hexagon:2610.00398v2

$\log_p 2 \cdot \log_p(3+\sqrt{2})$ IS NOT A p-ADIC LINEAR FORM IN LOGARITHMS

SHAWN KRISMAN

Abstract. Let p be a prime, $\mathbb{C}_p$ the completion of an algebraic closure of $\mathbb{Q}_p$, $\overline{\mathbb{Q}}$ the algebraic numbers in $\mathbb{C}_p$, L the $\mathbb{Q}$-vector space of p-adic logarithms of algebraic numbers, and $\mathcal{L} = \overline{\mathbb{Q}} + \overline{\mathbb{Q}}L$ the space of p-adic linear forms in logarithms of algebraic numbers with algebraic coefficients. We prove, in Lean 4 with Mathlib and from the three standard axioms only, that $\log_p 2 \cdot \log_p(3+\sqrt{2}) \notin \mathcal{L}$ for every prime $p \equiv \pm 3 \pmod 8$, together with a family of similar statements for real quadratic fields, and the general principle behind them: if σ is a continuous automorphism of $\mathbb{C}_p$ fixing a nonzero $t \in L$ and moving $u \in L$ to a conjugate $\sigma u \neq \pm u$ of finite orbit, then $tu \notin \mathcal{L}$. This is G. Diaz's use of complex conjugation with an element of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ in its place; the complex analogue $\log 2 \cdot \log(3+\sqrt{2}) \notin \mathcal{L}$ is open. The deep input is Roy's form of Waldschmidt's linear-subgroup theorem for $\mathbb{G}_{\mathrm{a}}^{d_0} \times \mathbb{G}_{\mathrm{m}}^{d_1}$ over $\mathbb{C}_p$, with a derivative subspace, which we also prove in Lean, from Philippon's multiplicity estimate; the strong six exponentials theorem and the inhomogeneous Baker–Brumer theorem in two logarithms over $\mathbb{C}_p$ follow. The p-adic linear-subgroup theorem has been used since Laurent and Roy, but we were unable to locate a proof written for $\mathbb{C}_p$ of the version with derivatives. The Lean development is the proof of record; the paper explains the statements, the route, and how to check the certificate. The code is available at `https://github.com/telaviv/p-adic-log-products`.

1. Main theorems

Fix a prime p. Let $\mathbb{C}_p$ be the completion of an algebraic closure of $\mathbb{Q}_p$, with the absolute value $|\cdot|$ normalized by $|p| = p^{-1}$; it is complete and algebraically closed [24, Ch. 3]. Let $\overline{\mathbb{Q}} \subset \mathbb{C}_p$ be the set of elements algebraic over $\mathbb{Q}$; it is an algebraic closure of $\mathbb{Q}$. Let

$$\mathcal{U} = \{x \in \mathbb{C}_p : |x-1| < 1\}, \qquad \log x = \sum_{n \geq 1} \frac{(-1)^{n+1}}{n}(x-1)^n \quad (x \in \mathcal{U}),$$

Date: October 21, 2026.

2020 *Mathematics Subject Classification.* Primary 11J81; Secondary 11J86, 11J61, 68V20.

Key words and phrases. p-adic transcendence, linear forms in logarithms, strong six exponentials theorem, linear-subgroup theorem, interpolation determinants, formal verification, Lean.

and, following Roy [25, p. 24],

$$L = \text{the } \mathbb{Q}\text{-span of } \log(\overline{\mathbb{Q}} \cap \mathcal{U}), \qquad \mathcal{L} = \overline{\mathbb{Q}} + \overline{\mathbb{Q}} \cdot L \subset \mathbb{C}_p.$$

Every $\alpha \in \overline{\mathbb{Q}}^\times$ has a power α^N with $\alpha^N p^{-m} \in \mathcal{U}$ for some $m \in \mathbb{Z}$, and $\log_p \alpha := N^{-1} \log(\alpha^N p^{-m})$ is the Iwasawa logarithm ($\log_p p = 0$); so $L = \log_p(\overline{\mathbb{Q}}^\times)$, and $\mathcal{L}$ is the set of numbers $\beta_0 + \sum_i \beta_i \log_p \alpha_i$ with $\beta_i \in \overline{\mathbb{Q}}$ and $\alpha_i \in \overline{\mathbb{Q}}^\times$: the p-adic linear forms in logarithms of algebraic numbers with algebraic coefficients, with a constant term.

The formalization is public at

`https://github.com/telaviv/p-adic-log-products`,

at the revision pinned in Section 6. Its endpoints are the following five statements. For each we give the name of the Lean declaration; Section 2 reproduces the Lean definitions of $\mathcal{U}$, log, $\overline{\mathbb{Q}}$, L, $\mathcal{L}$ and of the numbers involved, which is what a reader has to check to trust the certificate.

Theorem 1.1 (`LogIrr.e2_unconditional`, `LogIrr.e2'_unconditional`). *Let p be a prime with $p \equiv 3$ or $5 \pmod 8$, and let $\sqrt{2}$ be either square root of 2 in $\mathbb{C}_p$ (it lies in $\overline{\mathbb{Q}}_p \setminus \mathbb{Q}_p$). Then*

$$\log_p 2 \cdot \log_p(3 + \sqrt{2}) \notin \mathcal{L} \qquad \textit{and} \qquad \log_p 2 \cdot \log_p(3 - \sqrt{2}) \notin \mathcal{L}.$$

Theorem 1.1 is an instance of a uniform statement for real quadratic fields. For an integer d write $x = a' + b'\sqrt{d}$ for elements of $\mathbb{Z}[\sqrt{d}]$, $\bar{x} = a' - b'\sqrt{d}$ and $N(x) = x\bar{x}$.

Theorem 1.2 (`LogIrr.Quad.main_unconditional`). *Let $d > 0$ be an integer that is not a square modulo p, let $a \in \mathbb{Z}$ with $p \nmid a$ and $|a| \geq 2$, and let $x = a' + b'\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ with $a', b' > 0$, $p \nmid N(x)$ and $|N(x)| \geq 2$. Then $\log_p a \cdot \log_p x \notin \mathcal{L}$, and likewise $\log_p a \cdot \log_p \bar{x} \notin \mathcal{L}$ (`Quad.main'_unconditional`).*

The instances in the repository (`LogIrr/Inst/`) are: $d = 2$, $x = 3 + \sqrt{2}$, $p \equiv \pm 3 \pmod 8$, any such a (`e2a_unconditional`; with $a = 2$ this is Theorem 1.1); $d = 3$, $x = 4 + \sqrt{3}$, $p \equiv \pm 5 \pmod{12}$, $p \neq 13$ (`e4_unconditional`); $d = 5$, $x = 4 + \sqrt{5}$, $p \equiv \pm 2 \pmod 5$, $p \neq 2, 11$ (`e5_unconditional`). The congruence conditions say that d is a quadratic nonresidue modulo p, and the excluded primes divide $N(x)$.

Both theorems come from one principle. Call σ a *continuous automorphism* of $\mathbb{C}_p$ if it is an isometric ring automorphism (every element of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ extends uniquely to one, Section 3.1).

Theorem 1.3 (`LogIrr.thm51_pm_unconditional`, `thm51_unconditional`). *Let σ be a continuous automorphism of $\mathbb{C}_p$, let $t \in L$ be nonzero with $\sigma t = t$, and let $u \in L$ be nonzero with $\sigma^n u = u$ for some $n \geq 1$ and $\sigma u \neq \pm u$. Then $tu \notin \mathcal{L}$. More generally the conclusion holds if $\sigma t \in \overline{\mathbb{Q}} + \overline{\mathbb{Q}} t$, $t \neq 0$, and $u, \sigma u$ are linearly independent over $\mathbb{Q}$.*

This is [9, Cor. 2(2)] with σ in place of complex conjugation. Over $\mathbb{C}$ the only continuous automorphisms are the identity and conjugation, both of which fix $\log 2$ and $\log(3+\sqrt{2})$, and $\log 2 \cdot \log(3+\sqrt{2}) \notin \mathcal{L}$ is open [9, 33, 35]. Over $\mathbb{C}_p$ the group $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ acts continuously, which is the whole point.

The input to Theorem 1.3 is Roy's form of Waldschmidt's linear-subgroup theorem for $\mathbb{G}_{\mathrm{a}}^{d_0} \times \mathbb{G}_{\mathrm{m}}^{d_1}$ [25, Theorem 1], [31, Theorem 4.1], over $\mathbb{C}_p$. For $d_0, d_1 \geq 0$ put $E = \mathbb{C}_p^{d_0} \times \mathbb{C}_p^{d_1}$. A $\mathbb{C}_p$-subspace of E is *rational over* $\overline{\mathbb{Q}}$ if it is spanned by vectors with coordinates in $\overline{\mathbb{Q}}$.

Theorem 1.4 (`LogIrr.Padic.waldschmidtTheorem1_p`)**.** *Let $Y \subset \overline{\mathbb{Q}}^{d_0} \times L^{d_1}$ be a finite-dimensional $\mathbb{Q}$-subspace of E, let $W \subset E$ be a $\mathbb{C}_p$-subspace rational over $\overline{\mathbb{Q}}$, and let $V \subset E$ be a $\mathbb{C}_p$-subspace containing Y and W. If $V \neq E$, there are $d_0', d_1' \geq 0$ and a surjective $\mathbb{C}_p$-linear map $s\colon E \to E' = \mathbb{C}_p^{d_0'} \times \mathbb{C}_p^{d_1'}$ with $s(\overline{\mathbb{Q}}^{d_0} \times 0) \subset \overline{\mathbb{Q}}^{d_0'} \times 0$ and $s(0 \times \mathbb{Q}^{d_1}) \subset 0 \times \mathbb{Q}^{d_1'}$, such that $W' = s(W) \neq E'$ and, with $Y' = s(Y)$,*

$$\frac{d_1' + \dim_{\mathbb{Q}} Y'}{d_0' + d_1' - \dim_{\mathbb{C}_p} W'} \;\leq\; \frac{d_1}{d_0 + d_1 - \dim_{\mathbb{C}_p} V}.$$

This is Roy's Theorem 1 verbatim for $K = \mathbb{C}_p$. Roy states it for $K = \mathbb{C}$ and $K = \mathbb{C}_p$ at once, with a period lattice $\Omega = 0 \times \omega\mathbb{Q}^{d_1}$ where $\omega = 2\pi i$ over $\mathbb{C}$ and $\omega = 0$ over $\mathbb{C}_p$ [25, p. 24]; the terms $\dim_{\mathbb{Q}}(Y \cap \Omega)$ of his inequality vanish p-adically, and the Lean statement keeps them literally with $\Omega = 0$ (Section 2). Roy's reduction from Theorem 1.4 to his Corollary 2 is field-independent and is also formalized, so we get the two consequences that Theorem 1.3 actually uses.

Corollary 1.5 (strong six exponentials over $\mathbb{C}_p$; `LogIrr.royCor2`)**.** *If $x_1, x_2 \in \mathbb{C}_p$ are linearly independent over $\overline{\mathbb{Q}}$ and $y_1, y_2, y_3 \in \mathbb{C}_p$ are linearly independent over $\overline{\mathbb{Q}}$, then $x_i y_j \notin \mathcal{L}$ for some i, j. Equivalently* [25, Cor. 2]*: a 2×3 matrix with entries in $\mathcal{L}$ whose rows and whose columns are $\overline{\mathbb{Q}}$-linearly independent has rank 2.*

Corollary 1.6 (Baker–Brumer over $\mathbb{C}_p$, $n \leq 2$; `LogIrr.bakerBrumer`)**.** *A nonzero element of L is transcendental. If $\ell_1, \ell_2 \in L$ are linearly independent over $\mathbb{Q}$, then $1, \ell_1, \ell_2$ are linearly independent over $\overline{\mathbb{Q}}$.*

What is new. The mathematics of Theorems 1.1–1.3 is a transposition of Diaz's complex-conjugation argument [8, 9], and Theorem 1.4 is a statement Roy made in 1992 and attributed to Waldschmidt. The claims of novelty are therefore modest and all of the form "we could not find this in print" (the search is recorded in Section 4):

(1) no statement of the form "a product of two p-adic logarithms of algebraic numbers lies outside $\mathcal{L}$" was found in the literature; Momot [21, §1.3] explicitly leaves the ultrametric analogue of Diaz's results to a further paper;

(2) no proof written for $\mathbb{C}_p$ of the *mixed* linear-subgroup theorem (a $\mathbb{G}_{\mathrm{a}}$ factor, derivatives along a subspace $W \neq 0$, a general V) was found; the published p-adic results are the Schneider case without derivatives [29, 5] and the analytic subgroup theorem [20, 11, 12];
(3) we are not aware of an earlier machine-checked proof of any six-exponentials-type theorem, of a linear-subgroup theorem with derivatives, or of any p-adic transcendence theorem.

The proof of record for everything in this paper is the Lean library `LogIrr` [16], which depends only on Lean's three standard axioms and contains no `sorry`. The prose proofs were written first and the Lean files follow them; where they differ, the Lean files are authoritative.

2. The statements in Lean

Mathlib provides $\mathbb{C}_p$ as `PadicComplex p`, written `ℂ_[p]`, with its norm, completeness and algebraic closedness, and the generic exponential `NormedSpace.exp`; it has no p-adic logarithm, which the library defines. We reproduce the definitions on which the meaning of the theorems depends (`LogIrr/LogDisc.lean`, `Lp.lean`, `Arith.lean`). Throughout, `p` is a natural number with a `Fact p.Prime` instance.

```
def U : Set ℂ_[p] := {x | ‖x - 1‖ < 1}

noncomputable def logTerm (x : ℂ_[p]) (n : ℕ) : ℂ_[p] :=
  ((-1 : ℂ_[p]) ^ n / ((n : ℂ_[p]) + 1)) * (x - 1) ^ (n + 1)

noncomputable def logU (x : ℂ_[p]) : ℂ_[p] := ∑' n, logTerm p x n

abbrev Qb : IntermediateField ℚ ℂ_[p] := algebraicClosure ℚ ℂ_[p]

noncomputable def L : Submodule ℚ ℂ_[p] :=
  Submodule.span ℚ (logU p '' {x | x ∈ Qb p ∧ x ∈ U p})

noncomputable def Lt : Submodule (Qb p) ℂ_[p] :=
  Submodule.span (Qb p) (insert (1 : ℂ_[p]) (L p : Set ℂ_[p]))
```

So `U p` is $\mathcal{U}$, `logU p` is the series log (with the junk value of a non-convergent `tsum` off the disc, never used), `Qb p` is $\overline{\mathbb{Q}}$, `L p` is Roy's L and `Lt p` is $\mathcal{L}$. The numbers of Theorem 1.1 are defined with $N = p^2 - 1$ and a chosen square root `s2 p` of 2 in $\overline{\mathbb{Q}}_p \subset \mathbb{C}_p$:

```
def N : ℕ := (p + 1) * (p - 1)
def tE  : ℂ_[p] := ((N p : ℂ_[p]))⁻¹ * logU p ((2 : ℂ_[p]) ^ N p)
def uE  : ℂ_[p] := ((N p : ℂ_[p]))⁻¹ * logU p ((3 + s2 p) ^ N p)
def uE' : ℂ_[p] := ((N p : ℂ_[p]))⁻¹ * logU p ((3 - s2 p) ^ N p)

theorem e2_unconditional (h8 : p % 8 = 3 ∨ p % 8 = 5) :
    tE p * uE p ∉ Lt p
```

(The actual definitions apply a ring homomorphism $\mathbb{Z}[\sqrt{2}] \to \mathbb{C}_p$ to 2 and $3 \pm \sqrt{2}$; the display is the unfolded form.) Since $2^N, (3 \pm \sqrt{2})^N \equiv 1 \pmod{p}$ for $p \equiv \pm 3 \pmod 8$, these are $\log_p 2$, $\log_p(3+\sqrt{2})$, $\log_p(3-\sqrt{2})$ in the sense of Section 1; the identification with the Iwasawa logarithm is not needed inside the development, which works with Roy's L directly. Theorem 1.2 is stated for `Quad.tInt p R a`, which is $N^{-1}\log(a^N)$, and `Quad.logN p R x`, which is $N^{-1}\log(x^N)$ with $x \in \mathbb{Z}[\sqrt{d}]$ mapped into $\mathbb{C}_p$ along a chosen root `R` of d.

Theorem 1.4 is stated for an arbitrary field K of characteristic 0 and an arbitrary $\mathbb{Q}$-subspace `LK` playing the role of L (`LogIrr/Roy/Theorem1.lean`); with `E K d0 d1` the product $(\mathrm{Fin}\, d_0 \to K) \times (\mathrm{Fin}\, d_1 \to K)$, `AlgVec` and `RatVec` the predicates "all coordinates algebraic" and "all coordinates rational", `RationalOverQbar W` the predicate "W is the K-span of its algebraic points", and `Omega K d0 d1` the zero submodule:

```
def WaldschmidtTheorem1 (LK : Submodule ℚ K) : Prop :=
  ∀ (d0 d1 : ℕ) (Y : Submodule ℚ (E K d0 d1)) (W V : Submodule K (E K d0 d1)),
    FiniteDimensional ℚ Y →
    (∀ p ∈ Y, AlgVec p.1 ∧ ∀ j, p.2 j ∈ LK) →
    RationalOverQbar W →
    (∀ p ∈ Y, p ∈ V) → W ≤ V → V ≠ ⊤ →
    ∃ (d0' d1' : ℕ) (s : E K d0 d1 →ℓ[K] E K d0' d1'),
      Function.Surjective s ∧
      (∀ u : Fin d0 → K, AlgVec u → ∃ u', AlgVec u' ∧ s (u, 0) = (u', 0)) ∧
      (∀ v : Fin d1 → K, RatVec v → ∃ v', RatVec v' ∧ s (0, v) = (0, v')) ∧
      W.map s ≠ ⊤ ∧
      ((d1' : ℚ) - finrank ℚ ↑(Y.map (s.restrictScalars ℚ) ⊓ Omega K d0' d1')
          +
          finrank ℚ ↑(Y.map (s.restrictScalars ℚ))) /
        ((d0' + d1' : ℚ) - finrank K ↑(W.map s)) ≤
      ((d1 : ℚ) - finrank ℚ ↑(Y ⊓ Omega K d0 d1)) /
        ((d0 + d1 : ℚ) - finrank K ↑V)

theorem waldschmidtTheorem1_p : WaldschmidtTheorem1 ℂ_[p] (L p)
```

Corollary 1.5 is `RoyCor2 p`, the product form of Roy's Corollary 2 with "$\overline{\mathbb{Q}}$-linearly independent" expressed as: no nontrivial relation with algebraic coefficients; Corollary 1.6 is `BakerBrumer p`, the conjunction of the two statements as written (`LogIrr/Lp.lean`). Theorem 1.3 is stated for `ContAut p`, the structure of ring automorphisms of $\mathbb{C}_p$ that are isometries (`LogIrr/Galois.lean`).

3. Mathematical route

3.1. **The logarithm and the Galois action.** On $\mathcal{U}$ the series log converges and is a homomorphism $(\mathcal{U}, \cdot) \to (\mathbb{C}_p, +)$ (`LogIrr.logHom`; proved by a binomial double series, without formal power series). Its kernel consists of p-power roots of unity (`logKer`). On the disc $D = \{|x-1| < \rho_p\}$, $\rho_p = p^{-1/(p-1)}$, one has $\exp \circ \log = \mathrm{id}$, and $\log \circ \exp = \mathrm{id}$ on $\{|y| < \rho_p\}$ (`exp_logU`, `logU_exp`). The last two are proved without composing power

series: the defect $g(v) = \exp(\log v)/v$ satisfies $|g(v) - 1| \le |v - 1|^2/\rho_p$ by quadratic bounds on both series and is a homomorphism on D, while $|w^{p^k} - 1| = |w - 1|\, p^{-k}$ exactly on D; applying the bound to v^{p^k} gives $|g(v) - 1| \le |v - 1|^2 p^{-k}/\rho_p$ for every k, so $g(v) = 1$.

Every $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ is an isometry, by the uniqueness of the extended absolute value, and extends uniquely to a continuous ring automorphism of $\mathbb{C}_p$ fixing $\mathbb{Q}_p$. Any continuous ring homomorphism commutes with the series log on $\mathcal{U}$, and an isometric automorphism preserves $\overline{\mathbb{Q}}$, $\mathcal{U}$, L and $\mathcal{L}$ (`LogIrr/Galois.lean`, `Galois2.lean`). There is no branch issue: $\log_p$ is single-valued, so $\sigma(\log_p \alpha) = \log_p(\sigma\alpha)$ is an identity, not a congruence modulo $2\pi i\mathbb{Z}$.

3.2. **The conjugation argument.**

Proposition 3.1 (`LogIrr.thmA`)**.** *Let σ be a continuous automorphism of $\mathbb{C}_p$, $t \in \mathcal{L} \setminus \overline{\mathbb{Q}}$ and $u \in \mathcal{L}$. Suppose $\sigma t \in \overline{\mathbb{Q}} + \overline{\mathbb{Q}}t$ and that $1, u, \sigma u$ are linearly independent over $\overline{\mathbb{Q}}$. Then $tu \notin \mathcal{L}$.*

Proof. Write $\sigma t = a + bt$ with $a, b \in \overline{\mathbb{Q}}$; then $b \neq 0$, since $t \notin \overline{\mathbb{Q}}$ and σ preserves $\overline{\mathbb{Q}}$. Suppose $v = tu \in \mathcal{L}$. Then $\sigma v = a\,\sigma u + bt\,\sigma u$, so $t\,\sigma u = b^{-1}(\sigma v - a\,\sigma u) \in \mathcal{L}$, because $\sigma(\mathcal{L}) = \mathcal{L}$. The matrix

$$\begin{pmatrix} 1 & u & \sigma u \\ t & tu & t\,\sigma u \end{pmatrix}$$

has entries in $\mathcal{L}$, rank ≤ 1, rows that are $\overline{\mathbb{Q}}$-independent (as $t \notin \overline{\mathbb{Q}}$) and columns that are $\overline{\mathbb{Q}}$-independent (by hypothesis). Corollary 1.5 says its rank is 2. □

Theorem 1.3 follows from Proposition 3.1 and Corollary 1.6: a nonzero $t \in L$ is transcendental, and if $u, \sigma u \in L$ are $\mathbb{Q}$-independent then $1, u, \sigma u$ are $\overline{\mathbb{Q}}$-independent. For the first form of Theorem 1.3, if $\sigma u = ru$ with $r \in \mathbb{Q}$ then $\sigma^n u = r^n u$, so $r^n = 1$ and $r = \pm 1$ (`linearIndependent_pair_of_orbit`).

3.3. **The quadratic instances.**

Let $d > 0$ be a non-residue modulo p. Then d is not a square in $\mathbb{Q}_p$, $X^2 - d$ is irreducible over $\mathbb{Q}_p$, and some $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ swaps the two roots $\pm\sqrt{d}$; it fixes $\mathbb{Q}_p$, hence $t = \log_p a$ for $a \in \mathbb{Z}$, and sends $\log_p x$ to $\log_p \bar{x}$ for $x \in \mathbb{Z}[\sqrt{d}]$ (`LogIrr/Quad.lean`). For $N = p^2 - 1$ the Frobenius congruence $x^p \equiv \bar{x} \pmod p$ in $\mathbb{Z}[\sqrt{d}]$ (Euler's criterion for the non-residue d) gives $x^N \equiv 1 \pmod p$ whenever $p \nmid N(x)$, so $\log_p x = N^{-1}\log(x^N)$ is defined by the series and lies in L. That $t \neq 0$ follows from the kernel description: $a^{NM} = 1$ is impossible for $|a| \ge 2$.

The one arithmetic input of Theorem 1.2 is that $\log_p x$ and $\log_p \bar{x}$ are $\mathbb{Q}$-linearly independent when $a', b' > 0$, $p \nmid N(x)$ and $|N(x)| \ge 2$ (`Quad.linearIndependent_pair`). A relation gives $(x^b \bar{x}^c)^M = 1$ in $\mathbb{C}_p$ for integers b, c not both zero and some $M \ge 1$; applying σ and multiplying, $N(x)^{(b+c)M} = 1$ in $\mathbb{Q}$, so $c = -b$; then $x^{bM} = \bar{x}^{bM}$ in $\mathbb{Z}[\sqrt{d}]$, which is

impossible for $b \neq 0$ because the $\sqrt{d}$-coordinate of x^k is positive for all $k \geq 1$. For Theorem 1.1 the original development (`LogIrr/Indep.lean`) argues instead with the 2-adic and 7-adic valuations of a relation $2^{aM}(3+\sqrt{2})^{bM}(3-\sqrt{2})^{cM} = 1$ in $\mathbb{Z}[\sqrt{2}]$, which is a Euclidean domain in which $\sqrt{2}$, $3 \pm \sqrt{2}$ are non-associate primes; the repository keeps both proofs, and `Inst/Sqrt2.lean` re-derives Theorem 1.1 from Theorem 1.2.

Why these numbers: the hypotheses of Theorem 1.3 need a logarithm whose $\overline{\mathbb{Q}}$-line is σ-stable and a logarithm whose line is moved to an independent one. A rational a gives $t \in \mathbb{Q}_p$, fixed by all of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. Units such as $1+\sqrt{2}$ fail, since $\sigma\varepsilon = -\varepsilon^{-1}$ keeps the line stable; so do $\log_p 2 \cdot \log_p 3$ and all squares $(\log_p \alpha)^2$, whose lines are stable. The congruence $p \equiv \pm 3 \pmod 8$ is exactly the condition $\sqrt{2} \notin \mathbb{Q}_p$.

3.4. **From Theorem 1.4 to the corollaries.** Roy's derivation of his Corollary 2 from Theorem 1 [25, §§1–4] is linear algebra over K, $\overline{\mathbb{Q}}$ and $\mathbb{Q}$ together with the combinatorics of his admissible categories; the only field-dependent datum is ω. The formalization of that derivation over $\mathbb{C}$ [15] was ported to a field K of characteristic 0 and a $\mathbb{Q}$-subspace `LK` by a script (replacing $\mathbb{C}$ by K, the logarithms by `LK`, and Ω by 0) with a few hand patches; with $\Omega = 0$ every occurrence of the period terms collapses, which is Roy's remark on p. 24. The result (`LogIrr/Roy/`, about 2,700 lines) is

```
theorem strongSix_of_theorem1 :
    WaldschmidtTheorem1 K LK → StrongSixExponentials K LK
```

Corollary 1.6 is derived from Theorem 1.4 directly (`LogIrr/Roy/Baker.lean`), along the lines of [31, Cor. 3.3] to which Roy points in his Remark (iii), p. 37: transcendence of a nonzero $\ell \in L$ from the Gel'fond data $\mathbb{G}_{\mathrm{a}} \times \mathbb{G}_{\mathrm{m}}$, $Y = \mathbb{Q}(1,\ell)$, $W = V = K(1,\ell)$, where Roy's inequality forces s to kill Y; the homogeneous relation $\ell_2 = \beta_1\ell_1$ from Schneider data $\mathbb{G}_{\mathrm{a}} \times \mathbb{G}_{\mathrm{m}}$, $W = 0$; and the inhomogeneous relation $\ell_2 = \beta_0 + \beta_1\ell_1$ from $\mathbb{G}_{\mathrm{a}}^2 \times \mathbb{G}_{\mathrm{m}}$, $V = \{w = \beta_0 z_0 + \ell_1 z_1\}$, $W = K \cdot ((1,0),\beta_0)$, with a case analysis on the two blocks of s. Only two logarithms are needed for Theorem 1.3. The homogeneous statement for all n is Brumer's p-adic theorem [3]; we did not formalize it.

3.5. **Theorem 1.4: what changes over $\mathbb{C}_p$.** The proof over $\mathbb{C}$ [15] is a transcendence proof by Laurent's interpolation determinants [18]. Given (Y, W, V) and parameters (S, T, D_0, D_1) one forms the matrix of the derivatives $D_{w_1} \cdots D_{w_t} X^\lambda Y^\mu$ along a basis of the algebraic points of W, evaluated at the grid points $\exp_G(\sum s_i\eta_i)$, η_i a $\mathbb{Q}$-basis of Y. Either the columns are dependent, and Philippon's multiplicity estimate [23] produces an obstruction subgroup $H = h_0 \times T_U$ whose cokernel is the map s; or a maximal minor $\Delta \neq 0$ is bounded above analytically and below by Liouville's inequality, and the bounds contradict each other for large parameters. The p-adic proof keeps this architecture and the same parameters, and changes four things.

The multiplicity estimate needs nothing: `StrongSix.M2.multEst_of_isAlgClosed` of [15] is Philippon's theorem with derivatives on $\mathbb{G}_{\mathrm{a}}^{d_0} \times \mathbb{G}_{\mathrm{m}}^{d_1}$ over every algebraically closed field of characteristic 0 (following Roy's affine treatment in [32, Ch. 5, 8]), and $\overline{\mathbb{Q}} \subset \mathbb{C}_p$ is algebraically closed.

The field-generic half of the proof (the reduction to the case $1 \le \dim V$, $d_0 \le \dim V$; multilinearity of words of derivations; the interpolation matrix and the dichotomy; the exponent bookkeeping; the obstruction subgroup, the map s and $\dim s(W)$; the count of inequivalent grid points; the number field containing the data and the denominators and houses of the entries) was checked over $\mathbb{C}$ by the Lean kernel and re-checked over a field $\mathbb{K}$ after a mechanical port (`LogIrr/Thm1/`, about 1,700 lines). Three hand patches: Roy's preliminary quotient by $K \cdot (Y \cap \Omega)$ is vacuous since $\Omega = 0$; the point data no longer carry exp; and the step "equivalent grid points satisfy $s(\gamma - \gamma') \in \Omega'$", which over $\mathbb{C}$ uses $\ker \exp = 2\pi i\mathbb{Z}$, takes the multiplicative relation as a hypothesis, discharged p-adically by the injectivity of exp on its disc.

The p-adic half (`LogIrr/Padic/`, `LogIrr/PadicCore/`) replaces the archimedean ingredients:

(1) *The exponential and the small basis.* exp converges only on $|z| < \rho_p$. Every $\ell \in L$ satisfies $N\ell = \log y$ with $y \in \overline{\mathbb{Q}}$ arbitrarily close to 1: clear the denominators of a representation $\ell = \sum q_k \log x_k$ (induction over the span), then take a p-power, using $|x^{p^r} - 1| \le |x-1| \max(|x-1|^{p-1}, p^{-1})^r$. Hence a $\mathbb{Q}$-basis $\eta_1, \dots, \eta_\ell$ of Y can be rescaled by one integer N, which changes neither Y nor $\dim_{\mathbb{Q}} Y$, so that all second coordinates lie in the disc of exp and $\exp \eta_{i,2j}$ is algebraic, and all first coordinates are as small as required. Then exp is additive on the grid, the grid points are algebraic, and the injectivity of exp on its disc gives the multiplicative relation above. This is the rescaling $x'' = p^a x'$ of [29, §§4–5].

(2) *The entries.* The entry $(D_{w_1} \cdots D_{w_t} X^\lambda Y^\mu)(g_\gamma)$ at $g_\gamma = (\gamma_0, \exp \gamma_1)$ is the sum of its Taylor coefficients along $z \mapsto z\gamma$, computed algebraically as $c_k = (1/k!)(D_\gamma^k P)(e)$; the factor $1/k!$ is absorbed by the radius, and the Gauss norm of $D_{w_1} \cdots D_{w_t} X^\lambda Y^\mu$ is at most A^t when the coordinates of the w_i have norm $\le A$, since the integers produced by differentiation cost nothing p-adically. No analytic function of several variables is needed.

(3) *The Schwarz lemma.* The maximum modulus principle on $|z| = 2$ is replaced by the ultrametric multilinear expansion of the determinant with tails: the determinant of the Taylor-coefficient rows vanishes to order $\ge K = M(N - M^n) - \sum t_\nu$, a purely combinatorial count shared with the complex proof, and $|\Delta| \le A^{NT_J} p^{-K}$. This is the principle of [29, Lemme 3.4.p] and [5, §5]; there is no $N!$ and no maximum over a circle.

(4) *Liouville at the p-adic place.* For a nonzero algebraic integer β of a number field F of degree k and an embedding $\varphi\colon F \to \mathbb{C}_p$, $1 \le |\varphi\beta| \cdot \overline{|\beta|}^k$, where $\overline{|\beta|}$ is the house: the norm $N_{F/\mathbb{Q}}(\beta)$ is the product of the k embeddings $F \to \mathbb{C}_p$, which exist because $\mathbb{C}_p$ is algebraically closed, each factor is integral and so has $|\cdot| \le 1$, and $N_{F/\mathbb{Q}}(\beta)$ is a nonzero integer bounded by $\overline{|\beta|}^k$ at the complex places. The exponent is k rather than $k-1$ as over $\mathbb{C}$, which only changes constants.

The assembly is the complex one with the radius $r_0 = 1/p$, the two new bounds, and the logarithmic inequality $(M/2 - T_J)\log p \le T_J \log A + k\log N + k\log E + k\log H$ in place of its complex counterpart; the final growth comparison is reused verbatim. The p-adic analytic side is smaller than the complex one: no $N!$, no exponential of the size of the grid, no Siegel lemma, no auxiliary function on a polydisc.

Comparison with the published p-adic results. Waldschmidt [29] proves, for any complete non-archimedean field of characteristic 0 and residue characteristic p, the splitting theorem (Théorème 1.1.p) and the rank bound (Théorème 2.1.p) by Schneider's method, with a p-adic Siegel lemma, the ultrametric interpolation lemma and Masser's zero estimate without multiplicities; there is no derivative, no $\mathbb{G}_{\mathrm{a}}$ factor and no subspace W. Theorem 1.4 adds the $\mathbb{G}_{\mathrm{a}}^{d_0}$ factor (algebraic constants in the entries), derivatives along a $\overline{\mathbb{Q}}$-rational $W \neq 0$, the general V and the cokernel s, and uses interpolation determinants instead of Siegel's lemma. Théorème 2.1.p is the case $d_0 = 0$, $W = 0$, through Roy's §4. The analytic subgroup theorem of [12] is the Gel'fond case $W = V$ with one point. Dasgupta [5, §5] proves the p-adic Waldschmidt–Masser theorem (entries in L, no constants, no derivatives). Laurent's paper [17], which Roy says uses the p-adic theorem, was not accessible to us.

4. Related work

The p-adic linear-subgroup theorem. Serre proved the p-adic six exponentials theorem [27] and Brumer the p-adic Baker theorem [3]. Waldschmidt's [29] has a second part, "le cas p-adique", proving the several-variable generalization of the six exponentials theorem and the bound $r_p \ge r/2$ for the p-adic rank of units; the Budapest and Grenoble talks [30] present the same result. The mixed statement with a derivative subspace is Theorem 4.1 of [31], stated and proved over $\mathbb{C}$. Roy [25] states it for $K = \mathbb{C}$ or $\mathbb{C}_p$ with $\omega = 0$, builds his rank theory on it for both fields, and applies it p-adically in his §6; see also [26]. Later p-adic uses cite Roy: [13], [4, §3], [2, Thm 1.8], [19, Thm 2.2.1]. Waldschmidt's survey [35, §§5–6] says that for the strong six exponentials theorem "as always, the situation is the same in the p-adic case". On the Gel'fond side, the p-adic analytic subgroup theorem is due to Matev [20] and Fuchs–Pham [11, 12]; Dasgupta [5] and Dasgupta–Kakde [6] treat the archimedean and p-adic structural rank conjectures. We found no proof written for $\mathbb{C}_p$ of the mixed statement. The statement should be

regarded as folklore since Roy, and our claim is only that we could not locate a written proof.

Products of logarithms and conjugation. Diaz [8] used complex conjugation with the six exponentials theorem to show, for instance, that $\log a \cdot \log(2+i) \notin \mathcal{L}$ for real $\log a$, and in [9] derived from Roy's theorem partial cases of the strong four exponentials conjecture, including the "one of two implies both" upgrade that Theorem 1.3 transposes. Waldschmidt's surveys [34, 33] collect these results; none has p-adic content. Momot [21] generalizes Diaz by Weil restriction to real subfields and leaves the ultrametric analogue to a further paper. Betina–Dimitrov [2] and Maksoud [19] use the strong six exponentials theorem over $\overline{\mathbb{Q}}_p$ for "one of two" non-vanishing statements and leave "both" to the strong four exponentials conjecture; the quantities there are 2×2 minors, not products.

Formalizations. Machine-checked transcendence results before this work: e and π in several provers, Lindemann–Weierstrass [1, 10], Liouville numbers (Mathlib), Gelfond–Schneider in Lean [14], and the author's strong six exponentials theorem over $\mathbb{C}$ with Waldschmidt's theorem and Philippon's multiplicity estimate [15], on which the present library is built. The library [22] (unrefereed; its README reports standard axioms) claims the classical six exponentials theorem, qualitative Baker's theorem and Gelfond–Schneider over $\mathbb{C}$, and carries Roy's strong six exponentials theorem as a hypothesis; its README mentions a branch, not inspected by us, for Brumer's p-adic theorem. Mathlib has $\mathbb{C}_p$ and the generic exponential but no p-adic logarithm and no radius bound for exp over $\mathbb{C}_p$; these were built here. The novelty claims of Section 1 rest on web, arXiv and zbMATH searches recorded with the paper; MathSciNet was not available to us.

5. AI-assisted formalization

The prose proofs, the Lean code and the text of this paper were produced by AI models (Claude, Anthropic) working in Claude Code under the direction of the author, in the following order. A note was written stating Theorem 1.1 and proving it modulo two inputs labelled as taken from the literature, Corollaries 1.5 and 1.6 over $\mathbb{C}_p$, and checking line by line that Roy's reduction is field-independent. A second note classified every lemma of the complex Lean proof of Waldschmidt's theorem as field-independent or archimedean and supplied the four p-adic replacements of Section 3.5. The Lean files were then written against these notes: first Theorem 1.1 with Corollaries 1.5 and 1.6 as explicit hypotheses, then the two corollaries from Theorem 1.4 as a hypothesis, then Theorem 1.4 itself, so that each implication was checked before the next input was attempted. The complex formalization was reused by mechanical renaming where it was field-generic and reproved where it was not. The whole development took two days.

An independent AI session, separate from the ones that wrote the proofs, audited the definitions of Section 2 against Roy's paper and wrote the trust

document in the repository; another ran the literature search of Section 4. Apart from the check by the Lean kernel, all verification so far has been carried out by AI systems. No human expert has yet reviewed the Lean definitions against the literature or read the proofs; we would be grateful for corrections. The author is responsible for the intended statements and for the claims made here.

6. Formal artifact and verification

The formalization uses Lean 4 [7] and Mathlib [28].

Repository	`https://github.com/telaviv/p-adic-log-products`
Commit	`9e4570067a2140f7193e3befee3bf0f1335419d8`
Lean	`leanprover/lean4:v4.35.0`
Mathlib	`v4.35.0`
Mathlib commit	`56a005855ea17e0b0958f73ec801ae140b0a1679`
Dependency	`https://github.com/telaviv/strong-six-exponentials`
Dependency commit	`1625bdf3c0a7d9222bacd876d738d7540109bea6`

The toolchain and package revisions are pinned in `lean-toolchain` and `lake-manifest.json`. The library `LogIrr` has 50 files and about 10,400 lines; from the dependency it imports only field-generic modules (the multiplicity estimate, the invariant derivations, heights and houses, Liouville's inequality), none of which mentions $\mathbb{C}$.

Directory	Lines	Content
`LogIrr/` (top level)	3,022	the logarithm on $\mathcal{U}$, $\exp \circ \log$, the Galois action, the arithmetic of $3 \pm \sqrt{2}$, Proposition 3.1, Theorems 1.1, 1.2, 1.3
`LogIrr/Roy/`	3,376	Theorem 1.4 $\Rightarrow$ Corollaries 1.5, 1.6, over any field of characteristic 0
`LogIrr/Thm1/`	1,680	the field-generic half of the proof of Theorem 1.4
`LogIrr/Padic/`	982	the p-adic half and the assembly
`LogIrr/PadicCore/`	942	the p-adic exponential and the ultrametric determinant bound
`LogIrr/Inst/`	270	the instances of Theorem 1.2

To build the library at the pinned revision:

```
git clone https://github.com/telaviv/p-adic-log-products
cd p-adic-log-products
git checkout 9e4570067a2140f7193e3befee3bf0f1335419d8
lake exe cache get
lake build
```

The build compiles the dependency's multiplicity estimate and takes about fifteen minutes on a desktop once Mathlib is cached. To inspect the endpoints and their axiom closures, run `lake env lean Axioms.lean`; the file contains, among queries for the intermediate results,

```
#print axioms LogIrr.e2_unconditional
#print axioms LogIrr.Quad.main_unconditional
#print axioms LogIrr.thm51_pm_unconditional
#print axioms LogIrr.Padic.waldschmidtTheorem1_p
#print axioms LogIrr.royCor2
#print axioms LogIrr.bakerBrumer
```

Every one of the 44 queries yields `[propext, Classical.choice, Quot.sound]`; the output is recorded in the repository's `TRUST.md`. The source contains no `sorry`, no `axiom` declaration and no `native_decide`. These checks concern the named declarations and their dependencies; the mathematical meaning of the results also depends on the definitions reproduced in Section 2, and `TRUST.md` compares each of them with its source.

7. Open questions

(1) A proof written for $\mathbb{C}_p$ of the mixed Theorem 1.4 in the literature, perhaps in [17], would make Section 3.5 a confirmation rather than a first proof.
(2) The complex analogue of Theorem 1.1, and the strong four exponentials conjecture over $\mathbb{C}_p$: the method says nothing about $\log_p 2 \cdot \log_p 3$ or about $(\log_p \alpha)^2$, whose $\overline{\mathbb{Q}}$-lines are stable under $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$.
(3) A "swap" version of Theorem 1.3, with $\sigma t \in \overline{\mathbb{Q}} + \overline{\mathbb{Q}}u$ and $1, t, \sigma u$ independent, gives instances in cyclic cubic fields such as $\log_p \theta \cdot \log_p \tau\theta$ for $\theta = 2\cos(2\pi/7)$; it has no complex counterpart, since it needs a Galois element of order 3 acting continuously. It is proved in the project notes but not formalized.
(4) Brumer's theorem for all n, and the "one of two" statements of [2, 19] that the local Galois action upgrades to "both".

Acknowledgements

We thank Michel Waldschmidt for making his papers and [32] freely available.

References

1. Sophie Bernard, *Formalization of the Lindemann–Weierstrass theorem*, Interactive Theorem Proving (ITP 2017), Lecture Notes in Computer Science, vol. 10499, Springer, Cham, 2017, pp. 65–80.
2. Adel Betina and Mladen Dimitrov, *Geometry of the eigencurve at CM points and trivial zeros of Katz p-adic L-functions*, Adv. Math. **384** (2021), 107724.

3. Armand Brumer, *On the units of algebraic number fields*, Mathematika **14** (1967), 121–124.
4. Frank Calegari and Barry Mazur, *Nearly ordinary Galois deformations over arbitrary number fields*, J. Inst. Math. Jussieu **8** (2009), 99–177.
5. Samit Dasgupta, *Ranks of matrices of logarithms of algebraic numbers I: the theorems of Baker and Waldschmidt–Masser*, Essent. Number Theory **2** (2023), 93–138.
6. Samit Dasgupta and Mahesh Kakde, *Ranks of matrices of logarithms of algebraic numbers II: the matrix coefficient conjecture*, Adv. Math. **487** (2026), 110753.
7. Leonardo de Moura and Sebastian Ullrich, *The Lean 4 theorem prover and programming language*, Automated Deduction – CADE 28, Lecture Notes in Computer Science, vol. 12699, Springer, Cham, 2021, pp. 625–635.
8. Guy Diaz, *Utilisation de la conjugaison complexe dans l'étude de la transcendance de valeurs de la fonction exponentielle usuelle*, J. Théor. Nombres Bordeaux **16** (2004), 535–553.
9. ———, *Produits et quotients de combinaisons linéaires de logarithmes de nombres algébriques: conjectures et résultats partiels*, J. Théor. Nombres Bordeaux **19** (2007), 373–391.
10. Manuel Eberl, *The Hermite–Lindemann–Weierstraß transcendence theorem*, Archive of Formal Proofs, `https://isa-afp.org/entries/Hermite_Lindemann.html`, 2021.
11. Clemens Fuchs and Duc Hiep Pham, *Commutative algebraic groups and p-adic linear forms*, Acta Arith. **169** (2015), 115–147.
12. ———, *The p-adic analytic subgroup theorem revisited*, p-Adic Numbers Ultrametric Anal. Appl. **7** (2015), 143–156.
13. Jean-François Jaulent, *Classes logarithmiques des corps totalement réels*, Acta Arith. **103** (2002), 1–7.
14. Michail Karatarakis and Freek Wiedijk, *A formalization of the Gelfond–Schneider theorem*, arXiv:2603.24823, 2026.
15. Shawn Krisman, *A Lean formalization of Roy's strong six exponentials theorem*, Preprint and Lean library, `https://github.com/telaviv/strong-six-exponentials`, 2026.
16. ———, *p-adic-log-products: Lean 4 proofs of a p-adic linear-subgroup theorem and of products of p-adic logarithms outside the linear forms in logarithms*, `https://github.com/telaviv/p-adic-log-products`, 2026.
17. Michel Laurent, *Rang p-adique d'unités et action de groupes*, J. Reine Angew. Math. **399** (1989), 81–108.
18. ———, *Linear forms in two logarithms and interpolation determinants*, Acta Arith. **66** (1994), no. 2, 181–199.
19. Alexandre Maksoud, *On the rank of Leopoldt's and Gross's regulator maps*, Doc. Math. **28** (2023), 1441–1471.
20. Tzanko Matev, *The p-adic analytic subgroup theorem and applications*, arXiv:1010.3156, 2010.
21. Aleksander Momot, *Density of rational points on commutative group varieties and small transcendence degree*, arXiv:1011.3368, 2010.
22. Carlo Perassi, *diaz-modulus-lean: Transcendence theory in Lean 4*, `https://github.com/carlok/diaz-modulus-lean`, 2026, Accessed October 2026.
23. Patrice Philippon, *Lemmes de zéros dans les groupes algébriques commutatifs*, Bull. Soc. Math. France **114** (1986), 355–383, Errata et addenda: ibid. 115 (1987), 397–398.
24. Alain M. Robert, *A course in p-adic analysis*, Graduate Texts in Mathematics, vol. 198, Springer-Verlag, New York, 2000.
25. Damien Roy, *Matrices whose coefficients are linear forms in logarithms*, J. Number Theory **41** (1992), 22–47.
26. ———, *On the v-adic independence of algebraic numbers*, Advances in Number Theory (Kingston, 1991), Oxford Univ. Press, New York, 1993, pp. 441–451.

27. Jean-Pierre Serre, *Dépendance d'exponentielles p-adiques*, Séminaire Delange-Pisot-Poitou. Théorie des nombres **7** (1965/66), no. 2, Exp. No. 15, 14 pp.
28. The mathlib Community, *The Lean mathematical library*, Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP 2020) (New York), Association for Computing Machinery, 2020, pp. 367–381.
29. Michel Waldschmidt, *Transcendance et exponentielles en plusieurs variables*, Invent. Math. **63** (1981), 97–127.
30. ———, *A lower bound for the p-adic rank of the units of an algebraic number field*, Topics in Classical Number Theory (Budapest, 1981), Colloq. Math. Soc. János Bolyai, vol. 34, North-Holland, Amsterdam, 1984, pp. 1617–1650.
31. ———, *On the transcendence methods of Gel'fond and Schneider in several variables*, New Advances in Transcendence Theory (Durham, 1986) (Alan Baker, ed.), Cambridge Univ. Press, Cambridge, 1988, pp. 375–398.
32. ———, *Diophantine approximation on linear algebraic groups*, Grundlehren der Mathematischen Wissenschaften, vol. 326, Springer-Verlag, Berlin, 2000, Chapters 5 and 8 by Damien Roy.
33. ———, *Further variations on the six exponentials theorem*, Hardy-Ramanujan J. **28** (2005), 1–9.
34. ———, *Variations on the six exponentials theorem*, Algebra and Number Theory (Hyderabad, 2003), Hindustan Book Agency, Delhi, 2005, pp. 338–355.
35. ———, *The four exponentials problem and Schanuel's conjecture*, Mathematics Going Forward, Lecture Notes in Math., vol. 2313, Springer, Cham, 2023, pp. 579–592.