hexagon:2611.00938v1

DIVISIBILITY OF INVARIANT DERIVATIVES ON FORMAL GROUPS OF EVERY HEIGHT, ON A QUESTION OF KATZ

Abstract. In 1977 Katz asked for an explicit lower bound on the p-adic valuation of $(D^n f)(0)$, where D is the normalized invariant derivation of a one-parameter formal group of finite height h over a ring of p-adic integers and f is a power series with integral coefficients. He answered the question at height two, for functions whose translates by the points of order p sum to zero, with the bound $\lfloor np/(p^2-1)\rfloor$. For Lubin–Tate groups over unramified bases, results of Bannai and Kobayashi give the bound $c_h n-(h-1)$, where $c_h=\frac{1}{p-1}-\frac{1}{p^h-1}$. We prove this bound for every one-dimensional formal group whose multiplication by p is divisible by p below degree p^h, over any p-torsion-free $\mathbb{Z}_{(p)}$-algebra and for every integral f, together with the bound $\sum_{h\nmid j}\lfloor n/p^j\rfloor$. The slope c_h, the constant $h-1$, and the second bound at the powers of p cannot be improved. At height two it follows that Katz's bound holds for every integral function except at the orders divisible by p^2-1, where it can fail by one, and it does fail at the first of them. Over a ramified base the hypothesis cannot be weakened to the height of the special fibre, while an action of the Teichmüller roots of unity restores it. For the Cartier dual of the Honda formal group of height h we construct an integral model whose $h-1$ coordinate directions have the sharp slopes $p^i/(p^h-1)$, which add up to c_h, each with the optimal constant 1. The height-two case is the local exponent in the second step of the timeline in Alpöge's note on the Riemann hypothesis, where the bound is stated with a logarithmic loss; for integral functions on the formal group the loss is the constant 1. The results and their proofs were produced by GPT-6 Astra (ChatGPT Pro mode). They were checked by Claude Opus 5.5 at effort high and at effort max; the text was written by Claude Opus 5.5 at effort max and edited by Claude Fable 5.2 at effort max. No human has checked them.

1. The question and the results

1.1. **Katz's question.** Let p be a prime, R a ring of p-adic integers, and F a one-parameter commutative formal group over R with coordinate t. Its normalized invariant derivation is $D=v(t)\,\frac{d}{dt}$, where $v(t)=\partial_2 F(t,0)$, so that $(Dt)(0)=1$. Katz opened his 1977 paper on formal groups and p-adic interpolation with two questions about the numbers $c(n)=(D^n f)(0)$, $f\in R[[t]]$ [12, §I, pp. 55–56]: what are their divisibility properties, that is, which explicit integer-valued function $\phi(n)$ satisfies $\operatorname{ord} c(n)\geq\phi(n)$; and what are the congruences among the normalized numbers $c(n)/p^{\phi(n)}$. At height one there is nothing to divide by, and the theory of measures on $\mathbb{Z}_p$ answers the second question. At height two, for an absolutely unramified base and for functions f whose translates by the kernel of $[p]$ sum to zero, Katz stated

$$\operatorname{ord} c(n)\ \geq\ \left\lfloor\frac{np}{p^2-1}\right\rfloor$$

[12, §V, Lemma 1 and Corollary 2, pp. 62–63], as part of a theory of Galois measures on Tate modules, and proved it for the Lubin–Tate groups $G(\alpha)$ with $[p](X)=pX+\alpha X^{p^2}$ in 1981 [13, Main Theorem 3.11(I), p. 672]. His application is the supersingular case of the Bernoulli–Hurwitz numbers of a curve with complex multiplication [13, §IV]; Lang had obtained the weaker bound $\lfloor n/p\rfloor$ for these [15], as Katz records [12, p. 63].

This note answers the divisibility question at every height, for all integral functions, with the best possible constants.

Date: 23 November 2026.

1.2. **The theorems.** Throughout, p is a prime and $h \geq 1$ an integer; we put

$$q = p^h, \qquad c_h = \frac{1}{p-1} - \frac{1}{q-1} = \frac{q-p}{(p-1)(q-1)}, \qquad E_h(n) = \sum_{\substack{j \geq 1 \\ h \nmid j}} \Big\lfloor \frac{n}{p^j} \Big\rfloor .$$

Let R be a p-torsion-free $\mathbb{Z}_{(p)}$-algebra: a commutative ring in which every integer prime to p is invertible and p is not a zero divisor. For a power series g over $R[1/p]$ and $m \in \mathbb{Z}$, we write $g \in p^m R[[t]]$ when all coefficients of g lie in $p^m R$. Let F be a one-dimensional commutative formal group law over R and D its normalized invariant derivation. We say that F satisfies (H_h) if

$$[p]_F(t) \in pR[[t]] + t^q R[[t]],$$

that is, if multiplication by p reduces modulo p to a series in $t^q R/pR[[t]]$. The condition does not depend on the coordinate. In a new coordinate $t' = \varphi(t)$, with $\varphi \in tR[[t]]$ invertible under composition, multiplication by p is $\varphi \circ [p]_F \circ \varphi^{-1}$. Modulo p the series $[p]_F(\varphi^{-1}(t'))$ lies in the ideal generated by t'^q, and applying φ, a series without constant term, keeps it there. Over $R = W(k)$, k a perfect field of characteristic p, it says that the special fibre has height at least h.

Theorem A. *Let F satisfy (H_h). For every $n \geq 0$ and every $f \in R[[t]]$,*

$$D^n f \;\in\; p^{\,a_h(n)} R[[t]], \qquad a_h(n) = \max\Big\{ E_h(n),\ \lceil c_h n - (h-1) \rceil,\ 0 \Big\}.$$

The floor sum is $E_h(n) = c_h n - \frac{s_p(n)}{p-1} + \frac{s_q(n)}{q-1}$, where $s_b(n)$ is the sum of the base-b digits of n. The bounds are optimal in the following sense.

1. *If $pR \neq R$, then $(D^{q-1}t^{q-1})(0) = (q-1)!$ lies in $p^m R$ but not in $p^{m+1}R$, where $m = c_h(q-1) - (h-1)$. So no real constant smaller than $h-1$ can replace $h-1$.*
2. *If $R = W(k)$ and F has exact height h, then for every $j = hr + s$ with $0 \leq s < h$,*

$$v_p\big((D^{p^j} t^{p^s})(0)\big) = E_h(p^j), \qquad \textit{in particular} \qquad v_p\big((D^{q^r} t)(0)\big) = c_h(q^r - 1).$$

So no slope larger than c_h is possible, even with a sublinear error.

Neither bound in $a_h(n)$ dominates the other: at $n = p$ and $h \geq 3$ the floor sum gives 1 and the affine bound 0, while at $n = q^2 - 1$ and $h \geq 2$ the affine bound exceeds the floor sum by $h - 1$. The theorem asks nothing of F beyond (H_h); in particular no Lubin–Tate normal form and no complex multiplication is assumed.

At height two, $c_2 = p/(p^2-1) = \frac{1}{p} + \frac{1}{p^3} + \frac{1}{p^5} + \cdots$ and the constant is 1. Since $\lceil x - 1 \rceil = \lceil x \rceil - 1$, and $np/(p^2-1)$ is an integer exactly when $p^2 - 1$ divides n, Theorem A gives the following.

Theorem B. *Let F satisfy (H_2), for example Katz's group $G(\alpha)$ over the integers of any finite extension of $\mathbb{Q}_p$. For every integral f and every $n \geq 0$,*

$$D^n f \in p^{\,a_2(n)} R[[t]], \qquad a_2(n) = \max\Big\{ \sum_{r \geq 0} \Big\lfloor \frac{n}{p^{2r+1}} \Big\rfloor,\ \Big\lceil \frac{np}{p^2-1} \Big\rceil - 1,\ 0 \Big\}.$$

Hence $a_2(n) \geq \lfloor np/(p^2-1) \rfloor$ when $p^2 - 1 \nmid n$, and $a_2(n) \geq np/(p^2-1) - 1$ when $p^2 - 1 \mid n$; moreover $D^p R[[t]] \subseteq pR[[t]]$. If $pR \neq R$, the function $f = t^{p^2-1}$ at $n = p^2 - 1$ has $(D^n f)(0) = (p^2-1)!$, of valuation exactly $p - 1 = \lfloor np/(p^2-1) \rfloor - 1$.

So Katz's bound needs his condition on the translates only at the orders divisible by $p^2 - 1$, and there it loses at most one.

Example 1.1. Let $p = 2$ and $h = 2$, so that $q = 4$ and $c_2 = \frac{2}{3}$. For $1 \le n \le 9$ the two bounds, their maximum $a_2(n)$ and Katz's value are

n	1	2	3	4	5	6	7	8	9
$\lfloor n/2 \rfloor + \lfloor n/8 \rfloor + \cdots$	0	1	1	2	2	3	3	5	5
$\lceil 2n/3 \rceil - 1$	0	1	1	2	3	3	4	5	5
$a_2(n)$	0	1	1	2	3	3	4	5	5
$\lfloor 2n/3 \rfloor$	0	1	2	2	3	4	4	5	6

The last two rows differ exactly at $n = 3, 6, 9$, the multiples of $p^2 - 1 = 3$. At $n = 3$ the function $f = t^3$ has $(D^3 f)(0) = 3! = 6$, of valuation $1 = a_2(3)$: the bound of Theorem B is attained there, and Katz's value 2 needs his condition on f. At $n = 4$ the floor sum is attained: if F has exact height two over $W(k)$, then $v_2((D^4 t)(0)) = 2$ by Theorem A(2).

For the third theorem let $h \ge 2$, $d = h - 1$ and $\mathcal{O} = W(\mathbb{F}_q)$. The Honda formal group G_h over $\mathbb{Z}_p$ is the one with logarithm $\sum_{n \ge 0} T^{q^n}/p^n$; over $\mathcal{O}$ it is a Lubin–Tate group for the uniformizer p. Let M be the map of d-tuples of power series given by

$$M_1(X) = X_d^{p^2}, \qquad M_i(X) = X_{i-1}^{p} \quad (2 \le i \le d),$$

with $M_1(X) = X_1^{p^2}$ when $d = 1$, and let H be the d-dimensional formal group law with logarithm $\mathcal{L}(X) = \sum_{n \ge 0} p^{-n} M^{\circ n}(X)$. Write $D_1, \dots, D_d$ for its invariant derivations with $(D_i X_j)(0) = \delta_{ij}$, and put

$$c_i = \frac{p^i}{q - 1} \qquad (1 \le i \le d).$$

Theorem C. *The law H has coefficients in $\mathbb{Z}_p$, and over $\mathcal{O}$ its p-divisible group is isomorphic to the Cartier dual of that of G_h. For every $\mathbb{Z}_p$-algebra R, every $f \in R[[X_1, \dots, X_d]]$, every i and all n, $a_1, \dots, a_d \ge 0$,*

$$D_i^n f \in p^{\max\{0, \lceil c_i n - 1 \rceil\}} R[[X]], \qquad D_1^{a_1} \cdots D_d^{a_d} f \in p^{\sum_i \max\{0, \lceil c_i a_i - 1 \rceil\}} R[[X]],$$
$$D_1^{a_1} \cdots D_d^{a_d} f \in p^{\max\{0, \lceil \sum_i (c_i a_i - s_p(a_i)/(p-1)) \rceil\}} R[[X]].$$

The slopes and the constant are optimal: $v_p((D_i^{q^r} X_i)(0)) = c_i(q^r - 1)$ for all $r \ge 0$, and the single function $f_* = (\prod_{j<d} X_j^{p-1}) X_d^{p^2-1}$ satisfies $v_p((D_i^{q-1} f_*)(0)) = c_i(q-1) - 1$ for every i. Finally $c_1 + \cdots + c_d = c_h$.

1.3. **Why the results matter.** Katz's question is the first step of a programme: once the right power of p is known, the normalized derivatives can be interpolated, and at height one this is the theory of p-adic L-functions through measures on $\mathbb{Z}_p$ [12, §§III–V]. At height two the programme reaches Bernoulli–Hurwitz numbers at supersingular primes [13, 7, 4], and the general theory of Galois measures it announced was proved only recently [5]. Theorem A fixes the divisibility at every height with the optimal constant, for every integral function and every formal group satisfying (H_h).

The bound has a second, recent use. Alpöge's announcement of a proof of the Riemann hypothesis lists, as step 2 of its timeline, that $D^p \equiv 0$ on a curve with complex multiplication at a prime p inert in the field of complex multiplication, and that $D^a\theta(0)/\Omega^a$ is divisible by $p^{a/p + a/p^3 + \cdots - O(\log a)}$ [1, p. 3]. The exponent $a/p + a/p^3 + \cdots = c_2 a$ is the slope of Theorem B, the formal group of such a curve at such a prime being supersingular, of height two; and the congruence $D^p \equiv 0$ is the case $n = p$. Jaswal's reader's guide to the formalization finds this step there as a bound for theta kernels in several variables, with caps, omitted terms and a loss in $\log_p(2a)$ and its square [11, §4.4, pp. 28–30]. For integral formal functions, Theorem B replaces the logarithmic loss by the constant 1, which cannot be improved, and Theorem A gives the

analogous statement at every height. The passage from a theta function, a section of a line bundle, to an integral function in a formal coordinate needs a trivialization and the period Ω; Jaswal recalls the observation of Bannai and Kobayashi that at a supersingular prime the power series of the theta function is not integral [11, p. 30], [3, §4]. This note does not treat that passage.

Theorem C concerns several variables. The polarization of a principally polarized abelian variety identifies its p-divisible group with its Cartier dual, so a one-dimensional factor of height h comes with its dual, of dimension $h-1$, and derivatives in the directions of the dual enter every bound for theta functions in several variables. Theorem C shows that these directions have their own sharp slopes $p^i/(q-1)$, all smaller than c_h when $h \geq 3$, adding up to c_h, each with the optimal constant 1.

1.4. **Credit.** The question is Katz's [12, §I], and so is the height-two bound for functions whose translates by $\ker[p]$ sum to zero [12, Corollary 2], [13, Main Theorem 3.11]; the identity $\sum_n D(n)U^n = \exp(D(1)L(U))$ between translation operators and the logarithm, on which the proof of the affine bound rests, is his [13, Corollary 1.8, p. 669]. For Lubin–Tate groups over a field with ramification index $e \leq p-1$, Boxall interpolated Ω_p^{-k} times the k-th invariant derivative at 0 of the twisted averages $\Delta^{(\beta)}f$ of every integral f over the π-torsion, with $v(\Omega_p) = \frac{1}{p-1} - \frac{1}{e(q-1)}$ [6, Theorem B, p. 3]; for $e=1$ this is the slope c_h, with a constant depending on f. Bannai and Kobayashi bounded the derivatives of the powers of the exponential of a Lubin–Tate group, in any coordinate [4, Proposition 3.5, p. 10], and proved the factorial inequality $v_p(i!) \geq i\big(\frac{1}{p-1} - \frac{1}{e(q-1)}\big) - h + \frac{1}{e}$ with equality only at $i = q-1$ [4, Proposition 3.3, p. 8]; for $e=1$ together they give $v_p((D^n f)(0)) \geq c_h n - (h-1)$ for Lubin–Tate groups over unramified bases, with the optimal constant. (Page numbers of [4] refer to the arXiv version.)

What is proved here: Theorem A for every formal group satisfying (H_h), over any p-torsion-free $\mathbb{Z}_{(p)}$-algebra, with the floor sum E_h and its sharpness at every power of p; the comparison with Katz's bound in Theorem B; the two statements on ramified bases in Section 4; and Theorem C. The integral model of the dual is built with Hazewinkel's functional-equation lemma [10, §2], and its identification uses Tate's theory of p-divisible groups [19], the duality between Frobenius and Verschiebung [18, Exp. VII$_A$, 4.3] and Lubin–Tate theory [16], in Hazewinkel's account [10, §5].

1.5. **Context.** Katz's Galois measures for height-two formal groups over unramified bases were constructed by Ardakov and Berger for the Lubin–Tate group of $\mathbb{Q}_{p^2}$ [2], and by Berger for all height-two groups [5]; these results concern functions with the trace condition and the measures they define, not the divisibility of arbitrary integral functions. Schneider and Teitelbaum's p-adic Fourier theory, and its integral structure as studied by Bannai and Kobayashi [4], are the Lubin–Tate case of the same circle of ideas. Two recent papers extend p-adic Fourier theory to p-divisible groups: Graham, van Hoften and Howe construct integral and rigid-analytic Fourier transforms for p-divisible groups and their dual Tate modules in families [9, Theorems 7.0.2 and 7.2.6], and Kings and Sprang relate rigid generic fibres of p-divisible groups to character varieties [14, Theorem 7.1]. Neither computes the divisibility exponents of invariant derivatives, and neither gives the explicit integral model of Theorem C. Graham, van Hoften and Howe discuss how Katz's results relate to their integral restriction map [9, Remark 7.2.4]. On the side of Alpöge's argument, the reader's guide of Jaswal [11] is cited above; we know of no other treatment of the local bound. A recent post simplifies three other parts of that argument (the comparison of character sums, a logarithmic loss in the comparison of lattice slopes, and the deduction of the zero-free region), taking the arithmetic inputs as given [20]; it does not treat the local bound. A companion to this note writes out another passage of the same remark, its footnote 3, as a short proof of Deligne's bound for Frobenius eigenvalues [8]; the two notes do not depend on each other.

1.6. **Scope.** Proved: the bounds of Theorems A–C, the optimality of the slopes and of the constants, the sharpness of the floor sum at every power of p, and Propositions 4.1 and 4.2.

Three things are not proved. The first is the exact minimum of $v_p((D^n f)(0))$ over integral f at every order n. For $h \geq 3$ it is not $a_h(n)$ at every order, because the recursion of Proposition 3.1 gives a bound that exceeds $a_h(n)$ at some orders; for $p = 2$ and $h = 3$ the first such order is $n = 9$, where the recursion gives 7 and $a_3(9) = 6$. The second is any bound for theta functions, which needs the comparison discussed in Section 1.3. The third is Theorem C for the duals of formal groups other than G_h, which over $W(\overline{\mathbb{F}}_p)$ are deformations without the full action of $\mathcal{O}$.

1.7. **Proof overview.** There are two mechanisms. The first is a single operator identity. In a coordinate in which the logarithm is $z+bz^q+O(z^{q+1})$, which exists by (H_h) with pb integral, Katz's exponential formula expresses the integral translation operator Δ_q as $D^q/q! + bD$. Multiplying by $q!$ gives

$$D^q = p^{\,c_h(q-1)} u_0 D + p^{\,c_h(q-1)+1} T$$

with $u_0 \in R$ and T integral. So each further block of $q-1$ derivatives costs nothing and gains $c_h(q-1)$ powers of p. Below order q the derivatives are $n!$ times integral operators, and the worst case of $v_p(n!) - c_h n$ for $n < q$, at $n = q-1$, is exactly $-(h-1)$. This is where the constant comes from, and why it is optimal.

The second mechanism is a rescaling: over $R[\pi]$ with $\pi^{q-1} = p$, the group $\pi^{-1}F(\pi X, \pi Y)$ has its multiplication by p divisible by p, so its logarithm and exponential are integral. Hence the exponential of F has coefficients of valuation at least $-(n-1)/(q-1)$, which gives $v_p(n!) - \lfloor (n-1)/(q-1) \rfloor$ at each order; composing over the base-p digits of n gives the floor sum. Modulo π the rescaled logarithm is $t + \bar{a} t^q$, whose inverse has nonzero coefficients exactly at the powers of q; this gives sharpness.

For the dual of the Honda group the same two mechanisms work direction by direction, after the coordinates are rescaled with different weights $r_i = \frac{1}{p-1} - c_i$, chosen so that every arrow $X_j^{p^e}$ of M satisfies $p^e r_j - r_i = 1$. The operator identities $D_i^p = -(p-1)!\, D_{i+1} + pT_i$ and $D_d^{p^2} = p^p \epsilon' D_1 + p^{p+1} T_d$ with a unit ϵ', read off from the low terms of the logarithm, then descend along the cycle of M to $D_i^q = p^{p^i} u_i D_i + p^{p^i+1} U_i$. The hypothesis (H_h) is used only in Lemma 2.4 and in the rescaling, and exactness of the height only for sharpness.

2. Invariant derivations, translations and the logarithm

This section collects the identities used in the proofs. Let R be a p-torsion-free $\mathbb{Z}_{(p)}$-algebra, $K = R[1/p] = R \otimes \mathbb{Q}$, and F a one-dimensional commutative formal group law over R. Put $v(t) = \partial_2 F(t, 0) \in 1 + tR[[t]]$ and $D = v(t)\, d/dt$.

Lemma 2.1. *Let $L(t) = \int_0^t v(s)^{-1}\, ds \in K[[t]]$. Then $L(F(t,u)) = L(t) + L(u)$, $DL = 1$, and for every $g \in K[[t]]$ and $n \geq 0$,*

$$(D^n g)(0) = n!\, [z^n]\, g(E(z)),$$

where $E = L^{-1}$ is the compositional inverse. Moreover D is invariant: $D_u(g(F(t,u))) = (Dg)(F(t,u))$, where D_u is D acting on the variable u.

Proof. Differentiating the associativity $F(F(t,u),w) = F(t,F(u,w))$ in w at $w = 0$ gives $v(F(t,u)) = \partial_2 F(t,u)\, v(u)$. Hence $\partial_u L(F(t,u)) = \partial_2 F(t,u)/v(F(t,u)) = 1/v(u) = L'(u)$, so $L(F(t,u)) - L(u)$ does not depend on u, and its value at $u = 0$ is $L(t)$. Clearly $DL = v \cdot v^{-1} = 1$. In the coordinate $z = L(t)$ the derivation D is d/dz, which gives the evaluation formula by Taylor's formula for $g(E(z))$. Finally $D_u(g(F(t,u))) = g'(F(t,u))\, \partial_2 F(t,u)\, v(u) = g'(F(t,u))\, v(F(t,u))$. □

Define the translation operators $\Delta_j : R[[t]] \to R[[t]]$ by $g(F(t,u)) = \sum_{j\ge 0}(\Delta_j g)(t)\,u^j$. They are R-linear and preserve $R[[t]]$ because F has coefficients in R, and they commute with D by invariance.

Lemma 2.2 (Katz [13, Corollary 1.8])**.** *Over K, $\sum_{j\ge 0}\Delta_j u^j = \exp(L(u)\,D)$, that is, $\Delta_j = \sum_{k\ge 0}[u^j]\frac{L(u)^k}{k!}D^k$.*

Proof. For $g \in K[[t]]$ put $\tilde g = g \circ E$. By Lemma 2.1, $g(F(t,u)) = \tilde g(L(t)+L(u)) = \sum_k \frac{L(u)^k}{k!}\tilde g^{(k)}(L(t)) = \sum_k \frac{L(u)^k}{k!}(D^k g)(t)$. Each coefficient of u^j is a finite sum, since $L(u)^k$ has order k. □

Lemma 2.3 (coefficientwise bounds)**.** *Let $m \ge 0$ and suppose that $(D^n g)(0) \in p^m R'$ for every p-torsion-free $\mathbb{Z}_{(p)}$-algebra R' over R and every $g \in R'[[u]]$, where D is the invariant derivation of F over R'. Then $D^n f \in p^m R[[t]]$ for every $f \in R[[t]]$.*

Proof. Take $R' = R[[t]]$ and $g(u) = f(F(t,u)) \in R'[[u]]$. By invariance, $(D_u^n g)(0) = (D^n f)(F(t,0)) = (D^n f)(t)$. □

Lemma 2.4. *Write $[p]_F(t) = \sum_{m\ge 1} a_m t^m$, $a_1 = p$, and $L(t) = \sum_{m\ge 1}\ell_m t^m$, $\ell_1 = 1$. Then*

$$(p - p^m)\,\ell_m = a_m + \sum_{i=2}^{m-1} \ell_i\,[t^m]\,[p]_F(t)^i \qquad (m \ge 2).$$

If F satisfies (H_h), then $\ell_m \in R$ for $m < q$, and $p\ell_q \in R$.

Proof. The identity is the coefficient of t^m in $L([p]_F(t)) = pL(t)$, which holds by Lemma 2.1; the term $i = m$ contributes $p^m\ell_m$ and the term $i = 1$ contributes a_m. Suppose (H_h) and argue by induction on m. For $2 \le i \le m-1$, the coefficient $[t^m][p]_F(t)^i$ involves only coefficients a_k with $k \le m - i + 1 \le m - 1$; if $m \le q$, these lie in pR, so the coefficient lies in $p^i R \subseteq pR$. For $m < q$ also $a_m \in pR$, so the right side lies in pR; as $p - p^m = p(1 - p^{m-1})$ with $1 - p^{m-1}$ a unit of $\mathbb{Z}_{(p)}$ and R is p-torsion-free, $\ell_m \in R$. For $m = q$ the right side lies in R, so $p\ell_q \in R$. □

3. Proof of Theorem A

3.1. **The affine bound.** Put $B = c_h(q-1) = \frac{q-1}{p-1} - 1$; by Legendre's formula $v_p(q!) = \frac{q-1}{p-1} = B+1$.

Proposition 3.1. *Assume (H_h). Define integers $b(n)$ by $b(n) = v_p(n!)$ for $0 \le n < q$, and $b(n) = B + \min\{b(n-q+1),\, 1 + b(n-q)\}$ for $n \ge q$. Then $D^n R[[t]] \subseteq p^{b(n)} R[[t]]$ and $b(n) \ge c_h n - (h-1)$ for all $n \ge 0$. In particular $D^n R[[t]] \subseteq p^{\max\{0,\lceil c_h n - (h-1)\rceil\}} R[[t]]$.*

Proof. By Lemma 2.4, $z = t + \sum_{2\le m<q}\ell_m t^m$ lies in $R[[t]]$ and has linear coefficient 1, so it is a coordinate on F over R, and $R[[t]] = R[[z]]$. Since $t = z + O(z^2)$, the logarithm in this coordinate is $L = z + bz^q + O(z^{q+1})$ with $b = \ell_q$, $pb \in R$. The derivation D and the ideals $p^m R[[z]]$ do not depend on the coordinate. Let Δ_j be the translation operators in the coordinate z. By Lemma 2.2, for $j < q$ only $k = j$ contributes, since $L(u)^k = u^k + O(u^{k+q-1})$, so $\Delta_j = D^j/j!$; and $\Delta_q = D^q/q! + bD$, the term bD coming from $k = 1$. Put $w = q!/p^{B+1} \in \mathbb{Z}_{(p)}^\times$. Then

$$D^q = q!\,\Delta_q - q!\,bD = p^B u_0 D + p^{B+1}T, \qquad u_0 = -w\,pb \in R, \quad T = w\Delta_q. \tag{1}$$

For $n < q$, $D^n = n!\,\Delta_n$ maps $R[[z]]$ into $n!\,R[[z]] = p^{v_p(n!)}R[[z]]$. For $n \ge q$, $D^n f = D^q(D^{n-q}f) = p^B u_0 D^{n-q+1}f + p^{B+1}T(D^{n-q}f)$, which proves the containment by induction on n.

For the inequality, write $n < q$ in base p as $n = \sum_{j<h} d_j p^j$. By Legendre's formula $v_p(n!) = \frac{n - s_p(n)}{p-1}$, so

$$v_p(n!) - c_h n = \frac{n}{q-1} - \frac{s_p(n)}{p-1} = \sum_{j<h} d_j\Big(\frac{p^j}{q-1} - \frac{1}{p-1}\Big) \;\ge\; \sum_{j<h}(p-1)\Big(\frac{p^j}{q-1} - \frac{1}{p-1}\Big) = 1 - h,$$

because each bracket is at most 0 and $d_j \le p-1$. For $n \ge q$, by induction, $B + b(n-q+1) \ge c_h(q-1) + c_h(n-q+1) - (h-1) = c_h n - (h-1)$ and $B + 1 + b(n-q) \ge c_h n - (h-1) + (1-c_h)$, and $c_h < 1$. As $b(n)$ is an integer, $b(n) \ge \lceil c_h n - (h-1) \rceil$; and $b(n) \ge 0$. □

The recursion gives a bound that is in general larger than $\lceil c_h n - (h-1) \rceil$; we do not claim that it is the exact minimum.

3.2. **The floor-sum bound.**

Lemma 3.2 (rescaling)**.** *Assume* (H_h). *Let $R' = R[\pi] = R[x]/(x^{q-1} - p)$, a free R-module with basis $1, \pi, \dots, \pi^{q-2}$. Then $F_\pi(X,Y) = \pi^{-1}F(\pi X, \pi Y)$ is a formal group law over R' whose logarithm $L_\pi(t) = \pi^{-1}L(\pi t)$ and exponential $E_\pi(z) = \pi^{-1}E(\pi z)$ have coefficients in R'. Consequently, for $g \in R[[t]]$ and $n \ge 1$,*

$$(D^n g)(0) \in p^{\,v_p(n!) - \lfloor (n-1)/(q-1) \rfloor} R.$$

Proof. The monomial $X^i Y^j$ of F acquires the factor π^{i+j-1}, so F_π is integral, and $\pi^{-1}L(\pi t)$ is a normalized logarithm for it. Its multiplication by p is $\pi^{-1}[p]_F(\pi t) = pt + \sum_{m \ge 2} a_m \pi^{m-1} t^m$; for $m < q$, $a_m \in pR$, and for $m \ge q$, $\pi^{m-1} \in \pi^{q-1}R' = pR'$. So all its coefficients lie in pR', and the recursion of Lemma 2.4 for F_π (over R', also p-torsion-free) has right side in pR' in every degree; hence $L_\pi \in R'[[t]]$, and $E_\pi \in R'[[t]]$ as the inverse of an integral series with linear coefficient 1.

Since $E(z)^m = \pi^m E_\pi(z/\pi)^m$, we get $\pi^{n-m}[z^n]E(z)^m \in R'$, so $\pi^{n-1}[z^n]g(E(z)) \in R'$ for $n \ge 1$. Write $n - 1 = a(q-1) + c$ with $0 \le c < q-1$; then $\pi^{n-1} = p^a \pi^c$. If $y \in K$ and $p^a \pi^c y \in R'$, comparing the coefficient of π^c in the basis gives $p^a y \in R$. So $p^{\lfloor (n-1)/(q-1) \rfloor}[z^n]g(E(z)) \in R$, and Lemma 2.1 gives the claim, because $n!$ is $p^{v_p(n!)}$ times a unit of $\mathbb{Z}_{(p)}$. When n is a power of p, the case used below, the exponent is $\frac{n-1}{p-1} - \lfloor \frac{n-1}{q-1} \rfloor \ge 0$. □

Proposition 3.3. *Assume* (H_h). *Then $D^n R[[t]] \subseteq p^{E_h(n)} R[[t]]$, and $E_h(n) = c_h n - \frac{s_p(n)}{p-1} + \frac{s_q(n)}{q-1}$.*

Proof. By Lemmas 3.2 and 2.3, D^{p^j} maps $R[[t]]$ into $p^{A_j}R[[t]]$ with $A_j = v_p((p^j)!) - \lfloor \frac{p^j-1}{q-1} \rfloor$. Write $n = \sum_j d_j p^j$ in base p; then $D^n = \prod_j (D^{p^j})^{d_j}$ maps $R[[t]]$ into $p^{\sum_j d_j A_j} R[[t]]$. By Legendre, $\sum_j d_j v_p((p^j)!) = \sum_j d_j \frac{p^j-1}{p-1} = v_p(n!)$. Write $j = hr + s$ with $0 \le s < h$; then $\frac{p^j-1}{q-1} = p^s \frac{q^r-1}{q-1} + \frac{p^s-1}{q-1}$ with $0 \le \frac{p^s-1}{q-1} < 1$, so $\lfloor \frac{p^j-1}{q-1} \rfloor = \sum_{t=1}^{r} p^{j-ht}$ and

$$\sum_j d_j \Big\lfloor \frac{p^j - 1}{q-1} \Big\rfloor = \sum_{t \ge 1} \sum_{j \ge ht} d_j p^{j-ht} = \sum_{t \ge 1} \Big\lfloor \frac{n}{q^t} \Big\rfloor.$$

Hence $\sum_j d_j A_j = \sum_{i \ge 1} \lfloor n/p^i \rfloor - \sum_{t \ge 1} \lfloor n/p^{ht} \rfloor = E_h(n)$. Legendre's formula in bases p and q gives the closed form. □

3.3. **Sharpness.**

Proof of the sharpness statements of Theorem A. (1) For a normalized D, induction on $k \le n$ gives $D^k(t^n) = \frac{n!}{(n-k)!} t^{n-k} v(t)^k + O(t^{n-k+1})$, so $(D^n t^n)(0) = n!$. At $n = q-1$, $v_p((q-1)!) = \frac{q-1-h(p-1)}{p-1} = c_h(q-1) - (h-1) = m$. Write $(q-1)! = p^m u$ with $u \in \mathbb{Z}_{(p)}^\times$; if $p^m u \in p^{m+1}R$, then $u \in pR$ because R is p-torsion-free, and $1 \in pR$. A constant $C < h-1$ would require $(q-1)! \in p^{\lceil c_h(q-1) - C \rceil} R \subseteq p^{m+1}R$.

(2) Now $R = W(k)$ and a_q is a unit. The ring $R' = W(k)[\pi]$ is a discrete valuation ring with uniformizer π and residue field k. With the notation of Lemma 3.2, the series $\pi^{-1}[p]_F(\pi t)/p$ has coefficients $a_m \pi^{m-1}/p$; these lie in $\pi R'$ for $2 \le m < q$ (as $a_m \in pR$) and for $m > q$, and equal a_q for $m = q$. In the recursion of Lemma 2.4 for F_π, divided by p, the terms with $i \ge 2$ contain $[p]^i_{F_\pi}/p \in p^{i-1}R'[[t]]$, and $1 - p^{m-1} \equiv 1$. Hence $L_\pi \equiv t + \bar{a}_q t^q \pmod{\pi}$. Its

inverse over k is $\sum_{r\geq 0}\beta_r t^{q^r}$ with $\beta_0 = 1$ and $\beta_r = -\bar{a}_q\beta_{r-1}^q \neq 0$, since the q-th power map is additive in characteristic p. For $j = hr + s$, the coefficient of z^{p^j} in $E_\pi(z)^{p^s} \equiv \sum_r \beta_r^{p^s} z^{p^s q^r}$ is the unit $\beta_r^{p^s}$, so $[z^{p^j}]E(z)^{p^s} = \pi^{p^s-p^j}\cdot(\text{unit})$ has valuation $-\frac{p^j-p^s}{q-1} = -\lfloor\frac{p^j-1}{q-1}\rfloor$. By Lemma 2.1, $v_p((D^{p^j}t^{p^s})(0)) = A_j = E_h(p^j)$. For $s = 0$, $j = hr$: $E_h(q^r) = \frac{q^r-1}{p-1} - \frac{q^r-1}{q-1} = c_h(q^r-1)$. If $v_p((D^n f)(0)) \geq cn - o(n)$ held for all f with $c > c_h$, the values at $n = q^r$ would contradict this as $r \to \infty$. □

Remark 3.4 (the two ends). At height one, $c_1 = E_1(n) = 0$ and the bound is empty; for $\widehat{\mathbb{G}}_m$ with $D = (1+t)\,d/dt$ one has $D^n(1+t) = 1+t$. If $[p]_F \in pR[[t]]$ (infinite height), Lemma 2.4 gives $L, E \in R[[t]]$, and Lemma 2.1 gives $D^n R[[t]] \subseteq p^{v_p(n!)}R[[t]]$, attained by $f = L^n$. The error $v_p(n!) - \frac{n}{p-1} = -\frac{s_p(n)}{p-1}$ is unbounded, so the growth of the constant $h-1$ with h is forced.

Remark 3.5 (divided powers). At exact height h over $W(k)$ the invariant divided powers $D^n/n!$ are not integral: by the proof above, $(D^q t)(0)/q! = [z^q]E(z)$ has valuation -1. The integral operators are the Δ_n, and Theorem A measures how far D^n is from $n!\Delta_n$.

4. Height two, and ramified bases

Proof of Theorem B. For $h = 2$, $c_2 = p/(p^2-1)$, $h-1 = 1$ and $E_2(n) = \sum_{r\geq 0}\lfloor n/p^{2r+1}\rfloor$; this is Theorem A. For $x \in \mathbb{R}$, $\lceil x-1\rceil = \lceil x\rceil - 1$, which equals $\lfloor x\rfloor$ unless $x \in \mathbb{Z}$; and $x = np/(p^2-1)$ is an integer exactly when $p^2-1 \mid n$, because $\gcd(p, p^2-1) = 1$. At $n = p$, $E_2(p) = 1$. Katz's group $G(\alpha)$ has $[p](X) = pX + \alpha X^{p^2}$, which satisfies (H_2) over any ring containing α. The last statement is Theorem A(1) with $v_p((p^2-1)!) = p-1$. □

The next two propositions explain the hypothesis (H_h) over bases with ramification, where it is stronger than a condition on the height of the special fibre. The first gives a class of formal groups that satisfy it over any base. The second shows that the bounds of Theorem A fail for a formal group over a ramified discrete valuation ring whose special fibre has height h.

Proposition 4.1. *Let R be a p-torsion-free $W(\mathbb{F}_q)$-algebra and F a formal group law over R with endomorphisms $[\zeta]_F$, $\zeta \in \mu_{q-1} \subset W(\mathbb{F}_q)$, such that $[\zeta]_F \circ [\eta]_F = [\zeta\eta]_F$ and $[\zeta]_F(t) \equiv \zeta t \bmod t^2$. Then in the coordinate $x = (q-1)^{-1}\sum_\zeta \zeta^{-1}[\zeta]_F(t)$ the series $[p]_F(x)$ has nonzero coefficients only in degrees $\equiv 1 \pmod{q-1}$; in particular F satisfies (H_h), and the bounds of Theorem A hold for F. This applies to every formal $W(\mathbb{F}_q)$-module over R.*

Proof. Since $q-1$ is invertible, $x \in R[[t]]$ and $x = t + O(t^2)$. For $\eta \in \mu_{q-1}$, $x([\eta]_F t) = (q-1)^{-1}\sum_\zeta \zeta^{-1}[\zeta\eta]_F(t) = \eta\, x(t)$, so in the coordinate x the endomorphism $[\eta]_F$ is $x \mapsto \eta x$. It commutes with $[p]_F = \sum_m a_m x^m$, so $a_m(\eta^m - \eta) = 0$. If $q-1 \nmid m-1$ and η generates μ_{q-1}, then $\eta^{m-1}-1$ is a unit of $W(\mathbb{F}_q)$, its reduction being a nonzero element of $\mathbb{F}_q$; so $a_m = 0$. The least $m > 1$ with $m \equiv 1 \pmod{q-1}$ is q. □

Proposition 4.2. *Let $h \geq 2$, $e \geq 2$, k a finite field of characteristic p, and $A = W(k)[\varpi]$ with $\varpi^e = p$; normalize $v(p) = 1$. There is a formal group law F over A whose reduction modulo ϖ has height h and whose invariant derivation satisfies $(D^p t)(0) = (p-1)!\,\varpi$, of valuation $1/e < 1 = E_h(p)$. If $e > p$, then moreover $v((D^{p^s}t)(0)) = \frac{p^s-1}{e(p-1)}$ for all $s \geq 0$, so along the powers of p the growth is linear with slope $\frac{1}{e(p-1)} < c_2 \leq c_h$.*

Proof. The reduction Φ of G_h to k has height h and $\Phi(x,y) \equiv x+y$ modulo degree q, since the logarithm and the exponential of G_h are $T \pm T^q/p + \cdots$. Lubin and Tate construct a formal group law Γ over $W(k)[[t_1,\dots,t_{h-1}]]$ reducing to Φ at $t = 0$ and with $\Gamma \equiv x + y + t_1 C_p(x,y)$ modulo degree $p+1$, where $C_p(x,y) = ((x+y)^p - x^p - y^p)/p$ [17, Proposition 1.1, pp. 50–51]. Let F be its specialization at $t_1 = \varpi$, $t_2 = \cdots = t_{h-1} = 0$; it is a formal group law over A reducing to Φ,

and $F \equiv x+y+\varpi C_p(x,y)$ modulo degree $p+1$. Then $v(t)=\partial_2 F(t,0)=1+\varpi t^{p-1}+O(t^p)$, and by induction $D^k t=\frac{(p-1)!}{(p-k)!}\varpi\, t^{p-k}+O(t^{p-k+1})$ for $2\le k\le p$, so $(D^p t)(0)=(p-1)!\,\varpi$.

By induction on n, $[n]_F(t)\equiv nt+\varpi\frac{n^p-n}{p}t^p$ modulo degree $p+1$, using $C_p(nt,t)=\frac{(n+1)^p-n^p-1}{p}t^p$; so $[p]_F(t)=pt+\varpi(p^{p-1}-1)t^p+\sum_{m>p}a_m t^m$. Let $e>p$, choose β with $\beta^{p-1}=p/\varpi$ in an extension, and let A' be the valuation ring of $\mathrm{Frac}(A)(\beta)$; then $\rho=v(\beta)=\frac{e-1}{e(p-1)}$, and $p\rho>1$ because $e>p$. The law $F_\beta=\beta^{-1}F(\beta X,\beta Y)$ is integral over A', and its multiplication by p is $pt+p(p^{p-1}-1)t^p+\sum_{m>p}a_m\beta^{m-1}t^m$, where $v(a_m\beta^{m-1})\ge(m-1)\rho\ge p\rho>1$. Divided by p it reduces to $t-t^p$ modulo the maximal ideal. As in the proof of Theorem A(2), the logarithm of F_β is integral and reduces to $t-t^p$, whose inverse in characteristic p is $\sum_{s\ge0}t^{p^s}$. Hence $[z^{p^s}]E(z)=\beta^{1-p^s}\cdot(\text{unit})$ and $v((D^{p^s}t)(0))=\frac{p^s-1}{p-1}-(p^s-1)\rho=\frac{p^s-1}{e(p-1)}$. Finally $\frac{1}{e(p-1)}<\frac{1}{p(p-1)}<\frac{p}{p^2-1}=c_2$. □

By Proposition 4.1, such a deformation carries no action of the Teichmüller roots of unity lifting one on its special fibre, although its special fibre may carry one.

5. The Cartier dual of the Honda group

Keep the notation of Theorem C: $h\ge2$, $d=h-1$, $q=p^h$, M, $\mathcal{L}=\sum_n p^{-n}M^{\circ n}$. Each component $M^{\circ n}(X)_i$ is a single monomial $X_k^{p^E}$: following the arrows $X_{i-1}\to X_i$ (exponent p) and $X_d\to X_1$ (exponent p^2) backwards from i for n steps. One full cycle has d steps and total exponent $p^{(d-1)+2}=q$.

5.1. **Integrality.** The logarithm satisfies the functional equations

$$\mathcal{L}_1(X)=X_1+p^{-1}\mathcal{L}_d(X^{p^2}),\qquad \mathcal{L}_i(X)=X_i+p^{-1}\mathcal{L}_{i-1}(X^p)\quad(2\le i\le d),$$

where $X^{p^k}=(X_1^{p^k},\dots,X_d^{p^k})$. In the notation of Hazewinkel's functional-equation lemma [10, 2.1–2.3, pp. 73–74] take $B=\mathbb{Z}_p$, $L=\mathbb{Q}_p$, $\mathfrak{a}=p\mathbb{Z}_p$, $\sigma=\mathrm{id}$, $q=p$, s_1 the $d\times d$ matrix with entries $1/p$ in positions $(i,i-1)$, s_2 the matrix with entry $1/p$ in position $(1,d)$ (when $d=1$, $s_1=0$ and $s_2=(1/p)$), and $s_k=0$ for $k\ge3$. The conditions (2.2) hold, and $\mathcal{L}(X)-s_1\mathcal{L}(X^p)-s_2\mathcal{L}(X^{p^2})=X$. By (2.5), $H(X,Y)=\mathcal{L}^{-1}(\mathcal{L}(X)+\mathcal{L}(Y))$ has coefficients in $\mathbb{Z}_p$. The same lemma with $q=p^h$ and $s_1=1/p$ shows that G_h is integral.

5.2. **The rescaled model.** Let $R'=\mathbb{Z}_p[\pi]$ with $\pi^{q-1}=p$, a discrete valuation ring with residue field $\mathbb{F}_p$; put $S_h=\frac{q-1}{p-1}$, and for $1\le i\le d$

$$\alpha_i=\pi^{S_h-p^i},\qquad r_i=v(\alpha_i)=\frac{1}{p-1}-c_i>0.$$

For the arrow X_{i-1}^p in M_i one has $pr_{i-1}-r_i=\frac{(p-1)S_h}{q-1}=1$, and for the arrow $X_d^{p^2}$ in M_1 one has $p^2r_d-r_1=\frac{(p^2-1)S_h-pq+p}{q-1}=1$; in both cases the exponent of π in $\alpha_i^{-1}\alpha_k^{p^e}/p$ is exactly 0.

Lemma 5.1. *Put $\mathcal{L}'_i(Z)=\alpha_i^{-1}\mathcal{L}_i(\alpha_1Z_1,\dots,\alpha_dZ_d)$ and $\mathcal{E}'=(\mathcal{L}')^{-1}$. Then $\mathcal{L}',\mathcal{E}'$ have coefficients in R', $\mathcal{L}'\equiv Z+M(Z)$ and $\mathcal{E}'\equiv\sum_{n\ge0}(-1)^nM^{\circ n}(Z)$ modulo π. For the exponential $\mathcal{E}=\mathcal{L}^{-1}$ of H and every multi-index b, $v([t^b]\mathcal{E}_j)\ge r_j-\sum_i b_ir_i$, with equality when $[Z^b]\mathcal{E}'_j$ is a unit.*

Proof. The term $p^{-n}M^{\circ n}(X)_i=p^{-n}X_k^{p^E}$, along a path with exponents $p^{e_1},\dots,p^{e_n}$ and $E=e_1+\cdots+e_n$, becomes $\alpha_i^{-1}\alpha_k^{p^E}p^{-n}Z_k^{p^E}$. Using $p^{e_s}r_{k_s}=r_{k_{s-1}}+1$ along the path, its valuation is $1+p^{e_1}+p^{e_1+e_2}+\cdots+p^{e_1+\cdots+e_{n-1}}-n$, which is 0 for $n=1$ (with coefficient exactly 1, by the computation above) and at least $(n-1)(p-1)>0$ for $n\ge2$. So $\mathcal{L}'$ is integral and $\mathcal{L}'\equiv Z+M(Z)$ (mod π); its inverse is integral since its linear part is the identity. In characteristic p the map M

is additive, so $(\mathrm{id}+M)\circ\sum_n(-1)^n M^{\circ n}=\mathrm{id}$. Finally $\mathcal{E}_j(t)=\alpha_j\mathcal{E}'_j(t_1/\alpha_1,\dots,t_d/\alpha_d)$, which gives the valuations. □

5.3. **Identification with the dual.** Since $\mathcal{L}(M(X))=\sum_n p^{-n}M^{\circ(n+1)}(X)=p(\mathcal{L}(X)-X)$, we have $\mathcal{L}([p]_H(X))=p\mathcal{L}(X)=pX+\mathcal{L}(M(X))$, so $\mathcal{L}([p]_H(X))\equiv\mathcal{L}(M(X))$ modulo p, and by [10, (2.8), p. 75]

$$[p]_H(X)\equiv M(X)\pmod p.$$

In the same way $[p]_{G_h}(T)\equiv T^q \pmod p$, as in [10, (5.4)].

Let $S=\mathbb{Z}_p[[U_1,\dots,U_d]]\to S'=\mathbb{Z}_p[[X_1,\dots,X_d]]$ send U to $[p]_H(X)$. Modulo (p,U), S' becomes $\mathbb{F}_p[[X]]/(X_d^{p^2},X_1^p,\dots,X_{d-1}^p)$, of dimension $p^{d-1}\cdot p^2=q$ over $\mathbb{F}_p$, spanned by the monomials X^b with $b_i<p$ for $i<d$ and $b_d<p^2$. By the complete Nakayama lemma S' is a finite S-module generated by these monomials; as S and S' are regular local rings of the same dimension, S' is Cohen–Macaulay of full dimension over S and hence free, by the Auslander–Buchsbaum formula, of rank q. So H is a divisible formal Lie group of height h and dimension d, and its p-divisible group $H(p)$ is connected of height h [19, §2.2, Proposition 1]. Its Cartier dual $P=H(p)^D$ has dimension $h-d=1$ [19, §2.3, Proposition 3].

On the special fibre over $\mathbb{F}_p$, the relative Frobenius of H is $X\mapsto X^p$ and $[p]_H=M$, so $[p]_H^d=M^{\circ d}=\mathrm{Fr}_H^h$, a full cycle having exponent q. Cartier duality exchanges Frobenius and Verschiebung [18, Exp. VII$_A$, 4.3.3], so $[p]_P^d=\mathrm{Ver}_P^h$. Since $\mathrm{Ver}\circ\mathrm{Fr}=\mathrm{Fr}\circ\mathrm{Ver}=p$ [18, Exp. VII$_A$, 4.3 and 4.3.2], $\mathrm{Fr}_P^h\circ[p]_P^d=\mathrm{Fr}_P^h\,\mathrm{Ver}_P^h=p^h$, hence $(\mathrm{Fr}_P^h-p)\circ[p]_P^d=0$, and as $[p]_P$ is an epimorphism, $\mathrm{Fr}_P^h=[p]_P$. So P is connected and is the p-divisible group of a one-dimensional formal group Γ over $\mathbb{Z}_p$ [19, §2.2, Proposition 1], whose multiplication by p is $\equiv T^q \pmod p$ in any coordinate. Over $\mathcal{O}$, both $[p]_\Gamma$ and $[p]_{G_h}$ are Lubin–Tate series for the uniformizer p; by Lubin–Tate theory each group is the unique formal group law over $\mathcal{O}$ with its series as an endomorphism, and the two are strictly isomorphic [10, (5.1)], [16]. Hence over $\mathcal{O}$, $H(p)\cong P^D\cong\Gamma(p)^D\cong G_h(p)^D$. This proves the first assertion of Theorem C.

5.4. **The bounds.**

Proof of Theorem C. The coefficients of H lie in $\mathbb{Z}_p$, so the D_i are integral, commuting derivations, and in the logarithmic coordinates $t=\mathcal{L}(X)$ they are $\partial/\partial t_i$. As in Lemma 2.1, $(D^af)(0)=a!\,[t^a]f(\mathcal{E}(t))$ with $a!=\prod_i a_i!$. For f integral, each coefficient of $f(\mathcal{E}(t))$ in degree a is a sum of products of coefficients of the $\mathcal{E}_j$, of total degree a, so by Lemma 5.1 its valuation is at least $-\sum_i a_ir_i$. With Legendre's formula, $v_p((D^af)(0))\ge\sum_i(c_ia_i-\frac{s_p(a_i)}{p-1})$; the left side is an integer. Applying this to $f(H(X,Y))$ as a series in Y over $\mathbb{Z}_p[[X]]$ gives the third containment, as in Lemma 2.3.

For the directional bounds let Δ_b be the translation operators of H, defined by $f(H(X,Y))=\sum_b(\Delta_bf)(X)Y^b$; they are integral and commute with one another and with the D_i. As in Lemma 2.2, $\sum_b\Delta_bY^b=\exp(\sum_i\mathcal{L}_i(Y)D_i)$. A pure power of one variable arises in a product of monomials only from pure powers of that variable. The pure powers of Y_i of degree at most p occurring in $\mathcal{L}(Y)$ are Y_i in $\mathcal{L}_i$ and, for $i<d$, $p^{-1}Y_i^p$ in $\mathcal{L}_{i+1}$. The pure powers of Y_d of degree at most p^2 are Y_d in $\mathcal{L}_d$ and $p^{-1}Y_d^{p^2}$ in $\mathcal{L}_1$; the next ones have degree p^3 (in $\mathcal{L}_2$) or q (in $\mathcal{L}_d$), and p^4 when $h=2$. Comparing the coefficients of Y_i^p and $Y_d^{p^2}$ gives $\Delta_{pe_i}=D_i^p/p!+D_{i+1}/p$ for $i<d$, $\Delta_{pe_d}=D_d^p/p!$ and $\Delta_{p^2e_d}=D_d^{p^2}/(p^2)!+D_1/p$. Hence, with the units $\epsilon=-(p-1)!$ and $\epsilon'=-(p^2)!/p^{p+1}$ of $\mathbb{Z}_p$ and integral operators T_i,

$$D_i^p=\epsilon D_{i+1}+pT_i\ \ (i<d),\qquad D_d^p\in p\,\mathrm{End},\qquad D_d^{p^2}=p^p\epsilon' D_1+p^{p+1}T_d, \tag{2}$$

where End denotes the integral continuous operators on $\mathbb{Z}_p[[X]]$; when $d = 1$ only the last two occur. Put $R_i = p^{h-i}$. Descending induction on i, raising the first identity to the power p^{h-i-1}, gives $D_i^{R_i} \in p\,\mathrm{End}$, so $D_i^n \in p^{\lfloor n/R_i \rfloor}\,\mathrm{End}$.

Fix $i < d$ and put $B_i = p^i$. Start from $D_i^q = (D_i^p)^{p^{h-1}}$ and substitute the first identity of (2) along $j = i, i+1, \dots, d-1$: at the step $j = i+s$ it is raised to the power $N = p^{h-s-1}$, and $N/R_{j+1} = B_i$. The term of index $1 \le m \le N$ in the binomial expansion has valuation at least

$$v_p\tbinom{N}{m} + m + \Big\lfloor \frac{N-m}{R_{j+1}} \Big\rfloor = B_i + v_p\tbinom{N}{m} + m - \Big\lceil \frac{m}{R_{j+1}} \Big\rceil \;\ge\; B_i + 1,$$

since $\binom{N}{m}$ is divisible by p for $0 < m < N$, and for $m = N$ the bound is $N \ge p^{i+1} > B_i$. The leading term at the end is a unit times $D_d^{p^{i+1}} = (D_d^{p^2})^{p^{i-1}} = p^{B_i}(\epsilon' D_1 + pT_d)^{p^{i-1}}$, and modulo p the factor $(\epsilon' D_1 + pT_d)^{p^{i-1}}$ is a unit times $D_1^{p^{i-1}}$, which the first identities modulo p turn into a unit times D_i. For $i = d$ the same last step applies directly to $D_d^q = (D_d^{p^2})^{p^{d-1}}$. In all cases

$$D_i^q = p^{B_i} u_i D_i + p^{B_i+1} U_i, \qquad u_i \in \mathbb{Z}_p^\times,\ U_i \in \mathrm{End}\,.$$

Now $c_i(q-1) = B_i$ and $c_i R_i = \frac{q}{q-1}$. For $0 \le n < q$, let $kR_i \le n < (k+1)R_i$ with $0 \le k < p^i$. There $\lfloor n/R_i \rfloor = k$, and $c_i n - k$ is largest at $n = (k+1)R_i - 1$, where it equals $(k+1)\frac{q}{q-1} - c_i - k = 1 + \frac{k+1}{q-1} - c_i \le 1$, with equality only for $k+1 = p^i$, that is $n = q-1$. So $\lfloor n/R_i \rfloor \ge c_i n - 1$. For $n \ge q$, $D_i^n f = p^{B_i} u_i D_i^{n-q+1} f + p^{B_i+1} U_i D_i^{n-q} f$, and induction gives the bound $c_i n - 1$ for both terms, as in Proposition 3.1. This proves $D_i^n \in p^{\max\{0, \lceil c_i n - 1 \rceil\}}\,\mathrm{End}$, and composing gives the mixed bound. Base change to any $\mathbb{Z}_p$-algebra R preserves these containments.

Sharpness. By Lemma 5.1, the component i of $\mathcal{E}'(Z_i e_i)$ reduces to $\sum_{r \ge 0} (-1)^{dr} Z_i^{q^r}$, so $[t_i^{q^r}]\mathcal{E}_i$ has valuation $-(q^r - 1)r_i$ and $v_p((D_i^{q^r} X_i)(0)) = \frac{q^r - 1}{p-1} - (q^r - 1)r_i = c_i(q^r - 1)$. For the common witness, $\mathcal{L}$ is equivariant for the Teichmüller action $X_j \mapsto \zeta^{p^j} X_j$, $\zeta^{q-1} = 1$ (the exceptional arrow has weight $p^2 p^d \equiv p$), hence so is $\mathcal{E}$, and a monomial t_i^n in $\mathcal{E}_j(t_i e_i)$ requires $np^i \equiv p^j \pmod{q-1}$. The least such n is $m_{ij} = p^{j-i}$ for $j \ge i$ and p^{h+j-i} for $j < i$, and by Lemma 5.1 the coefficient there has valuation exactly $r_j - m_{ij} r_i$, the path from j back to i being a single monomial of $M^{\circ n}$. With $e_j = p - 1$ for $j < d$ and $e_d = p^2 - 1$ one checks $\sum_j e_j m_{ij} = q - 1$ and $\sum_j e_j r_j = d$, using $\sum_j e_j = (p-1)(h+p-1)$ and $\sum_j e_j p^j = p(q-1)$. So the lowest term of $f_*(\mathcal{E}(t_i e_i))$ has degree $q-1$ and valuation $d - (q-1)r_i$, and $v_p((D_i^{q-1} f_*)(0)) = v_p((q-1)!) + d - (q-1)r_i = p^i - 1 = c_i(q-1) - 1$. Finally $\sum_{i=1}^d c_i = \frac{p + \cdots + p^d}{q-1} = \frac{q-p}{(p-1)(q-1)} = c_h$. □

6. What remains open

The exact minimum of $v_p((D^n f)(0))$ over integral f, for each order n, is not determined. The bounds of Theorem A are attained at $n = q-1$ and at every power of p, and for $h \ge 3$ the recursion of Proposition 3.1 is strictly larger at some other orders; at height two no order where it is larger is known. For Alpöge's step 2 the remaining input is the comparison between normalized theta derivatives and derivatives of integral formal functions, with its period and frame; Theorem B gives the local exponent once that comparison is available, and nothing here bears on it. In several variables, the bounds of Theorem C are for the coordinate directions of one model of the dual; the optimal slopes along other lines through a formal group and its dual are not treated here.

Note on method

The results and their proofs were produced by GPT-6 Astra (ChatGPT Pro mode). The proofs were checked by Claude Opus 5.5 at effort high, and again line by line by Claude Opus 5.5 at

effort max, which also wrote this text, stated Theorem A over p-torsion-free $\mathbb{Z}_{(p)}$-algebras (the same proof applies) and gave Proposition 4.1 its present form. Claude Fable 5.2 at effort max edited the text and reread every proof. Of the sources it read only Alpöge's note and the abstract of [20]; the others were read at the cited places by Claude Opus 5.5 at effort max. Claude Opus 5.5 at effort max read the edited text again in full before deposit. No human has checked this note. Our text is dedicated to the public domain under CC0 1.0. The records of the checks are at the permanent page of this work, WB-0005: https://github.com/KokunoYumeto/mathematics-workbenches/blob/main/works/WB-0005.md.

References

[1] L. Alpöge, *Remark* (announcement on the Riemann hypothesis, with a Lean formalization), 20 November 2026, p. 3, timeline step 2. https://alpo.ge/remark.pdf.

[2] K. Ardakov and L. Berger, *Bounded functions on the character variety*, Münster J. Math. **17** (2024), 1–83, Theorem 1.6.1 (as described in [5, Introduction]).

[3] K. Bannai and S. Kobayashi, *Algebraic theta functions and the p-adic interpolation of Eisenstein–Kronecker numbers*, Duke Math. J. **153** (2010), 229–295, §4. arXiv:math/0610163.

[4] K. Bannai and S. Kobayashi, *Integral structures on p-adic Fourier theory*, Ann. Inst. Fourier **66** (2016), 521–550; arXiv:0804.4338, Propositions 3.1, 3.3 and 3.5 (arXiv pp. 7–10).

[5] L. Berger, *Galois measures and the Katz map*, arXiv:2504.20558 (v3, 16 October 2026).

[6] J. L. Boxall, *p-adic interpolation of logarithmic derivatives associated to certain Lubin–Tate formal groups*, Ann. Inst. Fourier **36** (1986), no. 3, 1–27, Theorem B (p. 3) and Lemma 13.

[7] M. Chellali, *Congruences entre nombres de Bernoulli–Hurwitz dans le cas supersingulier*, J. Number Theory **35** (1990), 157–179.

[8] *A short proof of Deligne's bound for Frobenius eigenvalues, after Alpöge*, Hexagon, hexagon:2611.00789 (21 November 2026). https://hexagonmath.org/2611.00789.

[9] A. Graham, P. van Hoften and S. Howe, *p-adic Fourier theory in families*, arXiv:2507.05374 (2025), Theorems 7.0.2, 7.2.6 and Remark 7.2.4.

[10] M. Hazewinkel, *On formal groups. The functional equation lemma and some of its applications*, Astérisque **63** (1979), 73–82: §2, (2.1)–(2.8), pp. 73–75; §5, (5.1)–(5.4), pp. 76–77.

[11] M. Jaswal, *The Riemann hypothesis for Dirichlet L-functions [after Levent Alpöge]*, Hexagon, hexagon:2611.00799v1 (21 November 2026), pp. 5 and 28–30. https://hexagonmath.org/2611.00799.

[12] N. M. Katz, *Formal groups and p-adic interpolation*, Astérisque **41–42** (1977), 55–65: §I, pp. 55–56; §V, Lemma 1 and Corollary 2, pp. 62–63.

[13] N. M. Katz, *Divisibilities, congruences, and Cartier duality*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28** (1981), 667–678: Theorem 1.6, p. 668; Corollary 1.8, p. 669; Main Theorem 3.11 and Lemma 3.12, pp. 672–673; §IV.

[14] G. Kings and J. Sprang, *p-adic L-functions for Hecke characters of totally imaginary fields*, arXiv:2603.15446 (2026), Theorem 7.1.

[15] H. Lang, *Kummersche Kongruenzen für die normierten Entwicklungskoeffizienten der Weierstraßschen $\wp$-Funktion*, Abh. Math. Sem. Hamburg **33** (1969), 183–196.

[16] J. Lubin and J. Tate, *Formal complex multiplication in local fields*, Ann. of Math. (2) **81** (1965), 380–387.

[17] J. Lubin and J. Tate, *Formal moduli for one-parameter formal Lie groups*, Bull. Soc. Math. France **94** (1966), 49–59, Proposition 1.1.

[18] M. Demazure and A. Grothendieck (eds.), *Schémas en groupes* (SGA 3), Exposé VII$_A$ (P. Gabriel), 4.3, 4.3.2 and 4.3.3.

[19] J. Tate, *p-divisible groups*, in Proc. Conf. Local Fields (Driebergen, 1966), Springer, 1967, 158–183: §2.2, Proposition 1; §2.3, Proposition 3.

[20] twinheterodox, *Three simplifications in the Alpöge–Claude argument for Dirichlet GRH*, Hexagon, hexagon:2611.00828 (November 2026). https://hexagonmath.org/2611.00828.