The exponent of p in $x^{p-1}-1$: Yamada's constant 283 lowered to 69

David Niedbala Giraudin
ORCID 0009-0009-1526-1178

hexagon:2610.00707v1

Abstract

Yamada (J. Number Theory 130, 2010) deduced from the method of interpolation determinants of Bugeaud and Laurent the bound $v_p(x^{p-1}-1) \le 283\,(p-1)\log y\,\log(xy)/(\log p)^2+4$, for multiplicatively independent integers x, y coprime to p. We replace 283 by 69. The new ingredient is an elementary bound, by rearrangement, on the spread of the exponents that occur in the Liouville inequality: it at least halves the height term of Yamada's criterion, involves no congruence class, and allows the parameters to be re-optimised. The proof is complete up to the lemmas of Bugeaud–Laurent (zero lemma, analytic upper bound) and of Laurent–Mignotte–Nesterenko (bound for the polynomial), which are used as they stand. A self-contained verifier checks the numerical inequalities.

1 Result

For a prime p and an integer x coprime to p, the exponent $v_p(x^{p-1}-1)$ equals 1 unless p is a Wieferich prime to base x. The trivial bound $v_p(x^{p-1}-1) < (p-1)\log x/\log p$ comes from $p^v \le x^{p-1}-1$. The theorems of Bugeaud–Laurent [1] on linear forms in two p-adic logarithms assume $\log A_i \ge \log p$ and give nothing better here. Yamada [3] removed this obstacle and obtained a non-trivial bound, with the constant 283.

Theorem 1. *Let p be a prime and $x, y \ge 2$ two multiplicatively independent integers, coprime to p. Then*

$$v_p\big(x^{p-1}-1\big) \;\le\; 69\,(p-1)\,\frac{\log y}{\log p}\,\frac{\log xy}{\log p} \;+\; 4.$$

Corollary 2. *For every odd prime p and every odd prime $q \ne p$,*

$$v_p\big(q^{p-1}-1\big) \le 69\,(p-1)\,\frac{\log 2\,\log 2q}{(\log p)^2}+4, \qquad v_p\big(2^{p-1}-1\big) \le 69\,(p-1)\,\frac{\log 3\,\log 6}{(\log p)^2}+4 \quad (p \ne 2,3).$$

The corollary follows with $(x,y)=(q,2)$ and $(x,y)=(2,3)$. Theorem 4 of [3], on $v_p(\sigma(q^c))$, is deduced from Theorem 2 of [3] by an inequality of Nagell, valid for $p \notin \{2,q\}$ (and $p \ne 2,3$ for $\sigma(2^c)$); in that range it therefore holds with 69 in place of 283.

	constant	additive term
Yamada 2010 [3], Theorem 2	283	4
Theorem 1	69	4

Theorem 1 gives nothing when $\log p \le 69\,\log y\,\log(xy)/\log x$, since the trivial bound is then better. For $y=2$ and x large it becomes non-trivial as soon as $p > 2^{69(1+o(1))}$, against $p > 2^{283(1+o(1))}$ in [3].

2 A rearrangement lemma

Fix integers $K, L \geq 1$, put $N = KL$ and $l_j = \lfloor (j-1)/K \rfloor$ for $1 \leq j \leq N$: each value $l \in \{0, \dots, L-1\}$ is taken exactly K times.

Lemma 3 (rearrangement)**.** *Let $R \geq 1$ and let $r_1, \dots, r_N$ be real numbers in $[0, R-1]$. Put $M = \frac{L-1}{2} \sum_j r_j$. For every permutation σ of $\{1, \dots, N\}$,*

$$\Big| \sum_{i=1}^{N} l_i \, r_{\sigma(i)} - M \Big| \;\leq\; G := \frac{(R-1)\, K \, \lfloor L^2/4 \rfloor}{2}.$$

The bound is attained when L is even, half of the r_j being 0 and the other half $R-1$.

Proof. Put $\bar{l} = (L-1)/2$. Since $\sum_i (l_i - \bar{l}) = K \sum_{l=0}^{L-1} (l - \bar{l}) = 0$,

$$\sum_i l_i r_{\sigma(i)} - M = \sum_i (l_i - \bar{l})\, r_{\sigma(i)} = \sum_i (l_i - \bar{l}) \Big(r_{\sigma(i)} - \frac{R-1}{2} \Big),$$

whose absolute value is at most $\frac{R-1}{2} \sum_i |l_i - \bar{l}| = \frac{R-1}{2} K \sum_{l=0}^{L-1} \big| l - \frac{L-1}{2} \big| = \frac{R-1}{2} K \lfloor L^2/4 \rfloor$. In the configuration indicated, the increasing matching gives equality. □

Lemma 10 of [1] bounds the same quantity by $\frac{NL(R+g-1)}{8} - \frac{gN^2L}{24(S+g-1)}$, for pairs (r_j, s_j) in a single class $m_1 r + m_2 s \equiv c \pmod g$. Lemma 6 of [3] replaces it by $G_Y = NL(R-1)/4$. Lemma 3 gives $G = NL(R-1)/8$ for L even and $G = NL(R-1)(1-L^{-2})/8$ for L odd, with no hypothesis on the r_j.

3 The improved criterion

For $L \geq 1$ put

$$\lambda_L = \frac{2\lfloor L^2/4 \rfloor}{L} \qquad \Big(\lambda_L = \tfrac{L}{2} \text{ if } L \text{ is even}, \quad \lambda_L = \tfrac{L^2-1}{2L} \text{ if } L \text{ is odd} \Big).$$

Theorem 4. *Let p be an odd prime, α_1, α_2 non-zero integers coprime to p, b_1, b_2 positive integers with $\gcd(b_1, b_2, p) = 1$, and $\Lambda = \alpha_1^{b_1} - \alpha_2^{b_2}$. Let ζ be a primitive $(p-1)$-th root of unity in $\mathbb{Z}_p$, $g = p-1$, and m_i integers such that $\alpha_i \equiv \zeta^{m_i} \pmod p$. Let $K \geq 3$, $L \geq 2$, $R_1, R_2, S_1, S_2 \geq 1$ be integers, $R = R_1 + R_2 - 1$, $S = S_1 + S_2 - 1$, $N = KL$ and*

$$b = \frac{(R-1)b_2 + (S-1)b_1}{2} \Big(\prod_{j=1}^{K-1} j! \Big)^{-2/(K^2-K)}.$$

Assume that there are classes c_1, c_2 modulo g such that

$$\#\{\alpha_1^r \alpha_2^s : 0 \leq r < R_1,\ 0 \leq s < S_1,\ m_1 r + m_2 s \equiv c_1\} \geq L, \tag{1}$$

$$\#\{b_2 r + b_1 s : 0 \leq r < R_2,\ 0 \leq s < S_2,\ m_1 r + m_2 s \equiv c_2\} > (K-1)L, \tag{2}$$

and that

$$K(L-1)\log p \;>\; 3\log N + (K-1)\log b + \lambda_L \big((R-1)\log|\alpha_1| + (S-1)\log|\alpha_2| \big). \tag{3}$$

Then $v_p(\Lambda) \leq KL - 1$.

Theorem 1 of [3] has the same form, with the coefficient L in place of λ_L in (3) (and any integer g with $\alpha_i^g \equiv 1$).

Proof. This is the proof of Theorem 1 of [1], in the case $\mathbb{Q}_p$: $D = e = f = 1$, $t = 0$ because p is odd, and $u = 0$ because $\gcd(b_1, b_2, p) = 1$. Only the arithmetic lower bound changes. Assume $v_p(\Lambda) \geq N - \frac{1}{2}$. The matrix $\mathcal{M}$ formed by the columns (r, s), $0 \leq r < R$, $0 \leq s < S$, $m_1 r + m_2 s \equiv c_1 + c_2$, with entries $\binom{rb_2+sb_1}{k}\alpha_1^{lr}\alpha_2^{ls}$ (rows (k, l), $0 \leq k < K$, $0 \leq l < L$) has rank N by the zero lemma ([1], Lemmas 6 and 7, which use only (1)–(2)). Let $\Delta \neq 0$ be a minor of order N. The analytic upper bound ([1], Lemma 8) gives

$$v_p(\Delta) \;\geq\; \frac{NK(L-1)}{2} - \frac{N \log N}{\log p}.$$

It uses the decomposition $\alpha_i = \zeta^{m_i}\theta_i$, $\theta_i \in 1 + p\mathbb{Z}_p$, and the fact that all columns lie in one class. It does not use the condition $\gcd(m_1, m_2, g) = 1$, which serves only in Lemma 10 of [1].

Arithmetic lower bound. Index the columns of Δ by (r_j, s_j), $1 \leq j \leq N$, and the rows by (k_i, l_i), with $l_i = \lfloor (i-1)/K \rfloor$. The determinant is $\Delta = \mathcal{P}(\alpha_1, \alpha_2)$ with

$$\mathcal{P}(X, Y) = \sum_{\sigma} \operatorname{sg}(\sigma) \prod_{i=1}^{N} \binom{r_{\sigma(i)}b_2 + s_{\sigma(i)}b_1}{k_i} X^{\sum_i l_i r_{\sigma(i)}} Y^{\sum_i l_i s_{\sigma(i)}} \in \mathbb{Z}[X, Y].$$

By Lemma 3, applied to the r_j and then to the s_j, all exponents of X (resp. Y) lie in $[M_1 - G_1, M_1 + G_1]$ (resp. $[M_2 - G_2, M_2 + G_2]$), with $G_1 = \frac{(R-1)K\lfloor L^2/4 \rfloor}{2}$ and $G_2 = \frac{(S-1)K\lfloor L^2/4 \rfloor}{2}$. Write $\Delta = \alpha_1^{U_1}\alpha_2^{U_2}\widetilde{\mathcal{P}}(\alpha_1, \alpha_2)$, where U_1 (resp. U_2) is the least exponent of X (resp. Y) among the monomials with non-zero coefficient, $\widetilde{\mathcal{P}} \in \mathbb{Z}[X, Y]$ has degrees at most $2G_1$ and $2G_2$, and $|\widetilde{\mathcal{P}}| = |\mathcal{P}|$ for the sup norm on the torus $|X| = |Y| = 1$. By Lemma 6 of [2],

$$|\mathcal{P}| \leq N^{N/2} b^{(K-1)N/2}.$$

Since $\widetilde{\mathcal{P}}(\alpha_1, \alpha_2)$ is a non-zero integer with the same p-adic valuation as Δ, and since the maximum principle on the polydisc, applied to $X^{2G_1}Y^{2G_2}\widetilde{\mathcal{P}}(1/X, 1/Y)$ with $|\alpha_i| \geq 1$, gives $|\widetilde{\mathcal{P}}(\alpha_1, \alpha_2)| \leq |\widetilde{\mathcal{P}}|\,|\alpha_1|^{2G_1}|\alpha_2|^{2G_2}$,

$$v_p(\Delta)\log p \leq \log|\widetilde{\mathcal{P}}(\alpha_1, \alpha_2)| \leq \frac{N}{2}\Big(\log N + (K-1)\log b\Big) + 2G_1 \log|\alpha_1| + 2G_2 \log|\alpha_2|.$$

Now $4G_1/N = \lambda_L(R-1)$ and $4G_2/N = \lambda_L(S-1)$. Comparing the two bounds for $v_p(\Delta)$ and multiplying by $2/N$ gives the negation of (3). Hence $v_p(\Lambda) < N - \frac{1}{2}$, that is $v_p(\Lambda) \leq N - 1$. □

4 Proof of Theorem 1

4.1 Reduction

Put $P = \log p$. If $P \leq 69 \log y \log(xy)/\log x$, the trivial bound $v_p(x^{p-1} - 1) < (p-1)\log x/P$ implies the theorem. From now on assume

$$P > P_0(x, y) := 69\,\frac{\log y\,\log(xy)}{\log x} \;\;\geq\;\; 69 \log 2. \tag{4}$$

In particular $p > 2^{69}$ is odd. We apply Theorem 4 with

$$(\alpha_1, \alpha_2) = (xy, y), \qquad b_1 = b_2 = g = p - 1, \qquad \Lambda = (xy)^{p-1} - y^{p-1} = y^{p-1}\big(x^{p-1} - 1\big),$$

so that $v_p(\Lambda) = v_p(x^{p-1} - 1)$. Write $a_1 = \log(xy)/P$, $a_2 = \log y/P$, $\Gamma = g\,a_1 a_2$, and take

$$L = 5, \quad k = \tfrac{69}{25}, \quad K = \lfloor kL\Gamma \rfloor + 1, \quad R_1 = \left\lfloor \sqrt{gLa_2/a_1} \right\rfloor + 1, \quad S_1 = \left\lfloor \sqrt{gLa_1/a_2} \right\rfloor + 1,$$

$$R_2 = \left\lfloor \sqrt{g(K-1)La_2/a_1} \right\rfloor + 1, \qquad S_2 = \left\lfloor \sqrt{g(K-1)La_1/a_2} \right\rfloor + 1.$$

Then $R_1 S_1 > gL$ and $R_2 S_2 > g(K-1)L$. The classes modulo g partition the boxes, so there is a class c_1 (resp. c_2) containing at least L (resp. more than $(K-1)L$) points of the box $R_1 \times S_1$ (resp. $R_2 \times S_2$). The numbers $\alpha_1^r\alpha_2^s$ are pairwise distinct by multiplicative independence, whence (1). Since $xy \geq 6$ and $y \geq 2$, under (4) we have $\Gamma \geq (e^{69\log 2} - 1)\log 2 \log 6/(69 \log 2)^2 > 3.2 \cdot 10^{17}$.

4.2 Degenerate case

If $(r,s) \mapsto (p-1)(r+s)$ is not injective on the class c_2 of the box $R_2 \times S_2$, two points $(r_1,s_1) \neq (r_2,s_2)$ of this class satisfy $r_1+s_1 = r_2+s_2$, whence $(m_1-m_2)(r_1-r_2) \equiv 0 \pmod g$. Since $\zeta^{m_1-m_2} \equiv x$, the order g_0 of x modulo p divides r_1-r_2, so $g_0 < R_2$. We have $v_p(x^{p-1}-1) = v_p(x^{g_0}-1)$ because $(p-1)/g_0$ is coprime to p, and $p^v \le x^{g_0}-1$. Hence

$$v_p(x^{p-1}-1) \le (R_2-1)\frac{\log x}{P} \le \sqrt{g \cdot kL\Gamma \cdot L\,a_2/a_1}\; a_1 = L\sqrt{k}\;\Gamma \le 8.31\,\Gamma,$$

which is stronger than the theorem.

4.3 Non-degenerate case

Then (2) holds, and it remains to check (3).

Lemma 5. *For $K \ge 2$,* $\displaystyle\frac{2}{K^2-K}\sum_{j=1}^{K-1} \log j! \;\ge\; \log(K-1) - \frac{3}{2} - \frac{\log(K-1)}{K}.$

Proof. We have $\log j! \ge \int_1^j \log t\,dt = j\log j - j + 1$ and $\sum_{j=1}^n j\log j \ge \int_1^n t\log t\,dt$. With $n = K-1$, $\sum_{j=1}^n \log j! \ge \frac{n^2}{2}\log n - \frac{3}{4}n^2 + \frac{n}{2} + \frac{1}{4}$. Multiply by $\frac{2}{n(n+1)}$ and bound term by term. □

Lemma 6. *We have* $\displaystyle\frac{\log b}{P} \le \beta := 1 + \frac{\log P + \log\bigl(\frac{1}{\log xy} + \frac{1}{\log y}\bigr) + \kappa}{P}$, *with* $\kappa = \frac{3}{2} - \log 2 - \frac{1}{2}\log k + \varepsilon$ *and* $\varepsilon = 10^{-8}$.

Proof. We have $R+S-2 \le (1+\sqrt{K-1})\sqrt{gL}\,(a_1+a_2)/\sqrt{a_1a_2}$ and $gLa_1a_2 = L\Gamma \le K/k$. Lemma 5 then gives, as in Lemma 13 of [1],

$$\log b \le \log g + \log\Bigl(\frac{1}{a_1} + \frac{1}{a_2}\Bigr) + \frac{3}{2} - \log 2 - \frac{1}{2}\log k + \eta(K),$$

with $\eta(K) = \log\frac{\sqrt{K}(1+\sqrt{K-1})}{K-1} + \frac{\log(K-1)}{K}$. Since $K > kL\Gamma > 4\cdot 10^{18}$, we have $\eta(K) < 10^{-8}$. We conclude with $g < p$ and $1/a_1 + 1/a_2 = P\bigl(\frac{1}{\log xy} + \frac{1}{\log y}\bigr)$. □

Lemma 7. *Under* (4), $\beta \le \beta^* := 1 + \dfrac{\log 69 + \kappa}{69\log 2} < 1.094786.$

Proof. Put $E = \log\bigl(\frac{1}{\log xy} + \frac{1}{\log y}\bigr) + \kappa$. If $\log P_0 + E \ge 1$, the function $P \mapsto (\log P + E)/P$ decreases on $[P_0,\infty)$ and its bound is attained at P_0. Otherwise its supremum on $\mathbb{R}_{>0}$ is $e^{E-1} < e^{-\log P_0} \le 1/(69\log 2)$, which is smaller than the bound sought. In the first case, with $u = \log y$, $w = \log x$ and $t = u/w$,

$$\log P_0 + E = \log 69 + \log(1+2t) + \kappa, \qquad P_0 = 69\,u\,(1+t),$$

so $(\log P_0 + E)/P_0 = h(t)/(69u)$ with $h(t) = (A + \log(1+2t))/(1+t)$ and $A = \log 69 + \kappa > 4.5$. We have $h(0) = A$, and $(1+t)^2 h'(t) = \frac{2(1+t)}{1+2t} - A - \log(1+2t) \le 2 - A < 0$. Hence $h(t) \le A$, and $u \ge \log 2$ gives the bound. □

Verification of (3). We have

$$(R-1)\log|\alpha_1| = (R-1)a_1P \le P\Bigl(\sqrt{L\Gamma} + \sqrt{g(K-1)La_1a_2}\Bigr) \le P\bigl(\sqrt{L\Gamma} + L\Gamma\sqrt{k}\bigr),$$

and likewise for $(S-1)\log|\alpha_2|$. Also $K-1 \le kL\Gamma$, $K \ge kL\Gamma$, $\log b \le \beta^* P$, and $N \le kL^2\Gamma + L$. It therefore suffices that

$$kL(L-1) \;>\; kL\beta^* + 2\lambda_5 L\sqrt{k} + 2\lambda_5\sqrt{L/\Gamma} + \frac{3\log(kL^2\Gamma + L)}{\Gamma P}.$$

With $L = 5$, $k = 69/25$ and $\lambda_5 = 12/5$:

$$kL(L - 1 - \beta^*) = 40.0919\ldots, \qquad 2\lambda_5 L\sqrt{k} = 39.8717\ldots,$$

and the last two terms are less than $2 \cdot 10^{-8}$ since $\Gamma > 3.2 \cdot 10^{17}$ and $P > 47$. The margin is 0.2201.

Theorem 4 gives $v_p(\Lambda) \le KL - 1 \le kL^2\Gamma + L - 1 = 69\,\Gamma + 4$, and $\Gamma = (p-1)\log y \log(xy)/P^2$. □

5 Remarks

Remark 8 (choice of L)**.** The same chain, with λ_L and the corresponding β^*, gives the minimal constants:

L	3	4	5	6	7	8	9
coefficient λ_L	75.27	70.09	68.29	84.44	95.04	116.30	132.85
coefficient L of [3]	337.75	263.13	282.79	327.95	387.46	457.97	538.12

The choice $L = 5$ is the best in the table. The choice $L = 4$ gives 71 with additive term 3.

Remark 9 (the constant 283)**.** Equation numbers refer to the published version of [3]. In [3, (24)], the intermediate bound $\log b \le \log p + \log\log p$ does not hold for $y = 2$. It would require $\log\bigl(\frac{1}{\log 2x} + \frac{1}{\log 2}\bigr) + \frac{3}{2} - \log 2 - \frac{1}{2}\log 11.32 \le 0$, whereas the left-hand side is positive for $3 \le x \le 12\,311\,938$, x not a power of 2 (it equals 0.287 at $x = 3$). With only the reduction $p > 2^{283}$ of [3], one finds at $(x, y) = (3, 2)$ and $\log p = 283\log 2$ that $\log b/\log p$ can reach $1.02837 > 1.027$, and (21) of [3] is no longer satisfied. Statement (6) of [3] nevertheless remains true. On the one hand, Lemma 3 gives $G \le NL(R-1)/8 \le G_Y$ with no hypothesis; Theorem 1 of [3] therefore holds even when $\gcd(m_1, m_2, p-1) \ne 1$, a case its Lemma 6 does not reach. On the other hand, the chain above, run with the coefficient L of [3] and the exact range (4), gives the minimal constant $282.79 \le 283$ at $L = 5$.

Remark 10 (additive term)**.** The analytic bound used here (Lemma 8 of [1]) contains the loss $N\log N/\log p$. Expanding the powers $\theta^{\ell z}$ as a binomial series in $\theta - 1$ instead of the exponential series gives $v_p(\Delta) \ge NK(L-1)/2$ with no loss as soon as $v_p(\Lambda) \ge N - 1$ [4, Corollary 3]; the conclusion of Theorem 4 becomes $v_p(\Lambda) \le KL - 2$, and the additive term 4 of Theorem 1 can be replaced by 3.

Remark 11 (large p)**.** Stewart [5, proof of Lemma 8, (41)], using the refinements of Yu [6], proves, for an integer $a \ge 2$ and $p \nmid a$ larger than an effectively computable but unspecified constant,

$$\mathrm{ord}_p(a^n - 1) < p\, e^{-\log p/(51.9\log\log p)} \log a \log n;$$

with $n = p - 1$, this bound is asymptotically better than bounds of the form $p/(\log p)^2$, those of [3] as well as Theorem 1. For $y = 2$, computation shows that it beats Theorem 1 only for $\log p$ larger than about $1.1 \cdot 10^4$ (and earlier if y is larger). Theorem 1, like that of [3], is explicit and holds for every p.

Remark 12 (scope)**.** Lemma 3 and Theorem 4 are proved here. The ingredients used as they stand are the zero lemma and the analytic bound (Lemmas 6 to 8 of [1]) and the bound $|\mathcal{P}| \le N^{N/2} b^{(K-1)N/2}$ (Lemma 6 of [2]).

Verification

The ancillary file `VERIF_FERMAT_69.py` (Python and numpy, no argument, about ten seconds) checks:

- Lemma 3, by brute force on 15 120 configurations, together with its equality case;
- Lemma 5 for $2 \le K \le 20\,000$;
- the bound β^*, against a grid of pairs (x, y);
- the final margin 0.2201;
- condition (3) at 40 explicit primes of up to 1521 bits, with the integer parameters built in decimal arithmetic with precision proportional to the size of p;
- the bound $\eta(K) < 10^{-8}$ for $K \ge kL \cdot 3.2 \cdot 10^{17}$;
- the calibration, which recovers $282.79 \le 283$ with the coefficient of [3], and the table of constants.

Acknowledgements. Technical assistance: Claude (Anthropic).

References

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

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

[3] T. Yamada, A note on the paper by Bugeaud and Laurent "Minoration effective de la distance p-adique entre puissances de nombres algébriques", *J. Number Theory* **130** (2010), 1889–1897; arXiv:math/0607072.

[4] D. Niedbala Giraudin, A kit for linear forms in three p-adic logarithms, note, 22 October 2026, unpublished.

[5] C. L. Stewart, On divisors of Lucas and Lehmer numbers, *Acta Math.* **211** (2013), 291–314.

[6] K. Yu, p-adic logarithmic forms and a problem of Erdős, *Acta Math.* **211** (2013), 315–382.