Elliptic Lehmer bounds over global fields

Abstract

We use reduction at one supersingular place to bound the height of a point on an elliptic curve in terms of its degree over the prime-to-p torsion field. Over a function field of characteristic p the lower bound is a constant times the reciprocal of the degree, including its inseparable part. Over a number field with such a place we obtain an exponent $1+\epsilon$ for every $\epsilon > 0$. The same count of pairs of conjugates gives both bounds. The difference comes from the contribution of the archimedean places to the sum of local heights.

hexagon:2611.00887v1

1 The degree in the lower bound

Let A be a point of infinite order in $E(K)$, and choose P with $[n]P = A$. Then $\widehat{h}(P) = \widehat{h}(A)/n^2$, while $[K(P) : K] \le n^2$ because $[n]$ has degree n^2. The elliptic Lehmer problem asks for a lower bound of the form $c/[K(P) : K]$ for every non-torsion P. The division points of A show why the exponent one is the natural one. For any $0 < \eta < 1$, their heights times $[K(P) : K]^{1-\eta}$ tend to zero as n grows.

We shall measure the degree after adjoining torsion. For a prime p, put

$$F = K\big(E[n] : (n, p) = 1\big), \qquad D = [F(P) : F].$$

Passing to F can make the degree smaller. The reason to use this field is that at a supersingular place above p, a power of Frobenius acts on every prime-to-p torsion group by the same integer. We use that scalar to compare conjugates of P. Throughout, $\widehat{h}$ is the canonical height for the divisor (O).

Theorem 1. *Let $P \in E(\overline{K})$ be a point of infinite order.*

1. *Suppose $K = \mathbf{F}_q(B)$ is the function field of a smooth projective geometrically integral curve over its full field of constants, of characteristic p. For every non-isotrivial elliptic curve E/K,*

$$\widehat{h}_{E,K}(P) \ge \frac{c_p}{D}$$

with $c_p > 0$ depending only on p. Here D is the total field degree and heights are measured in degrees of divisors over $\mathbf{F}_q$.

2. *Suppose K is a number field and E/K has good supersingular reduction at a place $v \mid p$. With the absolute logarithmic height there are positive constants c, C, depending on E, K, v, for which*

$$\widehat{h}_E(P) \ge \frac{c}{D} \exp\Big(-C\sqrt{\log(2D)}\Big).$$

In particular, $\widehat{h}_E(P) \ge c_\epsilon D^{-1-\epsilon}$ for every $\epsilon > 0$, with c_ϵ depending also on ϵ.

Both bounds imply the corresponding assertion with $[K(P) : K]$ in the denominator. Elkies proved that an elliptic curve over a number field with a real embedding has infinitely many primes of good supersingular reduction [19, 20]. Thus part (2) applies to every elliptic curve over $\mathbf{Q}$. We may choose p once for the curve, before choosing P. The same conclusion holds when $\mathbf{Q}(j_E)$ has a

real embedding. Apply Elkies to a model over the j-field and discard the finitely many bad places before comparing the reductions of the two models. For a general totally imaginary j-field, part (2) requires the indicated local hypothesis.

The local calculation is easiest to picture over $\mathbf{Q}$. Let $p \geq 5$ be a good supersingular prime. The trace of Frobenius is divisible by p and has absolute value at most $2\sqrt{p}$, so it is zero. The Frobenius relation on the special fiber becomes $\Phi^2 = [-p]$ [40, Ch. V, §§2–3]. In particular, if $A \in E(\mathbf{Q})$, then A and $[-p]A$ have the same reduction. The difference between $[-p]^i A$ and $[-p]^j A$, for $i < j$, already has i multiplications by $-p$ in common. Each of these multiplications brings the difference closer to the origin. For algebraic P we make the same comparison between two conjugates, choosing them so that their reductions agree after a Frobenius action. The earlier of the two levels still determines how many multiplications the difference has acquired.

1.1 Previous height bounds

Write $D_0 = [K(P) : K]$ in this discussion. The exponent-one question for elliptic curves goes back to Anderson and Masser [4] and is the analogue of Lehmer's question on Mahler measure [29]. Masser's counting theorem gives a lower bound of order $D_0^{-3}(\log D_0)^{-2}$ for an arbitrary elliptic curve over a number field [30, Corollary 1]. Hindry and Silverman obtained $D_0^{-2}(\log D_0)^{-2}$ when j_E is nonintegral [27]. Laurent proved the elliptic analogue of Dobrowolski's theorem for curves with complex multiplication, with lower bound of order

$$\frac{1}{D_0}\left(\frac{\log\log(3D_0)}{\log(2D_0)}\right)^3$$

[28, 17]. Here the implicit constants are for a fixed curve over a fixed field, and one may adjust them for small degrees. David and Hindry extended this type of estimate to CM abelian varieties [14]. For recent accounts of the number-field estimates, see Silverman [45, §8] and Gaudron and Rémond [22, Theorem 1.3], whose explicit bound gives the cubic dependence in dimension one. Galateau and Mahé proved the exact $1/D_0$ bound when $K(P)/K$ is Galois [21]. The point field in Theorem 1 may be nonnormal.

The relative question asks for a bound in terms of the degree left after enlarging the base. Amoroso and Zannier did this for the multiplicative group over the maximal abelian extension [3]. For a CM elliptic curve, Ratazzi obtained a bound of order

$$\frac{1}{D_{\mathrm{ab}}}\left(\frac{\log\log(5D_{\mathrm{ab}})}{\log(2D_{\mathrm{ab}})}\right)^{13}, \qquad D_{\mathrm{ab}} = [K^{\mathrm{ab}}(P) : K^{\mathrm{ab}}]$$

[35, Theorem 1.1]. Over a fixed extension K' defining the CM endomorphisms, the full torsion field lies in $(K')^{\mathrm{ab}}$. The bound over the larger field also gives a bound in terms of the degree over the full torsion field. Carrizosa states David's relative conjecture over the full torsion field and proves a CM version for abelian varieties in terms of an obstruction index [11, Conjecture 0.1 and Theorem 0.2]. The full proof is in [12]. Habegger [24, Introduction, (1.2)] singles out the exponent $1 + \epsilon$ for non-CM curves, even with D_0 as the degree. The number-field result here uses the degree over the prime-to-p torsion field and the bound it gives for D_0 is an immediate consequence.

At relative degree one the question becomes a height gap on a prescribed field. Baker and Silverman proved this over maximal abelian extensions, building on their earlier work for elliptic curves [5, 39, 7]. Habegger proved a gap for the Néron–Tate height on $E(\mathbf{Q}(E_{\mathrm{tors}}))$ [24, Theorem 2]. Plessis developed a criterion in terms of supersingular reduction, and Sahu used it to obtain a gap over $L(E_{\mathrm{tors}})$ for each fixed finite extension L/K when, for example, $\mathbf{Q}(j_E)$ has a real embedding [34, 36]. The results of Habegger and Sahu allow all torsion in the base field. Theorem 1 gives a single degree-dependent bound as the point field varies over the prime-to-p torsion field.

Over function fields, the lower bounds for rational points of Hindry and Silverman, Goldfeld and Szpiro, and Pacheco are tied to the conductor and the minimal discriminant [26, 23, 31]. In the degree aspect Silverman formulates the $1/D_0$ conjecture over algebraically closed constants and proves a bound of order $h_K(j_E)^{-2}D_0^{-2}$ in characteristic different from $2, 3$. See [43, Conjecture 1 and Theorem 2]. The corrigendum gives the explicit constant $1/18000$ for $D_0 \geq 6$ [44]. Pacheco's earlier preprint states an absolute inverse-degree estimate for semistable curves [32, Theorem 3.4]. In the proof of Proposition 3.2, equation (3.3) sums over places using a subset whose choice depends on the place. One can see the difficulty in the counting statement itself. Adjoining $E[\ell]$ for a prime $\ell \geq 5$ different from the characteristic already gives more than 24 points of height zero. In our count the individual pairs may depend on the place, but the averaging is over the same collection of global subsets at every place.

1.2 Frobenius and pair sums

Two lines of work meet in the proof. The first uses Frobenius to find a point in the kernel of reduction. At an ordinary CM place Baker compares a Galois conjugate with the image under a characteristic-zero lift of Frobenius [5, Lemma 3.3]. Silverman uses the characteristic polynomial of Frobenius to obtain a formal point at a place of good reduction [39, Theorem 4 and Corollary 5]. The local comparison used here occurs in Habegger's work on torsion fields [24, Lemmas 3.2, 8.3 and 8.5]. At Habegger's chosen supersingular prime, the square of Frobenius acts by a scalar on each prime-to-p torsion layer. Centrality lets the comparison give a local height contribution at every place over p. We use the same scalar on the torsion layer to align the reductions of whole orbits when the point itself has arbitrary degree over that layer.

The second line of work estimates sums of local heights of differences. Hindry and Silverman use Fourier averaging of the Bernoulli term at a multiplicative place [26, §1]. Baker and Petsche include the archimedean places in a global discrepancy inequality, and Petsche develops the nonarchimedean formulation for function fields [6, 33]. A further precedent is Silverman's elliptic Lehmer estimate for points satisfying a modular proximity condition [42, Theorem 4.1 and Corollary 4.1]. There the hypothesis supplies a prescribed amount of proximity to torsion. Here the local count supplies proximity between the points at different levels of the same orbit. Its sum grows quadratically in the number of levels after normalization, and the archimedean discrepancy determines how many levels we need.

The two-orbit calculation also recalls Dobrowolski's congruence between a polynomial and the polynomial of the pth powers of its roots [17]. Section 3 compares the passage from a first congruence to higher contact with the use of multiplicity in Stepanov's method and in the argument of Alpöge and Claude. It also explains how Dimitrov uses a congruence between two levels to obtain an inverse-degree bound for the house of an algebraic integer.

2 What the global height bounds

Let v be a place of good reduction, and normalize its valuation b by $b(\pi_v) = 1$. We keep this normalization in every extension. If A and B have the same reduction at $w \mid v$, the local height of their difference is measured by

$$i_w(A, B) = b\big(z(A - B)\big),$$

where z is an integral formal parameter at O and $A \neq B$. We call this the depth of contact. Set $i_w(A, B) = 0$ when the reductions differ. The question we need from the global theory is how large the sum of these depths can be for a set of points of prescribed heights.

Take $N \geq 2$ distinct points forming a set Z, all defined over a finite extension M/K. Give $w \mid v$ the relative weight $\beta_w = [M_w : K_v]/[M : K]$. These weights sum to one. The weight that converts b

to our global height is

$$\omega_v = \begin{cases} [\kappa(v) : \mathbf{F}_q], & K = \mathbf{F}_q(B), \\ [\kappa(v) : \mathbf{F}_p] \log p / [K : \mathbf{Q}], & K \text{ a number field.} \end{cases}$$

For instance, in the number-field normalization a uniformizer at v contributes $\log(p)/e(K_v/\mathbf{Q}_p)$ before multiplication by $[K_v : \mathbf{Q}_p]/[K : \mathbf{Q}]$. On the function-field side our convention for $x \in M$ is

$$h_K(x) = \frac{1}{[M : K]} \sum_w [\kappa(w) : \mathbf{F}_q] \max(0, -\operatorname{ord}_w x).$$

The corresponding canonical height is obtained from $\frac{1}{2} h_K(x(P))$ by the canonical-height limit [40, Ch. VIII, §9]. Over either global field it is positive on non-torsion points, by Northcott applied in a finite field of definition.

Write $\mathcal{I}_v(Z) = \omega_v \sum_{w|v} \beta_w \sum_{A \neq B} i_w(A, B)$, with A, B running over ordered pairs in Z. The height comparison we use is

$$\mathcal{I}_v(Z) - N\mathcal{E}_K(N) \;\le\; \sum_{A \neq B} \widehat{h}(A - B) \;\le\; 2N \sum_{A \in Z} \widehat{h}(A), \tag{1}$$

where

$$\mathcal{E}_K(N) = \begin{cases} h_K(j_E)/12, & K \text{ a function field}, \\ \frac{1}{2} \log N + h(j_E)/12 + 16/5, & K \text{ a number field.} \end{cases} \tag{2}$$

The upper bound is immediate from the height pairing. In fact the difference between the upper bound and the middle sum is $2\widehat{h}(\sum_{A \in Z} A)$.

For the lower bound, compute local heights after a finite extension giving semistable reduction [40, Ch. VII, Proposition 5.4]. We use the local-to-global decomposition and the local formulas for good reduction and Tate curves [41, Ch. VI, §§2, 4]. Good places contribute nonnegative intersections, and we keep those above v. At a multiplicative place the local height has, in addition to a nonnegative intersection, the term $\frac{1}{2} \log^+ |j_E| \, B_2(x_A - x_B)$. Here x_A is the component coordinate on the Tate circle and $B_2(x) = \{x\}^2 - \{x\} + 1/6$. Its Fourier series has positive coefficients at every nonzero frequency and zero constant term [6, Propositions 5 and 7]. The sum over all pairs is therefore nonnegative, and removing $A = B$ subtracts $NB_2(0) = N/6$ from the Bernoulli sum. This accounts for the factor $1/12$. At an archimedean place Proposition 4 of Baker and Petsche [6] bounds the loss by $N(\frac{1}{2} \log N + \frac{1}{12} \log^+ |j_E| + 16/5)$. Averaging the j-terms over all places gives $Nh(j_E)/12$, or $Nh_K(j_E)/12$ in divisor units [33, Proposition 7 and §2]. This proves (1) for each individual set Z, a point we will use when we average over several choices of Z.

3 Stepanov, theta lifts, and the Frobenius levels

Stepanov's method starts with a relation that holds at a rational point over a finite field. The relation first gives one zero. To obtain a useful bound, one must increase its order and keep track of the poles of the auxiliary function. The same distinction between finding contact and making it count appears in the argument here and in Alpöge and Claude's argument for the Riemann hypothesis [2]. A calculation from Bombieri's version makes the comparison precise.

3.1 From a Frobenius identity to a zero of high order

Let $X/\mathbf{F}_q$ be a smooth projective geometrically integral curve of genus g, with q a square. If $X(\mathbf{F}_q)$ is nonempty, fix $P_0 \in X(\mathbf{F}_q)$ and let $L(u) = H^0(X, \mathcal{O}_X(uP_0))$. Choose a power M of p dividing q,

and integers ℓ, n with $\ell M < q$. In Bombieri's presentation of Stepanov's method, one chooses a basis a_i of $L(\ell)$ with distinct pole orders and considers the two functions

$$f = \sum_i a_i^M b_i^q, \qquad \delta f = \sum_i a_i^M b_i, \qquad b_i \in L(n).$$

The coefficients b_i are determined by f. Indeed the nonzero terms in f have distinct pole orders modulo q, since the pole orders of the a_i^M are distinct and lie between 0 and $\ell M < q$. This makes δ a well-defined linear map from a space of dimension $\dim L(\ell) \dim L(n)$ to $L(\ell M + n)$. If the first dimension exceeds the second, some nonzero f satisfies $\delta f = 0$ [8, §II].

For $P \in X(\mathbf{F}_q) \setminus \{P_0\}$, we have $b_i(P)^q = b_i(P)$ and therefore $f(P) = \delta f(P) = 0$. The extra vanishing comes from the shape of f. Since M divides q, we can write

$$f = \left(\sum_i a_i b_i^{q/M} \right)^M .$$

A zero of the inner function contributes at least M to the order of vanishing of f. Counting zeros against poles now gives

$$M\big(\#X(\mathbf{F}_q) - 1\big) \le \ell M + nq.$$

Take $n = M + 2g$. By Riemann–Roch the dimension inequality holds if $\ell(g+1) > g(M+g+1)$. Thus one can take $\ell = \lfloor gM/(g+1) \rfloor + g + 1$, and the point bound has main term q and error at most $1 + \ell + 2gq/M$. For fixed $g \ge 1$, balancing the term of order M with the term of order q/M gives $M = \sqrt{q}$. This is a power of p when q is a square and satisfies $\ell M < q$ for q sufficiently large in terms of g [47, 8].

3.2 How the theta lifts enter the Riemann hypothesis argument

Alpöge and Claude use a chain of theta lifts between unitary groups of increasing rank in the role of the parameter M. A theta lift transfers an automorphic form by pairing it with a theta kernel. In the reconstruction of the argument, the kernels at inert primes of an imaginary quadratic field are studied using integral models of a CM elliptic curve. The local estimates give divisibility of the maps obtained from the lifts. This makes it possible to enlarge the source lattice of the period pairing while retaining integrality. The enlargement increases its arithmetic degree through the local indices. In this sense the repeated lifts supply the analogue of vanishing of higher order [1, §4.5].

The other half of the argument controls the pairing at the archimedean places. An upper bound for the norm of the composite uses bounds for the individual lift norms and the final pairing. On changing from integral formal parameters to complex coordinates, the bounds involve the periods of the CM curve. The Chowla–Selberg formula evaluates the relevant average of their logarithms [13]. Bost's slope inequality passes from estimates for a map of lattices to a comparison of arithmetic degrees. In rank one this is the familiar inequality $k \log p \le \log |u|$ for a nonzero integer u divisible by p^k. Multiplication by u still sends $p^{-k}\mathbf{Z}$ into $\mathbf{Z}$, and enlarging the source has raised its arithmetic degree by $k \log p$. In the reconstruction, a lower estimate coming from divisibility meets an upper estimate for the target slope and the height of the period map. Taking the rank-weighted average cancels the intermediate period-map height. The leading term of the resulting prime sum then cancels against the explicit main term used to center that sum. In the quadratic model, the logarithmic derivative $L'(1,\chi)/L(1,\chi)$ appears both in the CM period formula and in this prime sum. See Propositions 4.1 and 5.1 and §4.6 of [1] and Bost's exposition of the slope method [9].

After normalization by the number of lifts, the two terms that explain the choice of length have the rough sizes

$$\frac{x(\log x)^A}{r} \qquad \text{and} \qquad rx^\eta,$$

where r is the number of lifts, x is the scale of the prime sum, and $\eta > 0$ denotes a small exponent. The full estimate also controls errors involving the other parameters of the construction. At the scale of powers of x, the first term is a cost spread over all lifts and the second grows with the chain. The balance puts r at the scale $x^{1/2}$ up to small powers and logarithms. The resulting one-sided estimate for a centered, smoothed sum over prime powers feeds the analytic argument that excludes zeros to the right of the critical line [1, §2, (4.10), and Proposition 7.4].

3.3 What plays the part of multiplicity for elliptic heights

In the separable function-field proof, the role of the auxiliary function can already be seen in one residue disk. Let A and B be the monic polynomials of the formal coordinates of two conjugate orbits there. Scalar Frobenius gives the congruence $B \equiv A \pmod{\pi_v}$. At a root x of A, the valuation of the evaluation is

$$b(B(x)) = \sum_{B(y)=0} b(x-y) \geq 1.$$

Thus one gets a unit of total contact with x, even when the individual terms have fractional valuation. In characteristic p, applying $[p^a]$ to the two orbits multiplies the lower bound for contact by at least p^a. This is the formal-group counterpart of raising a function to a p-power in Bombieri's argument. The bound on what one can gain is the sum of global heights in (1). Since the error there is constant after division by N, two orbits with a fixed amount of amplification suffice in the separable case.

Over a number field, multiplicity now comes from comparing several levels. Once a formal difference has sufficient depth, further multiplication by p gives a lower bound that grows linearly with the number of multiplications. The points at levels $i < j$ have already undergone i common applications of the scalar multiplication used for one level. Counting their contact therefore produces a factor of at least $i + 1$ in the lower bound of Lemma 2. Adding over the pairs of levels gives

$$\sum_{0 \leq i < j < t} (i+1) = \frac{t(t^2-1)}{6}.$$

After dividing by the size of the point set, which has t levels, this gives a quadratic gain in t. The archimedean term in (2) grows as $\log(tD)$. Taking t of order $\sqrt{\log(2D)}$ makes the quadratic gain cover that term in (8). The multiplier A_t of the height in (8) grows exponentially in t, which accounts for the factor $\exp(-C\sqrt{\log(2D)})$ in the lower bound.

The square roots thus arise from different estimates. In the Riemann hypothesis argument a longer chain reduces one normalized error and increases another. For elliptic heights one takes enough levels for their pairwise contact to exceed a logarithmic error at infinity. In each case the choice of length is dictated by the global inequality that receives the local contribution.

3.4 Dimitrov's proof of Schinzel–Zassenhaus

Dimitrov's argument also begins with a congruence between two levels of an orbit. Here the orbit consists of the conjugates $\alpha_1, \ldots, \alpha_n$ of a nonzero algebraic integer α, and the two levels consist of their squares and their fourth powers. Write $R(\alpha) = \max_i |\alpha_i|$ for the house of α. Dimitrov proves that if α is not a root of unity, then

$$\log R(\alpha) \geq \frac{\log 2}{4n}.$$

The order $1/n$ is sharp, since $X^n - 2$ is Eisenstein at 2 and its roots have house $2^{1/n}$. The number $\log 2/4$ in Dimitrov's theorem is an explicit universal coefficient, and the capacity calculation below explains its value [37, 15]. To distinguish it from the largest possible coefficient, write $c_* = \inf_\alpha [\mathbf{Q}(\alpha) : \mathbf{Q}] \log R(\alpha)$ over nonzero algebraic integers of infinite multiplicative order. Boyd conjectured $c_* =$

$(3/2)\log\theta$, where θ is the real root of $X^3 - X - 1$. In fact the degree-three example with minimal polynomial $X^3 + X^2 - 1$ already gives the corresponding upper bound. Its real root is $1/\theta$ and its two complex roots have absolute value $\sqrt{\theta}$ [10].

The congruence gives an integral germ. For $j \geq 1$ put $P_j(T) = \prod_{i=1}^{n}(1 - \alpha_i^j T) \in \mathbf{Z}[T]$. The congruence $P_4 \equiv P_2 \pmod 4$ is the arithmetic input. Thus $P_2 P_4$ is a square modulo 4, and its square root with constant term 1 satisfies

$$f(T) = \sqrt{P_2(T)P_4(T)} = P_2(T)\sqrt{1 + 4W(T)} \in \mathbf{Z}[[T]], \qquad W = \frac{P_4 - P_2}{4P_2} \in T\mathbf{Z}[[T]].$$

The binomial series for $\sqrt{1 + 4W}$ is integral. The extra factor of 2 in the congruence matters because it makes the square root integral at the prime 2 [16, Lemma 2.1 and Proposition 2.2]. In our two-orbit calculation a congruence between the two monic polynomials gives a lower bound for the valuations of their evaluations. In Dimitrov's calculation the congruence makes *every* Taylor coefficient of an auxiliary germ an integer.

Capacity gives a rationality threshold. The possible finite branch points of $f(1/z)$ away from zero lie among the α_i^2 and α_i^4. Join each to the origin by a radial segment and denote the union by C. The complement of C in the sphere is simply connected, and the germ at infinity is holomorphic there. All the segments have length at most $R(\alpha)^4$, since $R(\alpha) \geq 1$. Dubinin's theorem bounds the logarithmic capacity of a union of k radial segments of length at most u by $u\,4^{-1/k}$. Since there are at most $2n$ segments, it gives

$$\operatorname{cap}(C) \leq R(\alpha)^4\, 4^{-1/(2n)}.$$

The factor $4^{-1/k}$ is sharp for a regular arrangement of k equal segments. In that arrangement the union is a polynomial inverse image of a single segment, whose capacity is one quarter of its length [18][16, Theorem 3].

The Pólya–Bertrandias rationality criterion says that an integral Laurent expansion at infinity which continues holomorphically to the connected complement in the sphere of a compact set of capacity less than one is rational. In its determinant proof, the Hankel determinants of the coefficients are integers. The capacity estimate makes the large determinants smaller than one in absolute value, so they vanish. Kronecker's criterion for Hankel determinants then gives a linear recurrence for the coefficients [16, Theorem 4 and Corollary 5]. Thus $4\log R(\alpha) < \log 4/(2n)$ forces f to be rational.

Here is how the proof excludes that outcome. If squaring preserves the degree, P_2 is irreducible over $\mathbf{Q}$ and $P_2 P_4$ can be a square only if $P_2 = P_4$. Equality would give $R(\alpha)^2 = R(\alpha)^4$, hence $R(\alpha) = 1$ and α would be a root of unity by Kronecker's theorem. If the degree drops on squaring, it is halved, since $[\mathbf{Q}(\alpha) : \mathbf{Q}(\alpha^2)] \leq 2$. Then $[\mathbf{Q}(\alpha^2) : \mathbf{Q}]\log R(\alpha^2) = n\log R(\alpha)$, and one applies induction to α^2. The degree drops therefore leave the same threshold for $n\log R(\alpha)$ [16, proof of Theorem 1].

Why two levels suffice. The capacity bound gives a definite threshold using the squares and fourth powers alone. There is no chain length to choose. This parallels the two-orbit proof in characteristic p, where a fixed choice of formal multiplication makes the local contact cover a bounded error. In the number-field Lehmer proof, the global quantity is an average of local heights and the error after normalization contains $\frac{1}{2}\log N$. There the number of levels grows to cover that error. Dimitrov's hypothesis controls the largest conjugate, which controls all the branch points at once. An average is weaker information about their locations. For an algebraic integer the identity

$$h(\alpha) = \frac{1}{n}\sum_i \log^+ |\alpha_i|$$

shows that using the house bound alone gives $h(\alpha) \geq (\log 2)/(4n^2)$. The same distinction appears in Habegger and Schmidt's dynamical extension, which gives inverse degree for the maximum escape rate and inverse square degree for the canonical height under their hypotheses [25, Theorem 1.1].

There is a numerical constant which the same argument does make sharp. In Dimitrov's power-series theorem, a nonrational integral power series satisfying a linear differential equation with at most k finite singularities has coefficient growth $\log^+(1/\rho) \geq (\log 4)/k$, where ρ is its radius of convergence. The germ $\sqrt{1-4T}$ has integral coefficients, one finite singularity for its differential equation, and radius $1/4$. Its reflected branch point gives exactly the radial segment $[0, 4]$ of capacity one [16, Theorem 7].

4 How Frobenius increases contact

We now fix a place v of good supersingular reduction. Its residue characteristic is p. We write q_v for its residue cardinality and $Q = p^2$ for the degree of $[p]$. The two numbers play different roles. If Φ is the q_v-power Frobenius on the special fiber, there are integers $h, s \geq 1$ such that

$$\Phi^h = [m], \qquad m = p^s. \tag{3}$$

Indeed $[q_v]$ and Φ^2 are purely inseparable isogenies of degree q_v^2. Over the perfect residue field they both factor through the relative q_v^2-power Frobenius followed by an isomorphism [46, Tag 0CCZ]. Hence $\Phi^2 = \alpha[q_v]$ for some automorphism α fixing O. This automorphism has finite order [40, Ch. III, Theorem 10.1] and commutes with $[q_v]$. Raising the equality to its order gives (3). We choose a positive scalar here so the same notation works for all residue fields.

Two elementary facts will let us turn equality of reductions into an estimate. The first gives the initial depth. Suppose A and B lie in two local extensions of ramification index at most e, and reduce to the same point. Both extensions contain the unramified field corresponding to the field of definition of that residue point. By smoothness, the point has a lift C over this unramified field [40, Ch. VII, Propositions 2.1–2.2]. The formal parameters of $A - C$ and $B - C$ each have valuation at least $1/e$. Subtracting in the integral formal group law gives

$$b(z(A - B)) \geq 1/e. \tag{4}$$

The common lift matters here. The compositum of the fields of A and B can have ramification index greater than e.

The second fact describes what happens to this initial depth under multiplication. For a point X reducing to O, abbreviate $b(z(X))$ to $b(X)$ and set $b(O) = +\infty$. The reduced formal group has height two [40, Ch. V, Theorem 3.1]. Consequently all coefficients of $[p](z)$ in degrees below Q lie in the maximal ideal. The remaining coefficients are integral, so

$$b([p]X) \geq \min\{Qb(X), 1 + b(X)\}.$$

Starting from a lower bound $b_* > 0$, after a multiplications this gives at least $x = \min\{1, Q^a b_*\}$. Each subsequent multiplication adds at least x to the lower bound. Indeed, if the bound has reached ℓx with $\ell \geq 1$, both $Q\ell x$ and $1 + \ell x$ are at least $(\ell + 1)x$. We shall use the result in the form

$$b([p^{a+j}]X) \geq (j + 1) \min\{1, Q^a b_*\}, \qquad j \geq 0. \tag{5}$$

5 Counting conjugates at two levels

Choose a finite torsion field $L = K(E[n])$, with $(n, p) = 1$, at which the degree of P has already fallen to $D = [F(P) : F]$. To see that one exists, take a K-basis of $K(P)$. The rank of its span

over F is determined by finitely many linear relations, whose coefficients all belong to some such L. Write $J = L(P)$, let J_s be its maximal separable subextension over L, and put

$$D_s = [J_s : L], \qquad I = [J : J_s], \qquad D = D_s I.$$

There are exactly D_s conjugates of P over L. Denote their set by S. The count uses these D_s conjugates. The factor I will enter through ramification. In characteristic zero $I = 1$. In the function-field case $J = J_s^{1/I}$ inside the chosen algebraic closure. Indeed $J \subseteq J_s^{1/I}$ by pure inseparability, and $[J_s^{1/I} : J_s] = I$ since J_s has p-rank one [46, Tag 0CCF]. At any place an Ith root of a uniformizer therefore lies in J. The local ramification index is multiplied by I, with the same residue field.

Good reduction makes L/K unramified at v. Reduction identifies the prime-to-p torsion of the generic and special fibers [40, Ch. VII, Proposition 3.1 and Theorem 4.1]. Thus at every place of L over v the hth power of arithmetic Frobenius has the same action $[m]$ on $E[n]$. This action determines a single element of $\mathrm{Gal}(L/K)$. Choose a lift τ to the absolute Galois group and extend it across purely inseparable elements. Locally at any prolongation w of v, let δ be a decomposition-group lift acting on residues by Φ^h. We can use δ in place of τ in forming $\tau^{-i}S$, for they have the same restriction to L. In particular $[m^i]\delta^{-i}U$ has the same reduction as U at w for every $U \in S$.

How many distinct points to count

Fix the number $t \geq 2$ of levels. Before taking the first level we multiply each conjugate by p a total of a times. We shall choose a below. The points of level i are

$$Z_i = [p^a m^i]\tau^{-i} S, \qquad 0 \leq i < t.$$

Points in different levels have different heights, since their heights are $Q^a m^{2i}\widehat{h}(P)$ and $\widehat{h}(P) > 0$. Within a level, two conjugates may have the same image. Let r_j be the number of conjugates above a given point of $[p^j]S$. All fibers have this size by Galois transitivity. As j increases, r_j is nondecreasing. For a given a, the last level thus has the fewest points, each with $r = r_{a+s(t-1)}$ original conjugates above it.

The depth that will occur in the count is $1/(Ir)$. We would like the preliminary multiplications to raise it to one. By (5) it suffices to have $Q^a \geq Ir$. Changing a also changes the last level, so we choose the first $a \geq 0$ for which

$$Q^a \geq I r_{a+s(t-1)}. \tag{6}$$

This choice exists because the right side is at most D. Write $d = D_s/r$ for the number of distinct points in the last level, and put $H = Q^a/(Ir)$. Then $1 \leq H < Q$. For $a > 0$, minimality gives $Q^{a-1} < I r_{a-1+s(t-1)} \leq Ir$. For $a = 0$, both I and r are one.

From each level take a subset $Y_i \subset Z_i$ of d distinct points. We average uniformly over all such choices, independently at different levels. This has a simple counting interpretation. At a fixed w the map $f_i(U) = [p^a m^i]\delta^{-i}U$ takes a uniformly chosen conjugate in S to a uniformly chosen point of Z_i, since every fiber has the same size. Hence, for $i < j$,

$$\mathbb{E} \sum_{A \in Y_i,\, B \in Y_j} i_w(A, B) = \left(\frac{d}{D_s}\right)^2 \sum_{U,V \in S} i_w(f_i(U), f_j(V)). \tag{7}$$

On the right we can count every ordered pair of original conjugates, even when several pairs give the same image. The prefactor accounts for all such repetitions.

Where the pairs come from

Lemma 2. *For every prolongation w of v and every $i < j$ the average in (7) is at least $dH(i+1)/(4Q)$.*

Proof. Take $U, V \in S$ with the same reduction at w. Undoing $j-i$ Frobenius actions and then applying $[m^{j-i}]$ gives a point $V' = [m^{j-i}]\delta^{-(j-i)}V$ with that same reduction. We can therefore apply our depth estimate to $U - V'$. Its relation to the two points we want to compare is

$$f_i(U) - f_j(V) = [p^a m^i]\delta^{-i}(U - V').$$

The local automorphism preserves depth. The factor $m^i = p^{si}$ thus gives at least i further multiplications after the first a. It remains to find sufficiently many pairs U, V and to bound their initial depths.

Fix the embedding of L determined by w. A place of J_s above it with ramification index e and residue degree f accounts for fe embeddings of J_s, each of which extends uniquely to J. Group these embeddings according to their restrictions to the maximal unramified subextension of the local field. There are f groups of e embeddings, and all embeddings within a group induce the same residue map. The field of definition of the corresponding conjugate has local ramification index Ie over K_v. The same upper bound holds after applying δ and an integer multiplication.

Suppose first that at least half the conjugates have $e \geq r$. A place of this kind gives fe^2 ordered pairs within its residue groups. Their initial depths are at least $1/(Ie)$ by (4). Since $Q^a/(Ie) \leq H < Q$, formula (5) gives each pair a final depth of at least

$$(i+1)\frac{Q^a}{QIe}.$$

This explains why large ramification is harmless here. The factor e in the denominator is recovered from the e partners available to each embedding. Summing over these places, for which $\sum fe \geq D_s/2$, gives a sum of at least $(i+1)D_sQ^a/(2QI)$ over ordered pairs of conjugates.

In the other case at least half the conjugates have $e < r$. For these conjugates (4) gives all the depth we need once we find two conjugates in the same residue disk. To find such pairs, sort the conjugates by their images under $[p^{a+s(t-1)}]$. Two in the same fiber differ by a point of p-power order. Every such point reduces to O, since the supersingular special fiber has no nonzero geometric p-power torsion. Write n_B for the number of selected conjugates in fiber B. With d fibers, Cauchy's inequality gives

$$\sum_B n_B^2 \geq \frac{(D_s/2)^2}{d} = \frac{D_s r}{4}.$$

Each of these pairs has initial depth at least $1/(Ir)$, even if the two local fields are different. We chose a so that $Q^a/(Ir) \geq 1$. Its final depth is therefore at least $i+1$. Using $H < Q$, we get a sum of at least $(i+1)D_sQ^a/(4QI)$.

The latter bound holds in both cases. Multiplying by $(d/D_s)^2$ in (7) proves the lemma. The pairs we used may depend on w. The average itself runs through the same finite collection of global sets at every place. □

6 Choosing the length of the tower

Let $Y = \bigcup_{i=0}^{t-1} Y_i$, which has exactly $N = dt$ points. Each pair of levels occurs in two orders. Discarding the nonnegative contacts within a level and summing Lemma 2 over the others gives

$$\frac{1}{N}\mathbb{E}\,\mathcal{I}_v(Y) \geq \frac{\omega_v H}{12Q}(t^2-1), \qquad \text{since} \qquad \sum_{0 \leq i < j < t} (i+1) = \frac{t(t^2-1)}{6}.$$

On the height side there is no dependence on which d points we chose. All points of Y_i have height $Q^a m^{2i}\widehat{h}(P)$. If $A_t = 1 + m^2 + \cdots + m^{2(t-1)}$, the right side of (1), divided by N, is $2dQ^a A_t \widehat{h}(P)$. All choices lie in one finite extension, so we may apply (1) there and take the average. Using $dQ^a = DH$, $H \geq 1$, and $d \leq D$, we arrive at

$$2DA_t\widehat{h}(P) \geq \frac{\omega_v}{12Q}(t^2-1) - \mathcal{E}_K(tD). \tag{8}$$

The quadratic term has a concrete origin. There are on the order of t^2 pairs of levels, and the contact in the pair $i < j$ grows with $i+1$. After dividing by the number of points, this leaves a gain of order t^2. Increasing t also increases the height multiplier A_t, so we take the first convenient value of t for which the right side is positive.

Over a function field. We must first find the place v. Pass to a fixed finite separable extension K_0/K over which E has semistable reduction. For example, Raynaud's criterion permits $K_0 = K(E[\ell])$ for a prime $\ell \geq 5$ different from p [38, Theorem 3.4]. Since j_E is nonconstant it maps the complete base curve of K_0 onto $\mathbf{P}^1$. A point above any supersingular j-value gives the desired place. Its j-value is finite, whereas a multiplicative fiber would give a pole [40, Ch. VII, Proposition 5.5].

Apply (8) over K_0. Its error term is $h_{K_0}(j_E)/12$, independent of the degree of P. Choose $t \geq 2$ once, so that

$$\frac{\omega_v}{12Q}(t^2-1) \geq 1 + h_{K_0}(j_E)/12.$$

This gives $\widehat{h}_{E,K_0}(P) \geq 1/(2A_t[K_0F(P) : K_0F])$. Write k_0 for the full constant field of K_0. Base extension can only decrease the relative degree, and

$$\widehat{h}_{E,K}(P) = \frac{[k_0 : \mathbf{F}_q]}{[K_0 : K]}\widehat{h}_{E,K_0}(P).$$

This proves the inverse-degree bound over K with a constant depending for now on E/K. The uniform constant in the theorem is obtained below.

Over a number field. Here the term $\frac{1}{2}\log(tD)$ in (2) determines how long the tower must be. Write $b_0 = \omega_v/(12Q)$ and $C_0 = h(j_E)/12 + 16/5$. Choose an integer $T \geq 2$ large enough that

$$b_0(t^2-1) - \tfrac{1}{2}\log t - C_0 \geq \tfrac{1}{2}b_0 t^2 \qquad (t \geq T).$$

It suffices to take

$$t = \max\left(T, \left\lceil \sqrt{(\log D + 2)/b_0} \right\rceil\right).$$

With this choice the right side of (8) is at least one. Since $A_t = (m^{2t}-1)/(m^2-1)$ and $t \ll_{E,K,v} \sqrt{\log(2D)}$, we get

$$\widehat{h}_E(P) \geq \frac{1}{2DA_t} \geq \frac{c}{D}\exp\left(-C\sqrt{\log(2D)}\right).$$

The inequality $C\sqrt{x} \leq \epsilon x + C^2/(4\epsilon)$, applied to $x = \log(2D)$, gives the asserted $D^{-1-\epsilon}$ bound with $c_\epsilon = c\,2^{-\epsilon}e^{-C^2/(4\epsilon)}$. If good supersingular reduction is acquired over a fixed finite extension K_0/K, the same conclusion follows by applying the bound over K_0. The absolute height is invariant under this extension and $[K_0F(P) : K_0F] \leq D$.

The constant over finite fields

The dependence on the function field and on the curve can both be removed by doing the calculation once on a curve with indeterminate j-invariant. Choose $E_*/\mathbf{F}_p(T)$ with $j(E_*) = T$ [40, Ch. III, Proposition 1.4] and let F_* be its prime-to-p torsion field. Denote by $c_* > 0$ the constant just proved for this curve. The Weil pairing puts every root of unity of order prime to p in F_* [40, Ch. III, Corollary 8.1.1], so F_* contains $\overline{\mathbf{F}}_p$.

Identify T with $j_E \in K$ and write $\Delta = [K : \mathbf{F}_q(j_E)]$. The curves E_* and E become isomorphic over an extension K'/K of degree at most two. Indeed, the automorphisms fixing O for a curve with nonconstant j are $\{\pm 1\}$, including in characteristics 2 and 3 [40, Ch. III, Theorem 10.1]. Write P_* for the point corresponding to P. The isomorphism identifies their torsion fields after base change, so $F_*K' = FK'$. We obtain

$$[F_*(P_*) : F_*] \le [F_*K' : F_*]\,[F_*K'(P_*) : F_*K'] \le 2\Delta D.$$

On the other hand, $\widehat{h}_{E,K}(P) = \Delta\,\widehat{h}_{E_*,\mathbf{F}_p(T)}(P_*)$. To see this, compare the two heights over K' and use the fact that base change multiplies a divisor-degree height by the field degree divided by the degree of the extension of constants. The fundamental equality for valuations gives this scaling even when $K/\mathbf{F}_q(j_E)$ has an inseparable part [48, Theorem 3.1.11]. The factor Δ in the height cancels the one in the degree bound, leaving $c_p = c_*/2$. This finishes the proof of Theorem 1.

For an isotrivial elliptic curve over finite constants one can prove the inverse-degree bound directly, with a constant depending on E/K. Take a finite extension K_0/K over which E becomes a constant curve E_0/k_0. Its prime-to-p division fields over K_0 are constant extensions. Choose such an L realizing $[L(P) : L] = [K_0F(P) : K_0F]$ and set $M = L(P)$. On the complete curve with function field M and full constant field k_M, the point P gives a morphism f to E_0. It is nonconstant because every constant point over $\overline{\mathbf{F}}_p$ is torsion. Pulling back (O) gives

$$\widehat{h}_{E,K_0}(P) = \frac{[k_M : k_0]}{[M : K_0]} \deg f \ge \frac{1}{[M : L]}.$$

Indeed $[k_M : k_0] \ge [L : K_0]$ since L/K_0 is constant. The height scaling above brings the inequality back to K.

Which torsion field enters in characteristic p

Let E again be non-isotrivial. Over a function field there is a further distinction between the field F used above, the field of all separably defined torsion, and the field of all geometric torsion. The separable p-primary torsion has bounded exponent by the argument in the next section, so adjoining it to F gives a finite extension. If T_{sep} is the field of all separably defined torsion, then $[F(P) : F] \le [T_{\mathrm{sep}} : F][T_{\mathrm{sep}}(P) : T_{\mathrm{sep}}]$. Thus the inverse-degree bound holds over T_{sep} with a constant allowed to depend on E/K.

The geometric p-power torsion changes the degree in a different way. Put $T = K(E(\overline{K})_{\mathrm{tors}})$. Since the non-isotrivial curve is generically ordinary, there are geometric points of order p^n for every n. If U has order p^n, then the dual of the quotient by $\langle U \rangle$ factors through the n-fold relative Frobenius over $K(U)$. Consequently $j_E^{1/p^n} \in K(U) \subset T$ [23, Lemma 14 and the following remark]. The case $n = 1$ is also in [49, Lemma 4.1]. Write $j_E = u^{p^b}$ with $u \in K \setminus K^p$. Since K has p-rank one, $K(u^{1/p^n}) = K^{1/p^n}$ for every n. Thus T contains the perfect closure of K and is itself perfect.

Now fix a non-torsion algebraic point A and choose $[p^n]P_n = A$. There are p^n geometric points in the fiber because E is ordinary. As $T(A)$ is perfect, this gives

$$[T(P_n) : T] \le [T(A) : T]p^n, qquad\widehat{h}(P_n) = p^{-2n}\widehat{h}(A).$$

In particular $[T(P_n) : T]\widehat{h}(P_n)$ tends to zero. This explains why the inverse-degree estimate for all algebraic points uses prime-to-p torsion or separably defined torsion in characteristic p.

7 A shorter proof for separable points in characteristic p

If P is separable over a function field and E is non-isotrivial, two orbits suffice. There are two reasons. A fixed multiplication removes all separable p-power torsion, and in equal characteristic each further multiplication by p multiplies every positive depth by at least p.

Work over the fixed semistable base of the function-field proof. Let b be the largest integer for which $j_E \in K^{p^b}$. This integer is finite since a pole order of j_E must then be divisible by p^b. Suppose a point of order p^n is rational over a finite separable extension K'/K. Quotient by the cyclic group it generates. The dual isogeny has kernel μ_{p^n}, hence is purely inseparable of degree p^n and identifies $E_{K'}$ with a p^n-Frobenius twist. Consequently $j_E^{1/p^n} \in K' \cap K^{\mathrm{perf}} = K$, so $n \le b$, as in the remark following Lemma 14 of Goldfeld and Szpiro [23], who credit Voloch with the observation. See also Zou [49, Lemma 4.1] for the equivalence at level p. It follows that multiplication by p is injective on $[p^b]E(K^{\mathrm{sep}})$.

Set $R = [p^b]P$. Let S be its orbit over a finite torsion field L realizing $d = [F(R) : F]$, and set $S' = [m]\tau^{-1}S$. Both orbits have d points and their positive heights differ. By (3), they have the same reductions with the same multiplicities at each $w \mid v$. Take a residue point occurring n times in each orbit, and lift it to a point C in an unramified extension of the completion of L. Using $z(X-C)$ as coordinate, form the monic polynomials A and B whose roots are the points of S and S' in this disk. Their coefficients lie in the unramified valuation ring, since the absolute Galois group of its fraction field fixes C and permutes the roots of each polynomial. Since both reduce to Z^n, their difference is divisible by π_v.

Evaluating at a root x of A now gives

$$\sum_{B(y)=0} b_v(x-y) = b_v(B(x)) = b_v\big((B-A)(x)\big) \ge 1, \qquad b_v = \mathrm{ord}_v\,.$$

Formal subtraction is $(X - Y)$ times a unit [33, (21)], so this is also the sum of the depths of the corresponding group differences. Summing over x and the residue disks gives at least d in total. The estimate permits fractional contact between individual pairs.

In characteristic p, pulling an invariant differential back by $[p]$ gives zero [40, Ch. III, Corollary 5.3]. Thus the derivative of the formal series $[p](Z)$ vanishes and all of its exponents are divisible by p. If M is a power of p, applying $[M]$ multiplies the lower bound for total contact by M. All $2d$ points remain distinct. Substituting the two amplified orbits in (1) and dividing by $2d$ gives

$$\omega_v M - \frac{h_K(j_E)}{12} \le 2dM^2(1+m^2)p^{2b}\widehat{h}_{E,K}(P).$$

Choose M once so that the left side is positive. Since $d \le [F(P) : F]$, this proves the desired bound.

References

[1] J. Adriazola, *An End-to-End Reconstruction of the Alpöge–Claude Route to the Riemann Hypothesis*, working manuscript, 2026.

[2] L. Alpöge, Note announcing the Alpöge–Claude argument for the Riemann hypothesis, 20 November 2026, announcement, p. 1.

[3] F. Amoroso and U. Zannier, *A relative Dobrowolski lower bound over abelian extensions*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) 29 (2000), 711–727. Numdam.

[4] M. Anderson and D. W. Masser, *Lower bounds for heights on elliptic curves*, Math. Z. 174 (1980), 23–34. DOI.

[5] M. Baker, *Lower bounds for the canonical height on elliptic curves over abelian extensions*, Int. Math. Res. Not. (2003), 1571–1582. arXiv:math/0212132.

[6] M. Baker and C. Petsche, *Global discrepancy and small points on elliptic curves*, Int. Math. Res. Not. (2005), 3791–3834. arXiv:math/0507228.

[7] M. Baker and J. H. Silverman, *A lower bound for the canonical height on abelian varieties over abelian extensions*, Math. Res. Lett. 11 (2004), 377–396. arXiv:math/0312393.

[8] E. Bombieri, *Counting points on curves over finite fields*, Séminaire Bourbaki, exp. 430 (1973), 234–241. Numdam.

[9] J.-B. Bost, *Périodes et isogénies des variétés abéliennes sur les corps de nombres*, Séminaire Bourbaki, Exp. 795, Astérisque 237 (1996), 115–161. Numdam.

[10] D. W. Boyd, *The maximal modulus of an algebraic integer*, Math. Comp. 45 (1985), 243–249. DOI.

[11] M. Carrizosa, *Problème de Lehmer et variétés abéliennes CM*, C. R. Math. Acad. Sci. Paris 346 (2008), 1219–1224. DOI.

[12] M. Carrizosa, *Petits points et multiplication complexe*, Int. Math. Res. Not. (2009), 3016–3097. DOI.

[13] S. Chowla and A. Selberg, *On Epstein's zeta-function*, J. Reine Angew. Math. 227 (1967), 86–110. DOI.

[14] S. David and M. Hindry, *Minoration de la hauteur de Néron–Tate sur les variétés abéliennes de type C.M.*, J. Reine Angew. Math. 529 (2000), 1–74. DOI.

[15] V. Dimitrov, *The Schinzel–Zassenhaus conjecture*, Ann. of Math., forthcoming. Journal record.

[16] V. Dimitrov, *A proof of the Schinzel–Zassenhaus conjecture on polynomials*, arXiv:1912.12545v1 (2019). The internal numbering cited in Section 3.4 refers to this version.

[17] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arith. 34 (1979), 391–401. DOI.

[18] V. N. Dubinin, *On the change in harmonic measure under symmetrization*, Math. USSR-Sb. 52 (1985), 267–273. DOI.

[19] N. D. Elkies, *The existence of infinitely many supersingular primes for every elliptic curve over* $\mathbf{Q}$, Invent. Math. 89 (1987), 561–567.

[20] N. D. Elkies, *Supersingular primes for elliptic curves over real number fields*, Compos. Math. 72 (1989), 165–172. Numdam.

[21] A. Galateau and V. Mahé, *Some consequences of Masser's counting theorem on elliptic curves*, Math. Z. 285 (2017), 613–629. DOI.

[22] É. Gaudron and G. Rémond, *Nombre de petits points sur une variété abélienne*, J. Inst. Math. Jussieu 24 (2025), 705–761. DOI.

[23] D. Goldfeld and L. Szpiro, *Bounds for the order of the Tate–Shafarevich group*, Compos. Math. 97 (1995), 71–87. Numdam.

[24] P. Habegger, *Small height and infinite nonabelian extensions*, Duke Math. J. 162 (2013), 2027–2076. arXiv:1109.5859.

[25] P. Habegger and H. Schmidt, *Lower bounds for the canonical height of a unicritical polynomial and capacity*, Forum Math. Sigma 12 (2024), e45, 1–20. DOI.

[26] M. Hindry and J. H. Silverman, *The canonical height and integral points on elliptic curves*, Invent. Math. 93 (1988), 419–450. Article.

[27] M. Hindry and J. H. Silverman, *On Lehmer's conjecture for elliptic curves*, Séminaire de Théorie des Nombres, Paris 1988–1989, Progr. Math. 91, Birkhäuser, Boston, 1990, pp. 103–116.

[28] M. Laurent, *Minoration de la hauteur de Néron–Tate*, Séminaire de Théorie des Nombres, Paris 1981–1982, Progr. Math. 38, Birkhäuser, Boston, 1983, pp. 137–151.

[29] D. H. Lehmer, *Factorization of certain cyclotomic functions*, Ann. of Math. (2) 34 (1933), 461–479. DOI.

[30] D. W. Masser, *Counting points of small height on elliptic curves*, Bull. Soc. Math. France 117 (1989), 247–265. DOI.

[31] A. Pacheco, *Integral points on elliptic curves over function fields of positive characteristic*, Bull. Austral. Math. Soc. 58 (1998), 353–357. DOI.

[32] A. Pacheco, *Analogues of Lehmer's problem in positive characteristic*, arXiv preprint (2003), math/0011102v6.

[33] C. Petsche, *Nonarchimedean equidistribution on elliptic curves with global applications*, Pacific J. Math. 242 (2009), 345–375. DOI.

[34] A. Plessis, *Bogomolov property of some infinite nonabelian extensions of a totally v-adic field*, Acta Arith. 213 (2024), 1–23. DOI.

[35] N. Ratazzi, *Théorème de Dobrowolski–Laurent pour les extensions abéliennes sur une courbe elliptique à multiplication complexe*, Int. Math. Res. Not. (2004), 3121–3152. DOI.

[36] S. Sahu, *Supersingular primes and Bogomolov property*, preprint, arXiv:2504.13498, 2025.

[37] A. Schinzel and H. Zassenhaus, *A refinement of two theorems of Kronecker*, Michigan Math. J. 12 (1965), 81–85.

[38] A. Silverberg and Yu. G. Zarhin, *Semistable reduction and torsion subgroups of abelian varieties*, Ann. Inst. Fourier 45 (1995), 403–420. DOI.

[39] J. H. Silverman, *A lower bound for the canonical height on elliptic curves over abelian extensions*, J. Number Theory 104 (2004), 353–372. arXiv:math/0305041.

[40] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., Grad. Texts in Math. 106, Springer, 2009. DOI.

[41] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Grad. Texts in Math. 151, Springer, 1994. DOI.

[42] J. H. Silverman, *Lehmer's conjecture for polynomials satisfying a congruence divisibility condition and an analogue for elliptic curves*, J. Théor. Nombres Bordeaux 24 (2012), 751–772. DOI.

[43] J. H. Silverman, *A Lehmer-type lower bound for the canonical height on elliptic curves over function fields*, J. Number Theory 262 (2024), 506–538. arXiv:2402.14771.

[44] J. H. Silverman, *Corrigendum to A Lehmer-type lower bound for the canonical height on elliptic curves over function fields*, J. Number Theory 279 (2026), 267–269. DOI.

[45] J. H. Silverman, *Canonical heights on abelian varieties*, Arizona Winter School lecture notes, 2024. Lecture notes.

[46] The Stacks Project Authors, *The Stacks Project*, Lemmas 33.36.10 and 53.13.4, Tag 0CCF and Tag 0CCZ.

[47] S. A. Stepanov, *On the number of points of a hyperelliptic curve over a finite prime field*, Math. USSR-Izv. 3 (1969), 1103–1114. DOI.

[48] H. Stichtenoth, *Algebraic Function Fields and Codes*, 2nd ed., Grad. Texts in Math. 254, Springer, 2009.

[49] H. Zou, *Rational multisections and unirationality of supersingular K3 surfaces*, preprint, arXiv:2611.26115, 2026.