Integrality of the p-adic height pairing at an anomalous prime is equivalent to a point of order p in $E(Q_p)$

Splitting of the reduction sequence, the vanishing of a Fermat quotient of the p-th division polynomial, and p-integrality of the height matrix on E(Q)/tors are one and the same condition; in rank one $v_p(Reg_p) \geq 0 \iff$ split, the non-split value being -1 exactly against the elementary baseline r $-$ 2

Kiichi Shiori Rin

Draft, 2026-09-24. Not submitted. See §8 for what is not claimed and §6 for the boundary between the machine-checked part and the paper part.

wvbks0 [at] gmail.com · `https://computoergosum.com/en/index.html`

Abstract

Let E/Q be an elliptic curve, p $\geq$ 5 a prime of good ordinary reduction, r the rank of E(Q), and Reg_p the cyclotomic p-adic regulator in the normalisation of [MST] used by [Har], $h_p(P)$ = 2 $log_p(\sigma_p(P)/d(P))$ with σ_p the Mazur–Tate sigma function. Call p *anomalous* when p | $\#E(F_p)$ ($a_p = 1$, that is $\#E(F_p)$ = p, for p $\geq$ 7) and E *split at p* when $E(Q_p)[p] \neq 0$.

At an anomalous prime Reg_p need not be p-integral: counting indices gives $v_p(Reg_p) \geq$ r $-$ 2 when p $\nmid \prod_\ell c_\ell$ and $\geq$ r otherwise (Theorem A). That baseline is elementary and it is not ours — the one negative entry of the table of [MST, §4.2], the precision loss 2 $v_p(n)$ of [Har], a hypothesis of [Ban]. What this note contributes is a local mechanism that governs the deficit, in both directions:

> **Integrality theorem for the p-adic regulator at split anomalous primes.** Suppose $\#E(F_p)$ = p, p $\nmid \prod_\ell c_\ell$, and that $\Lambda :=$ E(Q)/tors surjects onto $E(F_p)$. Then **every entry of the height matrix M_Λ on a basis of Λ lies in Z_p if and only if $E(Q_p)[p] \neq \mathbf{0}$**; in rank one, $v_p(Reg_p) \geq 0 \iff E(Q_p)[p] \neq 0$, the non-split value being $\mathbf{-1}$ **exactly**; and in the split case $v_p(Reg_p) \geq \max(\text{r} - 2, 0)$ in every rank.

Three things are separated throughout. The **baseline** r $-$ 2 is a known phenomenon. The equivalence for the **matrix** is the content of the note, and it holds in every rank. The bound on the **determinant** improves on the baseline in rank one only, since max(r$-$2, 0) = r$-$2 for r $\geq$ 2.

The proof is local and runs through one element $\lambda \in F_p$, the Fermat quotient $q_p(\varphi_p(x_0))/2$ of the p-th division polynomial at a lift of a nonzero class of $E(F_p)$. With P = (α/d^2, β/d^3) in lowest terms the height splits into a formal part of valuation b and 2 $log_p(\alpha/\beta)$ of valuation c $\geq$ 1 (Lemma 3); in a model with p | a_1 — always available, since p is odd — one has b $\geq$ 2 and $q_p(\alpha/\beta) = -\lambda$ (Theorem B), so the height is integral exactly when λ vanishes. Vélu's factorisation of multiplication by p kills λ in the split case (Theorem C, Corollary

D); conversely $\lambda = 0$ forces splitting, a known criterion (Proposition 6, [LR, Thm 4.1], [DW, Lemma 3.2]) proved here through the Euler identity for the weighted-homogeneous division polynomial and a residue computation at the cusp. CM curves split at every anomalous prime of good reduction (Theorem F). The arithmetic steps are theorems of Lean 4 with Mathlib (no `sorry`, no `native_decide`, axioms [propext, Classical.choice, Quot.sound]), the geometric inputs entering as hypotheses. Nothing here bears on the conjecture of Birch and Swinnerton-Dyer.

Keywords. p-adic height, p-adic regulator, anomalous prime, local torsion, division polynomial, Fermat quotient, Vélu isogeny, Tate curve, Lean 4.

MSC 2020. 11G50, 11G07, 11S31, 11Y40, 68V20.

1. Introduction

The cyclotomic p-adic height pairing of Mazur–Tate and Schneider attaches to E/Q and a prime p of good ordinary reduction a symmetric bilinear form on $\mathrm{E}(\mathrm{Q}) \otimes Q_p$, whose determinant Reg_p on a basis of $\Lambda := \mathrm{E}(\mathrm{Q})/\mathrm{tors}$ is the regulator in the p-adic analogue of the conjecture of Birch and Swinnerton-Dyer [MST] [BMS]. Unlike the archimedean regulator it is not known to be non-zero (Schneider's conjecture [SW, Conj. 4.1]), and nothing here bears on that.

This note concerns a coarser invariant, the valuation of Reg_p. At an *anomalous* prime — $\mathrm{p} \mid \#E(F_p)$, which for $\mathrm{p} \geq 7$ means $a_p = 1$, the notion of [Maz72] — it can be negative, because the points reducing to O at p form a subgroup of index divisible by p and dividing the determinant by the square of that index costs 2. This is the baseline $v_p(Reg_p) \geq \mathrm{r} - 2$ of Theorem A; it is known (§9), and it is attained.

What this note proves is that the deficit is present exactly when the reduction sequence $0 \to E_1(Q_p) \to E(Q_p) \to E(F_p) \to 0$ fails to split, that is exactly when $E(Q_p)$ contains no point of order p. Splitting makes the height of every point of Λ p-integral — a statement about the pairing, which the baseline gives in no rank — and its failure puts the valuation -1 into the matrix, in every rank, and into the determinant in rank one. The obstruction sits in the second p-adic digit of the height, where it is a Fermat quotient, and the route runs: decomposition of the height (Lemma 3), a criterion expressing that digit through one element $\lambda \in F_p$ (Theorem B), the vanishing of λ in the split case by Vélu's factorisation of multiplication by p (Theorem C, Corollary D), and its non-vanishing in the non-split case (Proposition 6), which is a known criterion for local torsion.

The materials are classical and we do not call the lemmas new; what we did not find in the sources we read is the equivalence itself, and the presentation of the local criterion through a Fermat quotient. §9 records where we looked, §6 draws the boundary between what a kernel has checked and what it has not, §7 lists what is open and §8 what is not claimed.

2. Setting and normalisation

The curve. E/Q is given by a global minimal Weierstrass equation with coefficients a_1, …, a_6, and $\mathrm{p} \geq 5$ is a prime of good ordinary reduction; $\Lambda := \mathrm{E}(\mathrm{Q})/\mathrm{tors}$ has rank r, and c_ℓ is the Tamagawa number at ℓ. Write $\mathrm{t} = -\mathrm{x}/\mathrm{y}$ for the parameter of the formal group $\hat{\mathrm{E}}$, $E_n(Q_p) := \{\mathrm{P} : v_p(t(P)) \geq \mathrm{n}\}$, and for $\mathrm{P} \in \mathrm{E}(\mathrm{Q})$

$$\mathrm{P} = (\alpha(\mathrm{P})/\mathrm{d}(\mathrm{P})^2,\ \beta(\mathrm{P})/\mathrm{d}(\mathrm{P})^3),\ \gcd(\alpha,\ \mathrm{d}) = \gcd(\beta,\ \mathrm{d}) = 1,\ \mathrm{d} \geq 1.$$

v_p is normalised by $v_p(p) = 1$, log_p is the Iwasawa logarithm with $log_p(p) = 0$, and for a p-adic unit u, $q_p(u) := (u^{p-1} - 1)/\mathrm{p} \bmod \mathrm{p}$ is the Fermat quotient. Then $q_p : Z_p^{\times} \to F_p$ is a surjective homomorphism and $v_p(log_p\ \mathrm{u}) = 1 + v_p(q_p(u))$, so "the second p-adic digit of log_p u" and "the Fermat quotient of u" are the same datum.

The height. The height is taken in the explicit form of [Har, §2.2], which quotes the definition of [MST]: if P satisfies

> (A1) P reduces to O at p, and (A2) P reduces to a nonsingular point at every bad prime,

then $h_p(P) = 2\ log_p(\sigma_p(P)/d(P))$; for a general point $h_p(Q) := h_p(nQ)/n^2$ with $\mathrm{n} = lcm(\#E(F_p),\ lcm_\ell\ c_\ell)$. This is 2p times the normalisation of [MST], so the two valuations of Reg_p differ by r. The pairing is $h_p(P,\ \mathrm{R}) = (h_p(P + R) - h_p(P) - h_p(R))/2$ and $Reg_p := det(h_p(P_i,\ P_j))$ on a basis of Λ.

Which σ matters. σ_p is the Mazur–Tate sigma function: the unique odd $\sigma(\mathrm{t}) = \mathrm{t} + \mathrm{c}_2\mathrm{t}^2 + \cdots$ with $\sigma_p \in tZ_p[[t]]$ solving $\mathrm{x}(\mathrm{t}) + \mathrm{c} = -(\mathrm{d}/\omega)((1/\sigma)(\mathrm{d}\sigma/\omega))$ with $\mathrm{c} = (\mathrm{b}_2 - \mathrm{E}_2(\mathrm{E},\ \omega))/12$ [Har, (2)], [MT91]; $\mathrm{c}_2 = \mathrm{a}_1/2$. Another constant in place of E_2 shifts h_p by a multiple of the square of the p-adic elliptic logarithm, and only this choice keeps the coefficients in Z_p. Every statement below is about σ_p.

Which model matters. $h_p(P)$ and $v_p(h_p(P))$ are invariants of E/Q, but the two halves b and c of the decomposition of Lemma 3 are not: the substitution $(\mathrm{x},\ \mathrm{y}) \mapsto (\mathrm{x},\ \mathrm{y} + \mathrm{sx})$ with $\mathrm{s} \in \mathrm{Z}$ carries a global minimal equation to a global minimal equation, fixes x, α, d, φ_p, ψ_p and λ, and moves only $\beta \mapsto \beta + \mathrm{s}\alpha\mathrm{d}$, so b and c trade with each other while min(b, c) stands. Since p is odd, s can be chosen with $\mathbf{p} \mid \mathbf{a}_1$, and that is the model in which Theorem B and Theorem S are proved; in it $\mathrm{b} \geq 2\mathrm{e}$ comes for free, and the whole question is c. Statements about b or c alone are statements about a model, and the invariant form of Theorem S is $v_p(h_p(pP')) = 1$.

Anomalous, split, ι. p is *anomalous* when $\mathrm{p} \mid \#E(F_p)$, which for $\mathrm{p} \geq 7$ means $\#E(F_p) = \mathrm{p}$ (§3.1); E is *split at p* when $E(Q_p)[p] \neq 0$; ι says that $\Lambda \to E(F_p)$ is onto.

Division polynomials. φ_n, ψ_n, ω_n are normalised by $\mathrm{x}(\mathrm{nQ}) = \varphi_n/{\psi_n}^2$, $\mathrm{y}(\mathrm{nQ}) = \omega_n/{\psi_n}^3$, with φ_n monic of degree n^2 in x. For odd n and a rational cyclic D of order n, the Vélu isogeny $\pi_D : \mathrm{E} \to \mathrm{E/D}$ has x-part $\bar{\varphi}/\bar{\psi}^2$ with $\bar{\psi}(x) = \prod_{\pm T \subset D \setminus O}(x - \mathrm{x}(\mathrm{T}))$ monic of degree $(\mathrm{n}-1)/2$ and $\bar{\varphi}$ monic of degree n. Modulo p, for E ordinary, $\varphi_p(x) = f(x^p)$ and $\psi_p(x) = g(x^p)$ in $F_p[A,\ \mathrm{B}][\mathrm{X}]$ with f monic of degree p in X, g of degree $(\mathrm{p}-1)/2$ with leading coefficient the Hasse invariant, and f/g^2 the x-part of the Verschiebung V; when p is anomalous, $\ker \mathrm{V} = E(F_p)$.

Grades. **[Lean]** kernel-checked, no `sorry`, no `native_decide`, axioms within [propext, Classical.choice, Quot.sound]; **[paper]** a complete proof here or cited; **[computation]** verified over a stated range; **[known]** in the literature. Where grades mix, the weakest governs.

3. Main theorems

Throughout, $\mathrm{p} \geq 5$ is a prime of good ordinary reduction for E.

3.1 The baseline, and the decomposition of the height

> **Theorem A (baseline) [paper.** *] Let $G := \{P \in E(Q) : (A1)$ and $(A2)$ hold$\}$ and $k := [\Lambda$: image of $G]$. Then $v_p(Reg_p) \geq r - 2\, v_p(k)$. If moreover $p \nmid \prod_\ell c_\ell$, then $v_p(k) \leq 1$, with equality exactly when the image of Λ in $E(F_p)$ meets $E(F_p)[p] \neq 0$, so that $> v_p(Reg_p) \geq r - 2$ in that case, $v_p(Reg_p) \geq r$ otherwise.*

The hypothesis is the one the proof uses and is weaker than $a_p = 1$: by Hasse, $\mathrm{p} \mid \#E(F_p)$ forces $\#E(F_p) \in \{\mathrm{p}, 2\mathrm{p}\}$ for $\mathrm{p} \geq 5$, and $2\mathrm{p}$ occurs only at $\mathrm{p} = 5$ with $a_p = -4$, so for $\mathrm{p} \geq 7$ it is exactly $a_p = 1$, $E(F_p) \cong \mathrm{Z/p}$ and the condition on Λ is ι, while at $\mathrm{p} = 5$ with $\#E(F_5) = 10$ it is strictly weaker than ι. **Everything after Lemma 4 assumes $\#E(F_p) = \mathbf{p}$**, and no statistic below mixes the two. The argument is index bookkeeping and nothing more (§4.2), and it is known (§9); we give it because the rest of the paper is measured against it. What it does *not* give is control on the entries of the height matrix, only on the determinant (§3.2).

For P satisfying (A1) and (A2), with $\mathrm{e} := v_p(t(P)) \geq 1$:

> **Lemma 1 [paper.** *] $\sigma_p(P)/d(P) \in Z_p^\times$. **Lemma 2 [paper].** $h_p(P) \in 2pZ_p$; more precisely $v_p(h_p(P)) = 1 + v_p(q_p(\sigma_p(P)/d(P)))$. **Lemma 3 (decomposition) [paper].** With $u(P) := \sigma_p(t)/t \in 1 + p^e Z_p$ and $n_\ell(P) := v_\ell(\alpha) - v_\ell(\beta) \in Z$, $> h_p(P) = 2\, log_p(u(P)) + 2\, \Sigma_{\ell \neq p}\, n_\ell(P)\, log_p(\ell) =: 2\Lambda_\sigma + 2A$, and, with $b := v_p(\Lambda_\sigma)$ and $c := v_p(A)$: $b \geq e$ (and $b \geq 2e$ when $p \mid a_1$), and $\mathbf{c \geq 1}$.*

By §2 the pair (b, c) depends on the model and $\min(\mathrm{b}, \mathrm{c})$ does not; in the model with $\mathrm{p} \mid \mathrm{a}_1$ one has $\mathrm{b} \geq 2\mathrm{e} \geq 2$ for free.

3.2 The main theorem

> **Integrality theorem for the p-adic regulator at split anomalous primes** (*Split-integrality theorem*) **[paper].** Suppose $\#E(F_p) = \mathrm{p}$, $\mathrm{p} \nmid \prod_\ell c_\ell$ and ι. Then, with M_Λ the height matrix on a basis of Λ, $>$ **(i)** every entry of M_Λ lies in Z_p $\iff E(Q_p)[p] \neq 0$; $>>$ **(ii)** if $\mathrm{r} = 1$, then $v_p(Reg_p) \geq 0 \iff E(Q_p)[p] \neq 0$, and in the non-split case $v_p(Reg_p) = -1$ exactly; $>>$ **(iii)** if $E(Q_p)[p] \neq 0$, then $v_p(Reg_p) \geq \max(\mathrm{r} - 2, 0)$ in every rank. Without ι the hypothesis of Theorem A is not met and that theorem already gives $v_p(Reg_p) \geq \mathrm{r}$.

Three things are being said, and only some of them are new against Theorem A.

The pairing. That the **entries** are integral, and that they cease to be exactly when $E(Q_p)[p] = 0$, does not follow from any determinant bound. The direction $\Longleftarrow$ of (i) is the mechanism of §4.8; the direction $\Longrightarrow$ is Theorem S, which produces an entry of valuation -1 whenever the reduction sequence does not split. This is what the proof gives, and it holds in every rank.

The determinant. Since $\max(\mathrm{r}-2, 0) = \mathrm{r}-2$ for $\mathrm{r} \geq 2$, the bound on $v_p(Reg_p)$ is new only in **rank one**, where the baseline -1 becomes 0 and, by (ii), is attained exactly in the non-split case: Theorem A says the rank-one regulator may fail to be integral, and (ii) says which curves those are.

The baseline. $\mathrm{r} - 2$ in higher rank is the elementary count of §4.2 and is not ours.

3.3 The criterion: one element of F_p

Let $\#E(F_p) = \mathrm{p}$, $\mathrm{P}' \in \mathrm{E(Q)}$ with reduction of exact order p and satisfying (A2), $\mathrm{P} := \mathrm{pP}'$, $\mathrm{e} := v_p(d(P))$.

Lemma 4 (splitting and depth) [paper. *] $E(Q_p)[p] \neq 0 \iff e \geq 2$. **Lemma 4′ (the same, read locally) [paper].** Let $\bar{\psi}(x) := \prod_{\pm T \subset E(F_p)\setminus O} (x - x(T)) \in F_p[x]$, monic of degree (p−1)/2. Then $\psi_p \equiv u \cdot \bar{\psi}^p \pmod p$ for some $u \in F_p^\times$; hence $p \mid \psi_p{}'$ and $> p^2 \mid \psi_p(x_0 + pk) - \psi_p(x_0)$ for all x_0, $k \in Z_p$. Consequently, for an integral lift x_0 of a class $\bar{x} \in E(F_p) \setminus O$: $v_p(\psi_p(x_0)) \geq 1$, $min(v_p(\psi_p(x_0))$, **2) depends on $\bar{x}$ only** and not on the lift, and $E(Q_p)[p] \neq 0 \iff v_p(\psi_p(x_0)) \geq 2$.*

The *exact* value of $v_p(\psi_p(x_0))$ is **not** a function of $\bar{x}$ alone once it is ≥ 2 (§5.2), which is why only the cut at 2 is used; Lemma 4′ is what makes the measurements of §5.2 legitimate.

Theorem B (criterion) [paper; arithmetic step in Lean. *] Put $\lambda := q_p(\varphi_p(P'))/2 \in F_p$. If $e \geq 2$, or if the model is chosen with $p \mid a_1$, then $q_p(\alpha(P)/\beta(P)) = -\lambda$, hence $\mathbf{c \geq 2 \iff \lambda = 0}$. **Theorem B′ (the general model) [paper].** Without either hypothesis $q_p(\alpha(P)/\beta(P)) = -\lambda - w_1/2$, where $w_1 := a_1 \cdot \omega_p(P') \cdot (\psi_p(P')/p)/\varphi_p(P')^2 \bmod p$. **Lemma 5 ($\lambda$ is local and finite) [paper].** $\varphi_p \bmod p$ is a polynomial in x^p, so $\varphi_p(x) \bmod p^2$ depends only on $x \bmod p$. Hence $\lambda = \lambda(E \bmod p^2, \bar{x})$ is a function of the reduction of E modulo p^2 and of the class $\bar{x} \in E(F_p) \setminus O$ alone: not of the global point, not of the height, not of the lift.*

By Theorem B and Lemma 3 the second p-adic digit of the height is λ, in a model chosen with $\mathrm{p} \mid \mathrm{a}_1$. The rest of §3 determines λ.

3.4 The two directions of the criterion

Theorem C (Vélu factorisation) [paper. *] Let K be a field of characteristic 0, E/K given by a Weierstrass equation, $n \geq 3$ odd, $D \subset E(\bar{K})$ a Galois-stable cyclic subgroup of order n, and $T \in D \setminus \{O\}$ with $x(T) \in K$. Then, with $\bar{\varphi}$ monic of degree n as in §2, $> \varphi_n(x(T)) = \bar{\varphi}(x(T))^n$. **Corollary D [paper].** If p is anomalous and $E(Q_p)[p] \neq 0$, then $\lambda(\bar{x}) = 0$ for every $\bar{x} \in E(F_p) \setminus O$. **Corollary E [paper; arithmetic step in Lean].** In the situation of §3.3, if E is split at p then $c \geq 2$.*

The converse holds, and the equivalence it produces is a known criterion for local torsion.

Proposition 6 (a known criterion, read as a Fermat quotient) [paper; known. *] Let $p \geq 5$ be a prime of good ordinary reduction with $\#E(F_p) = p$. Then for every $\bar{x} \in E(F_p) \setminus O$, $> \lambda(\bar{x}) = 0 \iff E(Q_p)[p] \neq 0$. Neither side depends on the lift x_0 or on the model, and both are determined by E mod p^2.*

The equivalence is known. It is the case n = 1 of Gross's tameness criterion — for good ordinary reduction with E[p] irreducible, the decomposition group at p is diagonalisable modulo p^{n+1} exactly when $j_E \equiv j_0 \pmod{p^{n+1}}$, j_0 the j-invariant of the canonical lift, quoted as [LR, Thm 4.1] — and it is the content of [DW, Lemma 3.2 and Cor. 3.5], where the primes with $E(Q_p)[p] \neq 0$ are the *local torsion primes* and the criterion reads: of the lifts of $\bar{E}$ to $\mathbb{Z}/p^2$, exactly those congruent to the canonical lift have a rational point of order p. What we did not find in the sources we read is the presentation of that condition as the vanishing of a Fermat quotient of φ_p at a single point (§9); the proof in §4.6 is independent of the sources above and gives the statement for all $p \geq 5$ without a bound.

3.5 The non-split case: the exact value

Theorem S [paper; arithmetic steps in Lean. *] Suppose $\#E(F_p) = p$, $p \nmid \prod_\ell c_\ell$, and let $P' \in E(Q)$ have reduction of exact order p and reduce to a nonsingular point at every bad prime; put $P := pP'$. If $E(Q_p)[p] = 0$ then $> v_p(h_p(P)) = 1$ exactly, hence $v_p(h_p(P')) = -1$.*

So in the non-split case the height of a point of $\Lambda \backslash \Lambda_0$ is not p-integral, which is the direction $\Longrightarrow$ of (i) and the exact value in (ii). The invariance is worth stating: the quantity that Theorem S pins down is $v_p(h_p(pP'))$, not b or c separately, and the model with $p \mid a_1$ is where the proof runs (§2, §4.7).

3.6 Two further properties of λ

Theorem H (scaling) [paper; arithmetic step in Lean. *] Let p be anomalous, $Q \in E(Z_p)$ with $\bar{Q} \neq O$, and m prime to p. Then $q_p(\varphi_p(x(mQ))) = m^2 \cdot q_p(\varphi_p(x(Q)))$, that is $\lambda(m\,\bar{x}) = m^2\,\lambda(\bar{x})$.* ***Corollary H' [paper, in Lean].*** *λ vanishes at one nonzero class of $E(F_p)$ if and only if it vanishes at all of them; λ is a quadratic, not a linear, function on $E(F_p) \cong Z/p$.* ***Theorem L (the canonical subgroup contributes a p-th power) [paper].*** *Let $C := \hat{E}[p]$, which is Q_p-rational for good ordinary reduction, $\pi_C : E \to E'' := E/C$ the Vélu isogeny with x-part $\varphi_C/{\psi_C}^2$, and $\hat{\pi}_C$ the dual with x-part $\varphi_{\hat{\pi}}/{\psi_{\hat{\pi}}}^2$, the leading coefficient of $\varphi_{\hat{\pi}}$ being A. For $Q \in E(Z_p)$ with $\bar{Q} \neq O$ and $\xi := \varphi_C(\bar{x})/\psi_C(\bar{x})^2$, $> A \cdot \varphi_p(\bar{x}) = (\psi_C(\bar{x})^2)^p \cdot \varphi_{\hat{\pi}}(\xi)$, so in $Q_p^\times/(Q_p^\times)^p$ the class of $\varphi_p(\bar{x})$ is that of $\varphi_{\hat{\pi}}(\xi)/A$, and $A = c^2$ with $\hat{\pi}_C^* \omega_E = c \cdot \omega_{E''}$.*

3.7 The CM case

Theorem F [paper, using Deuring's lifting theorem. *] Suppose E/Q has complex multiplication by an order O of conductor f in an imaginary quadratic field k, $p \geq 5$ is a prime of good reduction which is ordinary (equivalently, split in k), $p \nmid f$, and $a_p = 1$. Then $E(Q_p)[p] \neq 0$. (For E/Q the thirteen possible orders have $f \in \{1, 2, 3\}$, so $p \nmid f$ is automatic for $p \geq 5$.)* ***Corollary F' [paper].*** *If in addition $p \nmid \prod_\ell c_\ell$, then $v_p(Reg_p) \geq \max(r - 2, 0)$; in rank one, $v_p(Reg_p) \geq 0$. So a CM curve never shows the deficit at a prime of good ordinary reduction.*

3.8 A rank-theoretic refinement of the baseline

> **Theorem J [paper; determinant step in Lean.** *] Assume $\#E(F_p) = p$, ι, $p \nmid \prod_\ell c_\ell$. Let $\Lambda_0 := ker(\Lambda \to E(F_p))$, M_{Λ_0} the height matrix on a basis of Λ_0 (entries in pZ_p by Lemma 2), and $\rho_0 := rank_{F_p}((M_{\Lambda_0}/p) \bmod p)$. Then $v_p(Reg_p) = v_p(det\ M_{\Lambda_0}) - 2 \geq 2r - 2 - \rho_0$.*

With $\rho_0 \leq$ r this recovers Theorem A; the stronger bound max(2r−4, 0) that its shape suggests is **false** (§5.3).

4. Proofs

4.1 Lemmas 1–3

Lemma 1. $\sigma_p(t)/t \in 1 + tZ_p[[t]]$ and $v_p(t) =$ e ≥ 1, so $v_p(\sigma_p(t)) =$ e; from $v_p(x(P)) = -2$e and gcd(α, d) = 1 we get $v_p(d) =$ e and $v_p(\alpha) = 0$, whence $v_p(\sigma_p(P)/d(P)) = 0$. ■

Lemma 2. For w $\in Z_p^\times$ one has $w^{p-1} \in 1 + pZ_p$ and log(1 + px) $\in pZ_p$, so $v_p(log_p$ w$) \geq 1$, refined as in §2; apply this to w $= \sigma_p(P)/d(P)$. ■

Lemma 3. From t $= -$x/y and x $= \alpha/$d^2, y $= \beta/$d^3 we get t/d $= -\alpha/\beta$, hence $\sigma_p(P)/d(P)$ = u(P)·($-\alpha$(P)/β(P)) with u $= \sigma_p(t)/t \in 1 + p^eZ_p$. Taking log_p, using $log_p(-1) = 0$ and factoring α/β into primes $\ell \neq$ p (both are prime to p by Lemma 1), gives the decomposition with $n_\ell \in$ Z; each ℓ is a p-adic unit, so $v_p(log_p\ \ell) \geq 1$ by Lemma 2, and c ≥ 1 as the n_ℓ are rational integers. Finally u $\in 1 + p^eZ_p$ gives b $\geq$ e, and b ≥ 2e when p | a$_1$, the coefficient c$_2$ = a$_1$/2 of σ_p then being divisible by p. ■

4.2 Theorem A

(1) If P, R, P+R $\in$ G, Lemma 2 puts all three heights in $2pZ_p$ and p is odd, so $h_p(P, R) \in pZ_p$; the matrix M_G on a basis of the image of G has entries in pZ_p, and every term of the Leibniz expansion of det M_G has valuation $\geq$ r. (2) A change of basis between G and Λ has determinant $\pm$k, so det $M_G =$ k^2 det M_Λ and $v_p(Reg_p) \geq$ r $- 2v_p(k)$. (3) Λ/(image of G) embeds into $E(F_p) \times \prod_\ell \Phi_\ell(F_\ell)$, so for p $\nmid \prod_\ell c_\ell$ the p-part comes from $E(F_p)$, which by Hasse has order $<$ p^2, its p-part cyclic of order at most p. Hence $v_p(k) \leq 1$, with equality exactly when p | $\#E(F_p)$ and the reduction of Λ meets $E(F_p)[p]$. ■

4.3 Lemmas 4 and 4′

($\Longrightarrow$) Let $\tau \in E(Q_p)$ have order p. For p ≥ 5 the formal group $\hat{\mathrm{E}}(pZ_p)$ is torsion-free, so $\bar{\tau} \neq$ O, and $\#E(F_p) =$ p gives $E(F_p) = \langle\bar{\tau}\rangle$; hence R := P′ − j$\tau \in E_1(Q_p)$ for some j and pP′ = pR. For a formal group over Z_p, [p](t) = pt + (higher terms with Z_p coefficients), so $v_p([p](t)) \geq \min(1 + v_p(t), 2v_p(t)) \geq 2$ whenever $v_p(t) \geq 1$. Thus e $= v_p(t(pP')) \geq 2$.

($\Longleftarrow$, contrapositive) If $E(Q_p)[p] = 0$ then $E(Q_p)$ is torsion-free, prime-to-p torsion injecting into $E(F_p)$ of order p, and being a compact p-adic Lie group of dimension 1 it is $\cong Z_p$ with $E_1(Q_p) = pE(Q_p)$ of index p. Torsion-freeness lets one *extend* the formal logarithm by ℓ(P) := $log_E(pP)/p$, an injective homomorphism with $\ell(E(Q_p)) = Z_p$ and $\ell(E_1(Q_p)) = pZ_p$, since $log_E : E_1(Q_p) \cong pZ_p$ for p ≥ 5. So ℓ(P′) $\in Z_p^\times$ when $P' \neq$ O, $v_p(log_E(pP')) = 1$, and as $v_p(log_E(t)) = v_p(t)$ on E_1, e = 1. ■

Lemma 4′. E being ordinary at p, E[p] over $\bar{F}_p$ is an extension of the étale Z/p by μ_p, with p distinct geometric points each of multiplicity p, and Frobenius acts on $E[p]^{ét}$ through the unit root of $\mathrm{X}^2 - a_p X + \mathrm{p} \equiv \mathrm{X}^2 - \mathrm{X} \pmod{\mathrm{p}}$, hence trivially; so $E[p]^{ét} \subset E(F_p)$, with equality as $\#E(F_p) = \mathrm{p}$. The divisor of ψ_p mod p on the x-line is therefore $p \cdot \Sigma_{\pm T}(x(T))$ over the (p−1)/2 classes of $E(F_p) \setminus O$, which matches $\deg \psi_p - (\mathrm{p}-1)/2$ since ψ_p has leading coefficient p; hence $\psi_p \equiv u \cdot \bar{\psi}^p \pmod{\mathrm{p}}$, $\mathrm{p} \mid {\psi_p}'$, and $\mathrm{p}^2 \mid \psi_p(x_0 + pk) - \psi_p(x_0)$ by the step of Lemma 5, so $min(v_p(\psi_p(x_0)), 2)$ is a function of $\bar{x}$. For the last claim lift $\bar{x}$ to $\mathrm{Q} \in E(Z_p)$: as φ_p and ${\psi_p}^2$ are coprime with resultant a power of $\Delta \in Z_p^\times$ [known] and $v_p(x(pQ)) < 0$, we get $v_p(\psi_p(x(Q))) = v_p(t(pQ))$, and Lemma 4 gives $E(Q_p)[p] \neq 0 \iff v_p(\psi_p(x_0)) \geq 2$. ■

4.4 Theorem B, Theorem B′, Lemma 5

Step 1 (denominators do not matter). Write $\mathrm{x}(\mathrm{P}') = \mathrm{a}/\mathrm{d}'^2$, $\mathrm{y}(\mathrm{P}') = \mathrm{b}/\mathrm{d}'^3$ with $\mathrm{p} \nmid \mathrm{d}'$, possible as $\bar{P}' \neq \mathrm{O}$. Homogenising, $\Phi := {d'}^{2p^2}\varphi_p(P')$, $\Psi := {d'}^{p^2-1}\psi_p(P')$, $\tilde{\Omega} := {d'}^{3p^2}\omega_p(P')$ are integers, and

$$\mathrm{x}(\mathrm{P}) = \Phi/(\mathrm{d}'\Psi)^2,\ \mathrm{y}(\mathrm{P}) = \tilde{\Omega}/(d'\Psi)^3, \text{ so } \mathrm{d}(\mathrm{P}) = \mathrm{d}'|\Psi|,\ \alpha = \pm\Phi,\ \beta = \pm\tilde{\Omega},\ \alpha/\beta = (\varphi_p(P')/\omega_p(P')) \cdot {d'}^{-p^2}.$$

That $\mathrm{d}(\mathrm{P}) = \mathrm{d}'|\Psi|$ with no cancellation is where (A2) is used: it is what the factor $\prod_\ell c_\ell$ in the definition of P′ secures, and it fails without it (§5.5). As q_p is a homomorphism and $q_p({d'}^{p^2}) = 0$,

$$q_p(\alpha/\beta) = q_p(\varphi_p(P')) - q_p(\omega_p(P')). \quad (*)$$

Step 2 (the Weierstrass equation). Multiply it at pP′ by $\psi_p(P')^6$ and write $\varphi = \varphi_p(P')$, $\omega = \omega_p(P')$, $\psi = \psi_p(P')$:

$$\omega^2 + \mathrm{a}_1\varphi\omega\psi + \mathrm{a}_3\omega\psi^3 = \varphi^3 + \mathrm{a}_2\varphi^2\psi^2 + \mathrm{a}_4\varphi\psi^4 + \mathrm{a}_6\psi^6.$$

Since $v_p(\psi) = v_p(d(P)) = \mathrm{e}$ (as $\mathrm{p} \nmid \mathrm{d}'$), every term of $\omega^2 - \varphi^3$ other than $\mathrm{a}_1\varphi\omega\psi$ has valuation $\geq 2\mathrm{e}$, and that one has valuation $v_p(a_1) + \mathrm{e}$. Hence $\omega^2 \equiv \varphi^3 \pmod{\mathrm{p}^2}$ under either hypothesis of Theorem B: $\mathrm{e} \geq 2$, or $\mathrm{p} \mid \mathrm{a}_1$ with $\mathrm{e} \geq 1$.

Step 3. Write $\varphi^{p-1} = 1 + \mathrm{pA}'$, $\omega^{p-1} = 1 + \mathrm{pB}'$. Raising $\omega^2 \equiv \varphi^3 \pmod{\mathrm{p}^2}$ to the power p−1 gives $2\mathrm{B}' \equiv 3\mathrm{A}' \pmod{\mathrm{p}}$, so with $\lambda := \mathrm{A}'/2 \bmod \mathrm{p} = q_p(\varphi)/2$ we get $q_p(\varphi) = 2\lambda$, $q_p(\omega) = 3\lambda$, and $(*)$ gives $q_p(\alpha/\beta) = -\lambda$, while $\mathrm{c} \geq 2 \iff q_p(\alpha/\beta) = 0$ (§2). In the form $2(\mathrm{A}' - \mathrm{B}') = -\mathrm{A}'$ the implication $\lambda \neq 0 \implies q_p(\alpha/\beta) \neq 0$ needs no division. Under neither hypothesis the term $\mathrm{a}_1\varphi\omega\psi$ survives modulo p^2; dividing by φ^3 and using $q_p(1 + pw) = -\mathrm{w}$ gives the correction w_1 of Theorem B′. ■

Lemma 5. In characteristic p, $[\mathrm{p}] = \mathrm{V} \circ \mathrm{F}$ and E is defined over F_p, so $\mathrm{x} \circ [\mathrm{p}]$ is a rational function of x^p; hence φ_p mod p is a polynomial in x^p and ${\varphi_p}' \equiv 0 \pmod{\mathrm{p}}$. For a polynomial f with $\mathrm{p} \mid \mathrm{f}'(\mathrm{x})$ one has $\mathrm{p}^2 \mid \mathrm{f}(\mathrm{x} + \mathrm{pk}) - \mathrm{f}(\mathrm{x})$ (the Lean statement `eval_sub_eval_dvd_sq`), so $\varphi_p(x) \bmod \mathrm{p}^2$ depends only on x mod p. ■

4.5 Theorem C, Corollary D, Corollary E

Theorem C. D being Galois-stable of order n, π_D and $\hat{\pi}_D$ are defined over K and $[\mathrm{n}] = \hat{\pi}_D \circ \pi_D$. Fix a Weierstrass model of E/D and write $\mathrm{x} \circ \hat{\pi}_D = \varphi_{\hat{\pi}}/{\psi_{\hat{\pi}}}^2$ with $\varphi_{\hat{\pi}}(X) = \Sigma_{i \leq n}\, c_i\, X^i$, $c_n = \mathrm{A} \neq 0$ and $\deg {\psi_{\hat{\pi}}}^2 = \mathrm{n} - 1$. Clearing denominators in $\mathrm{x} \circ [\mathrm{n}] = (\varphi_{\hat{\pi}}/{\psi_{\hat{\pi}}}^2) \circ (\bar{\varphi}/\bar{\psi}^2)$,

$\mathrm{N(x)} := \Sigma_{i\le n}\ c_i\ \bar\varphi(x)^i\ \bar\psi(x)^{2(n-i)}$, $\mathrm{Den(x)} := \bar\psi^{2n}\cdot\psi_{\hat\pi}(\bar\varphi/\bar\psi^2)^2$, ${\varphi_n}/{\psi_n}^2 = \mathrm{N/Den}$.

Now $deg(\bar\varphi^i\ \bar\psi^{2(n-i)}) = \mathrm{n}^2 - \mathrm{n} + \mathrm{i}$, so i = n alone attains the top degree: deg N = n^2 with leading coefficient A ($\bar\varphi$ being monic) and deg Den = $\mathrm{n}^2 - 1$. Since x ∘ [n] : $\mathrm{P}^1 \to \mathrm{P}^1$ has degree n^2, and the degree of a reduced representation is the larger of the two, cancelling a common factor of degree d would give $\mathrm{n}^2 - \mathrm{d} = \mathrm{n}^2$; so d = 0, N/Den is reduced, and as φ_n and ${\psi_n}^2$ are coprime with φ_n monic, $\mathrm{N} = A\cdot\varphi_n$. At x = x(T) one has $\bar\psi(x(T)) = 0$, so every term with i < n vanishes and $\mathrm{N(x(T))} = A\cdot\bar\varphi(x(T))^n$. ■

Corollary D. Let $\tau \in E(Q_p)$ have order p; as in Lemma 4, $\bar\tau \neq \mathrm{O}$. D := $\langle\tau\rangle$ is $Q_p-rational$ with D\{O} ⊂ $E(Q_p)$, so x(T) ∈ Z_p and Theorem C gives $\varphi_p(x(T)) = \bar\varphi(x(T))^p$. Both sides are p-adic units, $\varphi_p = x(pQ){\psi_p}^2$ with $v_p(x(pQ)) = -2\mathrm{e}$ and $v_p(\psi_p) = \mathrm{e}$, so $q_p(\varphi_p(x(T)))$ $= p\cdot q_p(\bar\varphi(x(T))) = 0$ in F_p. The reduction D\{O} → $E(F_p)\setminus O$ is injective (D ∩ Ê = 0) between sets of cardinality p − 1, hence bijective, so x(T) mod p runs over all nonzero classes; by Lemma 5, λ ≡ 0. ■

Corollary E. Lemma 4 gives e ≥ 2, Corollary D gives λ = 0, Theorem B gives $q_p(\alpha/\beta)$ = 0, that is c ≥ 2. ■

4.6 Proposition 6, the direction λ = 0 ⟹ split

The statement is [known] (§3.4); the argument below is independent of the sources cited there and carries no bound on p. It is given in outline. The arithmetic steps are the Lean theorems of `PadicHeightValuation{5,6,7}` (§6); the analytic steps use the Tate parametrisation as recorded in [ATAEC] and [Dok].

(1) An Euler identity. φ_p is weighted homogeneous of weight $2\mathrm{p}^2$ for weights (4, 6, 2) on (A, B, x); giving $\mathrm{X} = x^p$ the weight 2p and reducing $4A\partial_A\varphi_p + 6B\partial_B\varphi_p + 2x\partial_x\varphi_p = 2p^2\varphi_p$ modulo p, both the right-hand side and $\partial_x\ f(x^p)$ vanish, leaving $4A\cdot\partial_A\ \mathrm{f} + 6B\cdot\partial_B\ \mathrm{f} = 0$ in $F_p[A, \mathrm{B}][\mathrm{X}]$. Hence A | ∂_B f; put $\tilde u := (\partial_B\ \mathrm{f})/\mathrm{A}$.

(2) One slope. For E_s : $\mathrm{y}^2 = \mathrm{x}^3 + (\mathrm{a}_4 + \mathrm{sp})\mathrm{x} + \mathrm{a}_6$ a Taylor expansion of φ_p in its coefficients gives $\lambda_s = \lambda_0 - \mathrm{s}\cdot\mathrm{B}_4/2$, and likewise a slope B in the a_6 direction. λ is invariant under (x, y) ↦ (u^2x, u^3y), φ_p transforming by the p-th power u^{2p^2}; with u = 1 + pt that invariance reads $4\mathrm{a}_4\mathrm{B}_4 + 6\mathrm{a}_6\mathrm{B} \equiv 0$, which is (1) again, so both slopes are multiples of one scalar $\rho(\bar x) = -\tilde u(\bar x)/(4f(\bar x))$, the denominator being non-zero by Vélu's formulas in the shape $\mathrm{f}(\mathrm{X}_0) = 4{Y_0}^2 g'(X_0)^2/{c_V}^2$. By Serre–Tate theory the family E_s exhausts the deformations of Ē over $\mathrm{Z/p}^2$ and exactly one member splits, where λ = 0 by Corollary D. An affine function with non-zero slope vanishes once, so ρ ≠ 0 gives the assertion.

(3) A dichotomy. $Res_X(\tilde u, \mathrm{g})$ has weight (p−1)(p−2)(p+3) = 12 m_p. Take the transversal family E_t : $\mathrm{y}^2 = \mathrm{x}^3 - 3\mathrm{x} + (2 + \mathrm{t})$ over $\bar F_p((t))$ at the cusp, of split multiplicative reduction with v(q) = v(Δ) = 1 [ATAEC, Thm V.5.3], [Dok, Thm A.1]; the Tate parametrisation [ATAEC, Thm V.3.1] gives ker V = ⟨q⟩ mod q^p, so the roots of g have $v(\beta_j - 1) = \mathrm{j}$ (1 ≤ j ≤ n := (p−1)/2), those of f have valuations {0, 1, 1, …, n, n}, and the Newton polygon of f gives $v(f(\beta_j)) = \mathrm{j(p-j)}$. Here $\tilde u = -(1/3)(\mathrm{d/dt})\mathrm{f}$, and differentiation lowers a valuation by at most 1, so $ord_\Delta\ Res_X(\tilde u, \mathrm{g}) \ge \Sigma_j\ (\mathrm{j(p-j)} - 1) = m_p$; weighted homogeneity then forces $Res_X(\tilde u, \mathrm{g}) = c_p\cdot\Delta^{m_p}$ with $c_p \in F_p$ constant. For each p, either ρ ≠ 0 for every ordinary curve over $\bar F_p$ and every point of ker V\{O}, or ρ = 0 for all of them.

(4) Which side. $E^{(p)}$ is the member of the same family at parameter t^p, hence defined over K^p, so d/dt reaches only the argument of the Tate parameter and $v(d\beta_j/dt) = \mathrm{j} - 1$ exactly. Of the p−2j+1 roots of f at distance j from β_j, the two flanking ones contribute 1/(1−u) + $1/(1 - u^{-1}) = 1$ between them, so $f'(\beta_j)/f(\beta_j)$ has valuation exactly −j with leading

coefficient p − 2j ≡ −2j. The chain rule gives $12\rho_j = (\mathrm{d}/\mathrm{dt})\log f(\beta_j) - f'(\beta_j)(d\beta_j/dt)/f(\beta_j)$ $= (-\mathrm{j}^2 + 2\mathrm{j}^2)/\mathrm{t} + \mathrm{O}(1)$: the residues $-\mathrm{j}^2$ and $-2\mathrm{j}^2$ differ by $\mathrm{j}^2 \neq 0$, so $v(\rho_j) = -1$, ord_Δ $Res_X(\tilde{u}, \mathrm{g}) = m_p$ exactly, and $c_p \neq 0$. ■

The naive estimate fails — the second term has valuation −1, not ≥ 0 — and what closes the argument is that the two residues differ.

4.7 Theorem S

Choose the model with p | a_1 (§2); e = 1 since E is not split (Lemma 4). Then b ≥ 2e = 2 by Lemma 3, and by Theorem B, applicable in this model for e ≥ 1, $q_p(\alpha/\beta) = -\lambda$ with $\lambda \neq 0$ by Proposition 6; so c = 1. From $h_p(P)/2 = \Lambda_\sigma + \Lambda$ with b ≥ 2 > 1 = c we get $v_p(h_p(P)/2) = 1$, and p is odd, so $v_p(h_p(P)) = 1$. Finally h_p is a quadratic form, so $h_p(P)$ $= p^2 h_p(P')$ and $v_p(h_p(P')) = -1$. ■

4.8 The main theorem

Put $\mathrm{n} := \prod_\ell c_\ell$, so p ∤ n. As h_p is a quadratic form, $v_p(h_p(P)) = v_p(h_p(nP))$; and nP satisfies (A2) for every P ∈ E(Q).

(⟸ of (i)), case $P \in \Lambda\backslash\Lambda_0$. Then $\bar{P}$ has order exactly p, $\#E(F_p)$ being p, and so does the reduction of $\mathrm{P}' := \mathrm{nP}$ as p ∤ n; $\mathrm{P}'' := \mathrm{pP}'$ satisfies (A1) and (A2). As E is split, Lemma 4 gives $\mathrm{e} = v_p(d(P'')) \geq 2$, hence b ≥ e ≥ 2 by Lemma 3 and c ≥ 2 by Corollary E, so $v_p(h_p(P'')) \geq 2$; and $h_p(P'') = p^2 h_p(P')$ gives $v_p(h_p(P)) = v_p(h_p(P')) \geq 0$.

(⟸ of (i)), case $P \in \Lambda_0$. Then nP satisfies (A1) and (A2), so $h_p(nP) \in 2pZ_p$ by Lemma 2 and $v_p(h_p(P)) \geq 1$.

So $v_p(h_p(P)) \geq 0$ for every P ∈ Λ. Polarising, $h_p(P, R) \in Z_p$ since p is odd; every entry of the height matrix on any basis of Λ lies in Z_p, every term of the Leibniz expansion has valuation ≥ 0, and $v_p(Reg_p) \geq 0$. With Theorem A this is (iii).

(⟹ of (i)). Suppose $E(Q_p)[p] = 0$. By ι there is P ∈ Λ whose reduction has order p; with $\mathrm{P}' := \mathrm{nP}$, Theorem S gives $v_p(h_p(P')) = -1$, hence $v_p(h_p(P)) = -1$. If every entry of M_Λ were in Z_p then so would be the value of the quadratic form at every point of Λ (the Lean statement `quadratic_value_mem_of_entries_mem`), a contradiction.

(ii). Let r = 1 and let Q generate Λ; by ι, $\mathrm{Q} \notin \Lambda_0$ and $Reg_p = h_p(Q)$. If E is split then $v_p(Reg_p) \geq 0$ by the first case above. If not, Theorem S gives $v_p(Reg_p) = -1$ exactly. ■

The choice of lattice is what carries the proof: what is needed is $v_p(h_p) \geq 0$ on Λ, not $v_p(h_p) \geq 2$ on Λ_0, and for a point of $\Lambda\backslash\Lambda_0$ it is enough that its reduction have order p.

4.9 Theorems H, L, F, J

Theorem H. The composition rule $\psi_{ab}(R) = \psi_b(R)^{a^2}\psi_a(bR)$ at (a,b) = (p,m) and (m,p), with $\varphi_k(x(R)) = x(kR)\psi_k(R)^2$ and φ_m monic of degree m^2 over $\mathrm{Z}[\mathrm{a}_1,\ldots,\mathrm{a}_6]$ evaluated at X := x(pQ) of valuation $-2\mathrm{e} \leq -2$, gives the exact identity

$$\varphi_p(x(mQ)) \cdot \psi_m(Q)^{2p^2} = \varphi_p(x(Q))^{m^2} \cdot (1 + \delta),\ \delta \in p^2 Z_p. \quad (\star)$$

Only even powers of $\psi_m(Q)$ occur, so $(\star)$ is well posed for every m prime to p. Its three division-polynomial values are p-adic units, $\psi_m(Q)^{2p^2}$ is a p-th power and $1 + \delta \in 1 + p^2 Z_p$, so q_p applied to $(\star)$ gives the claim; Corollary H′ follows since $E(F_p) \cong \mathrm{Z/p}$ and $\mathrm{m}^2 \neq 0$ in F_p. ■

Theorem L. Repeat the computation of Theorem C with D = C = $\hat{\mathrm{E}}$[p], Galois-stable for good ordinary reduction: N(x) = $\psi_C(x)^{2p}\cdot\varphi_{\hat{\pi}}(\varphi_C(x)/\psi_C(x)^2)$, the degree count is unchanged, so N = $A\cdot\varphi_p$ and evaluating at $\bar{x}$ gives the identity, the factor $(\psi_C(\bar{x})^2)^p$ being a p-th power. The leading coefficient of the x-part of $\hat{\pi}_C$ is c^{-2}, since $t_E(\hat{\pi}_C\ \mathrm{R}) = \mathrm{c}\cdot\mathrm{t}''(\mathrm{R}) + \mathrm{O}(\mathrm{t}''^2)$, whence A = c^2. ■

Theorem F. p splits in k, so k $\subset Q_p$ and the CM order acts on $E_{/Q_p}$ by Q_p − *endomorphisms*; by Deuring's lifting theorem $End(E_{/Q_p}) \to End(\bar{\mathrm{E}}_{/F_p})$ is an isomorphism for ordinary reduction, so Frobenius ϕ lifts to π with $\pi + \bar{\pi} = 1$ and $\pi\bar{\pi} = \mathrm{p}$. Put $\varrho := 1 - \pi = \bar{\pi}$, of degree p; on the special fibre $\bar{\varrho} = 1 - \phi$ is separable, as $(1-\phi)^*\omega = \omega \neq 0$, so ker ϱ is étale of order p over Z_p. On it $\pi = 1$, so Frobenius acts trivially, and its points, being étale, are defined over Q_p^{ur}, where Galois acts through Frobenius. Hence ker $\varrho \subset E(Q_p)$. ■

Theorem J. [Λ : Λ_0] = p gives det M_{Λ_0} = $\mathrm{p}^2\cdot$det M_Λ; the entries of M_{Λ_0} lie in pZ_p by Lemma 2, so M_{Λ_0} = p·N, and if N mod p has rank ρ_0, Smith normal form gives $v_p(det\ \mathrm{N}) \geq \mathrm{r} - \rho_0$. ■

5. Computations

All computations use PARI/GP 2.17.3 with `elldata` (Cremona's tables) on one core, with positive and negative controls; none is a proof, and no number is quoted outside its stated range.

The convention, made explicit. `ellpadicheight(E,p,n,P)` returns the coordinates [f, g] of the height on the basis (ω, η = xω) of $H^1_d R \otimes Q_p$; the height of §2 is

$$h_p(P) = -(\ \mathrm{f} - \mathrm{s}_2\cdot\mathrm{g}\ ),\ \mathrm{s}_2 := \texttt{ellpadics2(E,p,n)} = \mathrm{b}_2/12 - \mathrm{E}_2(\mathrm{E},\,\omega)/12,$$

since s_2 is precisely the constant c of [Har, (2)] that singles out σ_p: **the first component alone is a different height**, the one belonging to c = 0, whose σ is not in $tZ_p[[t]]$. As a control this reproduces the two entries of [MST, §4.2], v = −1 for 37A at p = 53 and v = +1 for 5077A at p = 5, their −2 shifted by r. Every count below was recomputed with h_p, the two conventions differing by a correction of valuation ≥ 0 that never moves a negative valuation.

5.1 The decomposition

Rank one, conductor ≤ 900, $a_p = 1$, p ≤ 43, p ∤ $\prod c_\ell$, ι, precision 14 — **474 boxes** — with P = nQ, n = $lcm(ord(\bar{Q}),\ \prod c_\ell)$, b := $v_p(h_p(P)/2 - log_p(\alpha/\beta))$, c := $v_p(log_p(\alpha/\beta))$, e := $v_p(d(P))$. Lemma 3 (c ≥ 1; b ≥ e; b ≥ 2e in the 223 boxes with p | a_1) and Corollary E (in the 45 split boxes) held without exception, and $v_p(h_p(P)) = \min(\mathrm{b},\,\mathrm{c})$ in 470 boxes, the other 4 having b = c with cancelling leading terms. Among the 429 non-split boxes c ≥ 2 occurred 26 times, all of them in Cremona's model with a_1 odd (§5.5). The choice of σ moves b in 98 boxes and $v_p(h_p)$ in none.

5.2 $\lambda = 0 \iff$ split

λ is measured with no rational point in sight: by Lemma 5 it is a function of E mod p^2 and $\bar{x}$, and by Lemma 4′ splitting is $v_p(\psi_p(x_0)) \geq 2$ for an integral lift. Over all curves of conductor N ≤ 1200 (any rank), 5 ≤ p ≤ 43, $a_p = 1$ — **1,445 boxes**, controls deg $\varphi_p = \mathrm{p}^2$ and leading coefficient 1 — these held with **no exception**: the scaling λ(m $\bar{x}$) = m^2 λ($\bar{x}$) for m = 2,

..., p−1 (Theorem H); $\psi_p \equiv u \cdot \bar{\psi}^p \pmod{\mathrm{p}}$ (Lemma 4′); the invariance of $min(v_p(\psi_p(x_0)),$ 2) and of λ under the lifts $\mathrm{x}_0 + \mathrm{kp}$, $\mathrm{k} \le 3$; and $\lambda = \mathbf{0} \iff$ **split** (158 split boxes, 158 with $\lambda = 0$, the same ones), which is Proposition 6. The identity ($\star$) was checked as an exact rational identity in 403 boxes and Theorem B′ in 310, both without exception, and splitting read independently, by `polrootspadic` on ψ_p, agreed wherever the PARI stack allowed it (1,234 boxes). One limit: the *exact* value of $v_p(\psi_p(x_0))$ is not invariant under change of lift, failing in 85 boxes — which is why only the cut at 2 is used, and is all that Lemma 4′ proves.

Proposition 6 was also tested where it is stated, over F_p rather than over the tables: running (A, B) over ${F_p}^2$ for the anomalous curves with $5 \le \mathrm{p} \le 157$ — 4,824 curves, 260,258 classes $\bar{x}$ — the slope ρ of §4.6 was non-zero without exception, the family E_s contained exactly one split member, and the zero of λ_s sat at that member. The identity $Res_X(\tilde{u}, \mathrm{g}) = c_p \cdot \Delta^{m_p}$ was verified exactly for p = 17, 19, 23 (m_p = 400, 561, 1001) at more points than the degree bound, and the cusp estimates — the valuations of the roots of f and g, $ord_t Res_X(\tilde{u}, \mathrm{g}) = m_p$, and the ratio of leading coefficients predicted by $12\rho_j = \mathrm{j}^2/\mathrm{t}$ — held for $\mathrm{p} \le 29$ without exception.

5.3 The height matrix, the regulator, and a bound that is too strong

Conductor ≤ 1500, $\mathrm{p} \le 19$, $a_p = 1$, $\mathrm{p} \nmid \prod c_\ell$, ι, ranks 1 and 2 — **659 boxes**: the minimum valuation of the entries of M_Λ is 0, 1 or 2 in the 71 split boxes and −1 in every one of the 588 non-split boxes, which is part (i) of the main theorem in both directions.

Rank 1, conductor ≤ 2000, $\mathrm{p} \le 23$, $a_p = 1$ — **1,107 boxes**: in the 8 where ι fails, $v_p(Reg_p) \in \{1,2\} \ge \mathrm{r}$ as Theorem A requires; of the other 1,099, every one of the 976 non-split boxes has $v_p(Reg_p) = -1$ exactly and every one of the 123 split boxes has $v_p(Reg_p) \in \{0,1,2\}$. Part (ii) accounts for the first; the distribution inside {0,1,2} is not accounted for by anything here.

Rank ≥ 2, conductor ≤ 9000, $\mathrm{p} \le 19$ — **262 boxes**: 23 split boxes of rank 2 with $v_p(Reg_p) \in \{0,1\}$, so the bound 0 is attained, and one split box of rank 3 with $v_p(Reg_p) = 1 = \max(\mathrm{r}-2, 0) < 2$, which **refutes** the stronger bound $\max(2\mathrm{r}-4, 0)$ suggested by the shape of Theorem J; in two of the 24 split boxes the height form does not vanish on the kernel of the reduction character, as that bound would require.

5.4 CM curves

Over all curves of conductor ≤ 1500 (8,163 curves, 138 with CM) and $\mathrm{p} \le 43$, all **14** anomalous CM boxes are split, against 178 of 1,935 in the non-CM boxes; the primes occurring are p = 7, 19, 37 for curves with j = 0, which is what $a_p = 1$ with $\pi\bar{\pi} = \mathrm{p}$ forces. This is the content of Theorem F, not independent evidence for it.

5.5 The model, and the exact value in the non-split case

Conductor ≤ 3000, $\mathrm{p} \le 23$, rank ≥ 1, $a_p = 1$, $\mathrm{p} \nmid \prod c_\ell$, ι, with $\mathrm{P}' = (\prod c_\ell) \cdot Q$ for a generator Q of non-zero reduction and $\mathrm{P} = \mathrm{pP}'$ computed exactly — **1,765 boxes**, in both Cremona's model and the model with $\mathrm{p} \mid \mathrm{a}_1$. In the model with $\mathrm{p} \mid \mathrm{a}_1$ the identity $q_p(\alpha/\beta) = -\lambda$ of Theorem B held in **1,765 of 1,765**, and **no non-split box had c ≥ 2**; the positive control, 185 split boxes with $\lambda = 0$ and $\mathrm{c} \ge 2$, held throughout. In Cremona's model the same identity failed in 719 boxes, all of them with $\mathrm{e} = 1$ and a_1 odd, and 90 non-split boxes had $\mathrm{c} \ge 2$, all of them with a_1 odd; the shift of §2 removes all 90. This is the numerical form of the remark that b and c are quantities of a model while min(b, c) is not.

The relation $d(P) = d' \cdot |\Psi|$ — no cancellation, Step 1 of §4.4 — held in every box, and fails when the factor $\prod_\ell c_\ell$ is dropped from P': (A2) is used at exactly that point. On the side of the height matrix, conductor ≤ 900 and $p \leq 13$ with `ellpadicheightmatrix` gave **239 boxes**: $min_{i,j}\ v_p(M_\Lambda[i,j]) = -1$ in all 206 non-split boxes and ≥ 0 in all 33 split ones.

6. What is proved in Lean and what is not

Eight files, each checking from `import Mathlib` alone, in the namespace `PadicHeight`: `PadicHeightValuation{,2,3,4,5,6,7,8}.lean`. Every statement is about integers, matrices, finite sums or p-adic congruences; Mathlib has neither the p-adic sigma function nor division polynomials nor Vélu's formulas nor the Tate curve, so the geometry and the p-adic analysis enter as hypotheses. The companion `statements-and-dependencies.md` lists all Lean names; the main line is

Statement	Lean name	File
Theorem A	`norm_det_div_sq_le`	1–4
Theorem B, step 3	`fermatQuot_sub_iff_of_sq_eq_cube`, `dvd_three_mul_sub_two_mul`, `sub_ne_zero_of_two_mul_eq_three_mul`	1–4, 8
Theorem B, the model with $p \mid a_1$	`sq_sub_cube_dvd_of_dvd_a1` (and `sq_sub_cube_dvd_of_sq_dvd_psi` for $e \geq 2$)	8
Lemmas 4′ and 5	`eval_sub_eval_dvd_sq`	1–4
Corollary D	`sq_dvd_pow_sub_one_of_isPow`	1–4
Corollary E	`sq_dvd_alpha_sub_beta_of_isPow`	1–4
Theorem H	`fermatQuot_scale`	1–4
Theorem J	`dvd_det_of_col_dvd`, `pow_succ_dvd_det_of_col`	1–4
Main theorem, linear algebra	`regulator_valuation_of_split_anomalous`	5
Main theorem (ii), equivalence	`regulator_valuation_of_split_anomalous_iff_split`	5
§4.6 (2), the single slope and the affine zero	`slope_of_rho`, `fermatQuot_deform`, `affine_zero_unique`, `lambda_eq_zero_iff_split`, `lambda_dichotomy`	5
§4.6 (3), the weight count and the Newton polygon	`weight_split`, `twelve_dvd_weight`, `sum_pole_orders`, `cusp_sum_eq_m`, `mul_compl_le_half_mul_half`, `eq_C_mul_of_dvd_of_natDegree_eq`	6
§4.6 (4), the residues	`inv_one_sub_add_inv_one_sub_inv`, `first_term_residue`, `second_term_leading_ne_zero`, `residues_do_not_cancel`, `twelve_mul_sum_cusp_orders`	7
Theorem S, the ledger	`exists_shift_dvd_a1`, `add_val_exactly_one`, `not_dvd_of_val_one`	8
Main theorem ($\Longrightarrow$ of (i))	`quadratic_value_mem_of_entries_mem`	8

How the main theorem appears there. `regulator_valuation_of_split_anomalous` takes as hypotheses that the entries of the height matrix on Λ_0 are divisible by p and that $\det M_{\Lambda_0} = p^2 \cdot \det M_\Lambda$, and concludes $p^{r-2} \mid \det M_\Lambda$; `regulator_valuation_of_split_anomalous_iff_split` takes the two halves — split $\Longrightarrow Reg_p \in Z_p$, and non-split $\Longrightarrow Reg_p = \mathbb{Z}/p$ with $p \nmid z$ — and turns them into the equivalence of (ii). That is, **integrality of the height matrix is a hypothesis there, not a conclusion**: what the kernel checks is the bookkeeping, and the geometry that produces the hypotheses is on paper.

Trust base. `#print axioms` is run at the end of each file on every theorem listed; every line reads `depends on axioms:` followed by a subset of [propext, Classical.choice, Quot.sound], and the logs are kept beside the sources. There is no `sorryAx` and no `Lean.ofReduceBool`, that is no `native_decide`; no `decide` is load-bearing, and each file checks with exit code 0 and no warnings.

What is not in Lean. The p-adic sigma function and the formula for h_p; the Iwasawa logarithm; division polynomials, their composition rule and their shape modulo p; Vélu's formulas and the degree count of Theorem C; [p] = V ∘ F and the group scheme E[p]; Serre–Tate theory; the Tate parametrisation and the valuations read off it; Deuring's lifting theorem; the structure of $E(Q_p)$ used in Lemma 4; the height pairing itself. So **the main theorem is not a Lean theorem**: what is machine-checked is the arithmetic skeleton along which its proof runs, and its grade is [paper].

7. What is open

1. **The quadratic residue class of the slope.** Over every anomalous curve over F_p with p ≤ 157 the slope ρ of §4.6 satisfies $(\rho/\mathrm{p}) = (-3/\mathrm{p})$, so that -3ρ is a square and $\rho(\bar{x}) = -3\mu(\bar{x})^2$ for a homomorphism $\mu : E(F_p) \to F_p$ determined up to sign. This is [computation] and nothing more; μ has no closed form here. At the cusp $\rho_j \approx 9\mathrm{j}^2/\Delta$, and the shape $\rho = 9L(\bar{x})^2/\Delta$ with L a homomorphism is excluded by the residue class together with the squareness of $-\Delta$.

2. **One source under §4.6.** The step "$E^{(p)}$ is the member of the family at parameter t^p" uses that the Tate parameter q, as a series in 1/j, has coefficients in the prime field. j(q) ∈ Z[[q]] is standard; the inverse series is what we did not locate in a source (§9), and [ATAEC] itself we did not retrieve.

3. **Exact values rather than bounds.** Part (iii) is a lower bound, and the distribution of $v_p(Reg_p)$ inside {0, 1, 2} in the split boxes of §5.3 is not explained by anything here; nor is the behaviour at p = 5 with $\#E(F_5) = 10$, which all statements after Lemma 4 exclude.

4. **The geometry in Lean.** §6 lists what would have to exist in Mathlib for the main theorem to become a Lean theorem.

8. What is not claimed

1. **Nothing here bears on the conjecture of Birch and Swinnerton-Dyer**, nor on Sha, on L-functions or on the rank: every statement is about the valuation of a p-adic regulator under hypotheses on the reduction at one prime. Schneider's conjecture is not proved either; its CM case is [known], due to [Ber82], which we did not retrieve.

2. **The baseline is not ours.** Theorem A is elementary and known (§9); what we add is the splitting hypothesis and its mechanism.

3. **The local criterion is not ours.** The equivalence of Proposition 6 is [known] ([LR, Thm 4.1] for Gross's criterion, [DW, Lemma 3.2, Cor. 3.5]); we give an independent proof and a presentation through a Fermat quotient, and we do not give it a name.

4. **The theorem is a lower bound in rank ≥ 2.** The exactness of §5.3 in the non-split case is Theorem S; in the split case nothing here predicts the value. Deuring's lifting theorem, Vélu's formulas, Serre–Tate theory, the composition rule for division polynomials, the coprimality of φ_p and ${\psi_p}^2$, and the Tate parametrisation are used as standard facts, and for the last we cite sources that quote [ATAEC] rather than [ATAEC] itself.

5. **The hypotheses are as used, not the weakest possible.** Everything from Lemma 4 on assumes p ≥ 5 and $\#E(F_p) = $ p, so $\#E(F_5) = 10$ lies outside, while Theorem A needs only p $\mid \#E(F_p)$.

6. **The computations are not kernel-checked, and the statistics are not statements.** All of §5 is PARI/GP with controls, at stated precision and over stated ranges; an earlier round used the height belonging to $\sigma \neq \sigma_p$, and every count here has been recomputed with h_p.

7. **No claim of priority, and no external review.** We searched [MST], [SW], [Har], [BMS], [BD], [Ban], [Wut], [BG], [LR], [DW], Sage's documentation and arXiv (§9): the baseline we found, the local criterion we found, the equivalence with integrality of the height matrix we did not, in a narrow search — no MathSciNet or zbMATH, and several primary sources not retrieved — so the statements may well be known. Observation, proofs, programs, Lean development and draft were produced by the same agent, and Lean's kernel, which covers §6 alone, is the only check not internal to the authors.

9. Related work

Where the baseline already is. In the table of [MST, §4.2], for curves of rank 1 to 5, the entry for 37A at p = 53 is the only one of negative valuation, and the text notes there that $\#E(F_p) = $ p, "i.e., p is anomalous" — the phenomenon, with no bound stated and no index in sight. [Har] has the mechanism as an estimate: the working precision must be raised by 2 $v_p(n)$, n = $lcm(\#E(F_p), lcm_\ell\ c_\ell)$, which is the "cost 2" of Theorem A as a loss of precision. [Ban, §2.2] uses the contrapositive as a hypothesis, non-anomalousness being what "extends the regulator estimate of Proposition 4.2 from $E^\circ(Q)$ to all of E(Q)", and that Proposition 4.2 is the positive half of Theorem A in rank two; Sage's `padic_regulator` documents the same example. So the baseline is known to practitioners; we did not find it written as a proposition, and we do not need it to be new.

Where the local criterion already is. Proposition 6 is the case n = 1 of Gross's tameness criterion, quoted as [LR, Thm 4.1]: for good ordinary reduction with E[p] irreducible, the decomposition group is diagonalisable modulo p^{n+1} exactly when $j_E \equiv j_0 \pmod{p^{n+1}}$, with j_0 the j-invariant of the canonical lift, determined by the modular equation. It is also [DW, Lemma 3.2 and Cor. 3.5], where a prime with $E(Q_p)[p] \neq 0$ is a *local torsion prime* and the criterion is that the lift to $\mathbb{Z}/p^2$ be the canonical one — of the p^d lifts exactly one has the larger p-rank — together with [DW, Prop. 2.1] for the fact that a local torsion prime is anomalous. The same statement circulates in cryptography, where the attacks on anomalous curves fail exactly for the lifts congruent to the canonical one modulo p^2. What we did not find is the criterion in the form $q_p(\varphi_p(x_0)) = 0$ — a Fermat quotient of a division polynomial at one point, which needs neither the j-invariant nor root-finding; the proof of §4.6 is independent of the sources above. Searches returning nothing on point (2026-09-24): `elliptic Wieferich prime`, `Fermat quotient elliptic curve`, `anomalous prime elliptic curve p-torsion`, `canonical lift p-torsion criterion mod p^2`. Near but different: the elliptic Wieferich primes of [Sil88] and [Vol] concern $N_p \cdot P$ modulo p^2 for a rational point P, not rationality of the p-torsion, and the division-polynomial criteria of [Deb] are modulo p.

What we did not find is the splitting hypothesis $E(Q_p)[p] \neq 0$ in connection with the valuation of Reg_p, or any statement that the height pairing is p-integral exactly under it. [SW] is our source for Schneider's conjecture; their §3.3 anomalous example is 446d1 at p =

5 with $\#E(F_5) = 10$, the p = 5 case of §3.1, and its $\mathrm{ord}_5(\mathrm{Reg}_5)$ is +1, not negative. The word "anomalous" does not occur in [BMS]. [Wut] studies the quantity e of §3.3 from the global side and [BG] the universal p-adic sigma function; [Kat] on Serre–Tate local moduli, the natural language for §4.6, we could not obtain. The nearest computation in the literature is [Ban] (2026), five rank-two CM curves at every good ordinary prime below 30,000 with a non-unit at 3 of 8,050 primes — the slice orthogonal to ours — which also formalises part of its argument in Lean 4.

References

[ATAEC] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, GTM 151. [not retrieved; Thm V.5.3, Thm V.3.1, Prop. V.6.1 and Exercise V.5.13 are cited as quoted in [Ked] and [Sym]; the minimality of the Tate model and the integrality of the coefficients of q as a series in 1/j we could not attach to numbered statements]

[Ban] B. S. Banwait, *Second derivatives of p-adic L-functions and the Shafarevich–Tate group of rank-two CM elliptic curves*, arXiv:2609.08431 (2026).

[BMS] J. S. Balakrishnan, J. S. Müller, W. A. Stein, *A p-adic analogue of the conjecture of Birch and Swinnerton-Dyer for modular abelian varieties*, arXiv:1210.2739.

[Ber82] D. Bertrand, *Valeurs de fonctions thêta et hauteurs p-adiques*, Progr. Math. **22**, Birkhäuser, 1982, 1–11. [not retrieved]

[BG] C. Blakestad, D. Grant, arXiv:1903.02480.

[BD] A. Burungale, D. Disegni, arXiv:1803.09268.

[Deb] C. Debry, *Beyond two criteria for supersingularity*, J. Théor. Nombres Bordeaux **26** (2014) 595–605.

[Dok] T. Dokchitser, V. Dokchitser, *Local invariants of isogenous elliptic curves*, arXiv:1208.5519, Thm A.1.

[DW] C. David, T. Weston, *Local torsion on elliptic curves and the deformation theory of Galois representations*, arXiv:math/0701882.

[Har] D. Harvey, *Efficient computation of p-adic heights*, arXiv:0708.3404.

[Kat] N. Katz, *Serre–Tate local moduli*. [not retrieved]

[Ked] K. S. Kedlaya, *The Tate curve*, lecture notes, MIT 18.727. [used only as a conduit for the statements of [ATAEC]]

[LR] Á. Lozano-Robledo, *Division fields of elliptic curves with minimal ramification*, Rev. Mat. Iberoam. **31** (2015) 1311–1332; Thm 4.1 quotes B. Gross, Duke Math. J. (1990), §§14–15.

[Maz72] B. Mazur, Invent. Math. **18** (1972). [not retrieved; the source of "anomalous"]

[MST] B. Mazur, W. Stein, J. Tate, *Computation of p-adic heights and log convergence*, Documenta Math. Extra Vol.: John H. Coates' Sixtieth Birthday (2006) 585–622.

[MT91] B. Mazur, J. Tate, *The p-adic sigma function*, Duke Math. J. **62** (1991) 663–688. [not retrieved]

[Sch] P. Schneider, *p-adic height pairings I, II* (1982, 1985). [not retrieved]

[Sil88] J. H. Silverman, *Wieferich's criterion and the abc-conjecture*, J. Number Theory **30** (1988) 226–237.

[SW] W. Stein, C. Wuthrich, *Algorithms for the arithmetic of elliptic curves using Iwasawa theory*, Math. Comp. **82** (2013) 1757–1792.

[Sym] *Symplectic criteria for elliptic curves, revisited*, arXiv:2509.19938, Prop. 2.2. [used only as a conduit for [ATAEC, Prop. V.6.1]]

[Vél] J. Vélu, *Isogénies entre courbes elliptiques* (1971). [not retrieved]

[Vol] J. F. Voloch, J. Number Theory **81** (2000) 205–209.

[Wut] C. Wuthrich, *On p-adic elliptic logarithms and p-adic approximation lattices* (2006).

Software: PARI/GP 2.17.3 with `elldata` (Cremona's tables, conductor < 500000); Sage, `src/sage/schemes/elliptic_curves/padics.py`, docstrings of `padic_regulator` and `padic_height`.