). 10.1090/bull/1819

[25] G. Romeo, Real convergence and periodicity of p-adic continued fractions. Ramanujan J. **68**, article 112 (2025). 10.1007/s11139-025-01264-7

[26] A.A. Ruban, Certain metric properties of the p-adic numbers. Siberian Math. J. **11**, 176–180 (1970). 10.1007/BF00970247

[27] A. Saito, J. Tamura and S. Yasutomi, Multidimensional p-adic continued fraction algorithms. Math. Comp. **89**, 351–372 (2020). 10.1090/mcom/3458. arXiv:1705.06122v3.

[28] H.P. Schlickewei, On linear forms with algebraic coefficients and Diophantine equations. J. Number Theory **9**, 381–392 (1977). 10.1016/0022-314X(77)90073-7

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

[30] J. H. Silverman, The Arithmetic of Elliptic Curves, 2nd ed., Chapter IX. Springer, Dordrecht (2009). 10.1007/978-0-387-09494-6

[31] Z. Wang and Y. Deng, Convergence, finiteness and periodicity of several new algorithms of p-adic continued fractions. Math. Comp. **93**, 2921–2942 (2024). 10.1090/mcom/3948. Preprint version, arXiv:2309.05601.

[32] S. Yasutomi, Certain multidimension p-adic continued fraction algorithm and cubic numbers. In: Diophantine Analysis and Related Fields 2018, Abstracts of the Talks, p. 2, Keio University, Yokohama (2018). Conference abstract.

[33] S. Yasutomi, Certain continued fraction algorithm converging simultaneously under $\mathbb{R}$ and $\mathbb{Q}_p$. RIMS Kôkyûroku **2285**, 36–42 (2024). Kyoto University Research Information Repository.

[34] S. Yasutomi, Simultaneous convergent continued fraction algorithm for real and p-adic fields with applications to quadratic fields. Funct. Approx. Comment. Math. **72**, 61–94 (2025). 10.7169/facm/2040514-24-5. Preprint version, arXiv:2309.09447v1, whose numbering is used here.

[35] S. Yasutomi, A. Saito and J. Tamura, Multidimensional p-adic continued fraction algorithms (in Japanese). RIMS Kôkyûroku **2092**, 63–74 (2018). Kyoto University repository.