Lower bounds for quadratic and cubic polynomials and subexponential Szpiro

Joint work with Héctor Pastén

José Cuevas Barrientos

Pontificia Universidad Católica de Chile

January 10, 2025

CIMPA

Given an integer n we define its **radical** as the positive number

$$\operatorname{Rad} n := \prod_{p \mid n} p,$$

where the product runs through the prime factors of n.
Given an elliptic curve E over $\mathbb{Q}$, we define its **conductor** as the number $N_E := \prod_p p^{f(p)}$, where the exponent $f(p)$ of the prime p is given by (when $p \nmid 6$)

$$f(p) := \begin{cases} 0, & \text{if } E \text{ has good reduction modulo } p, \\ 1, & \text{if } E \text{ has multiplicative reduction mod } p, \\ 2, & \text{if } E \text{ has additive reduction mod } p. \end{cases}$$

For the primes $p \in \{2, 3\}$, the definition is more complicated (see Silverman [**4**, p. 380]), but $0 \leq f(p) \leq 6$ (see Thm. IV.10.4 in [**4**, p. 385]).

Masser-Oesterlé's abc conjecture

Given $a+b=c$ in coprime integers, then for all $\epsilon > 0$ it holds

$$\max\{|a|,|b|,|c|\} \ll_\epsilon \operatorname{Rad}(abc)^{1+\epsilon}$$

Masser-Oesterlé's abc conjecture

Given $a+b=c$ in coprime integers, then for all $\epsilon > 0$ it holds

$$\max\{|a|, |b|, |c|\} \ll_\epsilon \operatorname{Rad}(abc)^{1+\epsilon}$$

The relationship with elliptic curves? The following!

Szpiro's conjecture

Let E be an elliptic curve over the field of rational numbers $\mathbb{Q}$ with minimal discriminant D_E and conductor N_E. Then for all $\epsilon > 0$

$$D_E \ll_\epsilon N_E^{1+\epsilon}.$$

Masser-Oesterlé's abc conjecture

Given $a+b=c$ in coprime integers, then for all $\epsilon > 0$ it holds

$$\max\{|a|,|b|,|c|\} \ll_\epsilon \mathrm{Rad}(abc)^{1+\epsilon}$$

The relationship with elliptic curves? The following!

Szpiro's conjecture

Let E be an elliptic curve over the field of rational numbers $\mathbb{Q}$ with minimal discriminant D_E and conductor N_E. Then for all $\epsilon > 0$

$$D_E \ll_\epsilon N_E^{1+\epsilon}.$$

Proposition

The abc conjecture (for exponents of the kind $6/5+\epsilon$) is equivalent to the Szpiro's conjecture.

What it was known (abc)

For $a + b = c$ in positive coprime integers with $R := \mathrm{Rad}(abc)$, it has been proven that:

Stewart–Tijdeman (1986)	$\log c \ll R^{15}$
Stewart–Yu (1991)	$\log c \ll R^{2/3+o(1)}$
Stewart–Yu (2001)	$\log c \ll R^{1/3}(\log R)^3$
Pastén (2022)	$\log c \ll_\eta \exp\left((1+\epsilon)(\log R)\dfrac{\log_3^* R}{\log_2^* R}\right) \qquad (a \leq c^{1-\eta})$
Pastén ([**2**], 2024)	$\log c \ll_\eta \exp\left(\kappa\sqrt{(\log R)\log_2 R}\right) \qquad (a \leq c^{1-\eta})$

What it was known (abc)

For $a+b=c$ in positive coprime integers with $R := \mathrm{Rad}(abc)$, it has been proven that:

Stewart–Tijdeman (1986)	$\log c \ll R^{15}$
Stewart–Yu (1991)	$\log c \ll R^{2/3+o(1)}$
Stewart–Yu (2001)	$\log c \ll R^{1/3}(\log R)^3$
Pastén (2022)	$\log c \ll_\eta \exp\left((1+\epsilon)(\log R)\frac{\log_3^* R}{\log_2^* R}\right) \quad (a \leq c^{1-\eta})$
Pastén ([**2**], 2024)	$\log c \ll_\eta \exp\left(\kappa\sqrt{(\log R)\log_2 R}\right) \quad (a \leq c^{1-\eta})$

Given an abc-triple, we may attach to it the **Frey curve**

$$E_{a,b,c}: \qquad y^2 = x(x+a)(x-b)$$

which (if $a \equiv -1 \pmod 4$ and $16 \mid b$) is semi-stable and its minimal discriminant and conductor are

$$D_{a,b,c} = \left(\frac{abc}{16}\right)^2, \qquad N_{a,b,c} = \mathrm{Rad}\left(\frac{abc}{16}\right),$$

so the bounds read...

What it was known (towards Szpiro)

Stewart–Tijdeman (1986)	$\log D \ll N^{15}$	for Frey curves
Stewart–Yu (1991)	$\log D \ll N^{2/3+o(1)}$	for Frey curves
Stewart–Yu (2001)	$\log D \ll N^{1/3}(\log N)^3$	for Frey curves
Murty–Pastén (2012)	$\log D \ll N \log N$	

What it was known (towards Szpiro)

Stewart–Tijdeman (1986)	$\log D \ll N^{15}$	for Frey curves
Stewart–Yu (1991)	$\log D \ll N^{2/3+o(1)}$	for Frey curves
Stewart–Yu (2001)	$\log D \ll N^{1/3}(\log N)^3$	for Frey curves
Murty–Pastén (2012)	$\log D \ll N \log N$	

Theorem 1 (C. B.–Pastén)

Let $A, B \in \mathbb{Z}[t]$ be coprime polynomials, not both constant, such that the discriminant $D = -16(4A^3 + 27B^2) \in \mathbb{Z}[t]$ is not the zero polynomial. Consider the elliptic surface (on the parameter t) of affine Weierstrass equation

$$E_t\colon \qquad y^2 = x^3 + A(t)x + B(t).$$

There is a(n effectively computable) constant $\kappa > 0$ depending only on $A(t)$ and $B(t)$, such that for every $|n| \gg 0$ one has

$$\log \varDelta_n \leq \exp\left(\kappa\sqrt{(\log^* N_n)\log_2^* N_n}\right).$$

Integer values of polynomials

Recently, Pastén used his theory of Shimura curves and his joint results with Ram Murty to obtain an improvement on a problem of Chowla:

Theorem (Pastén, [**2**])

Let $P(M)$ denote the greatest prime factor of the integer M, then

$$P(n^2+1) \gg \frac{(\log_2^* n)^2}{\log_3^* n}.$$

Recently, Pastén used his theory of Shimura curves and his joint results with Ram Murty to obtain an improvement on a problem of Chowla:

Theorem (Pastén, [2])

Let $P(M)$ denote the greatest prime factor of the integer M, then

$$P(n^2+1) \gg \frac{(\log_2^* n)^2}{\log_3^* n}.$$

Theorem 2 (C. B.–Pastén)

Let $f(x) \in \mathbb{Z}[x]$ be a quadratic polynomial with two complex roots or a cubic of the form $(ax+b)^3+c$ (with $ac \neq 0$). Then, for $n \gg 0$,

$$P(f(n)) \gg_f \frac{(\log_2^* n)^2}{\log_3^* n}.$$

Criterion

Let $f(x) \in \mathbb{Z}[x]$ be a polynomial with at least two different complex roots that satisfies the following property: there exists a constant $\mu := \mu(f) > 0$ such that

$$\forall n \gg 0, \qquad \prod_{p | f(n)} \nu_p(f(n)) \ll_f \mathrm{Rad}(f(n))^{\mu}. \tag{$*$}$$

Then there exists a constant $\kappa := \kappa(f) > 0$ such that

$$\forall n \gg 0, \qquad \log n \leq \exp\left(\kappa \sqrt{(\log \mathrm{Rad}\, f(n)) \log_2 \mathrm{Rad}\, f(n)}\right).$$

Corollary

$$P(f(n)) \gg_f \frac{(\log_2^* n)^2}{\log_3^* n}.$$

Toolbox

Theorem (Pastén [1, Cor. 16.3])

Let S be a finite set of prime numbers and let $\epsilon > 0$ be a positive real number. There is a constant $\kappa := \kappa(S, \epsilon) > 0$ with the following property:
For each elliptic curve E over $\mathbb{Q}$ which is semistable outside of S we have

$$\prod_{\substack{p \mid N_E \\ p \notin S}} \nu_p(D_E) \leq \kappa \cdot N_E^{11/2+\epsilon}.$$

Theorem (Murty–Pastén [3, Thm. 7.1])

There is an absolute and effective constant $\kappa > 0$ with the following property: for each elliptic curve E over $\mathbb{Q}$ one has

$$\log(D_E) \leq \kappa \cdot N_E \log N_E.$$

Proof of thm. 2 (quadratic case)

Write

$$f(x) = Ax^2 + Bx + C = \frac{1}{4A}((2Ax + B)^2 - \delta),$$

where $\delta := B^2 - 4AC$ is its discriminant.

Write

$$f(x) = Ax^2 + Bx + C = \frac{1}{4A}((2Ax+B)^2 - \delta),$$

where $\delta := B^2 - 4AC$ is its discriminant. Then, for each n, the affine Weierstrass equation

$$E_n\colon \qquad y^2 = x^3 - 3\delta x - 2\delta(2An+B) \tag{1}$$

defines an elliptic curve (with at most two exceptions) of discriminant $\Delta = -2^8 3^3 \cdot \delta^2 A f(n)$ and of j-invariant

$$j = -2^4 3^3 \frac{\delta}{Af(n)}.$$

Proof of thm. 2 (quadratic case)

Write

$$f(x) = Ax^2 + Bx + C = \frac{1}{4A}((2Ax+B)^2 - \delta),$$

where $\delta := B^2 - 4AC$ is its discriminant. Then, for each n, the affine Weierstrass equation

$$E_n : \qquad y^2 = x^3 - 3\delta x - 2\delta(2An + B) \tag{1}$$

defines an elliptic curve (with at most two exceptions) of discriminant $\Delta = -2^8 3^3 \cdot \delta^2 A f(n)$ and of j-invariant

$$j = -2^4 3^3 \frac{\delta}{Af(n)}.$$

Moreover, if $p \nmid 6\delta$ is a prime number, we see that the equation (1) is minimal at p. Also, we remark that $N_n \mid 6^8 \operatorname{Rad}(D_n)^2 \mid 6^8 \operatorname{Rad}(Af(n))^2$.

Claim

$$\nu_p(f(n)) = \nu_p(D_n) + (M-1) = \nu_p(D_n) + O_f(1).$$

First, notice that $\nu_p(f(n)) = \nu_p(\Delta) = \nu_p(D_n)$ when $p \nmid 6\delta A$. Otherwise, we have two scenarios:

Claim

$$\nu_p(f(n)) = \nu_p(D_n) + (M-1) = \nu_p(D_n) + O_f(1).$$

First, notice that $\nu_p(f(n)) = \nu_p(\Delta) = \nu_p(D_n)$ when $p \nmid 6\delta A$. Otherwise, we have two scenarios:

- $\nu_p(j) \geq 0$.
  In whose case $\nu_p(D_n) \leq 10$ by Tate's algorithm, and
  $\nu_p(f(n)) \leq \nu_p(2^4 3^3 \delta / A)$.

Claim

$$\nu_p(f(n)) = \nu_p(D_n) + (M-1) = \nu_p(D_n) + O_f(1).$$

First, notice that $\nu_p(f(n)) = \nu_p(\Delta) = \nu_p(D_n)$ when $p \nmid 6\delta A$. Otherwise, we have two scenarios:

- $\nu_p(j) \geq 0$.
  In whose case $\nu_p(D_n) \leq 10$ by Tate's algorithm, and
  $\nu_p(f(n)) \leq \nu_p(2^4 3^3 \delta / A)$.
- $\nu_p(j) < 0$. In whose case

$$\begin{aligned} |\nu_p(D_n) - \nu_p(f(n))| &\leq |\nu_p(D_n) + \nu_p(j)| + |-\nu_p(j) - \nu_p(f(n))| \\ &\leq 6 + |\nu_p(2^4 3^3 \delta / A)|. \end{aligned}$$

Claim

$$\nu_p(f(n)) = \nu_p(D_n) + (M-1) = \nu_p(D_n) + O_f(1).$$

First, notice that $\nu_p(f(n)) = \nu_p(\Delta) = \nu_p(D_n)$ when $p \nmid 6\delta A$. Otherwise, we have two scenarios:

- $\nu_p(j) \geq 0$.
  In whose case $\nu_p(D_n) \leq 10$ by Tate's algorithm, and
  $\nu_p(f(n)) \leq \nu_p(2^4 3^3 \delta / A)$.
- $\nu_p(j) < 0$. In whose case

$$\begin{aligned} |\nu_p(D_n) - \nu_p(f(n))| &\leq |\nu_p(D_n) + \nu_p(j)| + |-\nu_p(j) - \nu_p(f(n))| \\ &\leq 6 + |\nu_p(2^4 3^3 \delta / A)|. \end{aligned}$$

So $M = 11 + |\nu_p(2^4 3^3 \delta / A)|$ suffices.

Simplified Tate algorithm (for $p \nmid 6$)

Kodaira symbol	reduction	$\nu_p(D_E)$	
I_0	good	0	$\nu_p(j) \geq 0$
I_n	multiplicative	n	$\nu_p(j) = -n$
II	additive	2	$\tilde{j} = 0$
III	additive	3	$\tilde{j} = 1728$
IV	additive	4	$\tilde{j} = 0$
I_0^*	additive	6	$\nu_p(j) \geq 0$
I_n^*	additive	$6+n$	$\nu_p(j) = -n$
IV^*	additive	8	$\tilde{j} = 0$
III^*	additive	9	$\tilde{j} = 1728$
II^*	additive	10	$\tilde{j} = 0$

We treat the primes separately:

(i) If $p \nmid 6A\delta$, then, as $\nu_p(D_E) = -\nu_p(j)$, the curves E_n are semistable at p.

Theorem (Pastén [1, Cor. 16.3])

Let S be a finite set of prime numbers and let $\epsilon > 0$ be a positive real number. There is a constant $\kappa := \kappa(S, \epsilon) > 0$ with the following property:
For each elliptic curve E over $\mathbb{Q}$ which is semistable outside of S we have

$$\prod_{\substack{p \mid N_E \\ p \notin S}} \nu_p(D_E) \leq \kappa \cdot N_E^{11/2+\epsilon}.$$

Theorem (Murty–Pastén [3, Thm. 7.1])

There is an absolute and effective constant $\kappa > 0$ with the following property: for each elliptic curve E over $\mathbb{Q}$ one has

$$\log(D_E) \leq \kappa \cdot N_E \log N_E.$$

We treat the primes separately:

(i) If $p \nmid 6A\delta$, then, as $\nu_p(D_E) = -\nu_p(j)$, the curves E_n are semistable at p. So

$$\prod_{\substack{p \mid f(n) \\ p \nmid 6A\delta}} \nu_p(f(n)) = \prod_{\substack{p \mid f(n) \\ p \nmid 6A\delta}} \nu_p(D_E) \leq c_1 N_n^{11/2+\epsilon},$$

where c_1 depends on δ, A and $\epsilon > 0$. We will set $\epsilon = 1/4$ for comfort purposes.

We treat the primes separately:

(i) If $p \nmid 6A\delta$, then, as $\nu_p(D_E) = -\nu_p(j)$, the curves E_n are semistable at p. So

$$\prod_{\substack{p \mid f(n) \\ p \nmid 6A\delta}} \nu_p(f(n)) = \prod_{\substack{p \mid f(n) \\ p \nmid 6A\delta}} \nu_p(D_E) \leq c_1 N_n^{11/2+\epsilon},$$

where c_1 depends on δ, A and $\epsilon > 0$. We will set $\epsilon = 1/4$ for comfort purposes.

(ii) If $p \mid 6A\delta$, then by the result of Murty–Pastén

Toolbox

Theorem (Pastén [1, Cor. 16.3])

Let S be a finite set of prime numbers and let $\epsilon > 0$ be a positive real number. There is a constant $\kappa := \kappa(S, \epsilon) > 0$ with the following property:
For each elliptic curve E over $\mathbb{Q}$ which is semistable outside of S we have

$$\prod_{\substack{p \mid N_E \\ p \notin S}} \nu_p(D_E) \leq \kappa \cdot N_E^{11/2+\epsilon}.$$

Theorem (Murty–Pastén [3, Thm. 7.1])

There is an absolute and effective constant $\kappa > 0$ with the following property: for each elliptic curve E over $\mathbb{Q}$ one has

$$\log(D_E) \leq \kappa \cdot N_E \log N_E.$$

We treat the primes separately:

(i) If $p \nmid 6A\delta$, then, as $\nu_p(D_E) = -\nu_p(j)$, the curves E_n are semistable at p. So

$$\prod_{\substack{p|f(n)\\ p\nmid 6A\delta}} \nu_p(f(n)) = \prod_{\substack{p|f(n)\\ p\nmid 6A\delta}} \nu_p(D_E) \leq c_1 N_n^{11/2+\epsilon},$$

where c_1 depends on δ, A and $\epsilon > 0$. We will set $\epsilon = 1/4$ for comfort purposes.

(ii) If $p \mid 6A\delta$, then by the result of Murty–Pastén

$$\nu_p(D_E) \leq c_2 N_n \log N_n,$$

where $c_2 = c_2(A\delta) > 0$.

We treat the primes separately:

(i) If $p \nmid 6A\delta$, then, as $\nu_p(D_E) = -\nu_p(j)$, the curves E_n are semistable at p. So

$$\prod_{\substack{p \mid f(n) \\ p \nmid 6A\delta}} \nu_p(f(n)) = \prod_{\substack{p \mid f(n) \\ p \nmid 6A\delta}} \nu_p(D_E) \leq c_1 N_n^{11/2+\epsilon},$$

where c_1 depends on δ, A and $\epsilon > 0$. We will set $\epsilon = 1/4$ for comfort purposes.

(ii) If $p \mid 6A\delta$, then by the result of Murty–Pastén

$$\nu_p(D_E) \leq c_2 N_n \log N_n,$$

where $c_2 = c_2(A\delta) > 0$. If $p \mid f(n)$, then $\nu_p(f(n)) \leq M \cdot \nu_p(D_E)$ by the claim and, therefore,

$$\prod_{\substack{p \mid f(n) \\ p \mid 6\delta}} \nu_p(f(n)) \leq (c_2 M N_n \log N_n)^{\omega(6A\delta)},$$

where $\omega(6A\delta)$ is the number of prime factors of $6A\delta$.

We treat the primes separately:

(i) If $p \nmid 6A\delta$, then, as $\nu_p(D_E) = -\nu_p(j)$, the curves E_n are semistable at p. So

$$\prod_{\substack{p \mid f(n) \\ p \nmid 6A\delta}} \nu_p(f(n)) = \prod_{\substack{p \mid f(n) \\ p \nmid 6A\delta}} \nu_p(D_E) \leq c_1 N_n^{11/2+\epsilon},$$

where c_1 depends on δ, A and $\epsilon > 0$. We will set $\epsilon = 1/4$ for comfort purposes.

(ii) If $p \mid 6A\delta$, then by the result of Murty–Pastén

$$\nu_p(D_E) \leq c_2 N_n \log N_n,$$

where $c_2 = c_2(A\delta) > 0$. If $p \mid f(n)$, then $\nu_p(f(n)) \leq M \cdot \nu_p(D_E)$ by the claim and, therefore,

$$\prod_{\substack{p \mid f(n) \\ p \mid 6\delta}} \nu_p(f(n)) \leq (c_2 M N_n \log N_n)^{\omega(6A\delta)},$$

where $\omega(6A\delta)$ is the number of prime factors of $6A\delta$. Finally,

$$\prod_{p \mid f(n)} \nu_p(f(n)) \leq \kappa (\operatorname{Rad} f(n))^{\mu}, \qquad \mu = 6 + \omega(6A\delta),\ \kappa = c_1 (c_2 M)^{\omega(6A\delta)}$$

and by condition ($*$), the theorem follows from the corollary.

Main criterion

Criterion

Let $f(x) \in \mathbb{Z}[x]$ be a polynomial with at least two different complex roots that satisfies the following property: there exists a constant $\mu := \mu(f) > 0$ such that

$$\forall n \gg 0, \qquad \prod_{p \mid f(n)} \nu_p(f(n)) \ll_f \operatorname{Rad}(f(n))^{\mu}. \tag{$*$}$$

Then there exists a constant $\kappa := \kappa(f) > 0$ such that

$$\forall n \gg 0, \qquad \log n \leq \exp\left(\kappa \sqrt{(\log \operatorname{Rad} f(n)) \log_2 \operatorname{Rad} f(n)}\right).$$

Corollary

$$P(f(n)) \gg_f \frac{(\log_2^* n)^2}{\log_3^* n}.$$

References

1. Pastén, H. **Shimura curves and the abc conjecture.** *J. Number Theory* **254,** 214–335. doi:10.1016/j.jnt.2023.07.002 (2023).
2. Pastén, H. **The largest prime factor of $n^2 + 1$ and improvements on subexponential ABC.** *Invent. math.* **236,** 373–385. doi:10.1007/s00222-024-01244-6 (2024).
3. Ram Murty, M. & Pastén, H. **Modular forms and effective Diophantine approximation.** *J. Number Th.* **133,** 3739–3754. doi:10.1016/j.jnt.2013.05.006 (2013).
4. Silverman, J. H. ***Advanced Topics in the Arithmetic of Elliptic Curves.*** *Graduate Texts in Mathematics* **151** (Springer-Verlag, 1994).
5. Tate, J. ***Algorithm for determining the type of a singular fiber in an elliptic pencil.*** in *Modular Functions of One Variable IV* (eds Birch, B. J. & Kuyk, W.) (Springer Berlin Heidelberg, 1975), 33–52. doi:10.1007/BFb0097582.

QR Code

Bonus: the cubic case

For the polynomial $f(x) = (ax+b)^3 + c$, we use the elliptic surface

$$E_n\colon \qquad y^2 = x^3 + 3c(an+b)x + 2c^2,$$

which gives an elliptic curve except for at most three values of n. They have discriminant

$$\Delta_{E_n} = -2^6 3^3 c^3 f(n),$$

and j-invariant

$$j_{E_n} = -12^6 c^3 \frac{(an+b)^3}{f(n)}.$$

If $p \nmid 6c$ and $p \mid f(n)$, then $p \nmid (an+b)$ by construction of f. Hence, the elliptic curves E_n are semistable at p as well, and we proceed as before.