Mixed derivative congruences on cyclotomic Jacobians

twinheterodox
Prepared with Codex

November 28, 2026

hexagon:2611.01311v1

Abstract

We determine the exact p-divisibility of mixed invariant derivatives of explicit rational functions on hyperelliptic Jacobians. On the Jacobian of $y^2 = x^7 - 1$ at $p = 11$, the product of the three divisor abscissas has a mixed derivative of orders $(11, 9)$, in the directions dual to $x\,dx/y$ and dx/y, that is a unit at every regular integral point. Increasing either order by 1330 adds exactly 11 or 121 to its valuation, respectively, however often the two increases are combined. We compute the starting residue by Cartier and show that each shift multiplies the normalized residue by the same unit. One de Rham component determines whether the valuation is exact. The same construction gives a product of divisor abscissas attaining simultaneous equalities in arbitrarily many independent directions.

1 An exact law for one function

How divisible can the successive derivatives of an Abelian function be? On an elliptic curve there is one invariant direction. On a Jacobian there are several, and one can ask a sharper question. Can one keep both the function and the point fixed, vary several derivative orders independently, and still predict the first nonzero p-adic digit?

Consider the curve $C : y^2 = x^7 - 1$ and its Jacobian J. An unordered triple of finite points with distinct abscissas x_1, x_2, x_3 gives a chart of J by subtracting 3∞. Let D_i be the invariant fields dual to the Abel–Jacobi differentials induced by $x^{i-1}\,dx/y$, $1 \le i \le 3$. Our normalization uses dx/y throughout. At $p = 11$, put $F = x_1x_2x_3$. For every integral point T reducing into this chart, and all $k, \ell \ge 0$, we obtain

$$v_{11}\Big(D_2^{11+1330k} D_1^{9+1330\ell} F(T)\Big) = 11k + 121\ell. \tag{1}$$

At $(k, \ell) = (0, 0)$ the residue is 5. After division by the power of 11 in (1), the residue is $5 \cdot 4^{k+\ell}$ everywhere on the lattice. Each direction has its own valuation cost and the same multiplier 4, computed from the 121st derivative in (18). Even T can be chosen before the prime. Section 5 gives a single algebraic point that works for both prime classes $2, 4 \bmod 7$.

Here and below integral points may be taken over the integers of any finite unramified extension of $\mathbb{Q}_p$, with $v_p(p) = 1$. In genus G, the *divisor chart* means the locus represented by G finite points with distinct abscissas, after an extension splitting the divisor if necessary. Such a divisor contains no hyperelliptic pair and is nonspecial. Finite branch points are allowed. For a form with additional poles we require its contractions to be regular on the integral formal neighbourhood being used. We call such an integral point a *regular mark*.

The following family gives the size of the effect as the number of directions grows. For $1 \le i \le G$, the centered logarithms satisfy $dz_i = \sum_t x_t^{i-1} dx_t/y_t$ and $z_i(T) = 0$. Over the fraction field $D_i = \partial/\partial z_i$.

Theorem 1.1. *Let $h \geq 2$, $G = 2^h - 1$, $N = 2^{h+1} - 1$, and let J be the Jacobian of $y^2 = x^N - 1$. Write $F = \prod_{t=1}^{G} x_t$ on the divisor chart. If $p > N$ is prime and $p \equiv 2 \bmod N$, set $L = p^{h+1} - 1$ and $E_i = D_{2^i}$ for $0 \leq i < h$. Then for every regular mark T and all integers $k_i \geq 0$,*

$$v_p\left(\left(\prod_{i=0}^{h-1} E_i^{p-1+k_i L}\right) F(T)\right) = \sum_{i=0}^{h-1} p^{i+1} k_i. \tag{2}$$

The residue after division by this power of p is $c\, w^{\sum_i k_i}$, where $c, w \in \mathbb{F}_p^{\times}$ depend only on p and the curve. Formula (10) gives c as a product of binomial coefficients.

There are infinitely many such primes for each h, by Dirichlet's theorem. In genus seven, for example, $p = 17$ and the starting derivative $D_1^{16} D_2^{16} D_4^{16} F$ is 6 mod 17 at every regular mark. In genus three we determine an entire row of starting orders, including (1). For a Taylor coefficient of multi-index $\mathbf{n}$, subtract $\sum_i v_p(n_i!)$ from the derivative valuation. Thus (2) specifies the p-parts of the denominators of these multivariable Taylor coefficients.

Relation to earlier work. The local denominator estimates for theta expansions discussed in [1, §1.3] motivate asking when analogous bounds for individual Abelian functions are attained. Katz studied congruences among iterated invariant derivatives, obtaining a height-two divisibility bound for functions whose translates by all points of $\ker[p]$ sum to zero [6, §§I,V]. Alderliefste's Theorem C gives sharp directional bounds on the Cartier dual of a one-dimensional Honda formal group. It also bounds mixed derivatives by combining the directional bounds. Its proof obtains a recurrence from coefficients of group translation and exhibits one model function sharp along each pure axis at order $p^{h+1} - 1$ (in height $h + 1$) [1, §5.4]. Our use of that argument is in Section 4. Here the group occurs as a factor of a specified Jacobian. We identify a rational function on that Jacobian, compute its first unit derivative as a constant in the function field, and propagate it in all the directions simultaneously. Constancy is what gives equality at every regular mark.

Honda's work describes the characteristic-p Jacobians of the prime-degree members of this family (up to a quadratic twist), and character decompositions of formal groups of Fermat Jacobians [4, 5]. Yui computed the holomorphic Cartier–Manin matrix for $y^2 = 1 - x^7$ in precisely the classes $p \equiv 2, 4 \bmod 7$ and identified the isogeny type [9, Ex. 6.3]. Her later comparison with Fermat Jacobians singles out 11 and 23 [10, Rem. 6.3]. Here the extra differential of the second kind supplies the starting unit for the mixed derivatives. For the same hyperelliptic family, Ônishi obtained congruences for generalized Bernoulli–Hurwitz numbers using one Abelian coordinate at infinity and primes $p \equiv 1 \bmod N$ [8, Eq. (0.2), Thm. 7.1]. The prime classes used here put several holomorphic differentials into the same Frobenius orbit. This produces distinct directions whose restricted pth powers can be read from the curve.

How the proof works. A differential with a pole at infinity supplies the function to differentiate. The Cartier operator follows its character through the holomorphic differentials and yields a nonzero final derivative in characteristic p. A calculation on the formal group then shows what happens on increasing each derivative order by $p^{h+1} - 1$. The two calculations serve different purposes. The second gives a congruence of operators on all integral functions. The first decides whether its leading residue survives for the chosen function. For example, an extra factor of p in the starting derivative persists throughout the lattice.

2 The starting derivatives in genus three

Write $\eta_i = x^{i-1}dx/y$ on C, and write $\operatorname{Tr}\eta$ for the form on the divisor chart whose pullback to ordered divisors is $\sum_t \eta(P_t)$. Put $\omega_i = \operatorname{Tr}\eta_i$ for $1 \le i \le 3$. If Z is the local characteristic-zero primitive of $\Xi = \operatorname{Tr}\eta_4$ vanishing at the mark, division of X^3 by $\prod_t (X - x_t)$ gives

$$dZ = e_3\omega_1 - e_2\omega_2 + e_1\omega_3, \tag{3}$$

where e_i are the elementary symmetric functions of the abscissas. In particular the derivatives of Z of positive order can be computed from integral rational functions, even when Z has Taylor denominators.

For an odd prime $p \equiv 2, 4 \bmod 7$, put $(a, b) = (1, 2), (2, 1)$, respectively, and set $P = D_a,\ Q = D_b,\ g = PZ,\ f = QZ$. Thus $f = e_3$ at 11, and $f = -e_2$ at 23. In particular at 11 the companion contraction g is $-e_2$. With $m = (p-1)/2$, define in $\mathbb{F}_p$

$$c_N(i, j) = [X^{pj-i}](X^N - 1)^m, \qquad H = c_7(b, a), \quad B = c_7(4, b). \tag{4}$$

A coefficient is zero unless $pj - i = Nt$ with $0 \le t \le m$, when it equals $(-1)^{m-t}\binom{m}{t}$. Both H and B are nonzero.

We use the absolute Cartier operator $\mathcal{C}$ on closed rational one-forms over a perfect residue field. Thus $\mathcal{C}(u^p\xi) = u\mathcal{C}\xi$. Our convention for its contraction with a field D is

$$((\mathcal{C}\xi)(D))^p = \xi(D^p) - D^{p-1}(\xi(D)), \tag{5}$$

where D^p denotes the p-fold iterate on functions. This is Cartier's formula [2, §3, (6)]. For du the two terms on the right cancel, and for $u^{p-1}du$ their difference is $(Du)^p$. These examples also determine the formula by the Cartier isomorphism.

Indeed, $\eta_i = y^{-p}x^{i-1}(x^7 - 1)^m\,dx$, so Cartier selects exactly the terms of degree $pj - 1$ in the numerator. It commutes with pullback and addition, hence with the trace used here. For the holomorphic indices this is the usual hyperelliptic matrix calculation [9, §2]. Including η_4 gives one more nonzero step,

$$\mathcal{C}\Xi = B\omega_b, \qquad \mathcal{C}\omega_b = H\omega_a, \qquad \mathcal{C}\omega_a = \mathcal{C}\omega_3 = 0.$$

Pair first with the invariant basis in (5), whose contractions are constant, and then with Ξ. On the special fibre one obtains

$$P^p = HQ, \qquad Q^p = 0, \qquad Q^{p-1}f = -B, \qquad P^{p-1}g = Hf. \tag{6}$$

The first two equalities hold as derivations of the function field. In particular p differentiations in one direction act as one differentiation in the other.

Proposition 2.1. *For $0 \le j < p$, reduction modulo p gives identities of rational functions*

$$P^{pj}Q^{p-1-j}f = -H^jB, \qquad P^{pj+p-1}Q^{p-1-j}g = -H^{j+1}B. \tag{7}$$

For $0 \le j \le p$, the derivative $P^{pj}Q^{p-j}Z(T)$ is congruent to $-H^jB \bmod p$. The coefficient of $z_a^{pj}z_b^{p-j}$ in Z, with all other logarithmic coordinates set to zero, has valuation -1 at $j = 0$, $-j$ at $0 < j < p$, and $-(p+1)$ at $j = p$.

Proof. Consider first $j = 0$. The identity $Q^p = 0$ holds on the reduced function field. To compute Q^pZ, we first differentiate the primitive in characteristic zero. Its derivative $f = QZ$ is integral, so the remaining $p - 1$ differentiations give $\overline{Q^pZ} = Q^{p-1}\bar{f} = -B$ by (6).

For the whole row, the invariant fields commute, so we can replace each P^p by HQ and apply (6). The first identity of (7) gives the claim for Z up to $j = p - 1$. At that last index the second gives $P^{p^2}Z$. Division by $(pj)!(p-j)!$ and Legendre's formula give the last assertion. □

Corollary 2.2. *Let $L = p^3 - 1$. There is a unit $w_p \in \mathbb{F}_p^\times$ such that for every regular mark T, $1 \le j \le p-3$, and $k, \ell \ge 0$,*

$$p^{-kp-\ell p^2} P^{pj+kL} Q^{p-1-j+\ell L} f(T) \equiv -H^j B\, w_p^{k+\ell} \pmod{p}. \tag{8}$$

For Z itself the same formula holds with Q-order $p - j + \ell L$ and $1 \le j \le p-2$.

The proof follows the general operator calculation in Section 4. For $p = 11$ we have $H = 10$, $B = 5$, and calculation (18) gives $w_{11} = 4$. Thus $j = 1$ gives (1).

The two fields in coordinates. There is a rational coordinate description of (6). On the curve in characteristic p, vanishing Cartier image gives rational primitives $du = \eta_a$ and $dt = \eta_3$. Choose v_0 with $dv_0 = \eta_b - Hu^{p-1}du$, whose right-hand side also has zero Cartier image. On an ordered divisor put $X = \sum_t u_t$, $T' = \sum_t t_t$ and

$$Y = \sum_t v_{0,t} - H\, W(u_1, u_2, u_3), \qquad W(U_1, U_2, U_3) = \frac{(\sum U_i)^p - \sum U_i^p}{p}.$$

The polynomial W is formed over the integers before reduction. Differentiation gives $\omega_a = dX$, $\omega_b = dY + HX^{p-1}dX$, $\omega_3 = dT'$. Their wedge is nonzero, so these three symmetric functions form a p-basis of $K = k(J)$. In these coordinates

$$P = \partial_X - HX^{p-1}\partial_Y, \qquad Q = \partial_Y.$$

The coefficient of ∂_Y now explains how iterating P reaches the second direction. If $PF = 0$, then $P^p F = HQF = 0$, so both $\partial_Y F$ and $\partial_X F$ vanish. Hence $\ker P = K^p(T')$.

3 The differential that supplies the first unit

Let $N = 2G+1$ be odd, let $p > N$, and work on $J = \mathrm{Jac}(y^2 = x^N - 1)$. Choose an orbit $s_0, \dots, s_h$ of length $h+1$, $h \ge 2$, under multiplication by p mod N, with representatives in $\{1, \dots, N-1\}$. Assume that

$$(s_0, N) = 1, \qquad s_0, \dots, s_{h-1} \le G, \qquad s_h > G. \tag{9}$$

Thus the orbit contains h successive holomorphic indices and one index of the second kind. Write $E_i = D_{s_i}$ for $i < h$, and $H_i = c_N(s_{i+1}, s_i)$ for $0 \le i < h$. Every H_i is a unit. In fact $p > N$ ensures that if $1 \le j \le G$, $1 \le i < N$ and $pj \equiv i \bmod N$, then $0 \le (pj - i)/N \le (p-1)/2$. The largest possible output index of Cartier on η_i is G.

The classes of $\eta_1, \dots, \eta_{N-1}$ form a basis of $H^1_{\mathrm{dR}}(C)$ in characteristic zero. To see this explicitly, the differentials η_{G+j}, $1 \le j \le G$, have only a pole of order $2j$ at infinity and have zero residue there. An exact form with that leading pole would need a rational primitive with unique pole of order $2j - 1 < N$. But the affine coordinate ring is spanned by $x^a, x^a y$, of pole orders $2a, 2a + N$. This proves independence modulo holomorphic and exact forms by the largest pole in a linear relation. The dimension is $2G$.

For a differential η of the second kind write

$$\eta = \sum_{r=1}^{N-1} d_r \eta_r + dv, \qquad F_\eta = (\mathrm{Tr}\,\eta)(E_0).$$

We require integral reduction of this presentation, including the rational primitive v of its exact part. This ensures that dv reduces to an exact rational form. For fixed data over a number field

this excludes only finitely many primes, including ramified places when we use unramified local coefficients. Integral regularity near T is required for evaluation.

There is an intrinsic way to isolate the coefficient d_s for $s = s_h$. For the de Rham cup product $\langle\,,\,\rangle$, character orthogonality gives

$$d_s = \frac{\langle [\eta], [\eta_{N-s}] \rangle}{\langle [\eta_s], [\eta_{N-s}] \rangle}.$$

Indeed the complementary holomorphic character $N - s$ pairs only with s. In a parameter with $x = t^{-2}$ at infinity, $\eta_r = -2t^{N-2r-1}(1 + O(t^{2N}))\,dt$. The residue of a local primitive of η_s times η_{N-s} is $4/(N - 2s)$, a unit for $p > N$. A common sign convention for the pairing cancels from the ratio. After reduction modulo p, this pairing singles out the hyperplane on which the initial residue vanishes.

Theorem 3.1. *Under (9), let $q = p^{h+1}$, $L = q - 1$, $b_i = p^{i+1}$ and $B(\mathbf{k}) = \sum_{i<h} b_i k_i$. There is $w \in \mathbb{F}_p^\times$, depending only on the orbit and p, such that for all $k_i \geq 0$ the following quotient is integral at every regular mark and satisfies*

$$p^{-B(\mathbf{k})} \left(\prod_{i=0}^{h-1} E_i^{p-1+k_i L} \right) F_\eta(T) \equiv -\bar{d}_{s_h} \left(\prod_{i=0}^{h-1} H_i \right) w^{\sum_i k_i} \pmod{p}. \tag{10}$$

Consequently the predicted valuation $B(\mathbf{k})$ is exact precisely when d_{s_h} is a unit.

Proof of the starting case $\mathbf{k} = 0$. Let K be the function field of the special fibre over a perfect field k. By (4), a holomorphic η_r can contribute to the coefficient of η_{s_i} in its Cartier image only for $r \equiv p s_i \bmod N$. Applying (5) to the invariant basis gives

$$E_i^p = H_i E_{i+1} \quad (i < h - 1), \qquad E_{h-1}^p = 0.$$

At the last index the only source character is s_h. Cartier kills dv, so $((\mathcal{C}\,\mathrm{Tr}\,\eta)(E_{h-1}))^p = H_{h-1}\bar{d}_{s_h}$, including over a residue field larger than $\mathbb{F}_p$.

Put $D = E_0$, so $D^{p^h} = 0$. For a closed rational form ξ, iteration of (5) gives

$$D^{p^h-1}(\xi(D)) = -((\mathcal{C}\xi)(D^{p^{h-1}}))^p. \tag{11}$$

Indeed $p^h - 1 = (p - 1) + p(p^{h-1} - 1)$. Apply D^{p-1} first. The remaining positive power of D^p kills the pth power in (5). Repeat with $D^p, D^{p^2}, \ldots$. The last term $\xi(D^{p^h})$ vanishes. Since $D^{p^i} = (\prod_{r<i} H_r) E_i$ over $\mathbb{F}_p$, the unit factor disappears on raising the two operators to the $(p-1)$st power. Thus $\prod_i E_i^{p-1} = D^{p^h-1}$. Taking $\xi = \mathrm{Tr}\,\eta$ gives (10) at $\mathbf{k} = 0$. □

This computation also identifies the functions whose derivatives fill the entire characteristic-p chain. If $\bar{d}_{s_h} \neq 0$, then

$$F_\eta,\ DF_\eta,\ \ldots,\ D^{p^h-1}F_\eta$$

are a basis of K over the constant field $\ker D$. In a dependence, apply the power of D carrying the first nonzero term to the last one. All higher terms disappear and (11) makes the surviving term nonzero. Conversely D^j embeds $\ker D^{j+1}/\ker D^j$ into $\ker D$. There are at most p^h such one-dimensional increments. In particular vanishing of the terminal component shortens the chain.

For Theorem 1.1, the orbit is $(2^i)_{0\leq i\leq h}$. Its length is $h + 1$ since $2^{h+1} \equiv 1 \bmod N$ and $0 < 2^j - 1 < N$ for $0 < j < h + 1$. The terminal index is $G + 1$. For $\eta = \eta_{G+1}$, contraction with D_1 extracts the constant term of $X^G \bmod \prod_t (X - x_t)$. This is $(-1)^{G+1} \prod_t x_t = F$. For an arbitrary orbit, the corresponding contraction of η_{s_h} is the coefficient of X^{s_0-1} in the remainder of X^{s_h-1}. In particular the orbit $(2, 1, 4)$ at 11 gives $-e_2$ here. The opening product e_3 comes from the other contraction in (3).

4 From one nonzero derivative to infinitely many

At $p = 11$, why does the shift of 1330 in (1) raise the valuation by 11 along $P = D_2$ and by 121 along $Q = D_1$? On the formal subgroup the short step is $P^{11} \equiv 10Q \bmod 11$. The return step is $11^{-11}Q^{121} \equiv 7P \bmod 11$, with the 7 computed in (18). Starting from $P^{1331} = (P^{11})^{121}$ uses the return step once. Starting from $Q^{1331} = (Q^{121})^{11}$ uses it eleven times before P^{11} returns to Q. The estimates below justify these substitutions on integral functions and give

$$11^{-11}P^{1331} \equiv 4P, \qquad 11^{-121}Q^{1331} \equiv 4Q \pmod{11}.$$

One circuit thus returns from order 1331 to order one in either direction, giving the common shift $1331 - 1 = 1330$.

In general we work on the formal subgroup selected by (9). Translation restricts a function at T to this subgroup. Each E_i is tangent to it, so its iterates compute the original derivatives at T.

4.1 The formal group and its two types of coefficients

Let $R = W(\mathbb{F}_q)$. Let δ send (x, y) to $(\zeta_N x, y)$ over R. On J it sends each point of a representing divisor to its image, so $\delta^*\omega_j = \zeta_N^j \omega_j$. The orbit projector on the p-divisible group of J is

$$e = \frac{1}{N}\sum_{m=0}^{N-1}\left(\sum_{j=0}^{h}\zeta_N^{-ms_j}\right)\delta^m.$$

The inner sum is Frobenius invariant, so its coefficients belong to $\mathbb{Z}_p$ and give legitimate p-adic scalar endomorphisms. They are also unchanged on replacing m by pm. Since Galois sends δ to δ^p, the projector descends to $\mathbb{Z}_p$. Over R, its endomorphism ring contains $\mathcal{O} = e\mathbb{Z}_p[\delta] \simeq W(\mathbb{F}_q)$, the unramified factor associated with the primitive orbit.

The characters $1, \dots, G$ occur on holomorphic forms and their negatives occur in the Serre-dual quotient. Thus each nontrivial character of μ_N occurs once in characteristic-zero H^1. Comparison with Betti cohomology gives the same multiplicities for the orbit idempotent on the rational Tate module (duality does not change its rank). The image of e has height $h + 1$ and dimension h, with differentials indexed by $s_0, \dots, s_{h-1}$. Its special fibre is connected. Indeed its maximal étale quotient carries the $\mathcal{O}$-action. A nonzero such quotient would have rational Tate module of dimension at least $h + 1$ over $\mathbb{Q}_p$, leaving height zero for the positive-dimensional connected part. The image therefore defines a formal p-divisible group $\mathcal{G}$. Only this formal summand is needed.

Choose integral parameters t_i, $0 \le i < h$, with linear terms dual to E_i. By averaging over the Teichmüller units $\mu_{q-1} \subset \mathcal{O}^\times$ we may assume that they are eigenparameters. Choose the faithful character χ to be the embedding on t_0. Their weights, and those of the corresponding logarithms λ_i, are χ^{p^i}. Here $\lambda_i = z_{s_i}$, with $d\lambda_i(0) = dt_i(0)$. On $\mathcal{G}$ the other logarithms of J vanish. On the t_i-axis a term t_i^n of λ_j requires $np^i \equiv p^j \bmod (q-1)$. Thus the component with the same index starts with $t_i + O(t_i^q)$. If $i < h - 1$, the first possible off-axis term is $\beta_i t_i^p$ in λ_{i+1}. On the last axis the first is $\gamma t_{h-1}^{p^2}$ in λ_0. All other off-axis components start later on the respective axes.

For an integral formal function A, translate by the formal point $\mathbf{t}$. The coefficients $\Delta_{\mathbf{n}}$ of the resulting power series are integral translation operators. In characteristic zero Taylor's formula in the logarithms reads

$$\sum_{\mathbf{n}} \Delta_{\mathbf{n}}\mathbf{t}^{\mathbf{n}} = \exp\left(\sum_{i=0}^{h-1}\lambda_i(\mathbf{t})E_i\right). \tag{12}$$

The operators commute since $\mathcal{G}$ is commutative. This is the multivariable form of the translation identity in Katz [7, Cor. 1.8]. The use of its coefficients to produce a full-period operator recurrence

follows Alderliefste [1, §5.4]. We write U, V for integral operators formed from these coefficients and commuting with all of them. Comparing degree p on a short axis yields

$$E_i^p = \alpha_i E_{i+1} + pU_i, \qquad \alpha_i = -p!\,\beta_i, \qquad \bar{\alpha}_i = H_i \quad (i < h-1). \tag{13}$$

The scalar is integral by evaluating on a parameter dual to E_{i+1} at the origin, and its residue follows from the restricted-power identity. Thus $p\beta_i$ is a unit. To use the last axis we must likewise show that $p\gamma$ is a unit. Its coefficient is invisible to the short restricted powers.

Compare the first off-axis terms in $\lambda([p]\mathbf{t}) = p\lambda(\mathbf{t})$. In $[p]$ their coefficients are $(p - p^{p^2})\beta_i$ on the short axes and $(p - p^{p^2})\gamma$ on the last axis. Indeed through that first off-axis degree only the linear output and the pure term of the corresponding logarithm can contribute. This proves integrality of $p\gamma$.

For its nonvanishing reduce $[p]$ modulo p. It factors through relative Frobenius, so write its components as $A_0, \dots, A_{h-1}$ in $X_i = t_i^p$ and put $Y = X_{h-1}$. The linear block of $A_1, \dots, A_{h-1}$ in $X_0, \dots, X_{h-2}$ is diagonal up to indexing, with units from the short axes. For $j \geq 1$, a pure Y^n in A_j satisfies $np^h \equiv p^j \bmod (q-1)$. Its least possible degree is $p^{j+1} \geq p^2$. Solving $A_1 = \cdots = A_{h-1} = 0$ formally gives $X_i = O(Y^{p^2})$ for $i < h-1$. On the other hand the kernel of $[p]$ has length p^{h+1}, and the relative Frobenius substitution is finite free of rank p^h. Hence the quotient by all the A_j in the X-variables has length p. After the substitution into A_0 this forces order exactly p in Y. The substitution affects only degrees at least p^2, so the coefficient of Y^p in $A_0(0, \dots, 0, Y)$ is nonzero. This proves $p\gamma \in R^\times$. Degree p^2 in (12) on the last axis now gives

$$E_{h-1}^{p^2} = p^p v E_0 + p^{p+1} V, \qquad v = -\frac{(p^2)!\gamma}{p^p} \in R^\times. \tag{14}$$

Here $v_p((p^2)!) = p+1$. The residue $\bar{v}$ belongs to $\mathbb{F}_p$. In fact $\mathcal{G}, E_{h-1}, E_0$ descend to $\mathbb{Z}_p$, and the normalized operator $p^{-p}E_{h-1}^{p^2}$ is integral there by faithful flatness. Its residue determines $\bar{v}$ uniquely since E_0 is nonzero.

4.2 One full turn around the orbit

Say that an operator is divisible by p^a if it takes every integral formal function into p^a times the integral ring. Set $R_i = q/b_i = p^{h-i}$. The restricted-power chain gives $E_i^{R_i} \in p\,\mathrm{End}$. We claim that

$$E_i^q = p^{b_i} u_i E_i + p^{b_i+1} V_i, \qquad \bar{u}_i = w = \bar{v} \prod_{j=0}^{h-2} H_j \in \mathbb{F}_p^\times. \tag{15}$$

Here End denotes integral linear operators, and $u_i \in R^\times$.

Starting with E_i^q, use the short links (13) consecutively for $j = i, \dots, h-2$. At step j the exponent on E_j^p is $M = p^{h-j+i}$, with $M/R_{j+1} = b_i$. A binomial term containing m factors from pU_j has valuation at least

$$v_p\binom{M}{m} + m + \left\lfloor \frac{M-m}{R_{j+1}} \right\rfloor.$$

If $0 < m < M$, the binomial coefficient is divisible by p and $m - \lceil m/R_{j+1} \rceil \geq 0$. If $m = M$, then $M > b_i$. In both cases the term vanishes modulo p^{b_i+1}. The remaining power is $(E_{h-1}^{p^2})^{p^i}$. Using (14) leaves, after division by p^{b_i}, a unit times $E_0^{p^i}$ mod p. This last operator is $(\prod_{j<i} H_j)E_i$. Each short link with $j \geq i$ contributes $\bar{\alpha}_j$ raised to a power of p, and the last link contributes $\bar{v}^{p^i}$. All these residues are in $\mathbb{F}_p$, giving exactly the product in (15). Thus each passage around the full orbit contributes the same residue, irrespective of the starting direction.

Lemma 4.1. *Suppose $q = Rb$, $L = q - 1$, $R \geq 2$, and D^R is divisible by p. Suppose also that $D^q = p^b u D + p^{b+1} V$, where u is a scalar unit and V is integral and commutes with D. Then for every $n_0 \geq 2$ and every $k \geq 0$, as operators on integral functions,*

$$p^{-kb} D^{n_0+kL} \equiv u^k D^{n_0} \pmod{p}. \tag{16}$$

Proof. Let $a(n)$ denote the divisibility of D^n. First $a(n) \geq bn/L - 1$. For $n < q$, use $a(n) \geq \lfloor n/R \rfloor$ and check the right endpoint of each block of length R. For $n \geq q$, the recurrence gives $a(n) \geq \min\{b + a(n-q+1),\, b+1+a(n-q)\}$. Induction proves the bound because $L = q - 1$ and $b \leq L$. Now take $n = n_0 + kL$, $k > 0$. The error involves $D^{n-q} = D^{n_0-1+(k-1)L}$. The bound is strictly greater than $(k-1)b - 1$, hence its integral divisibility is at least $(k-1)b$. After division by p^{kb}, this leaves u times the previous normalized term modulo p, which proves (16). □

Completion of the proofs. Apply Lemma 4.1 to (15) with $n_0 = p - 1$ on each axis. On the orders $n = p - 1 + k_i L$ the integer lower bound $\lceil b_i n/L - 1 \rceil$ is exactly $k_i b_i$, since $0 < b_i(p-1)/L < 1$. The normalized operators are integral and commute. Their product times F_η reduces to its initial value from (11) multiplied by $w^{\sum k_i}$. This proves Theorems 3.1 and 1.1.

For Corollary 2.2, use the orbit $(a, b, 4)$, with $E_0 = P, E_1 = Q$, and take the base exponents $(pj, p-1-j)$ on f. Both are at least two for $1 \leq j \leq p-3$. Proposition 2.1 supplies the unit. For Z one first differentiates to f, or, at $j = p-2$, to g with base exponents $(pj-1, 2)$. For the latter pair (7) is applied with index $j - 1$. Thus (16) always acts on an integral function. □

5 One algebraic mark for both prime classes

Fix a primitive seventh root ρ, let $W_\lambda = (\lambda, 0)$, and put

$$T_* = [W_\rho + W_{\rho^2} + W_{\rho^4} - 3\infty].$$

Each $W_\lambda - \infty$ has order two by the divisor of $x - \lambda$, and their sum is a nonzero reduced divisor. The set $\{1, 2, 4\}$ is the subgroup of quadratic residues modulo seven, so the unordered triple and its conjugate are defined over $\mathbb{Q}(\sqrt{-7})$. For $p \equiv 2, 4 \bmod 7$ this quadratic field splits. The distinct branch abscissas stay distinct in the residue field of a splitting extension. Thus both conjugate marks lie in the divisor chart over $\mathbb{Z}_p$.

There is a direct way to compute here. For $\rho_i \in \{\rho, \rho^2, \rho^4\}$, use the local parameter $t_i = y_i$, so $x_i = \rho_i(1 + t_i^2)^{1/7}$. The centered Abel integrals and the primitive are

$$z_j = \frac{2}{7} \sum_i \rho_i^j \int_0^{t_i} (1 + t^2)^{j/7 - 1}\, dt \quad (1 \leq j \leq 4), \qquad Z = z_4. \tag{17}$$

The first three integrals have unit linear determinant by Vandermonde. Solving for t_i degree by degree expresses Z in z_1, z_2, z_3. The two-dimensional orbit factor in Section 4 has $z_3 = 0$ in these centered logarithms. Freije gives a construction of the Jacobian logarithm by summing integrals at a non-Weierstrass point [3, §II, Thm. 2]. Here the three distinct branch points give the explicit integrands in (17).

Let $s = \rho + \rho^2 + \rho^4$, so $s^2 + s + 2 = 0$, and put $R_* = P^p Q^{p-1} Z(T_*)$. If c_* is the coefficient of $z_a^p z_b^{p-1}$ in Z, then $pc_* = R_*/((p-1)!)^2$. Inverting (17) gives the following residues. The two rows at each prime use its two embeddings of the quadratic field.

p	$s \bmod p^2$	$R_* \bmod p^2$	$pc_* \bmod p^2$
11	15	82	71
11	105	27	16
23	32	445	215
23	496	215	514

For instance 82 and 27 both reduce to 5 mod 11. Their different second digits show exactly how much of this value Proposition 2.1 makes independent of the mark.

6 Verification

The proofs use the function-field Cartier identities and the integral operator recurrence. The six programs run by `make check` test both by evaluating derivatives in exact modular arithmetic. Two collaborating Codex sessions reviewed the mathematics and exposition. A separate AI audit of the November 28 draft reviewed the proofs and exposition and independently reproduced the numerical examples.

Two descriptions of a divisor. One computation differentiates the moving points on the curve, solving the Vandermonde system for $D_i x_t$ and applying the product rule. At two triples of nonbranch points it gives $60, 71 \bmod 121$ for $P^{11}Q^9 f$. At 23 it gives $238, 468 \bmod 529$ for $P^{23}Q^{21} f$. It also evaluates the left side of (1) at $(k, \ell) = (1, 0)$. After division by 11^{11}, this derivative is 9 mod 11.

The second implementation uses polynomial coordinates U, V, W with $UW + V^2 = X^7 - 1$, $U = \prod_t (X - x_t)$, $V(x_t) = y_t$. To make the multiplier 4 in (1) reproducible, one can compute on these coordinates alone. Write $U = X^3 + u_2 X^2 + u_1 X + u_0$, $b_1 = X^2 + u_2 X + u_1$, $b_2 = X + u_2$. If rem and quo denote remainder and quotient by U, the polynomial flows are

$$D_i U = -\operatorname{rem}(V b_i), \qquad D_i V = \tfrac{1}{2} \operatorname{rem}(W b_i),$$
$$D_i W = V \operatorname{quo}(W b_i) - W \operatorname{quo}(V b_i) \qquad (i = 1, 2).$$

Indeed $D_i x_t = y_t b_i(x_t)/U'(x_t)$. Differentiate $V(x_t) = y_t$ and $UW + V^2 = X^7 - 1$ to obtain the remaining equations. Iterating these polynomial identities by Leibniz's rule tests (15) on all ten variable coefficients of U, V, W. Both axes at two divisors give $w_{11} = 4$.

Computing w_{11} from the 121st derivative. Take $x_t = 4, 7, 8$ and lift the ordinates $2, 4, 1$ mod 11. The same polynomial flows give

$$P u_0(T) \equiv 2 \pmod{11}, \qquad Q^{121} u_0(T) \equiv 3 \cdot 11^{11} \pmod{11^{12}}. \tag{18}$$

Dividing the second residue, after normalization, by the first gives $\bar{v} = 3/2 = 7$ in $\mathbb{F}_{11}$ by (14). One circuit also uses the short step, so (15) gives $w_{11} = H\bar{v} = 10 \cdot 7 = 4$ in $\mathbb{F}_{11}$. The longer computation also yields $Q^{1341} Z / 11^{121} \equiv 2 \bmod 11$, providing a separate test of the larger valuation increment.

A test of the cohomological criterion. The genus-four curve $y^2 = x^9 - 1$ at $p = 13$ has orbit $(1, 4, 7)$, outside the family of Theorem 1.1. Both Cartier coefficients are 7. At two divisors, direct computation of $D_1^{12} D_4^{12}((\operatorname{Tr} \eta_r)(D_1))$ for $1 \le r \le 8$ gives $3 = -7^2 \bmod 13$ at $r = 7$ and zero at every other index. It also gives zero for $d(x^2)$. For $d(x^{13}/13)$ it gives 1 and 3 at the two divisors. Here $x^{12}dx$ reduces at 13, whereas its primitive has a factor 13 in the denominator. This accounts for the integral-primitive hypothesis.

Branch points and genus seven. A third implementation inverts (17) using divided-power arithmetic and checks the whole row of Proposition 2.1 in both embeddings at 11 and 23. Independently, ordinary Taylor flows recover the restricted-power coefficients in genera three and seven. A direct three-variable calculation in genus seven evaluates $D_1^{16} D_2^{16} D_4^{16} F$ at $p = 17$. Its value 6 agrees with the three Cartier coefficients $9, 11, 2$ through $-9 \cdot 11 \cdot 2 \equiv 6 \bmod 17$. The proof of (10) covers all translated orders in all dimensions.

References

[1] F. Alderliefste, *Divisibility of invariant derivatives on formal groups of every height, on a question of Katz*, preprint (2026), Hexagon 2611.00938v2.

[2] P. Cartier, *Une nouvelle opération sur les formes différentielles*, C. R. Acad. Sci. Paris **244** (1957), 426–428.

[3] M. N. Freije, *The formal group of the Jacobian of an algebraic curve*, Pacific J. Math. **157** (1993), 241–255. doi:10.2140/pjm.1993.157.241.

[4] T. Honda, *On the Jacobian variety of the algebraic curve* $y^2 = 1 - x^l$ *over a field of characteristic* $p > 0$, Osaka J. Math. **3** (1966), 189–194.

[5] T. Honda, *On the formal structure of the Jacobian variety of the Fermat curve over a p-adic integer ring*, Symposia Mathematica **XI** (1973), 271–284.

[6] N. M. Katz, *Formal groups and p-adic interpolation*, Astérisque **41–42** (1977), 55–65.

[7] N. M. Katz, *Divisibilities, congruences, and Cartier duality*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28** (1981), 667–678.

[8] Y. Ônishi, *Generalized Bernoulli–Hurwitz numbers and the universal Bernoulli numbers*, Russian Math. Surveys **66** (2011), 871–932. doi:10.1070/RM2011v066n05ABEH004763.

[9] N. Yui, *On the Jacobian varieties of hyperelliptic curves over fields of characteristic* $p > 2$, J. Algebra **52** (1978), 378–410. doi:10.1016/0021-8693(78)90247-8.

[10] N. Yui, *On the Jacobian variety of the Fermat curve*, J. Algebra **65** (1980), 1–35. doi:10.1016/0021-8693(80)90236-7.