

A linear-in-rank bound for integral arithmetic progressions on elliptic curves

Jake Crim

October 2026

Abstract

Every known bound on the length N of an x -progression on an elliptic curve of rank r has the shape $N \leq C^{1+r}$. We prove a bound that is linear in the rank for *integral* progressions, with an error depending only on the height of the model. Let $y^2 = x^3 + a_2x^2 + a_4x + a_6$ be an integral model and $H_f = 1 + |a_2| + |a_4| + |a_6|$. For every $\varepsilon > 0$, every integral x -progression of length N satisfies

$$N \leq \left(\frac{3}{2} + \varepsilon\right)s + C_\varepsilon \sqrt{1 + \log H_f},$$

where $s \leq r$ is the rank of the span of the progression. In particular $N \leq \left(\frac{3}{2} + o(1)\right)s$ whenever $\log H_f = o(N^2)$.

The proof has two halves.

- The *local theory* consists of exact point counts, the root-class lemma, pinned values, and a forbidden range of primes reaching $N^2/49$ by a shift-and-square argument. It forces $\log |b| \gg N^2$, where b is the common difference.
- The *spectral cap* is proved in an exact form. Splitting the Néron–Tate pairing into local kernels of positive type and summing the regularised diagonal terms over all places gives an identity in which the bad-prime corrections cancel. Combined with a uniform archimedean separation lemma, this yields $\lambda_{\max}(G) \leq \frac{3}{4} \log X + \frac{1}{4} \psi(N-1) + \frac{5}{4} \log H_f + 2$, where $X = \max |x_i|$.

Over function fields we prove an exact colouring formula for the Gram matrix of a progression of integral sections, which gives $N \leq \min(6\chi, \frac{3}{2}s)$. We also classify the 3-term Gram types on rational elliptic surfaces and show that all of them occur, and we show that all sign data are realised on elliptic $K3$ surfaces. The main bound is vacuous for every known example (all have $N \leq 14$); its interest is that it is linear rather than exponential in the rank.

2020 Mathematics Subject Classification. 11G05, 11G50, 11B25, 14J27.

Keywords. Elliptic curves, arithmetic progressions, canonical height, local heights, Mordell–Weil lattice, Bremner’s conjecture.

Contents

1	Introduction	2
2	Setting	3
3	Point counts, root classes and pinned values	4
4	The forbidden range	5

5	Primes dividing the common difference	8
6	Denominators of non-integral progressions	10
7	The trace inequality	10
8	Local kernels of positive type	11
8.1	An antisymmetrised positivity lemma	11
8.2	Local heights	11
8.3	Non-archimedean kernels	12
8.4	The archimedean kernel	13
8.5	The general cap and the exact diagonal	14
8.6	Archimedean separation	15
8.7	Integral progressions	16
9	The linear bound	18
10	Function fields: the exact version	19
10.1	Realising sign data: rational and $K3$ surfaces	21
11	Relation to earlier work	23
12	Comparison with the exponential bounds	24
13	Open problems	25
A	Computations	25

1 Introduction

Let $E/\mathbb{Q}$ be an elliptic curve given by a Weierstrass equation. An x -progression of length N is a sequence of points $P_0, \dots, P_{N-1} \in E(\mathbb{Q})$ whose x -coordinates form a non-constant arithmetic progression. Bremner [2] observed that such points tend to be independent in the Mordell–Weil group, and conjectured that long progressions force large rank. This was motivated in part by [3], where it is shown that the curves $y^2 = x(x^2 - n^2)$ of rank one have no non-trivial integral progressions. Garcia-Fritz and Pasten [7] proved this for families with fixed j -invariant, in the form $1+r \geq c(j_0) \log N$. Combined with the uniform Mordell–Lang theorem of Gao–Ge–Kühne [6], their method gives $N \leq c^{1+r}$ [9]; Harrison, Mudgal and Schmidt [10] give another proof with an effective absolute constant. All of these bounds are exponential in the rank.

In this paper we prove a bound that is *linear* in the rank for *integral* progressions, at the cost of a mild dependence on the height of the model. Write the model as

$$y^2 = x^3 + a_2x^2 + a_4x + a_6, \quad a_k \in \mathbb{Z}, \quad H_f = 1 + |a_2| + |a_4| + |a_6|, \quad (1)$$

and let s be the rank of the subgroup generated by the progression, so $s \leq r = \text{rank } E(\mathbb{Q})$.

Theorem 1.1. *For every $\varepsilon > 0$ there is an effective constant C_ε such that every integral x -progression of length N on (1) satisfies*

$$N \leq \left(\frac{3}{2} + \varepsilon\right)s + C_\varepsilon \sqrt{1 + \log H_f}.$$

In particular $N \leq (\frac{3}{2} + o(1))s$ along any sequence of progressions with $\log H_f = o(N^2)$.

The result also holds for every integral cubic model (Remark 8.14). It is Corollaries 9.3 and 9.4 below. The proof has two halves.

Local theory (Sections 3–6). A progression of length N reduces to too many points modulo small good primes. Combining exact point counts with a root-class lemma and Hasse’s bound, and then a shift-and-square argument based on Weil’s bound, we show that every prime $5 \leq p \leq ((N - 77)/7)^2$ divides $2b \operatorname{lc}(f) \operatorname{disc}(f)$ (Theorem 4.4). Hence $\log |b| \gg N^2$, so the points of a long progression have large height.

Spectral cap (Sections 7–8). Let G be the Gram matrix of the Néron–Tate pairing on the progression. Since $\operatorname{rank} G = s$, the trace inequality $\operatorname{tr} G \leq s \lambda_{\max}(G)$ bounds N as soon as $\lambda_{\max}(G)$ is controlled. We split the pairing into local kernels of positive type, using an antisymmetrised positivity lemma (Lemma 8.1), and prove an exact identity for the regularised diagonal in which all bad-prime corrections cancel (Theorem 8.7). With a uniform archimedean separation lemma this gives

$$\lambda_{\max}(G) \leq \frac{3}{4} \log X + \frac{1}{4} \psi(N - 1) + \frac{5}{4} \log H_f + 2, \quad X = \max_i |x_i|$$

(Theorem 8.10). Comparing with $\operatorname{tr} G \approx \frac{1}{2} N \log X$ gives Theorem 1.1.

Function fields (Section 10). Over $\mathbb{C}(t)$ the corresponding statements are exact: the Gram matrix of a progression of integral sections is determined by sign data at the zeros of the common difference (Theorem 10.1). We classify the 3-term types on rational elliptic surfaces and realise all sign data on elliptic $K3$ surfaces (Theorems 10.5 and 10.6).

Section 11 discusses the relation of the method to earlier work of Baker–Petsche, Hindry–Silverman and Helfgott–Venkatesh. Section 12 compares the consequences with those of [7], and Section 13 lists open problems. Statements marked *computer-assisted* rely on computations described in Appendix A.

Conventions

- $h(x) = \log \max(|u|, |v|)$ for $x = u/v$ in lowest terms.
- $\widehat{h}$ is the canonical height in Silverman’s normalisation, so $\widehat{h} \approx \frac{1}{2} h(x)$.
- Our pairing is $\langle P, Q \rangle = \frac{1}{4} (\widehat{h}(P + Q) - \widehat{h}(P - Q))$, so $\langle P, P \rangle = \widehat{h}(P)$. For points P_i we write $G_{ij} = \langle P_i, P_j \rangle$ and $\widehat{h}_i = \widehat{h}(P_i)$.
- The *span rank* s is the rank of the subgroup generated by the P_i ; it equals $\operatorname{rank} G$.
- $\psi(n) = \log \operatorname{lcm}(1, \dots, n) = \sum_p m_p(n) \log p$, with $m_p(n) = \max_{1 \leq k \leq n} v_p(k)$. Also $\vartheta(x) = \sum_{p \leq x} \log p$.

2 Setting

For the local theory (Sections 3–6) we work in an integral model

$$C : y^2 = f(x), \quad f \in \mathbb{Z}[x], \quad \deg f = m \in \{3, 4\}, \quad \operatorname{disc} f \neq 0, \quad (2)$$

with points $P_i = (x_i, y_i)$, $x_i = a + ib$ ($0 \leq i < N$), $a, b \in \mathbb{Z}$, $b \neq 0$, $y_i \in \mathbb{Z}$. Put

$$S = \{p \text{ prime} : p \mid 2b \operatorname{lc}(f) \operatorname{disc}(f)\}.$$

A rational progression $x_k = (\alpha + k\beta)/s^2$ becomes integral in a rescaled model, so working with integral progressions on integral models covers common-denominator progressions as well.

For the spectral half (Sections 7–9) we take a *monic* cubic model

$$W : y^2 = f(x) = x^3 + a_2x^2 + a_4x + a_6, \quad a_k \in \mathbb{Z}, \quad H_f := 1 + |a_2| + |a_4| + |a_6|. \quad (3)$$

Its discriminant is $\Delta_W = 16 \operatorname{disc} f$, and $\Delta_{\min}$ denotes the minimal discriminant of E . We write $X = \max_i |x_i|$ and $L = \log X$.

3 Point counts, root classes and pinned values

Recall that $2 \in S$, so every $p \notin S$ is odd, and $f \bmod p$ is a squarefree polynomial of degree m with unit leading coefficient. For $m = 3$ the reduction of (2) is then an elliptic curve $E_p/\mathbb{F}_p$ with exactly one point at infinity. We put $a_p = p + 1 - \#E_p(\mathbb{F}_p)$, so that $|a_p| \leq 2\sqrt{p}$ by Hasse.

Proposition 3.1 (Point counts). *Let $p \notin S$, and let z_p be the number of residues $x_i \bmod p$ at which $f \equiv 0 \pmod{p}$.*

- (a) $\#C^{\text{aff}}(\mathbb{F}_p) \geq 2(\min(N, p) - z_p) + z_p$.
- (b) *If $p \leq N$, then the residues $x_i \bmod p$ exhaust $\mathbb{F}_p$, and z_p is the number of roots of f in $\mathbb{F}_p$. If moreover $m = 3$, then $a_p = z_p - p$.*

Proof. Since $p \nmid b$, the residues $a + ib$ with $0 \leq i < \min(N, p)$ are pairwise distinct. At each such residue r we have $f(r) \equiv y_i^2$, a square. If $f(r) \not\equiv 0$, then $(r, \pm y_i)$ are two points; if $f(r) \equiv 0$, there is one point. This gives (a).

If $p \leq N$, every $x \in \mathbb{F}_p$ is such a residue. Hence $\#C^{\text{aff}}(\mathbb{F}_p) = 2p - z_p$, with z_p the number of roots of f in $\mathbb{F}_p$. Adding the single point at infinity gives $\#E_p(\mathbb{F}_p) = 2p - z_p + 1$, that is, $a_p = z_p - p$. $\square$

Lemma 3.2 (Root-class lemma). *Let $p \nmid b \operatorname{lc}(f) \operatorname{disc}(f)$, and let $r \in \mathbb{F}_p$ be a root of $f \bmod p$. Then at most one index i has $x_i \equiv r \pmod{p}$.*

Proof. Since $p \nmid \operatorname{lc}(f) \operatorname{disc}(f)$, the root r is simple, so $f'(r) \not\equiv 0$. By Hensel's lemma there is a unique $\tilde{r} \bmod p^2$ above r with $f(\tilde{r}) \equiv 0 \pmod{p^2}$.

If $x_i \equiv r$, then $p \mid y_i$, so $p^2 \mid f(x_i)$ and therefore $x_i \equiv \tilde{r} \pmod{p^2}$.

Now suppose two indices $i < i'$ satisfy $x_i \equiv x_{i'} \equiv r$. Then $i' \geq i + p$, so $i + p$ is also an index, and $x_{i+p} \equiv r$. By the previous paragraph $x_i \equiv x_{i+p} \equiv \tilde{r} \pmod{p^2}$. But $x_{i+p} - x_i = pb$ has p -adic valuation exactly 1, a contradiction. $\square$

Corollary 3.3. *If $p \notin S$ and $p \leq N$, then $z_p \leq \max(0, 2p - N)$. Moreover the roots of $f \bmod p$ lie in the residue classes $a + jb$ with $N - p \leq j \leq p - 1$.*

Proof. For $0 \leq j \leq p - 1$, the class $a + jb \bmod p$ contains the indices $i \equiv j \pmod{p}$ with $0 \leq i < N$. There are $\lfloor (N - 1 - j)/p \rfloor + 1 \geq 1$ of them, and the count is 1 exactly when $N - p \leq j \leq p - 1$.

By Lemma 3.2, every root class contains exactly one index. There are $\max(0, 2p - N)$ such classes. $\square$

Theorem 3.4 (Pinned values). *Let $m = 3$, $p \notin S$ and $p \leq N$. Then $a_p = z_p - p$, where $z_p \in \{0, 1, 3\}$ and $z_p \leq \max(0, 2p - N)$. Moreover:*

- (a) *No prime $p \geq 11$ with $p \leq N$ lies outside S .*
- (b) *The possible values for $p = 3, 5, 7$ are as follows.*

N	a_3	a_5	a_7
3	$-3, -2, 0$	–	–
4–5	$-3, -2$	$-4, -2$ ($N = 5$)	–
6–7	-3	$-4, -2$	-4 ($N = 7$)
8–9	-3	-4	-4
10–11	-3	$5 \in S$	-4
≥ 12	-3	$5 \in S$	$7 \in S$

In particular, for $N \geq 12$ every prime $p \leq N$ other than 3 lies in S , and $a_3 = -3$ if $3 \notin S$.

Proof. A squarefree cubic over $\mathbb{F}_p$ has 0, 1 or 3 roots in $\mathbb{F}_p$: if two roots are rational, so is the third. With Proposition 3.1(b) and Corollary 3.3, this gives $a_p = z_p - p$ with $z_p \in \{0, 1, 3\}$ and $z_p \leq \max(0, 2p - N)$. It remains to intersect with the Hasse bound $|z_p - p| \leq 2\sqrt{p}$.

- $p \geq 11$. Hasse would need $z_p \geq p - 2\sqrt{p} \geq 11 - 2\sqrt{11} > 4$, which is impossible.
- $p = 7$. Hasse forces $z_7 \geq 7 - 2\sqrt{7} > 1.7$, so $z_7 = 3$ and $a_7 = -4$. The constraint $3 \leq 14 - N$ requires $N \leq 11$.
- $p = 5$. Hasse forces $z_5 \geq 1$, so $z_5 \in \{1, 3\}$ and $a_5 \in \{-4, -2\}$. The constraint $z_5 \leq 10 - N$ excludes $z_5 = 3$ for $N \geq 8$ and excludes everything for $N \geq 10$.
- $p = 3$. Every $z_3 \in \{0, 1, 3\}$ is allowed by Hasse. The constraint $z_3 \leq 6 - N$ leaves $\{0, 1, 3\}$ for $N = 3$, $\{0, 1\}$ for $N = 4, 5$, and $\{0\}$ for $N \geq 6$.

□

4 The forbidden range

We use Weil’s bound in the following form [11, Thm. 11.23], [20, Thm. 2C’], [16, Thm. 5.41]. The hypothesis in [11] reads “ f is not a d -th power”. It has to be understood over $\overline{\mathbb{F}}_p$: for a nonsquare $c \in \mathbb{F}_p^\times$ the constant $f = c$ is not a square in $\mathbb{F}_p[X]$, yet $|\sum_x \chi(c)| = p$.

Lemma 4.1 (Weil). *Let p be odd and let χ be the quadratic character of $\mathbb{F}_p$. Let $G \in \mathbb{F}_p[X]$ be a polynomial that is not a constant multiple of a square, with d distinct roots in $\overline{\mathbb{F}}_p$. Then $|\sum_{x \in \mathbb{F}_p} \chi(G(x))| \leq (d - 1)\sqrt{p}$.*

Lemma 4.2 (Shift and square). *Let $p > m$, $p \notin S$ and $N \leq p$. Then for every integer H with $m + 1 \leq H < N$,*

$$(N - H)(H - m)^2 \leq Hp + (2m - 1)H(H - 1)\sqrt{p}. \quad (4)$$

Proof. Put $g(t) = f(a + bt) \in \mathbb{F}_p[t]$. Since $p \nmid b \operatorname{lc}(f) \operatorname{disc}(f)$, g is squarefree of degree m . Write $R \subset \overline{\mathbb{F}}_p$ for its root set, so $|R| = m$. For $x \in \mathbb{F}_p$ let

$$T(x) = \sum_{h=1}^H \chi(g(x + h)).$$

Lower bound. Take $x \in \{-1, 0, \dots, N - H - 1\}$. Then $x + h \in [0, N - 1]$ for $1 \leq h \leq H$, so $g(x + h) \equiv y_{x+h}^2$ and $\chi(g(x + h)) \in \{0, 1\}$. The values vanish only at roots of g , and there are at

most m such h (since $H < p$, the $x + h$ are distinct mod p). Hence $T(x) \geq H - m$. These $N - H$ values of x are distinct mod p , since $N \leq p$. Therefore

$$\sum_{x \in \mathbb{F}_p} T(x)^2 \geq (N - H)(H - m)^2.$$

Upper bound. Expanding,

$$\sum_{x \in \mathbb{F}_p} T(x)^2 = \sum_{h_1, h_2=1}^H \sum_x \chi(g(x + h_1)g(x + h_2)).$$

The H diagonal terms are each at most p .

For $h_1 \neq h_2$, put $G(X) = g(X + h_1)g(X + h_2)$. It has at most $2m$ distinct roots. It is a constant times a square only if every root is double, that is, only if $R - h_1 = R - h_2$. That would make R invariant under translation by $c = h_1 - h_2 \in \mathbb{F}_p^\times$. In characteristic p , the orbit of any point under translation by c has exactly p elements, and $p > m = |R|$, so this is impossible.

Lemma 4.1 therefore bounds each of the $H(H - 1)$ off-diagonal terms by $(2m - 1)\sqrt{p}$. $\square$

Corollary 4.3. *Let $p \notin S$ and $N \leq p$.*

(a) $N \leq (2m + 1)\sqrt{p}(1 + o(1))$ as $p \rightarrow \infty$. For cubics this reads $N \leq 7\sqrt{p}(1 + o(1))$.

(b) If $m = 3$ and $p \geq 144$, then $N \leq 7\sqrt{p} + 77$.

Proof. Put $u = \sqrt{p}$ and $H = \lfloor u \rfloor$. If $N \leq H$ there is nothing to prove, so assume $H < N$. Since $H \leq u$, we have $H(H - 1)\sqrt{p} \leq H \cdot p$, and (4) gives

$$(N - H)(H - m)^2 \leq 2mHp, \quad \text{so} \quad N \leq H + \frac{2mHp}{(H - m)^2}.$$

This is $(2m + 1)u(1 + O(1/u))$, which proves (a).

For (b), take $m = 3$ and $u \geq 12$. The function $H \mapsto H/(H - 3)^2$ is decreasing for $H > 3$, and $H \geq u - 1$, so

$$N \leq u + \frac{6(u - 1)u^2}{(u - 4)^2} = 7u + \frac{6u(7u - 16)}{(u - 4)^2}.$$

The last term is decreasing in u for $u > 4$, and equals 76.5 at $u = 12$. $\square$

Theorem 4.4 (Forbidden range, cubic case). *Let $m = 3$ and $N \geq 12$. Each prime p in the following ranges lies in S :*

- (i) $5 \leq p \leq N$;
- (ii) $N < p$ with $p + 2\sqrt{p} < 2N - 3$;
- (iii) $\max(N, 144) \leq p < ((N - 77)/7)^2$.

Consequently every prime $5 \leq p \leq Y_N$ lies in S , where

$$Y_N := \max\left(2N - 2\sqrt{2N} - 5, \left(\frac{N - 77}{7}\right)^2 \mathbf{1}_{N \geq 154}\right).$$

Proof. (i) is Theorem 3.4.

(ii) Suppose $p > N$ and $p \notin S$. Then the N residues $x_i \bmod p$ are distinct, and $z_p \leq 3$. Proposition 3.1(a) and the affine form of Hasse's bound [11, Thm. 11.25] give $2N - z_p \leq \#C^{\text{aff}}(\mathbb{F}_p) \leq p + 2\sqrt{p}$. So any prime with $p + 2\sqrt{p} < 2N - 3$ must lie in S .

(iii) is the contrapositive of Corollary 4.3(b).

For the consequence: if $p \leq 2N - 2\sqrt{2N} - 5$, then $p + 2\sqrt{p} \leq 2N - 5 < 2N - 3$. So the ranges (i)–(iii) cover every prime in $[5, Y_N]$. $\square$

Corollary 4.5 (Height of the progression). *Let $m = 3$ and $N \geq 12$. Then*

$$\log |2b \operatorname{lc}(f) \operatorname{disc}(f)| \geq \vartheta(Y_N) - \log 3.$$

In particular $\log |2b \operatorname{lc}(f) \operatorname{disc}(f)| \geq (1 - o(1))N^2/49$. By [19, (3.16)], $\vartheta(x) \geq x(1 - 1/\log x)$ for $x \geq 41$.

Proof. The primes in S are distinct prime divisors of $2b \operatorname{lc}(f) \operatorname{disc}(f)$. By Theorem 4.4, together with $2 \in S$, they include every prime $p \leq Y_N$ except possibly 3. $\square$

N	point counting reaches	shift-and-square reaches	$N^2/49$	Y_N (explicit)
50	79	–	51	75
130	223	229	345	222
145	251	293	429	250
200	359	619	816	355
400	739	2819	3265	2129
1000	1907	19213	20408	17386

Table 1: The largest prime forced into S by Theorem 4.4(ii), and by inequality (4) optimised exactly over H . Shift-and-square first beats point counting at $N = 130$. See Appendix A.

Remark 4.6 (Reading of Theorem 4.4). The common difference b can absorb the forced primes. Theorem 4.4 is therefore a statement about the *height of the progression* (or of the model), not about the curve alone.

Point counting alone, range (ii), forces only $\vartheta(2N) \sim 2N$. The shift-and-square range improves this by a factor of order N . That improvement is what makes $\psi(N - 1)$ negligible in Section 9 and yields the constant $3/2$; with range (ii) alone the same argument gives $7/4$.

The $\sqrt{p}$ scale is the natural limit of one-variable methods: square-root cancellation is all that Lemma 4.1 provides. Burgess's bound [11, Thm. 12.6] treats $\chi(n)$ with a linear argument, via [11, Cor. 11.24], and no analogue for $\chi(g(t))$ with $\deg g \geq 2$ is known. A random model for runs of squares predicts runs of length about $3 \log_2 p$, so the true forbidden range is probably exponential in N . Nothing below uses this.

Remark 4.7 (Quartics). For $m = 4$ the same arguments give: every prime $11 \leq p \leq N$ lies in S ; and every prime $p \geq N$ with $N > 9\sqrt{p}(1 + o(1))$ lies in S . For the first claim, a smooth genus-one quartic model has at most $p + 1 + 2\sqrt{p}$ points, while Proposition 3.1(a) gives $2p - 4$ affine points. The second claim is Corollary 4.3(a).

5 Primes dividing the common difference

Theorem 5.1 (Damped mechanism). *In the model (2), let $p \geq 3$ with $v_p(b) = 1$, $p \nmid \text{lc}(f)$, and $p \mid y_0$, $p \mid y_1$. Then:*

- (a) $f(a) \equiv f'(a) \equiv 0 \pmod{p}$, so $p \mid \text{disc } f$;
- (b) every P_k reduces to the singular point $(a \bmod p, 0)$ of $C \bmod p$;
- (c) if $m = 3$ and the model is minimal at p , then E has bad reduction at p .

Proof. All x_k are congruent to $a \bmod p$, and $p \mid y_0$ gives $f(a) \equiv 0$. From $p \mid y_0, y_1$ we get $p^2 \mid f(x_0)$ and $p^2 \mid f(x_1)$. Since $x_1 = x_0 + b$ with $p^2 \mid b^2$,

$$f(x_1) \equiv f(x_0) + bf'(x_0) \pmod{p^2},$$

so $p^2 \mid bf'(x_0)$. As $v_p(b) = 1$, this gives $p \mid f'(x_0)$, hence $f'(a) \equiv 0$. This proves (a).

For (b): $y_k^2 = f(x_k) \equiv f(a) \equiv 0$, so every P_k reduces to $(a, 0)$, which is singular by (a).

For (c) (with $m = 3$): $\Delta = 16 \text{disc } f$, and for a model minimal at p , bad reduction is equivalent to $p \mid \Delta$. $\square$

Definition 5.2. Let p divide the common difference of the progression in a model minimal at p . The prime p is a *smooth zero* if every P_i reduces to a nonsingular point mod p , and a *damped zero* otherwise.

Theorem 5.3 (Smooth-prime formula). *Let p be odd and let $y^2 = f(x)$ (with f monic) be minimal at p . Let $P_i, P_j \in E(\mathbb{Z}_p)$ satisfy the following:*

- $x_i \equiv x_j \pmod{p}$;
- both reduce to nonsingular points;
- $y_i \equiv \varepsilon y_j \not\equiv 0 \pmod{p}$ with $\varepsilon = \pm 1$.

Then the local pairing $\lambda_p(i, j) := \frac{1}{4}(\lambda_p(P_i + P_j) - \lambda_p(P_i - P_j))$ is

$$\lambda_p(i, j) = -\varepsilon \cdot \frac{1}{4} v_p(x_i - x_j) \log p.$$

Here λ_p is the local height of §8.2.

Proof. Take $\varepsilon = +1$. By the addition law,

$$x(P_i - P_j) = \left(\frac{y_i + y_j}{x_i - x_j} \right)^2 - a_2 - x_i - x_j.$$

Here $y_i + y_j \equiv 2y_j$ is a unit and $v_p(x_i - x_j) \geq 1$, so $v_p(x(P_i - P_j)) = -2v_p(x_i - x_j)$. Hence $P_i - P_j \in E_1$ with level $v_p(x_i - x_j)$.

Reduction is a homomorphism $E_0(\mathbb{Q}_p) \rightarrow \tilde{E}_{ns}(\mathbb{F}_p)$. The reductions of P_i and P_j coincide and are not 2-torsion (since $\bar{y} \neq 0$), so $P_i + P_j$ reduces to $2\bar{P} \neq \bar{O}$ and has level 0.

By (L2) of §8.2, $\lambda_p(P_i + P_j) - \lambda_p(P_i - P_j) = -v_p(x_i - x_j) \log p$. The case $\varepsilon = -1$ is the same with the roles of $P_i \pm P_j$ exchanged. $\square$

At a smooth zero all P_i reduce to $\pm \bar{P}$ for a single $\bar{P}$, since all the x_i agree mod p . When $\bar{P} \notin E[2]$, Theorem 5.3 shows that the p -adic part of the Gram matrix is a rank-one sign pattern $-\varepsilon \varepsilon^T$, weighted by $v_p(x_i - x_j)$.

Proposition 5.4 (All zeros damped on the nine 8-term solutions). (computer-assisted) *Consider the nine 8-term solutions listed by their y -values Y_k ($0 \leq k \leq 7$) in Table 2. They were found by a search over cubics with $0 \leq y_0, \dots, y_3 \leq 300$; the completeness of that search is not used here. Write $Y_k^2 = c_3k^3 + c_2k^2 + c_1k + c_0$, and use the progression model*

$$Y^2 = X^3 + c_2X^2 + c_1c_3X + c_0c_3^2, \quad X_k = c_3k,$$

which has common difference $b = c_3$. Then:

- *every prime dividing the common difference $d_{\min}$ of the minimal model is damped (23 of 23), of Kodaira types IV, I₃, I₄, I₇, I₈, I₁₆, I₁^{*};*
- *each of the 18 odd damped primes satisfies $v_p(b) = v_p(d_{\min}) = 1$ and $p \mid Y_k$ for all k , so Theorem 5.1 explains all of them.*

$(Y_0, \dots, Y_7)$	primes of $d_{\min}$ (all damped), Kodaira type
(1, 7, 7, 5, 1, 1, 7, 13)	none ($d_{\min} = 1$; this is 5077a1)
(167, 223, 223, 197, 167, 167, 223, 323)	5, 7, 13: IV
(3, 49, 53, 45, 29, 7, 21, 53)	3: I ₇ ; 11: I ₃
(41, 127, 139, 125, 97, 71, 83, 139)	2, 7: IV; 13: I ₃
(82, 121, 128, 121, 110, 107, 124, 163)	2: I ₁₆ ; 7: IV
(31, 52, 47, 34, 35, 64, 107, 158)	2: I ₈ ; 5, 7: I ₄
(139, 23, 31, 115, 173, 209, 217, 181)	2: I ₁ [*] ; 7, 11: I ₄
(169, 157, 119, 67, 55, 131, 233, 349)	2: I ₁ [*] ; 7, 11: I ₄
(217, 251, 205, 109, 17, 187, 379, 595)	3: IV; 5, 7, 11: I ₄

Table 2: Proposition 5.4.

Remark 5.5 (Which model to test in). The hypothesis $p \mid y_k$ of Theorem 5.1 is not invariant under changes of coordinates $y \mapsto y + sx + t$. It must therefore be tested in the progression model, not in a minimal model reached by such a change. In the progression model it holds for every odd damped prime in Table 2.

Proposition 5.6 (Smooth zeros exist). (computer-assisted) *Smooth zeros at good primes occur on progressions of length 7 and 8, and hence of every length ≤ 8 .*

(a) **Length 7.** *For $r, s \in \mathbb{Z}$ put*

$$A = |r^2 - 2rs - s^2|, \quad B = |r^2 + 2rs - s^2|, \quad C = r^2 + s^2, \quad c = \frac{B^2 - A^2}{12},$$

and $q(k) = A^2 + ck(k-4)(k-5)$. Then

$$q(0) = q(4) = q(5) = A^2, \quad q(1) = q(2) = q(6) = B^2, \quad q(3) = C^2.$$

The last identity holds because $A^2 + B^2 = 2C^2$. Take $r = 343$, $s = 1$; all of A, B, C are then even, and halving them gives

$$Y = (58481, 59167, 59167, 58825, 58481, 58481, 59167).$$

This gives a 7-term integral progression on a curve of rank exactly 7. The prime 7 is a smooth zero: it has good reduction, $v_7(d_{\min}) = 1$, and the sign vector is $\varepsilon = (+, +, +, -, +, +, +)$. The other primes of $d_{\min} = 34314 = 2 \cdot 3 \cdot 7 \cdot 19 \cdot 43$ are damped; 19 and 43 have type IV.

- (b) **Length 8.** With $s = 1$, requiring $q(7) = (7B^2 - 5A^2)/2$ to be a square gives $W^2 = r^4 + 24r^3 + 2r^2 - 24r + 1$. This is a genus-one curve with Jacobian $E' = [0, 2, 0, -580, 1144]$, of rank 1 with generator $G = (-18, 80)$. The map is $r = (12x - 24 \pm y)/(284 - 2x)$.

The point $146G$ gives an 8-term progression with Y_k of about 8300 digits. In a model minimal at 7 (by Tate's algorithm), 7 has good reduction, $v_7(b) = 1$, all Y_k are 7-adic units, and $Y \bmod 7$ takes values ± 1 . So 7 is a smooth zero.

Problem 5.7. Does a 7-term x -progression with no collinear triple have a smooth zero at a good prime? The family in Proposition 5.6 has many collinear triples.

6 Denominators of non-integral progressions

Proposition 6.1 (Denominator rule). *Let $y^2 = x^3 + a_2x^2 + a_4x + a_6$ be integral, and let $x_1 + x_3 = 2x_2$ with $x_i = x(P_i)$. Fix a prime p and put $e_i = \max(0, -v_p(x_i)/2)$ and $e = \max_i e_i$. Assume $e > 0$.*

- (a) *Let p be odd. Then e is attained at least twice. The pattern $e_1 = e_3 > e_2$ forces $p \equiv 1 \pmod{4}$. The pattern $e_1 = e_2 > e_3$ (or $e_2 = e_3 > e_1$) forces $p \equiv \pm 1 \pmod{8}$. In particular, for $p \equiv 3 \pmod{8}$ all three e_i are equal.*
- (b) *Let $p = 2$ and $a_2 = 0$. Then $e_1 = e_2 = e_3$.*

Proof. Let $e_i > 0$. In the formal group, $x = z^{-2} - a_2 - a_4z^2 - \dots$ with $v_p(z) = e_i$. Hence $u_i := p^{2e_i}x_i = w_i^2(1 - a_2z^2 - \dots)$, where $w_i = p^{e_i}/z$ is a unit. So u_i is a unit congruent to a nonzero square mod p . When $a_2 = 0$ the correction factor is $1 + O(z^4)$, so $u_i \equiv 1 \pmod{8}$ if $p = 2$.

(a) If e were attained only at i , then x_i would have strictly smaller valuation than the other two terms of $x_1 + x_3 - 2x_2 = 0$. This is impossible.

- If $e_1 = e_3 = e > e_2$, then $u_1 + u_3 = 2p^{2e}x_2 \equiv 0 \pmod{p}$. So -1 is a square mod p .
- If $e_1 = e_2 = e > e_3$, then $u_1 \equiv 2u_2 \pmod{p}$. So 2 is a square mod p .

(b) Use $v_2(2) = 1$ and $u_i \equiv 1 \pmod{8}$.

- $e_1 = e_3 = e > e_2$: then $v_2(u_1 + u_3) = 1$, while $v_2(2^{2e+1}x_2) \geq 3$.
- $e_1 = e_2 = e > e_3$: then $v_2(u_1 + 2^{2e}x_3) = 0$, while $v_2(2u_2) = 1$.
- A unique maximum: the same valuation argument as in (a).

All three cases are contradictions. □

7 The trace inequality

Lemma 7.1. *Let G be real symmetric positive semidefinite of rank s . Then $\text{tr } G \leq s \lambda_{\max}(G)$. In particular, if M has unit diagonal, then $N = \text{tr } M \leq s \lambda_{\max}(M)$.*

Proof. $\text{tr } G$ is the sum of the s nonzero eigenvalues, each of which is at most $\lambda_{\max}(G)$. □

The Néron–Tate pairing is positive definite on $E(\mathbb{Q}) \otimes \mathbb{R}$, so $\text{rank } G = s$. The quantity that matters is therefore $\lambda_{\max}(G)$, not the mean squared cosine. Arguments through $N^2 = (\text{tr } M)^2 \leq s \text{tr}(M^2)$ (Alon's lemma) lose everything once the typical cosine stays above $s^{-1/2}$.

8 Local kernels of positive type

8.1 An antisymmetrised positivity lemma

Lemma 8.1. *Let $\mathcal{G}$ be a compact abelian group, and let $F : \mathcal{G} \rightarrow \mathbb{R}$ be continuous and even with absolutely convergent Fourier series $F = \sum_{\chi} \widehat{F}(\chi)\chi$. Assume $\widehat{F}(\chi) \geq 0$ for every character χ with $\chi^2 \neq 1$. Then for all $g_1, \dots, g_n \in \mathcal{G}$ the matrix*

$$S_{ij} = F(g_i - g_j) - F(g_i + g_j) \quad (1 \leq i, j \leq n)$$

is positive semidefinite. Its diagonal is $S_{ii} = F(0) - F(2g_i)$. Adding a constant to F does not change S .

Proof. For $c \in \mathbb{R}^n$ put $a_{\chi} = \sum_i c_i \chi(g_i)$. Then

$$\sum_{i,j} c_i c_j S_{ij} = \sum_{\chi} \widehat{F}(\chi) (|a_{\chi}|^2 - a_{\chi}^2).$$

Since F is real and even, $\widehat{F}(\bar{\chi}) = \widehat{F}(\chi) \in \mathbb{R}$, and $a_{\bar{\chi}} = \bar{a}_{\chi}$. Two kinds of terms appear:

- a real character ($\chi = \bar{\chi}$) has $a_{\chi} \in \mathbb{R}$, so its term vanishes;
- a pair $\{\chi, \bar{\chi}\}$ with $\chi^2 \neq 1$ contributes $\widehat{F}(\chi)(2|a_{\chi}|^2 - 2\operatorname{Re} a_{\chi}^2) = 4\widehat{F}(\chi)(\operatorname{Im} a_{\chi})^2 \geq 0$.

A constant only changes the coefficient of the trivial character, which is real. $\square$

8.2 Local heights

We use the Néron functions $\lambda_v : E(\mathbb{Q}_v) \setminus \{O\} \rightarrow \mathbb{R}$ in Silverman's normalisation [26, Ch. VI]. They are model-independent, even and continuous. We need the following facts.

(L1) $\widehat{h}(P) = \sum_v \lambda_v(P)$ for $P \in E(\mathbb{Q}) \setminus \{O\}$ [26, Thm. VI.2.1].

(L2) Let p be a prime and use a model minimal at p . Let $E_0 \supseteq E_1 \supseteq E_2 \supseteq \dots$ be the usual filtration of $E(\mathbb{Q}_p)$, where $E_k = \{R : v_p(x(R)) \leq -2k\} \cup \{O\}$ for $k \geq 1$. Define the level $\ell_p(R) = \max\{k : R \in E_k\}$ (so $\ell_p(R) = 0$ if $R \notin E_1$) and $\gamma_p = \frac{1}{12} v_p(\Delta_{\min}) \log p$.

- For $R \in E_0 \setminus \{O\}$: $\lambda_p(R) = \gamma_p + \ell_p(R) \log p$ [26, Thm. VI.4.1].
- For $R \notin E_0$: $\lambda_p(R) = \gamma_p + c_p(\pi R) \log p$, where $\pi : E(\mathbb{Q}_p) \rightarrow \Phi_p$ is the projection to the component group, $c_p(0) = 0$, and c_p is even and depends only on the component. Its values are listed in Table 3 [23, Thm. 5.2], [4, §2].

(L3) Write $E(\mathbb{C}) = \mathbb{C}/\Lambda$ for the lattice Λ of the model (3), with $x = \wp(z) - a_2/3$ and $2y = \wp'(z)$, so $dx/2y = dz$. Then $\Delta(\Lambda) = \Delta_W$, and

$$\lambda_{\infty}(z) = -\log \left| e^{-\frac{1}{2} z \eta(z)} \sigma(z) \Delta(\Lambda)^{1/12} \right|,$$

where η is the $\mathbb{R}$ -linear extension of the quasi-period map [26, §VI.3]. Since $\sigma(z) = z + O(z^5)$,

$$\lambda_{\infty}(z) + \log |z| \longrightarrow -\frac{1}{12} \log |\Delta_W| \quad (z \rightarrow 0).$$

type	$\Phi_p(\overline{\mathbb{F}}_p)$	$-c_p$ on non-zero classes	$\widehat{c}_p(\chi), \chi^2 \neq 1$
I_m (split)	$\mathbb{Z}/m$	$i(m-i)/(2m)$ on class i	$1/(4m \sin^2(\pi k/m))$ for $\chi = e(k \cdot /m)$
I_m (non-split)	$\Phi(\mathbb{Q}_p) \subseteq \mathbb{Z}/2$	as above	(no such χ)
II, II^*	0	—	—
III, III^*	$\mathbb{Z}/2$	$\frac{1}{4}, \frac{3}{4}$	(no such χ)
IV, IV^*	$\mathbb{Z}/3$	$\frac{1}{3}, \frac{2}{3}$ (constant)	$\frac{1}{9}, \frac{2}{9}$
I_m^*, m odd	$\mathbb{Z}/4$	$\frac{1}{2}$ (order 2), $\frac{m+4}{8}$ (order 4)	$\frac{1}{8}$
I_m^*, m even	$(\mathbb{Z}/2)^2$	$\frac{1}{2}, \frac{m+4}{8}, \frac{m+4}{8}$	(no such χ)

Table 3: Component corrections in Silverman’s normalisation: half the values of [4, Table 2], since $\lambda^{\text{CPS}} = 2\lambda + \frac{1}{6} \log |\Delta|$ [4, (11)]; and their Fourier coefficients on characters of order > 2 .

8.3 Non-archimedean kernels

For a prime p and an integer $K \geq 0$ define $F_{p,K} : E(\mathbb{Q}_p) \rightarrow \mathbb{R}$ by

$$F_{p,K}(R) = c_p(\pi R) \log p + \log p \cdot \min(\ell_p(R), K) = c_p(\pi R) \log p + \log p \sum_{k=1}^K \mathbf{1}_{E_k}(R),$$

with $\ell_p(O) = \infty$, so that $F_{p,K}(O) = K \log p$.

Lemma 8.2. *$F_{p,K}$ satisfies the hypotheses of Lemma 8.1 on $\mathcal{G} = E(\mathbb{Q}_p)$. Moreover, for $R \neq O$,*

$$\lambda_p(R) - F_{p,K}(R) = \gamma_p + \log p \cdot (\ell_p(R) - K)^+. \quad (5)$$

Proof. $E(\mathbb{Q}_p)$ is a compact abelian group, and $F_{p,K}$ factors through the finite quotient $E(\mathbb{Q}_p)/E_{K+1}$, so its Fourier series is a finite sum. $F_{p,K}$ is even because c_p is even and each E_k is a subgroup.

The indicator of a finite-index subgroup H has Fourier coefficients $[\mathcal{G} : H]^{-1} \geq 0$ on $H^\perp$ and 0 elsewhere. The function $c_p \circ \pi$ has coefficient $\widehat{c}_p(\chi)$ on characters trivial on E_0 , and 0 elsewhere. A character χ of $\Phi_p(\mathbb{Q}_p)$ with $\chi^2 \neq 1$ is the restriction of characters of $\Phi_p(\overline{\mathbb{F}}_p)$, all of order > 2 . So Proposition 8.3 below gives $\widehat{F}_{p,K}(\chi) \geq 0$ whenever $\chi^2 \neq 1$.

Identity (5) follows directly from (L2). $\square$

Proposition 8.3 (Bad-prime positivity). *For every Kodaira type, $\widehat{c}_p(\chi) \geq 0$ for every character χ of $\Phi_p(\overline{\mathbb{F}}_p)$ of order > 2 . Here $\widehat{c}(\chi) = |\Phi|^{-1} \sum_g c(g) \bar{\chi}(g)$.*

Proof. If $\Phi \subseteq (\mathbb{Z}/2)^2$, there is nothing to prove. The remaining cases are as follows.

- IV and IV^* ($\Phi = \mathbb{Z}/3$). Evenness makes c constant, equal to $-\alpha < 0$, on the two non-zero classes. So $\widehat{c}(\chi) = -\frac{\alpha}{3}(\omega + \bar{\omega}) = \frac{\alpha}{3} > 0$.
- I_m^* with m odd ($\Phi = \mathbb{Z}/4$). Let $\chi(1) = i$. Evenness gives $c(1) = c(3)$, so $\widehat{c}(\chi) = \frac{1}{4}(-ic(1) - c(2) + ic(3)) = -\frac{1}{4}c(2) = \frac{1}{8}$.
- I_m ($\Phi = \mathbb{Z}/m$, $c(i) = -i(m-i)/(2m)$). Let $\zeta = e^{-2\pi i k/m} \neq 1$. Using $\sum_{i < m} i \zeta^i = m/(\zeta - 1)$ and $\sum_{i < m} i^2 \zeta^i = m(m(\zeta - 1) - 2\zeta)/(\zeta - 1)^2$, we get $\sum_{i < m} i(m-i)\zeta^i = 2m\zeta/(\zeta - 1)^2$. Hence

$$\widehat{c}(k) = -\frac{1}{m} \cdot \frac{\zeta}{(\zeta - 1)^2} = \frac{1}{4m \sin^2(\pi k/m)} > 0.$$

This was also checked numerically for $m < 200$ (Appendix A). $\square$

8.4 The archimedean kernel

Let A be the covolume of Λ , and let $\Lambda^* = \{\xi \in \mathbb{C} : \operatorname{Re}(\bar{\xi}\omega) \in \mathbb{Z} \ \forall \omega \in \Lambda\}$ be the dual lattice. Characters of $\mathbb{C}/\Lambda$ are $e_\xi(z) = e^{2\pi i \operatorname{Re}(\bar{\xi}z)}$ with $\xi \in \Lambda^*$. Let ω_1 be a shortest nonzero period.

Lemma 8.4 (λ_∞ is a Green function). *In the sense of distributions on $\mathbb{C}$,*

$$\Delta \lambda_\infty = \frac{2\pi}{A} - 2\pi \sum_{\omega \in \Lambda} \delta_\omega.$$

Consequently $\widehat{\lambda_\infty}(\xi) = 1/(2\pi A|\xi|^2) > 0$ for $\xi \in \Lambda^* \setminus \{0\}$.

Proof. The function $-\log|\sigma|$ has Laplacian $-2\pi \sum_{\omega} \delta_\omega$, since σ is entire with simple zeros exactly on Λ . The term $\log|\Delta|^{1/12}$ is constant.

For the remaining term, write $\eta(z) = \alpha z + \beta \bar{z}$. The Legendre relation $\eta(\omega_1)\omega_2 - \eta(\omega_2)\omega_1 = 2\pi i$, with the orientation $\operatorname{Im}(\bar{\omega}_1\omega_2) = A$, gives $\beta \cdot 2iA = 2\pi i$, so $\beta = \pi/A$. Hence

$$\operatorname{Re}\left(\frac{1}{2}z\eta(z)\right) = \frac{1}{2}\operatorname{Re}(\alpha z^2) + \frac{\pi}{2A}|z|^2$$

has Laplacian $2\pi/A$. This gives the formula for $\Delta \lambda_\infty$.

Now let $g = \sum_{\xi \neq 0} e_\xi/(2\pi A|\xi|^2)$. By Poisson summation, $\sum_{\xi \in \Lambda^*} e_\xi = A \sum_{\omega} \delta_\omega$, so $\Delta g = 2\pi/A - 2\pi \sum_{\omega} \delta_\omega$. Thus $\lambda_\infty - g$ is a Λ -periodic harmonic distribution, hence constant by Weyl's lemma. $\square$

Let ν_ρ be the uniform probability measure on the disc $\{|w| \leq \rho\}$. Put $\mu = \nu_\rho * \nu_\rho$, which is radial, supported in $\{|w| \leq 2\rho\}$, and has second moment $M_2 = \int |w|^2 d\mu$. Define the smoothed kernel

$$F_\infty(z) = \int \lambda_\infty(z+w) d\mu(w).$$

Lemma 8.5 (Smoothing). *Assume $2\rho < |\omega_1|$.*

(a) F_∞ satisfies the hypotheses of Lemma 8.1 on $\mathbb{C}/\Lambda$.

(b) If $d(z, \Lambda) > 2\rho$, then $F_\infty(z) = \lambda_\infty(z) + \frac{\pi}{2A}M_2$.

(c) $F_\infty(0) = -\log \rho + \frac{1}{4} - \frac{1}{12} \log |\Delta_W| + \frac{\pi}{2A}M_2$.

Proof. (a) $\widehat{F_\infty}(\xi) = \widehat{\lambda_\infty}(\xi) |\widehat{\nu_\rho}(\xi)|^2 \geq 0$. The disc transform is $\widehat{\nu_\rho}(\xi) = 2J_1(2\pi\rho|\xi|)/(2\pi\rho|\xi|) = O(|\xi|^{-3/2})$, so $\widehat{F_\infty}(\xi) = O(|\xi|^{-5})$. This is summable over Λ^* , which makes F_∞ continuous with an absolutely convergent Fourier series. Evenness is inherited from λ_∞ .

(b) By Lemma 8.4, $w \mapsto \lambda_\infty(z+w) - \frac{\pi}{2A}|w|^2$ is harmonic on $|w| \leq 2\rho$. Its average over each circle $|w| = t$ therefore equals its value at 0. Since μ is radial, $\int \lambda_\infty(z+w) d\mu = \lambda_\infty(z) + \frac{\pi}{2A}M_2$.

(c) On $|w| < |\omega_1|$, write $\lambda_\infty(w) = -\log|w| + k(w)$. Here k is smooth with $\Delta k = 2\pi/A$, and $k(0) = -\frac{1}{12} \log |\Delta_W|$ by (L3). As in (b), $\int k d\mu = k(0) + \frac{\pi}{2A}M_2$.

For the logarithmic part, the potential of ν_ρ is

$$U(z) = \int -\log|z-w| d\nu_\rho(w) = -\log \rho + \frac{1}{2}(1 - |z|^2/\rho^2) \quad (|z| \leq \rho).$$

Since ν_ρ is symmetric, $\int -\log|w| d\mu = \iint -\log|w_1 + w_2| d\nu_\rho d\nu_\rho = \int U d\nu_\rho = -\log \rho + \frac{1}{4}$. $\square$

8.5 The general cap and the exact diagonal

Theorem 8.6 (Spectral cap, general form). *Let $P_1, \dots, P_n \in E(\mathbb{Q})$ with $P_i \pm P_j \neq O$ for $i \neq j$ and $2P_i \neq O$. For each place v let F_v satisfy the hypotheses of Lemma 8.1 on $E(\mathbb{Q}_v)$, with $F_v(P_i \pm P_j) = \lambda_v(P_i \pm P_j) - \kappa_v$ ($i \neq j$) for constants κ_v . Assume $F_v = 0$ and $\kappa_v = \gamma_v$ for all but finitely many v . Put*

$$S_{ij}^v = F_v(P_i - P_j) - F_v(P_i + P_j), \quad D_i = \sum_v S_{ii}^v, \quad B_i = \sum_v [\lambda_v(2P_i) + F_v(0) - F_v(2P_i)].$$

Then

$$G \preceq \text{diag}(\widehat{h}(P_i) + \tfrac{1}{4}D_i) = \tfrac{1}{4} \text{diag}(B_i), \quad \text{so} \quad \lambda_{\max}(G) \leq \tfrac{1}{4} \max_i B_i.$$

Proof. For $i \neq j$, (L1) gives $4G_{ij} = \widehat{h}(P_i + P_j) - \widehat{h}(P_i - P_j) = \sum_v (\lambda_v(P_i + P_j) - \lambda_v(P_i - P_j)) = -\sum_v S_{ij}^v$; the constants κ_v cancel. Hence

$$4G = \text{diag}(4\widehat{h}_i + D_i) - \sum_v S^v,$$

and each $S^v \succeq 0$ by Lemma 8.1. Finally, $4\widehat{h}_i = \widehat{h}(2P_i) = \sum_v \lambda_v(2P_i)$ by (L1), so $4\widehat{h}_i + D_i = B_i$. $\square$

Theorem 8.7 (Exact regularised diagonal). *In Theorem 8.6, take the following kernels:*

- at each prime p , $F_p = F_{p, K_p}$ with $K_p \geq \max_{i \neq j} \ell_p(P_i \pm P_j)$;
- at the archimedean place, F_∞ as in Lemma 8.5, with $2\rho < \min(|\omega_1|, \delta)$, where

$$\delta = \min\{d(P_i \pm P_j, \Lambda) \ (i \neq j), \ d(2P_i, \Lambda)\}.$$

Then the hypotheses of Theorem 8.6 hold, and

$$B_i = -\log \rho + \tfrac{1}{4} + \tfrac{1}{12} \log \left| \frac{\Delta_{\min}}{\Delta_W} \right| + \sum_p \max(K_p, \ell_p(2P_i)) \log p. \quad (6)$$

Proof. The hypotheses hold by Lemmas 8.2 and 8.5(a),(b), with $\kappa_p = \gamma_p$ and $\kappa_\infty = -\frac{\pi}{2A} M_2$. For all but finitely many p every level involved is 0; take $K_p = 0$ there, and then $F_p = 0$.

At a prime p , (5) applied to $2P_i$ gives

$$\lambda_p(2P_i) + F_p(0) - F_p(2P_i) = \gamma_p + \max(K_p, \ell_p(2P_i)) \log p.$$

At ∞ , Lemma 8.5(b),(c) gives

$$\lambda_\infty(2P_i) + F_\infty(0) - F_\infty(2P_i) = -\log \rho + \tfrac{1}{4} - \tfrac{1}{12} \log |\Delta_W|.$$

Sum over all places and use $\sum_p \gamma_p = \frac{1}{12} \log |\Delta_{\min}|$. $\square$

Remark 8.8. Three features of (6) are worth noting.

- The component corrections c_p have cancelled. Bad primes enter only through positivity (Proposition 8.3) and through levels. In particular no bound for the local height differences α_p of [4] is needed.
- The archimedean smoothing is *exact* on the off-diagonal entries, because λ_∞ has constant Laplacian away from Λ . Smoothing is therefore two-sided automatically: it holds for test vectors of every sign pattern.
- The only analytic input is the separation δ .

8.6 Archimedean separation

Proposition 8.9 (Distance lemma). *For the model (3), define*

$$\kappa_\infty := \max \left(\sup_{Q \in E(\mathbb{C}) \setminus \{O\}} \left[-\log d(Q, \Lambda) - \frac{1}{2} \log \max(1, |x(Q)|) \right], -\log |\omega_1| \right).$$

Then

$$\kappa_\infty \leq 2 + \frac{1}{12} (\log |\Delta_W| + \log^+ |j|) + \frac{1}{2} \log(1 + |a_2|/3) \leq 3.61 + \frac{4}{3} \log H_f.$$

Proof. Write $\Lambda = \omega_1 \Lambda_\tau$ with $\Lambda_\tau = \mathbb{Z} + \tau \mathbb{Z}$, where τ lies in the standard fundamental domain: $|\tau| \geq 1$, $|\operatorname{Re} \tau| \leq \frac{1}{2}$, and $y = \operatorname{Im} \tau \geq \sqrt{3}/2$.

Step 1: the normalised lattice. We claim that for all $z \notin \Lambda_\tau$,

$$-\log d(z, \Lambda_\tau) - \frac{1}{2} \log \max(1, |\wp_\tau(z)|) \leq c_0 := 1.68.$$

The nonzero points of Λ_τ have mutual distances ≥ 1 . Discs of radius $\frac{1}{2}$ around them are therefore disjoint, so $\#\{\omega \neq 0 : |\omega| \leq R\} \leq 4(R + \frac{1}{2})^2$. Partial summation then gives $\sum_{\omega \neq 0} |\omega|^{-3} \leq 19$.

For $|w| \leq \frac{1}{4}$ and $\omega \neq 0$,

$$|(w - \omega)^{-2} - \omega^{-2}| \leq 4|w|/|\omega|^3, \quad \text{so} \quad |\wp_\tau(w) - w^{-2}| \leq 76|w|.$$

Put $r_1 = 152^{-1/3} \approx 0.187$. If $|w| < r_1$, then $|\wp_\tau(w)| \geq \frac{1}{2}|w|^{-2} > 1$.

Now let $d = d(z, \Lambda_\tau)$.

- If $d < r_1$, write $z = \omega_0 + w$ with $|w| = d$. Then the left side is at most $-\log d - \frac{1}{2} \log(\frac{1}{2}d^{-2}) = \frac{1}{2} \log 2$.
- If $d \geq r_1$, the left side is at most $-\log r_1 < 1.68$.

Step 2: rescaling. We have $d(z, \Lambda) = |\omega_1| d(z/\omega_1, \Lambda_\tau)$ and $\wp_\Lambda(z) = \omega_1^{-2} \wp_\tau(z/\omega_1)$. Also $|\wp_\Lambda| \leq |x| + |a_2|/3$, so

$$\max(1, |\wp_\Lambda|) \leq (1 + |a_2|/3) \max(1, |x|), \quad \max(1, |\omega_1|^{-2} |\wp_\tau|) \geq \min(1, |\omega_1|^{-2}) \max(1, |\wp_\tau|).$$

Combining these with Step 1 gives

$$-\log d(Q, \Lambda) - \frac{1}{2} \log \max(1, |x(Q)|) \leq c_0 + \max(0, -\log |\omega_1|) + \frac{1}{2} \log(1 + |a_2|/3).$$

Step 3: bounding $-\log |\omega_1|$. Homogeneity gives $\Delta(\Lambda) = \omega_1^{-12} \Delta(\Lambda_\tau)$, and $\Delta(\Lambda_\tau) = (2\pi)^{12} q \prod_n (1 - q^n)^{24}$ with $|q| = e^{-2\pi y} \leq e^{-\pi\sqrt{3}}$. So $|\Delta(\Lambda_\tau)| \geq 0.9(2\pi)^{12} e^{-2\pi y}$.

For the j -invariant, $j(\tau) = q^{-1} + 744 + \sum_{n \geq 1} c_n q^n$ with $c_n > 0$. Hence

$$\left| \sum c_n q^n \right| \leq j(i\sqrt{3}/2) - e^{\pi\sqrt{3}} - 744 < 1335,$$

so $|j| \geq e^{2\pi y} - 2079$. Therefore $2\pi y \leq \log^+ |j| + \log 2080$, and

$$-\log |\omega_1| = \frac{1}{12} (\log |\Delta_W| - \log |\Delta(\Lambda_\tau)|) \leq \frac{1}{12} (\log |\Delta_W| + \log^+ |j|) - 1.19.$$

This bounds both terms in the definition of κ_∞ .

Step 4: in terms of H_f . We have $|\operatorname{disc} f| \leq 54H_f^4$, so $\log |\Delta_W| \leq \log 864 + 4 \log H_f$. Also $|c_4| = |16a_2^2 - 48a_4| \leq 64H_f^2$ and $|\Delta_W| \geq 1$, so $\log^+ |j| \leq 3 \log(64H_f^2)$. $\square$

8.7 Integral progressions

Theorem 8.10 (Spectral cap for integral progressions). *Let W be as in (3), and let $P_0, \dots, P_{N-1} \in E(\mathbb{Z})$ with $x_i = a + ib$, $b \neq 0$, $N \geq 3$. Let $I \subseteq \{0, \dots, N-1\}$ be any set of indices with $y_i \neq 0$ for $i \in I$, and let $G_I = (\langle P_i, P_j \rangle)_{i,j \in I}$. Then, with $L = \log X$,*

$$\begin{aligned} \lambda_{\max}(G_I) &\leq \frac{1}{4} \left(3L + \psi(N-1) + \kappa_\infty + \frac{7}{2} \log H_f + 3.58 \right) \\ &\leq \frac{3}{4}L + \frac{1}{4}\psi(N-1) + \frac{5}{4} \log H_f + 2. \end{aligned}$$

Proof. Let $u \in \mathbb{Z}$ be such that $\Delta_W = u^{12} \Delta_{\min}$. Write $u_p = v_p(u)$, so that $\sum_p u_p \log p = \frac{1}{12} \log |\Delta_W / \Delta_{\min}|$. Write $\ell_p^W(R) = \max(0, -\frac{1}{2}v_p(x(R)))$, with x the coordinate of W .

Step 1: comparing levels. The model W is obtained from a minimal model by $x = u^2 x' + r$ with $r \in \mathbb{Z}$ [25, VII.1.3]. If $R \in E_k$ with $k > u_p$, then $v_p(x(R)) = 2u_p - 2k < 0$. Hence $\ell_p(R) \leq \ell_p^W(R) + u_p$ for every R .

Step 2: levels of $P_i \pm P_j$. Put $D = x_i - x_j = (i - j)b$, and let $u_\pm = x(P_i \pm P_j)$. A direct computation (also verified symbolically, Appendix A) gives

$$(u_+ + u_-)D^2 = 2[(x_i + x_j)(x_i x_j + a_4) + 2a_2 x_i x_j + 2a_6], \quad u_+ u_- D^2 = (x_i x_j - a_4)^2 - 4a_6(x_i + x_j) - 4a_2 a_6.$$

Both right-hand sides are integers, so $v_p(u_+ + u_-)$ and $v_p(u_+ u_-)$ are at least $-2v_p(D)$. If $v_p(u_+)$ and $v_p(u_-)$ are both negative, the product bound gives $\ell_p^W(u_+) + \ell_p^W(u_-) \leq v_p(D)$. If exactly one is negative, the sum bound gives the same inequality. Hence $\ell_p^W(P_i + P_j) + \ell_p^W(P_i - P_j) \leq v_p(D) \leq v_p(b) + m_p(N-1)$.

Step 3: levels of $2P_i$. We have $x(2P) = (x^4 - 2a_4 x^2 - 8a_6 x + a_4^2 - 4a_2 a_6)/(4y^2)$, so $\ell_p^W(2P_i) \leq v_p(2y_i)$.

Step 4: choice of K_p and summation. Take $K_p = u_p + v_p(b) + m_p(N-1)$. This is admissible by Steps 1–2. By Step 3,

$$\max(K_p, \ell_p(2P_i)) \leq u_p + v_p(b) + m_p(N-1) + v_p(2y_i).$$

Summing over p , the term $\sum u_p \log p$ cancels the term $\frac{1}{12} \log |\Delta_{\min} / \Delta_W|$ in (6). This leaves

$$B_i \leq -\log \rho + \frac{1}{4} + \log |b| + \psi(N-1) + \log |2y_i|. \quad (7)$$

Step 5: archimedean separation. Since $X \geq (N-1)|b|/2 \geq |b| \geq 1$, we have $X^3/b^2 \geq X \geq 1$, and $y_i^2 = f(x_i) \leq H_f X^3$. We bound $|x(Q)|$ for each point that enters δ .

- $Q = P_i \pm P_j$. By the addition law, $|x(P_i \pm P_j)| \leq 4H_f X^3/b^2 + |a_2| + 2X \leq 7H_f X^3/b^2$, using $H_f + 2X \leq 3H_f X^3/b^2$.
- $Q = 2P_i$. Every root of f has absolute value at most H_f . If $|x_i| \geq 2H_f$, then $|f(x_i)| \geq |x_i|^3/8$, and the numerator of $x(2P_i)$ is at most $8H_f^2|x_i|^4$; so $|x(2P_i)| \leq 16H_f^2 X$. If $|x_i| < 2H_f$, then $|y_i| \geq 1$, so $|x(2P_i)| \leq 2H_f^2(2H_f)^4 = 32H_f^6$. In either case $|x(2P_i)| \leq 48H_f^6 X^3/b^2$.

Let $M = 48H_f^6 X^3/b^2 \geq 1$, so that $\max(1, |x(Q)|) \leq M$ for every Q entering δ . Proposition 8.9 gives $-\log \delta \leq \frac{1}{2} \log M + \kappa_\infty$ and $-\log |\omega_1| \leq \kappa_\infty$. Since (7) holds for every admissible $\rho < \frac{1}{2} \min(\delta, |\omega_1|)$, we may let ρ increase to this value:

$$-\log\left(\frac{1}{2} \min(\delta, |\omega_1|)\right) \leq \log 2 + \kappa_\infty + \frac{1}{2} \log M = \log 2 + \kappa_\infty + \frac{1}{2} \log 48 + 3 \log H_f + \frac{3}{2}L - \log |b|.$$

Combine this with (7) and $\log |2y_i| \leq \log 2 + \frac{1}{2} \log H_f + \frac{3}{2} L$. The $\log |b|$ terms cancel, and we get

$$B_i \leq 3L + \psi(N-1) + \kappa_\infty + \frac{7}{2} \log H_f + (2 \log 2 + \frac{1}{2} \log 48 + \frac{1}{4}).$$

The constant in parentheses is less than 3.58. Now apply Theorem 8.6 to the points P_i , $i \in I$; the hypotheses $P_i \pm P_j \neq O$ and $2P_i \neq O$ hold because the x_i are distinct and $y_i \neq 0$. The final form follows from Proposition 8.9. $\square$

Corollary 8.11 (Height form). *Let $C^-(E) = \sup_{P \in E(\mathbb{Q}) \setminus \{O\}} (\frac{1}{2} h(x(P)) - \widehat{h}(P))$. Silverman [24, Thm. 1.1] gives $C^-(E) \leq \frac{1}{24} h(j) + \mu(E) + 0.973$, where $\mu(E) = \frac{1}{12} h(\Delta) + \frac{1}{12} h_\infty(j) + \frac{1}{2} h_\infty(b_2/12) + \frac{1}{2} \log 2^*$. For the model (3) we have $b_2 = 4a_2$, $h(\Delta) \leq \log 864 + 4 \log H_f$ and $h(j), h_\infty(j) \leq \log \max(|c_4|^3, |\Delta_W|) \leq 12.48 + 6 \log H_f$. Hence*

$$C^-(E) \leq 3.45 + \frac{19}{12} \log H_f. \quad (8)$$

In the setting of Theorem 8.10,

$$\lambda_{\max}(G_I) \leq \frac{3}{2} \max_i \widehat{h}(P_i) + \frac{1}{4} \psi(N-1) + \frac{3}{2} C^-(E) + \frac{5}{4} \log H_f + 2.$$

Proof. Take i^* with $|x_{i^*}| = X$. Then $\frac{1}{2} L = \frac{1}{2} h(x_{i^*}) \leq \widehat{h}(P_{i^*}) + C^-(E)$. $\square$

Remark 8.12 (Numerical check). Theorem 8.7, with the actual levels and the actual δ , was tested on 104 integral progressions of length ≥ 4 . These were all such progressions on the curves $y^2 = x^3 + a_2 x^2 + a_4 x + a_6$ with $a_2 \in \{0, \pm 1, 2\}$, $|a_4|, |a_6| \leq 60$ and $-60 \leq x < 200$.

The ratio $\lambda_{\max}(G)/\frac{1}{4} \max_i B_i$ never exceeded 0.819. The ratio of $\lambda_{\max}(G)$ to the explicit bound of Theorem 8.10 never exceeded 0.27.

On the 8-term progression $x = -12, -8, \dots, 16$ on $y^2 = x^3 - 112x + 400$ (which is $5077a1$), and on its rescalings $x \mapsto u^2 x$ for $u = 2, 3, 5, 6$ (non-minimal models), the exact ratio was the same in every model: 0.626. This is consistent with the model independence of (6). See Appendix A.

Remark 8.13 (The archimedean diagonal place by place). The archimedean contribution to the diagonal has the heuristic size $D_i^\infty \approx \frac{3}{2} \log X - \log |b| - \frac{1}{2} \log |x_i|$. Lemma 8.5 gives it exactly:

$$D_i^\infty = S_{ii}^\infty = F_\infty(0) - F_\infty(2P_i) = -\log \rho + \frac{1}{4} - \frac{1}{12} \log |\Delta_W| - \lambda_\infty(2P_i).$$

To recover the heuristic size:

- Insert $-\log \rho \leq \frac{3}{2} L - \log |b| + \kappa_\infty + \frac{1}{2} \log 48 + 3 \log H_f + \log 2$ from Step 5 of Theorem 8.10.
- If $|x_i| \geq 8H_f$, the duplication formula gives $|x(2P_i)| \geq |x_i|/6$.
- A lower bound $\lambda_\infty(Q) \geq \frac{1}{2} \log \max(1, |x(Q)|) - \frac{1}{12} \log |\Delta_W| - O(1 + \log H_f)$ is the archimedean half of the explicit height-difference bounds [24, Thm. 5.5] (after the normalisation change [4, (11)]), [4, §§7–10].

Together these give

$$D_i^\infty \leq \frac{3}{2} L - \log |b| - \frac{1}{2} \log |x_i| + O(1 + \log H_f),$$

Theorem 8.10 does not use this per-place form. It sums $\lambda_v(2P_i)$ over all places into $4\widehat{h}(P_i)$, so no archimedean height-difference bound enters the cap itself.

Remark 8.14 (Other integral cubic models). Every integral cubic model reduces to (3) without changing the points, the span, or the fact that the x -coordinates form a progression.

- For $y^2 = cx^3 + a_2x^2 + a_4x + a_6$, the substitution $(X, Y) = (cx, cy)$ gives $Y^2 = X^3 + a_2X^2 + ca_4X + c^2a_6$. The new progression has difference cb , and $H \leq c^2H_f$.
- For a general Weierstrass equation, the substitution $(X, Y) = (4x, 4(2y + a_1x + a_3))$ gives $Y^2 = X^3 + b_2X^2 + 8b_4X + 16b_6$. The new progression has difference $4b$, and the new height is polynomial in the old coefficients.

So Theorem 8.10 and Section 9 apply to all integral cubic models, with $\log H_f$ replaced by $O(1 + \log H)$. Quartic models $y^2 = g(x)$ are different: the map to the Jacobian does not carry progressions to progressions, so they are left open (Section 13).

9 The linear bound

Lemma 9.1. *For an integer progression $x_i = a + ib$ ($0 \leq i < N$) with $X = \max |x_i|$, all but at most one index satisfy $|x_i| \geq X/(2N)$.*

Proof. Write $x_i = b(i - t)$ with $t = -a/b \in \mathbb{R}$, and let $M = \max_i |i - t| = X/|b|$. Let i_0 be an index nearest to t ; every other index has $|i - t| \geq \frac{1}{2}$.

- If $M \leq N$, then $|i - t|/M \geq 1/(2N)$.
- If $M > N$, then t lies outside $[0, N-1]$, so $|i - t| \geq M - (N-1)$ for every i , and $(M - N + 1)/M > 1/N$.

□

Theorem 9.2 (Linear bound, explicit form). *Let W be as in (3), and let $P_0, \dots, P_{N-1} \in E(\mathbb{Z})$ with $x_i = a + ib$, $b \neq 0$, $N \geq 12$. Let s be the span rank. Then*

- (a) $L \geq \log |b| \geq \vartheta(Y_N) - \log 6 - \log |\text{disc } f|$;
- (b) $(N - 4)(\frac{1}{2}L - \frac{1}{2}\log(2N) - C^-(E)) \leq s(\frac{3}{4}L + \frac{1}{4}\psi(N - 1) + \frac{5}{4}\log H_f + 2)$.

Proof. (a) Corollary 4.5 with $\text{lc}(f) = 1$ gives the second inequality. The first is $X \geq |b|$.

(b) Let I be the set of indices $i \neq i_0$ (with i_0 from Lemma 9.1) such that $y_i \neq 0$. At most three x_i are roots of f , so $|I| \geq N - 4$. For $i \in I$,

$$\widehat{h}(P_i) \geq \frac{1}{2} \log \max(1, |x_i|) - C^-(E) \geq \frac{1}{2}L - \frac{1}{2} \log 2N - C^-(E).$$

The principal submatrix G_I has rank $\leq s$. Lemma 7.1 and Theorem 8.10 give

$$\sum_{i \in I} \widehat{h}(P_i) = \text{tr } G_I \leq s \lambda_{\max}(G_I).$$

If the bracket on the left of (b) is negative, (b) holds trivially. □

Corollary 9.3. *If $N \rightarrow \infty$ along a sequence of integral progressions on models with $\log H_f = o(N^2)$, then*

$$N \leq \left(\frac{3}{2} + o(1)\right)s \leq \left(\frac{3}{2} + o(1)\right)r.$$

Proof. We have $|\text{disc } f| \leq 54H_f^4$, and $\vartheta(Y_N) = (1 + o(1))N^2/49$. So (a) gives $L \geq (1 - o(1))N^2/49$. Every other term in (b) is $o(L)$: $\psi(N - 1) \leq 1.04N$ [12, Lemma 4.3], [19], $\log 2N$, $\log H_f$, and $C^-(E)$ by (8). Dividing (b) by L gives $N - 4 \leq s(\frac{3}{2} + o(1))$. □

Corollary 9.4 (General form). *For every $\varepsilon > 0$ there is an effective C_ε such that every integral x -progression on a model (3) satisfies*

$$N \leq \left(\frac{3}{2} + \varepsilon\right)s + C_\varepsilon \sqrt{1 + \log H_f}.$$

Proof. Choose $K = K(\varepsilon)$ and $N_1 = N_1(\varepsilon)$ large. Suppose $N \geq N_1$ and $N^2 \geq K(1 + \log H_f)$. Then by Theorem 9.2(a), $L \geq N^2/60$ once K and N_1 are large. Moreover, by (8), $C^-(E) + \frac{5}{4} \log H_f + 2 \leq 6(1 + \log H_f) \leq 6N^2/K \leq 360L/K$, and $\psi(N-1) \leq 63L/N$. So the ratio of the bracket on the right of (b) to the bracket on the left is at most $\frac{3}{2} + \varepsilon$, and $N \leq (\frac{3}{2} + \varepsilon)s + 4$.

Otherwise $N < \max(N_1, \sqrt{K(1 + \log H_f)})$. □

N	20	50	100	150	200	500	1000	5000	∞
bound on $(N-4)/s$	3.10	2.03	1.89	1.78	1.69	1.56	1.53	1.505	3/2

Table 4: The ratio $(\frac{3}{4}L + \frac{1}{4}\psi(N-1))/(\frac{1}{2}L - \frac{1}{2}\log 2N)$ with L the forced lower bound (curve constants omitted, i.e. H_f bounded). The forced primes are those of Table 1, optimised exactly. With point counting alone the ratio would tend to $7/4$.

Remark 9.5. The theorem is vacuous for every known example: all have $N \leq 8$ on cubics, and $N \leq 14$ on quartics (MacLeod [17]). It becomes meaningful around $N \approx 50$, provided $\log H_f$ is small compared with N^2 .

The constant $\frac{3}{2}$ is the limit of the method. The diagonal (6) contains the separation term ($\approx \frac{3}{2}L - \log |b|$) and the denominator of $x(2P_i)$ ($\approx \frac{3}{2}L$), while the trace only sees $\hat{h} \approx \frac{1}{2}L$. The cosine bound $\lambda_{\max}(M) \leq \frac{3}{2}$ is attained in the function-field example 10.3.

Corollary 9.6 (Families). *For fixed $\varepsilon > 0$:*

- (a) Quadratic twists. *Fix $y^2 = f(x)$ as in (3), and for squarefree D consider the twist model $y^2 = x^3 + Da_2x^2 + D^2a_4x + D^3a_6$. It has $H \leq |D|^3H_f$. So its longest integral progression satisfies*

$$\beta_{\text{int}} \leq \left(\frac{3}{2} + \varepsilon\right)r(E^{(D)}) + O_{\varepsilon,E}(\sqrt{\log |D|}) \ll_E \omega(D) + \sqrt{\log |D|},$$

using $r(E^{(D)}) \ll_E 1 + \omega(D)$ from a 2-descent.

- (b) Mordell and congruent-number curves. *On $y^2 = x^3 + n$ and on $y^2 = x^3 - n^2x$, integral progressions satisfy $\beta_{\text{int}} \leq (\frac{3}{2} + \varepsilon)r + O_\varepsilon(\sqrt{\log |n|})$.*

10 Function fields: the exact version

Let $\mathcal{S} \rightarrow \mathbb{P}^1$ be an elliptic surface over $\mathbb{C}$ with zero section O , arithmetic genus χ , and minimal Weierstrass equation $y^2 = x^3 + A_2x^2 + A_4x + A_6$ with $\deg A_k \leq k\chi$. Assume all singular fibres are irreducible.

A section P is *integral* ($P \cdot O = 0$) exactly when $x(P), y(P)$ are polynomials of degree $\leq 2\chi$ and $\leq 3\chi$ respectively. For such sections, Shioda's formula [22], [21, Ch. 6] reads

$$\langle P, Q \rangle = \chi - (P \cdot Q) \quad (P \neq Q), \quad \langle P, P \rangle = 2\chi.$$

Theorem 10.1 (Exact colouring formula). *Let $P_0, \dots, P_{N-1}$ be integral sections with $x_i = a + ib$, where $a, b \in \mathbb{C}[t]$ and $b \neq 0$. Regard b as a section of $\mathcal{O}(2\chi)$, with zeros v of multiplicity e_v (including ∞ with multiplicity $2\chi - \deg b$), so that $\sum_v e_v = 2\chi$. Assume $y_i(v) \neq 0$ for all i and v . Fix a square root η_v of the common value $f_v(a(v))$, and put $c_v(i) = y_i(v)/\eta_v \in \{\pm 1\}$. Then*

$$\langle P_i, P_j \rangle = -\frac{1}{2} \sum_v e_v c_v(i) c_v(j) \quad (i \neq j), \quad \langle P_i, P_i \rangle = 2\chi.$$

Equivalently, the cosine matrix is $M = \frac{1}{2}(3I - C)$ with $C = \sum_v w_v c_v c_v^T$ and $w_v = e_v/2\chi$, so that $\sum_v w_v = 1$.

Proof. Two distinct integral sections can meet only over points where $x_i = x_j$. Since $x_i - x_j = (i - j)b$ and $i - j \in \mathbb{C}^\times$, these are exactly the zeros of b .

Over a finite zero v , $y_i(v)^2 = y_j(v)^2 = f_v(a(v)) \neq 0$, so the sections meet iff $c_v(i) = c_v(j)$. At the common point $\partial_y(y^2 - f) = 2y \neq 0$, so (t, x) are local coordinates on $\mathcal{S}$. The sections are the graphs $x = x_i(t)$ and $x = x_j(t)$, and their intersection multiplicity is $\text{ord}_v(x_i - x_j) = e_v$. At ∞ , use the chart $s = 1/t$, $X = s^{2\chi}x$, $Y = s^{3\chi}y$; the same computation gives $e_\infty = 2\chi - \deg b$.

Hence

$$P_i \cdot P_j = \sum_v e_v \mathbf{1}[c_v(i) = c_v(j)] = \chi + \frac{1}{2} \sum_v e_v c_v(i) c_v(j).$$

Substitute this into Shioda's formula. □

Corollary 10.2. *In the setting of Theorem 10.1:*

- (a) $N \leq 3/\max_v w_v \leq 6\chi$, and $N \leq \frac{3}{2}s$. Here $s \leq \rho - 2 \leq 10\chi - 2$ by Shioda–Tate.
- (b) If $\chi = 1$ (rational elliptic surfaces), then $N \leq 6$. Equality forces two simple zeros with $c_1 \perp c_2$, $s = 4$, and a relation lattice of dimension 2.
- (c) A double zero of b gives $C = cc^T$, so $N \leq 3$, and $N = 3$ forces a dependence.

Proof. $M \succeq 0$ forces $\lambda_{\max}(C) \leq 3$. Since $C \succeq w_v c_v c_v^T$, we have $\lambda_{\max}(C) \geq w_v N$. Also $\max_v w_v \geq 1/(2\chi)$, because there are at most 2χ zeros. Next, $C \succeq 0$ gives $\lambda_{\max}(M) \leq \frac{3}{2}$, and Lemma 7.1 gives $N \leq s\lambda_{\max}(M) \leq \frac{3}{2}s$.

For (b) with $N = 6$: we need $w_1 = w_2 = \frac{1}{2}$ and $\lambda_{\max}(C) = 3$. The nonzero eigenvalues of $\frac{1}{2}(c_1 c_1^T + c_2 c_2^T)$ are $\frac{1}{2}(6 \pm |c_1 \cdot c_2|)$, so $c_1 \cdot c_2 = 0$. Then C has the eigenvalue 3 twice, so M has nullity 2 and $s = 4$.

For (c): if $C = cc^T$, then $\lambda_{\max}(C) = N \leq 3$, and $N = 3$ gives $\lambda_{\min}(M) = 0$. □

Example 10.3 (An $A_2 \oplus A_1$ progression). (computer-assisted) On the rational elliptic surface

$$y^2 = x^3 + (22t^2 - 46t + 13)x^2 + (8t^4 - 24t^3 + 9t^2 + 4t - 2)x + (t^3 - 2t^2 - 4t + 1)^2,$$

whose discriminant is squarefree of degree 12 (so all fibres are I_1), the sections

$$x = -t, 0, t \quad \text{with} \quad y = t^3 - 6t^2 + 3t - 1, \quad t^3 - 2t^2 - 4t + 1, \quad t^3 + 2t^2 - 5t + 1$$

are integral. Here $b = t$ has simple zeros at 0 and ∞ , with colourings $(-, +, +)$ and $(+, +, +)$.

Theorem 10.1 gives the Gram matrix $\begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & -1 \\ 0 & -1 & 2 \end{pmatrix}$, of type $A_2 \oplus A_1$, with $\lambda_{\max}(M) = \frac{3}{2}$.

10.1 Realising sign data: rational and $K3$ surfaces

Throughout this subsection, a 3-term progression is indexed by $i \in \{-1, 0, 1\}$, with $x_i = a + ib$. Replacing P_i by $-P_i$ leaves the x -progression unchanged and flips $c_v(i)$ at every zero v simultaneously. We call two sets of sign data *equivalent* if they differ by such flips, by a global sign at a single zero (the choice of η_v), and by relabelling the zeros.

Lemma 10.4 (Interpolation criterion). *Let $a, b \in \mathbb{C}[t]$ with $\deg a \leq 2\chi$, and let b be squarefree of degree exactly 2χ , with zeros $v_1, \dots, v_{2\chi}$. Let $y_{-1}, y_0, y_1 \in \mathbb{C}[t]$ have degree $\leq 3\chi$. Then there is a monic cubic $f = x^3 + A_2x^2 + A_4x + A_6$ with $\deg A_k \leq k\chi$ and $y_i^2 = f(a + ib)$ for $i = -1, 0, 1$ if and only if, at every zero v of b ,*

$$y_{-1}(v)^2 = y_0(v)^2 = y_1(v)^2 \quad \text{and} \quad (y_1y_1' - 2y_0y_0' + y_{-1}y_{-1}')(v) = 0. \quad (9)$$

If $y_0(v) \neq 0$ and $y_i(v) = c_v(i)\eta_v$, the second condition is the linear condition $c_v(1)y_1'(v) - 2c_v(0)y_0'(v) + c_v(-1)y_{-1}'(v) = 0$.

Proof. Lagrange interpolation at the three nodes $a-b, a, a+b$ shows that every monic cubic through the three points (x_i, y_i^2) has the form

$$f(x) = (x - a + b)(x - a)(x - a - b) + y_0^2 + (x - a)D_1 + (x - a)^2D_2,$$

where

$$D_1 = \frac{y_1^2 - y_{-1}^2}{2b}, \quad D_2 = \frac{y_1^2 - 2y_0^2 + y_{-1}^2}{2b^2},$$

and this f is unique. So f has polynomial coefficients if and only if $b \mid y_1^2 - y_{-1}^2$ and $b^2 \mid y_1^2 - 2y_0^2 + y_{-1}^2$. Since b is squarefree, these divisibilities are exactly the conditions (9). The first condition gives the value conditions, and the derivative of the second-difference numerator gives the derivative condition.

The degree bounds are then automatic. The numerators have degree $\leq 6\chi$ and $\deg b = 2\chi$, so $\deg D_2 \leq 2\chi$ and $\deg D_1 \leq 4\chi$. Expanding f in powers of x gives $\deg A_2 \leq 2\chi$, $\deg A_4 \leq 4\chi$ and $\deg A_6 \leq 6\chi$. $\square$

So the progressions with prescribed sign data at the zeros of b form a linear family. There are 3 linear conditions per zero, on $3(3\chi + 1)$ coefficients. “All fibres I_1 ” (Δ squarefree of degree 12χ , which in particular makes the Weierstrass model minimal and all fibres irreducible) is a Zariski-open condition on this family. Hence a single member with all fibres I_1 shows that the generic member has all fibres I_1 too.

Theorem 10.5 (3-term types on rational elliptic surfaces). *Let $\chi = 1$, and assume all singular fibres are irreducible.*

- (a) *Classification. Suppose b has two simple zeros v_1, v_2 . Up to equivalence, the sign data are classified by $d = c_{v_1}c_{v_2} \in \{\pm 1\}^3 / \pm 1$ (coordinatewise product), which takes four values. The Gram matrices are as follows.*

d	Gram matrix of (P_{-1}, P_0, P_1)	type
$(+, +, +)$	$\begin{pmatrix} 2 & -1 & -1 \\ -1 & 2 & -1 \\ -1 & -1 & 2 \end{pmatrix}$	A_2 ; $P_{-1} + P_0 + P_1 = O$ (collinear)
$(-, +, +)$	$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & -1 \\ 0 & -1 & 2 \end{pmatrix}$	$A_1 \oplus A_2$, end term orthogonal
$(+, +, -)$	$\begin{pmatrix} 2 & -1 & 0 \\ -1 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$	$A_2 \oplus A_1$, end term orthogonal
$(+, -, +)$	$\begin{pmatrix} 2 & 0 & -1 \\ 0 & 2 & 0 \\ -1 & 0 & 2 \end{pmatrix}$	$A_2 \oplus A_1$, middle term orthogonal

If b has a double zero, the Gram matrix is of type A_2 and the three points are collinear.

(b) Realisation. All five cases occur with all fibres I_1 .

Proof. (a) Use the flips to make $c_{v_1} = (+, +, +)$. Then $c_{v_2} = d$, and d is defined up to the global sign at v_2 . Theorem 10.1 gives $\langle P_i, P_j \rangle = -\frac{1}{2}(1 + d(i)d(j))$ for $i \neq j$, which produces the four matrices.

For a double zero, $\langle P_i, P_j \rangle = -c(i)c(j)$. After flips the Gram matrix is A_2 , which has rank 2 with kernel $(1, 1, 1)$. So $P_{-1} + P_0 + P_1$ has height 0. The Mordell–Weil group of a rational elliptic surface with irreducible fibres is torsion-free: it is the E_8 lattice [21, Ch. 8]. So $P_{-1} + P_0 + P_1 = O$. In the $d = (+, +, +)$ case the same argument applies.

(b) Lemma 10.4 reduces realisation to linear algebra. One explicit member of each family with Δ squarefree of degree 12 is listed in Appendix A, item A.9. In each one, $y_0(v) \neq 0$ at the zeros of b , and the Gram matrix was recomputed independently of Theorem 10.1, from intersection numbers. For example, for $d = (+, -, +)$ take

$$a = 2t^2 + 2t + 3, \quad b = t^2 - t, \quad \begin{cases} y_{-1} = -16t^3 + 35t^2 - 15t + 2, \\ y_0 = -t^3 + t^2 - 8t + 2, \\ y_1 = 2t^3 + 3t^2 - t + 2, \end{cases}$$

with f given by Lemma 10.4. For the double zero, take a collinear triple on the line $y = mx + k$ and put $f = (mx + k)^2 + \prod_i (x - x_i)$ with $b = t^2$. $\square$

Theorem 10.6 (Sign data on elliptic $K3$ surfaces). *Let $\chi = 2$, let b have four simple zeros, and assume all fibres are I_1 .*

(a) *Normalise $c_{v_1} = (+, +, +)$. The sign data at the other three zeros then form one of 20 multisets of classes. All 20 are realised, so every equivalence class of sign data occurs. Their Gram matrices, given by Theorem 10.1, agree with direct intersection counts.*

(b) *The old Gram matrix $\begin{pmatrix} 4 & -1 & 1 \\ -1 & 4 & 0 \\ 1 & 0 & 4 \end{pmatrix}$, with a cosine $+\frac{1}{4}$, is realised by the sign data*

$$((+, +, +), (-, +, +), (+, +, -), (+, -, +)).$$

(c) *Sign data with $c_v(-1)c_v(1)$ constant across the four zeros are realised as well. They give $\langle P_{-1}, P_1 \rangle = \pm 2$, that is, a cosine $\pm \frac{1}{2}$.*

Proof. (a) Each of the other three zeros carries one of four classes, and the zeros are unordered, which gives $\binom{6}{3} = 20$ multisets. This overcounts equivalence classes, because the choice of reference zero is not fixed, but it covers all of them. For realisation, see item A.9 of the appendix.

- For each class, Lemma 10.4 yields a linear family, from which a member was drawn.
- Each member has Δ squarefree of degree 24, and $y_0(v) \neq 0$ at all four zeros.
- In each case the Gram matrix was computed from intersection numbers, and it equals the formula.

(b) is one of the 20 cases. Explicitly, $b = t(t-1)(t+1)(t-2)$ and $a = -3t^3 + 2t^2 + t - 3$, with

$$\begin{aligned} y_{-1} &= \frac{13}{2}t^6 - 20t^5 + 51t^4 - 38t^3 - \frac{101}{2}t^2 + 63t - 3, \\ y_0 &= t^6 - 2t^5 + 35t^4 - 32t^3 - 38t^2 + 30t - 3, \\ y_1 &= -3t^6 - t^5 + 2t^4 - t^3 - 3t - 3, \end{aligned}$$

and f is given by Lemma 10.4.

(c) These are the cases $c_{v_k} \in \{(+, +, +), (+, -, +)\}$ for $k = 2, 3, 4$, and all of them are realised. $\square$

Remark 10.7 (Signs and obtuseness). A positive cosine is not an invariant of a progression: replacing P_i by $-P_i$ keeps the x -progression and changes signs in the Gram matrix. The invariant quantity is $\Pi = G_{-1,0} G_{0,1} G_{-1,1}$. When $\Pi \leq 0$, such flips make every off-diagonal entry ≤ 0 , so the triple is obtuse up to sign. For four simple zeros, $\Pi \leq 0$ always holds. To see this, write $u_v = c_v(-1)c_v(0)$ and $w_v = c_v(0)c_v(1)$. Then $\Pi = -\frac{1}{8}S_u S_w S_{uw}$, where $S_u = \sum_v u_v$. If S_u and S_w are both nonzero, each of u and w has at most one entry differing from the majority, and a check of the cases gives $S_u S_w S_{uw} \geq 0$. For example, the matrix in (b) becomes $\begin{pmatrix} 4 & -1 & -1 \\ -1 & 4 & 0 \\ -1 & 0 & 4 \end{pmatrix}$ after flipping P_1 .

11 Relation to earlier work

The analytic ingredients of Section 8 are not new. What appears to be new is how they are combined.

- **Positive-type Néron functions.** Baker and Petsche [1, Prop. 2, (13)] prove that the archimedean Néron function has nonnegative Fourier coefficients $\widehat{\lambda}(\gamma_\omega) = b/(2\pi|\omega'|^2)$; compare Lemma 8.4. They smooth it by convolution with a heat kernel, where we use a disc measure (Lemma 8.5). For multiplicative reduction they use the Fourier positivity of the Bernoulli term [1, Prop. 5]. Their Theorem 8 sums local discrepancies into a global lower bound for $\sum_{i \neq j} \widehat{h}(P_i - P_j)$.
- **Fourier positivity at bad places.** Hindry and Silverman [12, §3, §4] use the positivity of $\widehat{B}_2$, through the Blanksby–Montgomery–Fejér argument, to bound weighted sums of local heights at places of multiplicative reduction. To handle additive reduction they pass to multiples of the point.
- **Average Green-function bounds.** Faltings and Elkies bound the average of the Arakelov–Green function over pairs of n points from below by $-O((\log n)/n)$. Wilms [14] gives an alternative, effective proof. This is the Riemann-surface analogue of Baker–Petsche’s archimedean discrepancy, and like it, it controls the quadratic form at the all-ones vector only.

- **Gram matrices and lattice symmetry.** Prakash [13] bounds Néron–Tate heights by spectral-gap criteria for automorphisms acting on the Mordell–Weil lattice. That work uses the height Gram matrix, but for a different purpose: effective Mordell rather than progressions.
- **Quasi-orthogonality.** Helfgott and Venkatesh [15, §3] prove that integral points are nearly orthogonal in the Mordell–Weil lattice, using local heights and a Mumford-type gap principle.

What the present argument adds:

- (a) *Antisymmetrisation* (Lemma 8.1). The kernel $F(g_i - g_j) - F(g_i + g_j)$ is insensitive to real characters, and it yields a matrix inequality $G \preceq \frac{1}{4} \text{diag}(B_i)$ valid for every test vector. Baker–Petsche’s kernel $\lambda(P_i - P_j)$ controls only the quadratic form at the all-ones vector, i.e. $\mathbf{1}^T G \mathbf{1} - \text{tr } G$, and positivity of the full Fourier series is needed there.
- (b) *Additive reduction without base change.* Positivity at characters of order > 2 holds for every Kodaira type (Proposition 8.3), and the component terms cancel from the diagonal (Theorem 8.7). Baker–Petsche work over a field where E is semistable; Hindry–Silverman replace P by a multiple.
- (c) *The exact diagonal identity* (6), together with its application to progressions via the local theory of Sections 3–6.

We have not found (a) or (c) in the literature checked ([1, 18, 12, 15, 4, 24, 14, 13]). A wider search of matrix forms of the Mumford gap principle is still advisable before claiming novelty.

12 Comparison with the exponential bounds

Several results bound progression length exponentially in the rank:

- Garcia-Fritz and Pasten [7]: $1 + r \geq c(j_0) \log \max\{\beta_x, \beta_y\}$ for curves with fixed j -invariant, with $c(j_0) \asymp 1/\log \log H(j_0)$.
- Combined with Gao–Ge–Kühne [6], their method gives the uniform bound $n \leq c(d)^{1+\text{rank } \Gamma}$ [9, Thm. 1.1].
- Harrison, Mudgal and Schmidt [10] prove $|A| \leq C^{1+r}$ with an effective absolute C .
- [8] deduces uniform boundedness of progression lengths from uniform boundedness of ranks, via Dimitrov–Gao–Habegger [5].

Corollary 9.4 concerns integral progressions only. It is linear in the span rank, but has a $\sqrt{\log H_f}$ dependence on the model. The two kinds of result are complementary, and the useful bound is the minimum of the two.

result	statement	effect of Corollaries 9.4 and 9.6
[7, Thm. 1.1]	$1 + r \geq c(j_0) \log \beta$	$s \geq (\frac{2}{3} - \varepsilon)N - O_\varepsilon(\sqrt{1 + \log H_f})$: linear, and about the span itself (Bremner’s “tend to be independent”)
[7, Cor. 1.3] (twists) [7, Cors. 1.4, 1.5]	$\beta(E^{(D)}) \leq C(E)^{\omega(D)+1}$ bounded ranks $\Rightarrow$ bounded β ; Mohanty	$\beta_{\text{int}}(E^{(D)}) \ll_E \omega(D) + \sqrt{\log D }$ not improved: the $\sqrt{\log H_f}$ term blocks uniformity; unconditionally $\beta_{\text{int}}(y^2 = x^3 + n) \leq (\frac{3}{2} + \varepsilon)r + O(\sqrt{\log n })$
[7, Thms. 1.6, 1.7]	bounded average moments	moments not improved (the average of $(\log n)^{k/2}$ grows). Using the bounded averages of κ^r ($\kappa > 1$) that [7] uses, for $B \gg \sqrt{\log x}$ the tail $\Pr(\beta_{\text{int}} > B)$ decays exponentially in B ; the bound $\beta \leq e^{O(1+r)}$ gives only polynomial decay
[7, Thm. 1.2] (torsion)	no long progressions of torsion	not touched

13 Open problems

1. Remove the $\sqrt{\log H_f}$ term in Theorem 1.1, for instance via a Lang-type lower bound for $\widehat{h}$ on progression points. This would make the bound uniform in E .
2. Extend the spectral cap to rational points with mixed denominators. The exact identity (6) holds for arbitrary points; what changes is the level bound of Step 2 of Theorem 8.10.
3. Treat quartic models, such as MacLeod’s 14-term examples [17]. The local theory applies, but the spectral half needs the local heights of the Jacobian.
4. Does a 7-term x -progression with no collinear triple have a smooth zero at a good prime?
5. Extend Theorem 10.5 to $N \geq 4$ terms on rational elliptic surfaces. For $N = 6$, Corollary 10.2 forces $c_1 \perp c_2$.
6. Determine whether the antisymmetrised kernel of Lemma 8.1 appears in matrix forms of the Mumford gap principle; see Section 11.

A Computations

All computations were run with PARI/GP 2.17.2 (through `cypari2`) and SymPy.

- A.1 *Identities.* The sum and product formulae for $x(P \pm Q)$ in Step 2 of Theorem 8.10, and the duplication numerator in Step 3, were verified symbolically for $y^2 = x^3 + a_2x^2 + a_4x + a_6$.
- A.2 *Fourier coefficients.* $\widehat{c}(k) = 1/(4m \sin^2(\pi k/m))$ for type I_m was checked to 10^{-9} for all $m < 200$ and all k .
- A.3 *Archimedean constants.* $j(i\sqrt{3}/2) = 2309.5777\dots$, so the tail in Step 3 of Proposition 8.9 is 1334.8. The factor $|\prod(1 - q^n)|^{24}$ was at least 0.957 on 2000 random τ . A random search over τ and z gave an empirical value $0.62 < c_0 = 1.68$ for Step 1.
- A.4 *Forbidden range.* Tables 1 and 4 were computed by evaluating (4) exactly, for every H , using the monotonicity in p . They agree with the earlier figures (293, 2819, 19213). A sampled check gives $\max(N_{\max}(p) - 7\sqrt{p}) \approx 30$, well inside the proved 77.

A.5 *Spectral cap.* As in Remark 8.12. The levels were computed on `ellminimalmodel`, the distances via `ellpointtoz` with a search over nearby lattice points, and G from $\frac{1}{2}\text{ellheight}$. No violation occurred.

A.6 *Nine 8-term solutions.* Proposition 5.4. Damped primes were detected by the vanishing of both partial derivatives at the reduction, in the minimal model; types came from `elllocalred`.

A.7 *Smooth zeros.* Proposition 5.6.

- Length 7: `ellrank` returns $[7, 7]$; 7 has type I_0 ; 19 and 43 have type IV.
- Length 8: from $146G$, on a model minimal at 7 (from `elllocalred`): good reduction, $v_7(b) = 1$, and $Y \bmod 7 \in \{\pm 1\}$.

A.8 *Function-field example.* The section identities and the discriminant of Example 10.3 were checked symbolically.

A.9 *Realising sign data* (Theorems 10.5 and 10.6). For $\chi = 1$ we took $b = t(t - 1)$, and for $\chi = 2$ we took $b = t(t - 1)(t + 1)(t - 2)$. For each class of sign data:

- we solved the linear conditions of Lemma 10.4 and drew a random small integer member together with a random a ;
- we checked $y_i^2 = f(x_i)$ and $\deg A_k \leq k\chi$;
- we checked that Δ is squarefree of degree 12χ and that $y_0(v) \neq 0$ at every zero of b ;
- we computed $P_i \cdot P_j$ as $\deg \gcd(x_i - x_j, y_i - y_j)$ plus the same quantity at $t = \infty$, in the chart $(s^{2\chi}x, s^{3\chi}y)$, and recovered the Gram matrix from $\langle P_i, P_j \rangle = \chi - P_i \cdot P_j$.

All 4 classes for $\chi = 1$ with simple zeros, the collinear double-zero case, and all 20 multisets for $\chi = 2$ were realised. In every case the intersection-count Gram matrix equals the formula of Theorem 10.1. The scripts are available from the author on request.

Use of AI tools

This paper is the result of human-directed work with Claude (Anthropic), accessed through a Claude Pro subscription. Over many conversations, the author directed the research, and synthesized and assembled the results with Claude's assistance. Claude contributed substantially to developing the proofs, to running the computations reported in Appendix A, and to drafting the text. The author takes responsibility for the content of the paper.

References

- [1] M. Baker, C. Petsche, *Global discrepancy and small points on elliptic curves*, IMRN 2005; arXiv:math/0507228.
- [2] A. Bremner, *On arithmetic progressions on elliptic curves*, Experiment. Math. 8 (1999), no. 4, 409–413.
- [3] A. Bremner, J. H. Silverman, N. Tzanakis, *Integral points in arithmetic progression on $y^2 = x(x^2 - n^2)$* , J. Number Theory 80 (2000), 187–208.

- [4] J. E. Cremona, M. Prickett, S. Siksek, *Height difference bounds for elliptic curves over number fields*, J. Number Theory 116 (2006), 42–68.
- [5] V. Dimitrov, Z. Gao, P. Habegger, *Uniformity in Mordell–Lang for curves*, Ann. of Math. 194 (2021), 237–298.
- [6] Z. Gao, T. Ge, L. Kühne, *The uniform Mordell–Lang conjecture*, arXiv:2105.15085.
- [7] N. Garcia-Fritz, H. Pasten, *Elliptic curves with long arithmetic progressions have large rank*, IMRN 2021; arXiv:1910.14485.
- [8] N. Garcia-Fritz, H. Pasten, *A note on Bremner’s conjecture and uniformity*, arXiv:2604.04850.
- [9] N. Garcia-Fritz, H. Pasten, *Patterns on elliptic curves beyond Bremner’s conjecture*, arXiv:2605.14962.
- [10] J. Harrison, A. Mudgal, H. Schmidt, *Uniform sum-product phenomenon for algebraic groups and Bremner’s conjecture*, arXiv:2603.06483.
- [11] H. Iwaniec, E. Kowalski, *Analytic Number Theory*, AMS Colloq. Publ. 53, 2004.
- [12] M. Hindry, J. H. Silverman, *The canonical height and integral points on elliptic curves*, Invent. Math. 93 (1988), 419–450.
- [13] M. Prakash, *Effective height bounds from Mordell–Weil lattice symmetries*, arXiv:2509.22672.
- [14] R. Wilms, *An alternative proof of the Faltings–Elkies bound*, arXiv:2310.03648.
- [15] H. A. Helfgott, A. Venkatesh, *Integral points on elliptic curves and 3-torsion in class groups*, J. Amer. Math. Soc. 19 (2006), 527–550.
- [16] R. Lidl, H. Niederreiter, *Finite Fields*, Encycl. Math. Appl. 20, 2nd ed., Cambridge Univ. Press, 1997.
- [17] A. J. MacLeod, *14-term arithmetic progressions on quartic elliptic curves*, J. Integer Seq. 9 (2006), 06.1.2.
- [18] C. Petsche, *Small rational points on elliptic curves over number fields*, arXiv:math/0508160.
- [19] J. B. Rosser, L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. 6 (1962), 64–94.
- [20] W. M. Schmidt, *Equations over Finite Fields: An Elementary Approach*, LNM 536, Springer, 1976.
- [21] M. Schütt, T. Shioda, *Mordell–Weil Lattices*, Ergeb. Math. 70, Springer, 2019.
- [22] T. Shioda, *On the Mordell–Weil lattices*, Comment. Math. Univ. St. Paul. 39 (1990), 211–240.
- [23] J. H. Silverman, *Computing heights on elliptic curves*, Math. Comp. 51 (1988), 339–358.
- [24] J. H. Silverman, *The difference between the Weil height and the canonical height on elliptic curves*, Math. Comp. 55 (1990), 723–743.
- [25] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., GTM 106, Springer, 2009.
- [26] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, GTM 151, Springer, 1994.