A kit for linear forms in three p-adic logarithms

David Niedbala Giraudin
ORCID 0009-0009-1526-1178

Version 4, 30 October 2026; references updated 3 November 2026

hexagon:2610.00706v2

Abstract

We transpose to the p-adic case the kit of Mignotte and Voutier for linear forms in three logarithms. The new tool is a lower bound for the p-adic valuation of interpolation determinants with no factorial loss: it is obtained by expanding the powers $\theta^{\ell z}$ as binomial series in $\theta-1$, and then transporting an order of vanishing that we compute optimally for generic points, by means of the initial forms of the space of exponential polynomials involved. It holds for every prime p. Combined with a rearrangement bound for the spread of the exponents and with Gouillon's zero lemma applied within a Teichmüller class, it gives a criterion of the form of criterion (2.8) of Mignotte–Voutier, in which $\log\rho$ is replaced by $\log p$ and the height term contains no analytic contribution. For two logarithms, in $\mathbb{Q}_p$ with p odd, it improves Lemma 8 of Bugeaud–Laurent. A change of basis in the multiplicative group reduces to the case of principal units: the factor $g=p-1$ leaves the volumes and moves into the heights. On examples, with exponents up to 10^{10} or 10^{30}, the complete bounds (degenerate cases included) are 154 to 667 times smaller than those of Yu's explicit theorem for $p\in\{5,13\}$, 608 to 1980 times for $p\in\{7,11\}$ (where the explicit form of Yu goes through $\mathbb{Q}(i)$), and 73 to 105 times for $p=101$.

1 Results

Explicit lower bounds for linear forms in logarithms come in two forms: general theorems, in $\log B$ (Matveev in the complex case, Yu in the p-adic case), and methods of interpolation determinants, in $(\log B)^2$ but with much smaller constants, which serve to reduce a first bound. For two logarithms, the latter exist in both cases (Laurent [6]; Bugeaud–Laurent [2], then Chim [3] with a dependence in $\log B$). For three logarithms, Mignotte and Voutier [7] gave a kit for the complex case. To our knowledge there was none for the p-adic case; we give one here.

Setting

Let p be a prime, $\alpha_1,\alpha_2,\alpha_3\geq 2$ integers prime to p, multiplicatively independent, and $b_1,b_2,b_3\geq 1$ integers with $\gcd(b_1,b_2,b_3)=1$ and $p\nmid b_3$. Put

$$\Lambda=\alpha_1^{b_1}\alpha_2^{b_2}-\alpha_3^{b_3}\neq 0,\qquad \beta_1=\frac{b_1}{b_3},\quad \beta_2=\frac{b_2}{b_3},\qquad g=\begin{cases}p-1 & p\neq 2,\\ 1 & p=2.\end{cases}$$

Write $d_1=\gcd(b_1,b_3)$, $d_2=\gcd(b_2,b_3)$, $b_3'=b_3/d_1$, $b_1'=b_1/d_1$, $b_3''=b_3/d_2$, $b_2''=b_2/d_2$. For p odd, write $\alpha_i=\zeta^{n_i}\theta_i$, where ζ is a primitive $(p-1)$-th root of unity in $\mathbb{Z}_p$, $n_i\in\mathbb{Z}$ and $\theta_i\in 1+p\mathbb{Z}_p$; for $p=2$, take $n_i=0$ and $\theta_i=\alpha_i\in 1+2\mathbb{Z}_2$.

Let $K,L\geq 1$ be integers, $N=K(K+1)L/2$, and consider the family of the N indices (k_i,m_i,ℓ_i) with $k_i+m_i\leq K-1$ and $0\leq\ell_i\leq L-1$; each value of ℓ is taken $K(K+1)/2$ times. For N distinct triples (r_j,s_j,t_j) of non-negative integers, put

$$\Delta=\det\Big(\tbinom{r_jb_3'+t_jb_1'}{k_i}\tbinom{s_jb_3''+t_jb_2''}{m_i}\,\alpha_1^{\ell_ir_j}\alpha_2^{\ell_is_j}\alpha_3^{\ell_it_j}\Big)_{1\leq i,j\leq N}\in\mathbb{Z},$$

which is the determinant (2.6) of [7]. Let D_V be the multiset $\{a+c : 0 \le a \le K-1,\ 0 \le c \le (K-a)L-1\}$, of cardinality N, and, for $0 \le I \le N$, let $\Theta_V(I)$ be the sum of the I smallest elements of D_V. This number is at least the quantity $\Theta(K-1, I)$ of [7, (3.1)] used in Waldschmidt's multiplicity lemma.

Theorem 1 (analytic upper bound with no loss)**.** *Assume $n_1 r_j + n_2 s_j + n_3 t_j \equiv c \pmod g$ for one c and every j. Then*

$$v_p(\Delta) \ \ge \ \min_{0 \le I \le N} \Big((N-I)\, v_p(\Lambda) + \Theta_V(I) \Big) - \sum_{i=1}^{N} (k_i + m_i).$$

If moreover $v_p(\Lambda) \ge KL - 1$, then

$$v_p(\Delta) \ \ge \ \frac{N}{2} \cdot \frac{(2K+1)(L-1)}{3}.$$

With Waldschmidt's bound, the main term would be $\frac{N^2}{2K}$, that of Proposition 3.7 of [7]; here it is asymptotically $\frac{N^2}{2K} \cdot \frac{4}{3}$. No loss of the type $v_p(n!)$ occurs, and no hypothesis on the size of K or L relative to p is required.

Put

$$E(K,L) = \frac{(2K+1)(L-1)}{3}, \qquad \lambda_L = \frac{2\lfloor L^2/4 \rfloor}{L},$$

and, as in (2.5) of [7],

$$b = \frac{(R-1)b_3 + (T-1)b_1}{2d_1} \cdot \frac{(S-1)b_3 + (T-1)b_2}{2d_2} \cdot \Big(\prod_{k=1}^{K-1} (k!)^{K-k} \Big)^{-12/(K(K-1)(K+1))}.$$

Theorem 2 (criterion for three p-adic logarithms)**.** *Let $K \ge 2$, $L \ge 2$, $R_j, S_j, T_j \ge 1$ $(j = 1,2,3)$ be integers, $R > R_1 + R_2 + R_3$, $S > S_1 + S_2 + S_3$, $T > T_1 + T_2 + T_3$, $\chi > 0$, $V = \sqrt{(R_1+1)(S_1+1)(T_1+1)}$ and $\mathcal{M} = \max\{R_1+S_1+1, S_1+T_1+1, R_1+T_1+1, \chi V\}$. Assume*

$$\begin{aligned}
&\text{(Z1)} \quad (R_1+1)(S_1+1)(T_1+1) > g\,K\,\mathcal{M} \quad \text{and} \quad (R_1+1)(S_1+1)(T_1+1) > g\,L,\\
&\text{(Z2)} \quad (R_2+1)(S_2+1)(T_2+1) > g \max\{2KL,\, K^2\},\\
&\text{(Z3)} \quad (R_3+1)(S_3+1)(T_3+1) > 3g\,K^2 L,
\end{aligned}$$

$$E(K,L)\log p \ > \ \log N + \frac{2(K-1)}{3}\log b + \lambda_L\big((R-1)\log\alpha_1 + (S-1)\log\alpha_2 + (T-1)\log\alpha_3\big). \quad (1)$$

Then $v_p(\Lambda) \le KL - 2$, unless one of the conditions (2.14), (2.15) of [7] holds.

Recall that (2.14) is $b_1 \le \max\{R_1, R_2\}$, $b_2 \le \max\{S_1, S_2\}$, $b_3 \le \max\{T_1, T_2\}$; in that case $v_p(\Lambda) \le \log|\Lambda|/\log p \le (b_1\log\alpha_1 + b_2\log\alpha_2 + b_3\log\alpha_3)/\log p$. Condition (2.15) is the existence of coprime integers $(u_1, u_2, u_3) \ne 0$ with $u_1 b_1 + u_2 b_2 + u_3 b_3 = 0$ and $|u_1| \le U_1$, $|u_2| \le U_2$, $|u_3| \le U_3$, where $U_1 = \frac{(S_1+1)(T_1+1)}{\mathcal{M} - \max\{S_1, T_1\}}$, etc. [7, (2.15)]; it reduces to two logarithms (Section 6).

Compared with (2.8) of [7], criterion (1) replaces $\log\rho$ by $\log p$, and the term $gL(a_1R + a_2S + a_3T)$, where $a_i \ge \rho|\log\alpha_i| + \log\alpha_i$ in the real case, by $\lambda_L \sum (R-1)\log\alpha_i \approx \frac{L}{4}\sum R \cdot 2\log\alpha_i$: there is no analytic term in $\rho|\log\alpha_i|$; moreover, the main term of the left-hand side is $\frac{2KL}{3}$ instead of $\frac{KL}{2}$. The price is the factor g in the volumes of the boxes. The hypothesis $p \nmid b_3$ concerns the exponent of the isolated term; Yu's theorem does not require it.

Corollary 3 (two logarithms)**.** *Let p be a prime, $\gamma_1 = a_1/c_1$, $\gamma_2 = a_2/c_2$ two multiplicatively independent rationals with $p \nmid a_1c_1a_2c_2$, $h_i \ge \log\max\{|a_i|, |c_i|\}$, and $b_1, b_2 \ge 1$ integers with $p \nmid b_2$. Put $\Lambda_2 = \gamma_1^{b_1} - \gamma_2^{b_2}$ and $\gamma_i = \zeta^{n_i}\theta_i$ as above ($n_i = 0$ if $p = 2$). Let $\Lambda^* \subset \mathbb{Z}^2$ be a sublattice of index g contained in $\{(r,s) : n_1 r + n_2 s \equiv 0 \pmod g\}$ (one always exists). Let*

$K \geq 3$, $L \geq 2$, $R_1, R_2, S_1, S_2 \geq 1$, $R = R_1 + R_2 - 1$, $S = S_1 + S_2 - 1$, $N = KL$ *and* $b = \frac{(R-1)b_2+(S-1)b_1}{2}\big(\prod_{k=1}^{K-1} k!\big)^{-2/(K^2-K)}$. *Assume that there are translates* C_1, C_2 *of* Λ^* *such that*

$$\#\{\gamma_1^r\gamma_2^s : r < R_1,\, s < S_1,\, (r,s) \in C_1\} \geq L,$$
$$\#\{b_2 r + b_1 s : r < R_2,\, s < S_2,\, (r,s) \in C_2\} > (K-1)L,$$

and that

$$K(L-1)\log p > \log N + (K-1)\log b + \kappa_1 h_1 + \kappa_2 h_2,$$

where $\kappa_1 = \min\big\{\lambda_L(R-1),\ \frac{L(R+g-1)}{2} - \frac{gNL}{6(S+g-1)}\big\}$ *and* $\kappa_2 = \min\big\{\lambda_L(S-1),\ \frac{L(S+g-1)}{2} - \frac{gNL}{6(R+g-1)}\big\}$. *Then* $v_p(\Lambda_2) \leq KL-2$. *In particular, the bound* $v_p(x^{p-1}-1) \leq 69(p-1)\frac{\log y \log xy}{(\log p)^2} + 4$ *of [9], which lowers Yamada's constant* 283 *[10], holds with* 3 *instead of* 4.

2 Analytic bound (Theorem 1)

2.1 Setting up

Assume $v_p(\Lambda) \geq 1$, otherwise there is nothing to prove. Then $\zeta^{n_3 b_3} = \zeta^{n_1 b_1 + n_2 b_2}$ and $\theta_3^{b_3} = \theta_1^{b_1}\theta_2^{b_2}(1+\varepsilon)$ with $1 + \varepsilon = 1 - \Lambda/(\alpha_1^{b_1}\alpha_2^{b_2})$, so $v_p(\varepsilon) = v_p(\Lambda)$. Since $p \nmid b_3$, raising to the power b_3 is a bijection of $1 + p\mathbb{Z}_p$ (of $1 + 2\mathbb{Z}_2$ if $p = 2$), and $\theta_3 = \theta_1^{\beta_1}\theta_2^{\beta_2}(1+\varepsilon)^{1/b_3}$, powers with exponent in $\mathbb{Z}_{(p)}$ being defined by the binomial series. Put $z_{1,j} = r_j + t_j\beta_1$, $z_{2,j} = s_j + t_j\beta_2 \in \mathbb{Z}_{(p)}$, $X_j = b_3' z_{1,j}$, $Y_j = b_3'' z_{2,j} \in \mathbb{Z}$. All columns being in the class c, row i contains the common factor $\zeta^{\ell_i c}$, of valuation zero, and

$$v_p(\Delta) = v_p\Big(\det\big(\tbinom{X_j}{k_i}\tbinom{Y_j}{m_i}\theta_1^{\ell_i z_{1,j}}\theta_2^{\ell_i z_{2,j}}(1+\varepsilon)^{\ell_i t_j/b_3}\big)\Big).$$

Write $(1+\varepsilon)^{\ell_i t_j/b_3} = 1 + \varepsilon\,\delta_{ij}$; since $(1+\varepsilon)^e - 1 = \sum_{n\geq 1}\binom{e}{n}\varepsilon^n$ for $e \in \mathbb{Z}_p$, we have $\delta_{ij} \in \mathbb{Z}_p$. By multilinearity in the rows, the determinant equals $\sum_{I\subset\{1,\dots,N\}} \varepsilon^{N-|I|} F_I(\theta_1 - 1, \theta_2 - 1)$, where $F_I(u_1, u_2)$ is the determinant whose row i is $\binom{X_j}{k_i}\binom{Y_j}{m_i}(1+u_1)^{\ell_i z_{1,j}}(1+u_2)^{\ell_i z_{2,j}}$, multiplied entry by entry by δ_{ij} if $i \notin I$.

2.2 Integrality

For $z \in \mathbb{Z}_p$, $(1+u)^z = \sum_{a\geq 0}\binom{z}{a}u^a$ has its coefficients in $\mathbb{Z}_p$. Hence $F_I \in \mathbb{Z}_p[[u_1, u_2]]$. If F_I has order at least A at the origin, the series converges at $u = \theta - 1$, since $v_p(\theta_i - 1) \geq 1$, and $v_p(F_I(\theta - 1)) \geq A$: each monomial of total degree $d \geq A$ has valuation at least d.

2.3 Order of vanishing

Let $\vartheta \in \mathbb{C}^2\setminus\{0\}$, $\lambda_0, \dots, \lambda_{L-1}$ pairwise distinct, and $V = \mathrm{Span}\{z_1^k z_2^m e^{\lambda_\ell \vartheta\cdot z} : k+m \leq K-1,\ \ell < L\}$.

Proposition 4 (multiplicity [8])**.** *Let* $I \subset \{1,\dots,N\}$, $\xi_1, \dots, \xi_N \in \mathbb{C}^2$, *and* $\Psi(x)$ *an* $N \times N$ *determinant whose rows of index* $i \in I$ *are* $(\varphi_i(x\xi_j))_j$ *with* $\varphi_i \in V$, *the other rows having entries analytic in* x. *Then* $\mathrm{ord}_0\,\Psi \geq \Theta_V(|I|)$.

Proof. Let $w = \vartheta \cdot z$ and u a complementary linear form. Then $V = \bigoplus_{a<K} u^a W_a$ with $W_a = \mathrm{Span}\{w^b e^{\lambda_\ell w} : b \leq K-1-a\}$, the solution space of $\prod_\ell(\frac{d}{dw} - \lambda_\ell)^{K-a} y = 0$, of order $n_a = (K-a)L$: a non-zero element of W_a has order at most $n_a - 1$ at $w = 0$ (uniqueness for the Cauchy problem). The initial form of a non-zero $f = \sum_a u^a f_a \in V$ is therefore a combination of monomials $u^a w^c$ with $c \leq n_a - 1$, with no cancellation between distinct indices a. For a subspace $W \subset V$ of dimension I', a basis of W with independent initial forms has initial degrees forming a sub-multiset of D_V; for arbitrary points, the corresponding determinant has order at least the sum of these degrees, hence at least $\Theta_V(I')$. We conclude by a Laplace expansion of Ψ along the rows with index in I (the complementary minors are analytic). □

Lemma 5. *F_I has order at least $\Theta_V(|I|) - \sum_{i=1}^N (k_i + m_i)$ at the origin.*

Proof. Put $G_I(\omega_1, \omega_2) = F_I(e^{\omega_1} - 1, e^{\omega_2} - 1) \in \mathbb{Q}_p[[\omega]]$. Since $(1+u)^z = \exp(z \log(1+u))$ in $\mathbb{Q}_p[[u]]$, row i of G_I is $\binom{X_j}{k_i}\binom{Y_j}{m_i} \exp\big(\ell_i(\omega_1 z_{1,j} + \omega_2 z_{2,j})\big)$, multiplied by δ_{ij} if $i \notin I$. The polynomial $\binom{b_3' z_1}{k}\binom{b_3'' z_2}{m}$ is a combination of monomials $z_1^{\mu_1} z_2^{\mu_2}$ with $\mu_1 + \mu_2 \le k + m$. By multilinearity, G_I is a combination of determinants $G_{I,\mu}$ whose row i is $z_{1,j}^{\mu_{i,1}} z_{2,j}^{\mu_{i,2}} \exp(\ell_i\, \omega \cdot z_j)$ (times δ_{ij} if $i \notin I$), with $d_i := \mu_{i,1} + \mu_{i,2} \le k_i + m_i \le K - 1$. For such a determinant and $\vartheta = (\vartheta_1, \vartheta_2) \in \mathbb{C}^2 \setminus \{0\}$, the function

$$\Psi(x) = \det\Big((x z_{1,j})^{\mu_{i,1}} (x z_{2,j})^{\mu_{i,2}} \exp\big(\ell_i(\vartheta_1 x z_{1,j} + \vartheta_2 x z_{2,j})\big)[\delta_{ij}] \Big) = x^{\sum d_i}\, G_{I,\mu}(x\vartheta_1, x\vartheta_2)$$

vanishes at $x = 0$ to order at least $\Theta_V(|I|)$, by Proposition 4 ($\lambda_\ell = \ell$; the rows of index $i \in I$ lie in V, the others are multiplied by constants). The $z_{i,j}$ are rational and the δ_{ij} enter polynomially: the identity, true for arbitrary complex δ_{ij}, holds formally. The homogeneous components of $G_{I,\mu}$ of degree $< \Theta_V(|I|) - \sum d_i$ therefore vanish at every $\vartheta \neq 0$, hence identically. Thus G_I has order at least $\Theta_V(|I|) - \sum(k_i + m_i)$. Finally $F_I(u) = G_I(\log(1+u_1), \log(1+u_2))$, and substituting series with no constant term and with linear part the identity does not decrease the order. □

End of the proof. We obtain $v_p(\Delta) \ge \min_I \big((N - |I|) v_p(\Lambda) + \Theta_V(|I|)\big) - \sum(k_i + m_i)$, for all $K, L \ge 1$. If $v_p(\Lambda) \ge KL - 1$, since every element of D_V is at most $KL - 1$, the minimum is attained at $I = N$, and $\Theta_V(N) - \sum_i (k_i + m_i) = \frac{N(2K+1)(L-1)}{6}$ by a direct computation ($\sum_i (k_i + m_i) = LK(K+1)(K-1)/3$). □

Remark 6. The first inequality of Theorem 1 is attained in many small configurations: the verifier finds equality there. For generic points and $I = N$, Proposition 4 is optimal [8].

3 Arithmetic bound

Lemma 7 (rearrangement)**.** *Let $\ell_1, \dots, \ell_N$ take each value $0, \dots, L-1$ exactly Q times ($N = QL$) and let $r_1, \dots, r_N \in [0, R-1]$. For every permutation σ, $\big|\sum_i \ell_i r_{\sigma(i)} - \frac{L-1}{2} \sum_j r_j\big| \le \frac{(R-1)Q\lfloor L^2/4 \rfloor}{2}$.*

Proof. Since $\sum_i (\ell_i - \frac{L-1}{2}) = 0$, the difference equals $\sum_i (\ell_i - \frac{L-1}{2})(r_{\sigma(i)} - \frac{R-1}{2})$, whose absolute value is at most $\frac{R-1}{2} Q \sum_{\ell=0}^{L-1} |\ell - \frac{L-1}{2}| = \frac{R-1}{2} Q \lfloor L^2/4 \rfloor$. □

Proposition 8. *If $\Delta \neq 0$, then*

$$\frac{2}{N}\, v_p(\Delta) \log p \le \log N + \frac{2(K-1)}{3} \log b + \lambda_L\big((R-1)\log\alpha_1 + (S-1)\log\alpha_2 + (T-1)\log\alpha_3\big),$$

where R, S, T are strict upper bounds for the coordinates of the points.

Proof. As in Proposition 3.9 of [7], $\Delta = \mathcal{P}(\alpha_1, \alpha_2, \alpha_3)$ with $\mathcal{P} \in \mathbb{Z}[X_1, X_2, X_3]$, whose monomials have exponents $(\sum \ell_i r_{\sigma(i)}, \sum \ell_i s_{\sigma(i)}, \sum \ell_i t_{\sigma(i)})$, and $|\mathcal{P}| \le N^{N/2} b^{(K-1)N/3}$ for the sup norm on the torus. Lemma 7, with $Q = K(K+1)/2$, places these exponents in intervals of lengths $2G_1, 2G_2, 2G_3$, where $G_1 = \frac{(R-1)K(K+1)\lfloor L^2/4 \rfloor}{4}$, etc. Write $\Delta = \alpha^U \widetilde{\mathcal{P}}(\alpha)$, where U_i is the least exponent of X_i among the monomials with non-zero coefficient; $\widetilde{\mathcal{P}} \in \mathbb{Z}[X]$ has degrees at most $2G_i$ and $|\widetilde{\mathcal{P}}| = |\mathcal{P}|$. The integer $\widetilde{\mathcal{P}}(\alpha)$ is non-zero, with the same valuation as Δ. By the maximum principle on the polydisc applied to $X^{2G} \widetilde{\mathcal{P}}(1/X)$, with $\alpha_i \ge 1$, $|\widetilde{\mathcal{P}}(\alpha)| \le |\mathcal{P}| \prod \alpha_i^{2G_i}$. We conclude with $p^{v_p(\Delta)} \le |\widetilde{\mathcal{P}}(\alpha)|$ and $4G_1/N = \lambda_L(R-1)$. □

4 Zero lemma within a class

Proposition 9. *Under (Z1)–(Z3), and if neither (2.14) nor (2.15) of [7] holds, there is a class c modulo g such that the matrix formed by the columns (r,s,t), $0 \le r < R$, $0 \le s < S$, $0 \le t < T$, $n_1 r + n_2 s + n_3 t \equiv c$, has rank N.*

Proof. For $j = 1,2,3$, let $B_j = [0,R_j] \times [0,S_j] \times [0,T_j]$ and let c_j be a class containing the largest number $C_j \ge |B_j|/g$ of points of B_j. Let Σ_j be the image of the points of B_j of class c_j under $\psi(r,s,t) = (r + t\beta_1, s + t\beta_2, \alpha_1^r \alpha_2^s \alpha_3^t)$, and $c = c_1 + c_2 + c_3$. Since $R > R_1 + R_2 + R_3$ (and likewise for S,T), $\Sigma_1 + \Sigma_2 + \Sigma_3$ is contained in the image of the points of class c of the large box. A linear relation between the rows gives a non-zero polynomial $P(X_1, X_2, Y)$, of total degree at most $K-1$ in (X_1, X_2) and of degree at most $L-1$ in Y, vanishing on this image. We check the hypotheses (3.17)–(3.19) of Proposition 3.11 of [7] (Gouillon's lemma [4]; the matrix is integral, and we work over $\mathbb{C}$) exactly as in Section 4 of [7], replacing the cardinalities of the boxes by the C_j.

- ψ is injective: a collision would give $\alpha_3^{mb_3} = \alpha_1^{mb_1} \alpha_2^{mb_2}$ for some $m > 0$, whence $\Lambda = 0$.
- The values $\alpha_1^r \alpha_2^s \alpha_3^t$ are pairwise distinct, by multiplicative independence. Hence $\#\{y\} = C_j$, and (4.2), (4.3) of [7] follow from $C_1 > L$ and $C_2 > 2KL$, guaranteed by (Z1), (Z2).
- Outside (2.14), $(r,s,t) \mapsto (r + t\beta_1, s + t\beta_2)$ is injective on B_1 and B_2 (Lemma 3.17 of [7]), whence (4.4) by $C_2 > K^2$.
- Outside (2.15), each fibre of $(x_1, x_2) \mapsto \lambda x_1 + \mu x_2$ on the whole box B_1 has fewer than $\mathcal{M}$ elements (Lemma 3.21 of [7]), a fortiori on its points of class c_1; whence $\#\{\lambda x_1 + \mu x_2\} \ge C_1/\mathcal{M} > K$ by (Z1).
- $\#\Sigma_3 = C_3 > 3K^2 L$ by (Z3).

Hence $P = 0$, a contradiction. □

5 Proofs of Theorem 2 and Corollary 3

Theorem 2. By Proposition 9, one can choose N columns of class c forming a minor $\Delta \neq 0$. If $v_p(\Lambda) \ge KL - 1$, Theorem 1 gives $\frac{2}{N} v_p(\Delta) \ge E(K,L)$, and Proposition 8 contradicts (1). Hence $v_p(\Lambda) \le KL - 2$.

Corollary 3. We follow the proof of Theorem 1 of [2] with the powers γ_i^r themselves (without raising to the power p^t), the matrix $\left(\binom{rb_2 + sb_1}{k} \gamma_1^{\ell r} \gamma_2^{\ell s}\right)$ (rows (k,ℓ), $k < K$, $\ell < L$; columns in the translate $C_1 + C_2$ of Λ^*, which is contained in one class), and the zero lemma of Lemmas 6–7 of [2], which gives rank N (it only requires $E_1 + E_2 \subset C_1 + C_2$). For the analytic bound, we proceed as in Theorem 1, with one variable $z_j = r_j + s_j b_1/b_2$ ($p \nmid b_2$), with $\theta_2 = \theta_1^{b_1/b_2}(1+\varepsilon)^{1/b_2}$, $v_p(\varepsilon) = v_p(\Lambda_2)$. We expand each binomial into monomials z^{μ_i}, $\mu_i \le k_i$, and pass as in Lemma 5 to $\Psi(x) = x^{\sum \mu_i} G_{I,\mu}(x\vartheta)$, whose row i is a series $\sum_a c_{i,a} x^a z_j^a$ (times δ_{ij} if $i \notin I$). Expanding by multilinearity, two rows of I assigned the same exponent a are proportional; the non-zero terms therefore have distinct exponents on I, and the order is at least $|I|(|I|-1)/2$. We obtain $v_p(\Delta) \ge \min_I \big((N-I)v_p(\Lambda_2) + I(I-1)/2\big) - LK(K-1)/2$, which equals $NK(L-1)/2$ as soon as $v_p(\Lambda_2) \ge N - 1$. For p odd, this replaces the bound $NK(L-1)/2 - N\log N/\log p$ of Lemma 8 of [2]. For the arithmetic bound, we use the bound $|\mathcal{P}| \le N^{N/2} b^{(K-1)N/2}$ of Lemma 6 of [5] (used in Lemma 11 of [2]), and we bound the spread of the exponents in two ways. Lemma 7 with $Q = K$ gives $4G_1/N = \lambda_L(R-1)$. On the other hand, let g' be the index of the projection of Λ^* on the first coordinate and g'' that of $\Lambda^* \cap (\{0\} \times \mathbb{Z})$; then $g'g'' = g$. The first coordinates of the points of $C_1 + C_2$ lie in a progression of difference g', and each is taken at most $\lfloor (S-1)/g'' \rfloor + 1$ times. The proof of Lemma 10 of [2] then applies word for word (it uses the hypothesis $\gcd(m_1, m_2, g) = 1$ only to obtain this structure) and gives $4G_1/N \le \frac{L(R+g-1)}{2} - \frac{gNL}{6(S+g-1)}$. We take the minimum, and likewise

for G_2. If $A = c_1^{V_1-U_1} c_2^{V_2-U_2} \widetilde{\mathcal{P}}(\gamma_1,\gamma_2) \in \mathbb{Z}$ (U_i, V_i the least and largest exponents, $V_i - U_i \le 2G_i$), the maximum principle applied to the homogenised polynomial gives $|A| \le |\mathcal{P}|\, e^{2G_1 h_1 + 2G_2 h_2}$, and $v_p(\Delta) = v_p(A)$. If $v_p(\Lambda_2) \ge N-1$, we obtain the negation of the criterion; hence $v_p(\Lambda_2) \le N-2$.

In the bound for $v_p(x^{p-1}-1)$ of [9], the chain is the same with $\log N$ instead of $3\log N$ (which only helps) and the conclusion $KL-2$ instead of $KL-1$. With $L=5$ and $K = \lfloor 69L\Gamma/25 \rfloor + 1$, we obtain $KL - 2 \le 69\,\Gamma + 3$. □

6 Degenerate cases

Assume (2.15), with $u_3 \neq 0$. Put $x = \alpha_3^{b_3}\alpha_1^{-b_1}\alpha_2^{-b_2}$, so that $v_p(\Lambda) = v_p(x-1) \le v_p(x^{u_3}-1)$. Since $u_3 b_3 = -u_1 b_1 - u_2 b_2$,

$$x^{u_3} = \gamma_1^{-b_1}\gamma_2^{-b_2}, \qquad \gamma_1 = \alpha_1^{u_3}\alpha_3^{u_1}, \quad \gamma_2 = \alpha_2^{u_3}\alpha_3^{u_2},$$

with $h(\gamma_1) \le U_3 \log\alpha_1 + U_1 \log\alpha_3$ and $h(\gamma_2) \le U_3\log\alpha_2 + U_2\log\alpha_3$; γ_1, γ_2 are multiplicatively independent. If $u_3 = 0$, then $u_1 u_2 \neq 0$ and $x^{u_1} = (\alpha_1^{u_2}\alpha_2^{-u_1})^{b_2}(\alpha_3^{u_1})^{b_3}$. In both cases we are reduced to a form in two logarithms of rationals, to which we apply the better of the two results listed below. Corollary 3 requires that p does not divide the second exponent; if p divides the second but not the first, we exchange the roles of γ_1 and γ_2 as well as those of the R_j and the S_j, which leaves the criterion unchanged. If p divides both remaining exponents, we write the form as $y^{p^k}-1$ with $v_p(y^{p^k}-1) \le v_p(y-1)+k$ (p odd), which costs at most $\log B/\log p$; Theorem 3 of [2] does not need this. The two results are:

- Theorem 3 of [2];
- Corollary 3, with boxes $R_1S_1 > gL$, $R_2S_2 > g(K-1)L$ and translates of Λ^* chosen by pigeonhole. If $b_2 r + b_1 s$ is not injective on the box $R_2 \times S_2$, then $b_1/d \le R_2 - 1$ and $b_2/d \le S_2 - 1$ with $d = \gcd(b_1,b_2)$, and Λ_2 is, up to a unit, $\gamma^d - 1$ with $h(\gamma) \le (R_2-1)h_1 + (S_2-1)h_2$. For p odd, if g_0 is the order of γ modulo p, then $v_p(\gamma^d-1) = 0$ if $g_0 \nmid d$, and otherwise $v_p(\gamma^d-1) = v_p(\gamma^{g_0}-1) + v_p(d) \le \big((p-1)h(\gamma) + \log 2 + \log B\big)/\log p$.

7 Change of basis: reduction to $g = 1$

Restricting to Teichmüller classes puts the factor g into the volumes of the boxes (Z1)–(Z3), and (Z1) combines it with χ. It can be avoided by a change of basis in the multiplicative group, at the price of larger heights.

Write ω for the Teichmüller character: $\omega(\alpha_i) = \zeta^{n_i}$.

Proposition 10. *Let p be odd, and let n_1, n_2, n_3 be the Teichmüller indices of $\alpha_1, \alpha_2, \alpha_3$. Let $\Lambda_0 = \{x \in \mathbb{Z}^3 : n_1x_1 + n_2x_2 + n_3x_3 \equiv 0 \pmod g\}$, let e_1, e_2, e_3 be a basis of Λ_0, and put $\gamma_j = \alpha_1^{e_{j1}}\alpha_2^{e_{j2}}\alpha_3^{e_{j3}} \in \mathbb{Q}^\times$.*

1. *The γ_j are multiplicatively independent and $\gamma_j \equiv 1 \pmod p$.*
2. *If $v_p(\Lambda) \ge 1$, the vector $\beta = (b_1, b_2, -b_3)$ lies in Λ_0; write $\beta = \sum_j b'_j e_j$ with $b'_j \in \mathbb{Z}$. Then $|b'_j| \le \kappa'_j B$, where $B = \max b_i$ and $\kappa'_j = \sum_k |(E^{-1})_{kj}|$, E being the matrix with rows e_j.*
3. *$v_p(\Lambda) = v_p\big(\gamma_1^{b'_1}\gamma_2^{b'_2}\gamma_3^{b'_3} - 1\big)$. If $\delta = \gcd(b'_1, b'_2, b'_3)$, then $v_p(\Lambda) = v_p\big(\gamma^{b'/\delta} - 1\big) + v_p(\delta)$.*

Proof. (1) E is invertible; $\omega(\gamma_j) = \zeta^{n\cdot e_j} = 1$, so $\gamma_j \in 1 + p\mathbb{Z}_p$. (2) $\Lambda = \alpha_3^{b_3}(\alpha^\beta - 1)$, and $v_p(\Lambda) \ge 1$ gives $\omega(\alpha^\beta) = \zeta^{n\cdot\beta} = 1$. (3) $\alpha^\beta = \gamma^{b'}$, and for $y \in 1 + p\mathbb{Z}_p$, p odd, $v_p(y^\delta - 1) = v_p(y-1) + v_p(\delta)$. □

Theorem 11 (version with $g = 1$)**.** *Let $\gamma_1, \gamma_2, \gamma_3$ be multiplicatively independent rationals u_j/w_j with $\gamma_j \equiv 1 \pmod p$ (p any prime), $h_j \ge \log\max\{|u_j|, |w_j|\}$, and $\Lambda' = \gamma_1^{\beta_1}\gamma_2^{\beta_2} - \gamma_3^{\beta_3} \neq 0$ with*

$\beta_j \geq 1$, $\gcd(\beta_1, \beta_2, \beta_3) = 1$, $p \nmid \beta_3$. *Then the conclusion of Theorem 2 holds for* Λ' *when one takes* $n_i = 0$ *and* $g = 1$ *in (Z1)–(Z3), and* h_j *instead of* $\log \alpha_j$ *in* (1)*; in case (2.14),* $v_p(\Lambda') \leq (\log 2 + \sum_j \beta_j h_j)/\log p$.

Proof. Theorem 1 only uses $\theta_j = \gamma_j \in 1 + p\mathbb{Z}_p$; all columns are in a single class. The zero lemma (Proposition 9) only uses multiplicative independence and combinatorial properties of the exponents. In Proposition 8, $\Delta \in \mathbb{Z}_{(p)}$, and the integer $A = \prod_j w_j^{V_j - U_j} \widetilde{\mathcal{P}}(\gamma)$ satisfies $v_p(A) \geq v_p(\Delta)$; the maximum principle on the polydisc, applied to the homogenised polynomial, gives $|A| \leq |\mathcal{P}|\, e^{\sum_j 2G_j h_j}$, as in Corollary 3. □

Corollary 3 holds likewise with g replaced by the index of Λ^*; for principal units one takes $\Lambda^* = \mathbb{Z}^2$ (index 1), its proof using only $g'g'' = [\mathbb{Z}^2 : \Lambda^*]$.

We apply Theorem 11 to the form $\gamma^{b'/\delta} - 1$. Since b'/δ is primitive, one of its coordinates, say j_0, is prime to p. For $j \neq j_0$, replace γ_j by γ_j^{-1} if $b'_j < 0$; replace γ_{j_0} by $\gamma_{j_0}^{-1}$ if $b'_{j_0} > 0$. Up to a unit, the form becomes $\gamma_a^{|b'_a|/\delta} \gamma_b^{|b'_b|/\delta} - \gamma_{j_0}^{|b'_{j_0}|/\delta}$. If one b'_j vanishes, it has two logarithms and falls under Corollary 3 (index 1) or [2, Théorème 3]; if two vanish, $v_p(\gamma_j^m - 1) \leq (h_j + \log 2 + \log m)/\log p$. Since we do not know which coordinate is isolated, we take the maximum of the three bounds, and add $\log(\max_j \kappa'_j B)/\log p$ for $v_p(\delta)$. This method requires neither $p \nmid b_3$ nor $\gcd(b_1, b_2, b_3) = 1$.

We choose the basis minimising the product of the heights h_j among combinations of short vectors of Λ_0. The factor g then moves into the heights, whereas the method of classes pays it in the volumes, and squared in (Z1) ($V_1 > (gK\chi)^2$ roughly). It cannot disappear: if the α_i are pairwise coprime and $\gamma_j = u_j/w_j$ is written in lowest terms, then $u_j w_j$ is the product of the $\alpha_i^{|e_{ji}|}$, so $h(\gamma_j) \geq \frac{1}{2} \sum_i |e_{ji}| \log \alpha_i$, and Hadamard's inequality (in the form $|\det M| \leq \prod_j \sum_i |M_{ji}|$) gives

$$h(\gamma_1) h(\gamma_2) h(\gamma_3) \;\geq\; \frac{[\mathbb{Z}^3 : \Lambda_0]}{8} \log \alpha_1 \log \alpha_2 \log \alpha_3.$$

This lower bound needs the coprimality: when the α_i share prime factors, cancellations in γ_j can make the heights smaller. In the examples below, where the α_i are distinct primes, the product of the heights is 1.2 to 1.4 times $g \log \alpha_1 \log \alpha_2 \log \alpha_3$.

p	B	heights h_j	classes (Section 6)	change of basis	Yu [11, 1]	ratio
5	10^{10}	1.79 1.95 2.08	$1.04 \cdot 10^7$	$4.62 \cdot 10^6$	$3.08 \cdot 10^9$	667
5	10^{30}	1.79 1.95 2.08	$9.26 \cdot 10^7$	$3.98 \cdot 10^7$	$9.24 \cdot 10^9$	232
7	10^{10}	2.08 2.20 2.30	$6.37 \cdot 10^6$	$2.68 \cdot 10^6$	$4.27 \cdot 10^9$	1592
7	10^{30}	2.08 2.20 2.30	$5.54 \cdot 10^7$	$2.11 \cdot 10^7$	$1.28 \cdot 10^{10}$	608
11	10^{10}	2.48 2.64 3.30	$9.10 \cdot 10^6$	$2.10 \cdot 10^6$	$4.16 \cdot 10^9$	1980
11	10^{30}	2.48 2.64 3.30	$6.72 \cdot 10^7$	$1.60 \cdot 10^7$	$1.25 \cdot 10^{10}$	780
13	10^{10}	2.64 2.77 3.30	$9.62 \cdot 10^6$	$1.75 \cdot 10^6$	$6.37 \cdot 10^8$	364
13	10^{30}	2.64 2.77 3.30	$7.02 \cdot 10^7$	$1.24 \cdot 10^7$	$1.91 \cdot 10^9$	154
101	10^{10}	4.68 4.85 8.88	$5.27 \cdot 10^8$	$2.33 \cdot 10^6$	$2.43 \cdot 10^8$	105
101	10^{30}	4.68 4.85 8.88	$1.25 \cdot 10^9$	$9.98 \cdot 10^6$	$7.29 \cdot 10^8$	73

Table 1: Complete upper bounds for $v_p(\Lambda)$ for $\Lambda = \alpha_1^{b_1}\alpha_2^{b_2} - \alpha_3^{b_3}$, $b_i \leq B$ ($\alpha = (2, 3, 5)$ if $p = 7$, $(2, 3, 7)$ otherwise), degenerate cases included; the column "classes" assumes $p \nmid b_3$, the column "change of basis" does not. Column "classes": restriction to Teichmüller classes (Section 6). Column "change of basis": Proposition 10, then Theorem 11, maximum over the three choices of the isolated coordinate. The bases, the $B' = \max_j \kappa'_j B$ and the parameters are in the verifier; for instance, for $p = 101$, $e_1 = (-2, -3, 1)$, $e_2 = (-7, 3, 0)$, $e_3 = (-5, 1, 4)$, of index 100, $\gamma = (7/108,\ 27/128,\ 7203/32)$ and $B' = 0.48\, B$. The ratio is that of Yu to the change of basis. Yu's theorem is taken in the explicit form of [1, Theorem 3.1, Corollary 3.3] ($n = 3$; field $\mathbb{Q}$ for $p \equiv 1 \pmod 4$, $\mathbb{Q}(i)$ for $p \equiv 3 \pmod 4$, which penalises Yu by a factor of order $p/2$ for $p = 7$ and 11).

8 Scope

Proved here: Theorem 1, Lemma 7, Propositions 4, 8, 9 and 10, Corollary 3, Theorem 11 and their assembly. The change of basis of Proposition 10 is an elementary reduction, probably known; we have not seen it used with p-adic interpolation determinants, where one usually restricts the points to a class [2]. Used as they stand: Gouillon's zero lemma [4], in the form of Proposition 3.11 of [7]; Lemmas 3.5, 3.17, 3.21 and the bound for $|\mathcal{P}|$ (Proposition 3.9) of [7]; Lemmas 6–7, 9–10 (in the form adapted to translates of Λ^*) and Theorem 3 of [2]; Lemma 4 and the bound for $|\mathcal{P}|$ of Lemma 6 of [5] (two logarithms). The refinement $-N/(12RST)$ of the spread (the g of [7]) is not used.

Verification

The ancillary file `VERIF_KIT3P.py` (Python and numpy, no argument, about 15 seconds) checks:

- Proposition 4: exact order, computed in $\mathbb{F}_q[[x]]$, of determinants at generic points and at points of the lattice of the kit; closed formulas;
- Theorem 1 for three logarithms, on integer determinants computed exactly, for $p = 2$, 3, 5, 7, 11 and 13, with an exact relation and with $v_p(\varepsilon) = 1$, 2, 4 or 7;
- the analytic bound for two logarithms, on integer determinants computed exactly, for $p = 2$, 3, 5, 7 and 11 with an exact relation, and for $p = 2$, 3, 5 and 7 with $v_p(\varepsilon) = 1$, 2, 3 or 5;
- Proposition 9: rank N of the matrices restricted to each class, for minimal boxes satisfying (Z1)–(Z3);
- the bound for the spread in Corollary 3 drawn from Lemma 10 of [2], on translates of all sublattices of index $g \leq 12$ (Hermite normal form), with an adversarial choice of the points;
- for the change of basis, in exact arithmetic: the basis, its index, $\gamma_j \equiv 1 \pmod{p}$, the heights, the κ'_j, then the criterion and the degenerate cases for the three isolated coordinates, and the cases where one b'_j vanishes;
- each row of the method of classes: (Z1)–(Z3) and (1) at the parameters indicated, the bounds U_i, both cases of (2.15) by the better of [2, Theorem 3] and Corollary 3, the case (2.14), and Yu's constant.

The verifier prints its messages in French.

Acknowledgements. Technical assistance: Claude (Anthropic).

References

[1] A. Alvarado, A. Koutsianas, B. Malmskog, C. Rasmussen, C. Vincent, M. West, A robust implementation for solving the S-unit equation and several applications, arXiv:1903.00977.

[2] Y. Bugeaud, M. Laurent, Minoration effective de la distance p-adique entre puissances de nombres algébriques, *J. Number Theory* **61** (1996), 311–342.

[3] K. C. Chim, Lower bounds for linear forms in two p-adic logarithms, *J. Number Theory* **266** (2025), 295–349.

[4] N. Gouillon, Un lemme de zéros, *C. R. Acad. Sci. Paris, Sér. I* **335** (2002), 167–170.

[5] M. Laurent, M. Mignotte, Y. Nesterenko, Formes linéaires en deux logarithmes et déterminants d'interpolation, *J. Number Theory* **55** (1995), 285–321.

[6] M. Laurent, Linear forms in two logarithms and interpolation determinants II, *Acta Arith.* **133** (2008), 325–348.

[7] M. Mignotte, P. Voutier, A kit for linear forms in three logarithms, *Math. Comp.* **93** (2024), 1903–1951; arXiv:2205.08899.

[8] D. Niedbala Giraudin, An optimal multiplicity estimate for interpolation determinants in three logarithms, Hexagon preprint hexagon:2610.00704, 2026.

[9] D. Niedbala Giraudin, The exponent of p in $x^{p-1} - 1$: Yamada's constant 283 lowered to 69, Hexagon preprint hexagon:2610.00707, 2026.

[10] T. Yamada, A note on the paper by Bugeaud and Laurent, *J. Number Theory* **130** (2010), 1889–1897.

[11] K. Yu, p-adic logarithmic forms and group varieties III, *Forum Math.* **19** (2007), 187–280.