Lower bounds on heights of points on elliptic curves over function fields

Marco Streng

(Universiteit Leiden)

Joint work with Bartosz Naskręcki

Foundations of Computational Mathematics
Workshop on Computational Number Theory
Vienna, July 2026

slides:
`https://www.math.leidenuniv.nl/~streng`

- Let k be a field and let C/k be a (smooth, projective, geometrically irreducible algebraic) curve.
- Let $K = k(C)$ be the field of rational functions on C.
- We look at elliptic curves over K.

Example:

- $k = \mathbb{R}$, $\qquad C = \mathbb{P}^1$, $\qquad K = \mathbb{R}(t)$
- $E : y^2 = x^3 - t^3 x + t$.

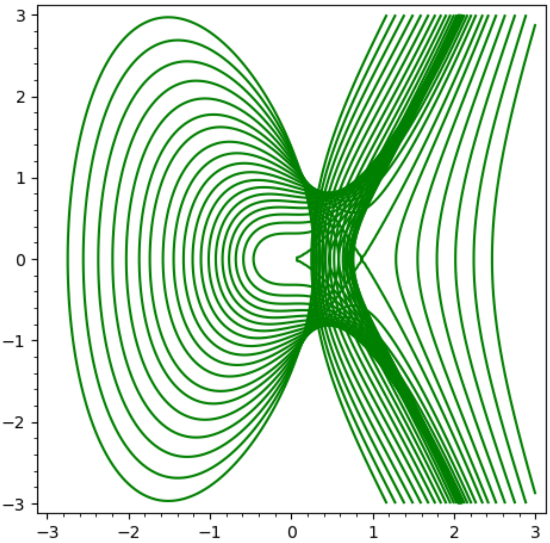
Why?

- Analogy with number fields:
  $\mathbb{F}_q(t) \leftrightsquigarrow \mathbb{Q}$,
  $\mathbb{F}_q(C) \leftrightsquigarrow K/\mathbb{Q}$.
- (Elliptic) surfaces.
- Families of elliptic curves.

- Let k be a field and let C/k be a (smooth, projective, geometrically irreducible algebraic) curve.
- Let $K = k(C)$ be the field of rational functions on C.
- We look at elliptic curves over K.

Example:

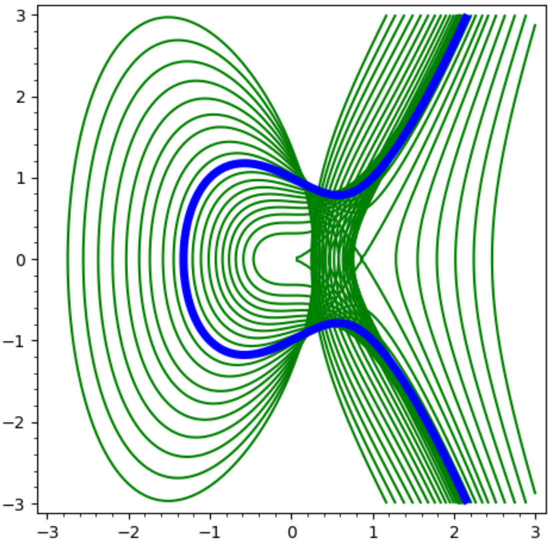
- $k = \mathbb{R}, \qquad C = \mathbb{P}^1, \qquad K = \mathbb{R}(t)$
- $E : y^2 = x^3 - t^3x + t.$



- Let k be a field and let C/k be a (smooth, projective, geometrically irreducible algebraic) curve.
- Let $K = k(C)$ be the field of rational functions on C.
- We look at elliptic curves over K.

Example:

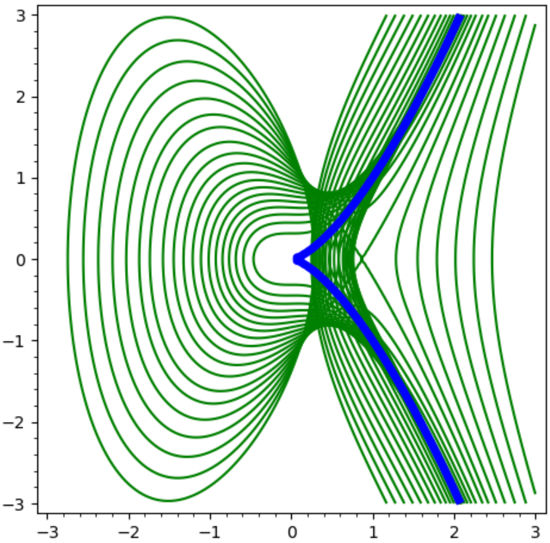
- $k = \mathbb{R}$, $C = \mathbb{P}^1$, $K = \mathbb{R}(t)$
- $E : y^2 = x^3 - t^3 x + t$,
- $t = 1$, good fibre (elliptic curve)



- Let k be a field and let C/k be a (smooth, projective, geometrically irreducible algebraic) curve.
- Let $K = k(C)$ be the field of rational functions on C.
- We look at elliptic curves over K.

Example:

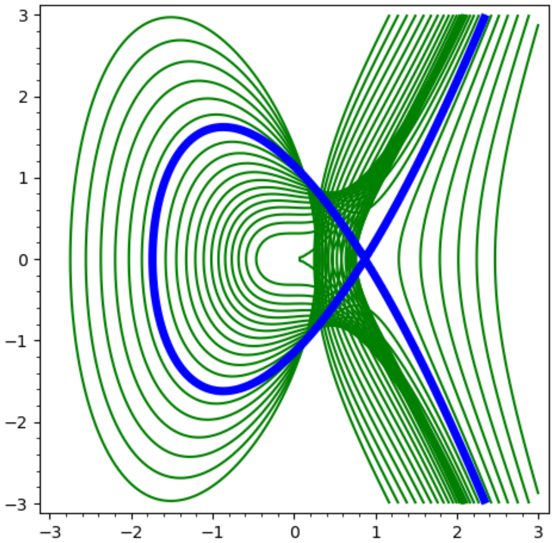
- $k = \mathbb{R}, \qquad C = \mathbb{P}^1, \qquad K = \mathbb{R}(t)$
- $E : y^2 = x^3 - t^3 x + t,$
- $t = 0$, bad fibre (additive)



- Let k be a field and let C/k be a (smooth, projective, geometrically irreducible algebraic) curve.
- Let $K = k(C)$ be the field of rational functions on C.
- We look at elliptic curves over K.

Example:

- $k = \mathbb{R}, \qquad C = \mathbb{P}^1, \qquad K = \mathbb{R}(t)$
- $E : y^2 = x^3 - t^3 x + t,$
- $t = \sqrt[7]{27/4}$, bad fibre (multiplicative)



- The *height* of $x = \frac{a}{b} \in \mathbb{Q}$ is

$$h(x) = \max\{\log|a|, \log|b|\}$$

  if $\gcd(a, b) = 1$.
- Why?
  - It is like the bit size of x.
  - Given $B > 0$, there are finitely many $x \in \mathbb{Q}$ with $h(x) \leq B$.
  - Heights are important in the study of Diophantine equations.
- Heights also exist on number fields.

Examples:

$$h\left(\frac{-12345}{6789}\right) = \log(12345),$$

$$h\left(\frac{12345}{678910}\right) = \log(678910).$$

Let k be a field, for simplicity assume k is perfect, (e.g. finite, or algebraically closed), let C/k be a curve, and let $K = k(C)$.

- The *height* of $f \in K$ is

$$h(f) = \deg(f) := \sum_{v \in C(\overline{k})} \max\{0, -\mathrm{ord}_v(f)\} \qquad \text{(number of poles, with multiplicity)}$$

$$= \sum_{v \in C(\overline{k})} \max\{0, \mathrm{ord}_v(f)\} \quad \text{if } f \neq 0 \quad \text{(nr. of zeroes, with multiplicity).}$$

- Example: $C = \mathbb{P}^1$, $K = k(T)$, $f = \frac{a}{b}$ with $a, b \in k[T]$, $b \neq 0$,

$$h(f) = \max\{\deg a, \deg b\} \quad \text{if} \quad \gcd(a, b) = 1.$$

Let k be a field, for simplicity assume k is perfect, (e.g. finite, or algebraically closed), let C/k be a curve, and let $K = k(C)$.

- The *height* of $f \in K$ is

$$h(f) = \deg(f) := \sum_{v \in C(\overline{k})} \max\{0, -\mathrm{ord}_v(f)\} \qquad \text{(number of poles, with multiplicity)}$$
$$= \sum_{v \in C(\overline{k})} \max\{0, \mathrm{ord}_v(f)\} \quad \text{if } f \neq 0 \quad \text{(nr. of zeroes, with multiplicity).}$$

- Example: $C = \mathbb{P}^1$, $K = k(T)$, $f = \frac{a}{b}$ with $a, b \in k[T]$, $b \neq 0$,

$$h(f) = \max\{\deg a, \deg b\} \quad \text{if} \quad \gcd(a, b) = 1.$$

Let K be a number field or a function field
(for simplicity: k perfect of characteristic $\notin \{2,3\}$).
Let E/K be an elliptic curve, $E : y^2 = x^3 + Ax + B$.
Let $P \in E(K)$ be a point, so $x(P), y(P) \in K$.

- Naive height:

$$h(P) = \frac{1}{2}\, h(x(P))$$

depends on the Weierstrass equation.

Example

$K = \mathbb{F}_7(t)$,
$E : y^2 = x^3 - t^3 x + t$,

$P = \left(4t^2 + 5t + 4, (t+2)^3\right)$,
$h(P) = \frac{1}{2}\, 2 = 1$,

Let K be a number field or a function field
(for simplicity: k perfect of characteristic $\notin \{2,3\}$).
Let E/K be an elliptic curve, $E : y^2 = x^3 + Ax + B$.
Let $P \in E(K)$ be a point, so $x(P), y(P) \in K$.

- Naive height:

$$h(P) = \frac{1}{2}\, h(x(P))$$

depends on the Weierstrass equation.

Example

$$K = \mathbb{F}_7(t),$$
$$E : y^2 = x^3 - t^3 x + t,$$
$$P = \left(4t^2 + 5t + 4, (t+2)^3\right),$$
$$h(P) = \tfrac{1}{2}\, 2 = 1,$$
$$2P = \left(t^2 + t + 1, t^3 + t^2 + 2t + 1\right),$$
$$h(2P) = \tfrac{1}{2}\, 2 = 1,$$

Let K be a number field or a function field
(for simplicity: k perfect of characteristic $\notin \{2,3\}$).
Let E/K be an elliptic curve, $E : y^2 = x^3 + Ax + B$.
Let $P \in E(K)$ be a point, so $x(P), y(P) \in K$.

- Naive height:

$$h(P) = \frac{1}{2}\, h(x(P))$$

depends on the Weierstrass equation.

Example

$$K = \mathbb{F}_7(t),$$
$$E : y^2 = x^3 - t^3 x + t,$$

$$P = \left(4t^2 + 5t + 4, (t+2)^3\right),$$
$$h(P) = \tfrac{1}{2}\, 2 = 1,$$

$$2P = \left(t^2 + t + 1, t^3 + t^2 + 2t + 1\right),$$
$$h(2P) = \tfrac{1}{2}\, 2 = 1,$$

$$3P = \left(\tfrac{2t^4+3t^3+2t^2+4t+4}{t^2+t+2}, \ldots\right),$$
$$h(3P) = \tfrac{1}{2}\, 4 = 2,$$

Let K be a number field or a function field
(for simplicity: k perfect of characteristic $\notin \{2,3\}$).
Let E/K be an elliptic curve, $E : y^2 = x^3 + Ax + B$.
Let $P \in E(K)$ be a point, so $x(P), y(P) \in K$.

- Naive height:

$$h(P) = \frac{1}{2}\, h(x(P))$$

  depends on the Weierstrass equation.

- Canonical height:

$$\widehat{h}(P) = \lim_{n\to\infty} \frac{h(nP)}{n^2}.$$

- Note:

$$\widehat{h}(mP) = m^2\, \widehat{h}(P).$$

Example

$$K = \mathbb{F}_7(t),$$
$$E : y^2 = x^3 - t^3x + t,$$

$$P = \left(4t^2 + 5t + 4, (t+2)^3\right),$$
$$h(P) = \tfrac{1}{2}\, 2 = 1,$$

$$2P = \left(t^2 + t + 1, t^3 + t^2 + 2t + 1\right)$$
$$h(2P) = \tfrac{1}{2}\, 2 = 1,$$

$$3P = \left(\frac{2t^4+3t^3+2t^2+4t+4}{t^2+t+2}, \ldots\right),$$
$$h(3P) = \tfrac{1}{2}\, 4 = 2,$$

$$100P = \left(\frac{t^{2858}+\ldots}{t^{2856}+\ldots}, \ldots\right),$$
$$h(100P) = \tfrac{1}{2}\, 2858 = 1429.$$

Let K be a number field or a function field
(for simplicity: k perfect of characteristic $\notin \{2,3\}$).
Let E/K be an elliptic curve, $E : y^2 = x^3 + Ax + B$.
Let $P \in E(K)$ be a point, so $x(P), y(P) \in K$.

- Naive height:
$$h(P) = \frac{1}{2}\, h(x(P))$$
depends on the Weierstrass equation.
- Canonical height:
$$\widehat{h}(P) = \lim_{n\to\infty} \frac{h(nP)}{n^2}.$$
- Note:
$$\widehat{h}(mP) = m^2\, \widehat{h}(P).$$

Example

$$K = \mathbb{F}_7(t),$$
$$E : y^2 = x^3 - t^3 x + t,$$
$$P = \left(4t^2 + 5t + 4, (t+2)^3\right),$$
$$h(P) = \tfrac{1}{2}\, 2 = 1,$$
$$2P = \left(t^2 + t + 1, t^3 + t^2 + 2t + 1\right),$$
$$h(2P) = \tfrac{1}{2}\, 2 = 1,$$
$$3P = \left(\tfrac{2t^4+3t^3+2t^2+4t+4}{t^2+t+2}, \ldots\right),$$
$$h(3P) = \tfrac{1}{2}\, 4 = 2,$$
$$100P = \left(\tfrac{t^{2858}+\ldots}{t^{2856}+\ldots}, \ldots\right),$$
$$h(100P) = \tfrac{1}{2}\, 2858 = 1429.$$

Let K be a number field or a function field
(for simplicity: k perfect of characteristic $\notin \{2,3\}$).
Let E/K be an elliptic curve, $E : y^2 = x^3 + Ax + B$.
Let $P \in E(K)$ be a point, so $x(P), y(P) \in K$.

- Naive height:

$$h(P) = \frac{1}{2}\, h(x(P))$$

  depends on the Weierstrass equation.

- Canonical height:

$$\widehat{h}(P) = \lim_{n\to\infty} \frac{h(nP)}{n^2}.$$

- Note:

$$\widehat{h}(mP) = m^2\, \widehat{h}(P).$$

Example

$K = \mathbb{F}_7(t)$,
$E : y^2 = x^3 - t^3 x + t$,
$P = \left(4t^2 + 5t + 4, (t+2)^3\right)$,

$$\begin{aligned} h(1P) &= 1 \\ h(2P) &= 1 \\ h(3P) &= 2 \\ h(4P) &= 3 \\ h(5P) &= 4 \\ h(100P) &= 1429 \end{aligned}$$

Let K be a number field or a function field
(for simplicity: k perfect of characteristic $\notin \{2,3\}$).
Let E/K be an elliptic curve, $E : y^2 = x^3 + Ax + B$.
Let $P \in E(K)$ be a point, so $x(P), y(P) \in K$.

- Naive height:

$$h(P) = \frac{1}{2}\, h(x(P))$$

  depends on the Weierstrass equation.

- Canonical height:

$$\widehat{h}(P) = \lim_{n\to\infty} \frac{h(nP)}{n^2}.$$

- Note:

$$\widehat{h}(mP) = m^2\, \widehat{h}(P).$$

Example

$K = \mathbb{F}_7(t)$,
$E : y^2 = x^3 - t^3 x + t$,
$P = \left(4t^2 + 5t + 4, (t+2)^3\right)$,

$$\begin{aligned}
\tfrac{1}{1^2} h(1P) &= \tfrac{1}{1} &&= 1\\
\tfrac{1}{2^2} h(2P) &= \tfrac{1}{4} &&= 0.25\\
\tfrac{1}{3^2} h(3P) &= \tfrac{2}{9} &&= 0.2222\ldots\\
\tfrac{1}{4^2} h(4P) &= \tfrac{3}{16} &&= 0.1875\\
\tfrac{1}{5^2} h(5P) &= \tfrac{4}{25} &&= 0.16\\
\tfrac{1}{100^2} h(100P) &= \tfrac{1429}{10000} &&= 0.1429
\end{aligned}$$

Let K be a number field or a function field
(for simplicity: k perfect of characteristic $\notin \{2,3\}$).
Let E/K be an elliptic curve, $E : y^2 = x^3 + Ax + B$.
Let $P \in E(K)$ be a point, so $x(P), y(P) \in K$.

- Naive height:

$$h(P) = \frac{1}{2}\, h(x(P))$$

depends on the Weierstrass equation.

- Canonical height:

$$\widehat{h}(P) = \lim_{n\to\infty} \frac{h(nP)}{n^2}.$$

- Note:

$$\widehat{h}(mP) = m^2\, \widehat{h}(P).$$

Example

$K = \mathbb{F}_7(t)$,

$E : y^2 = x^3 - t^3 x + t$,

$P = \left(4t^2 + 5t + 4, (t+2)^3\right)$,

$$\begin{aligned}
\tfrac{1}{1^2} h(1P) &= \tfrac{1}{1} &&= 1\\
\tfrac{1}{2^2} h(2P) &= \tfrac{1}{4} &&= 0.25\\
\tfrac{1}{3^2} h(3P) &= \tfrac{2}{9} &&= 0.2222\ldots\\
\tfrac{1}{4^2} h(4P) &= \tfrac{3}{16} &&= 0.1875\\
\tfrac{1}{5^2} h(5P) &= \tfrac{4}{25} &&= 0.16\\
\tfrac{1}{100^2} h(100P) &= \tfrac{1429}{10000} &&= 0.1429
\end{aligned}$$

Fact: $\widehat{h}(P) = \frac{1}{7} \approx 0.142857$.

Conjecture (Lang)

There are $c_1,\ c_2 \in \mathbb{R}$ with $c_1 > 0$ such that for all elliptic curves $E/\mathbb{Q}$ and all $P \in E(\mathbb{Q})$ of infinite order, we have

$$\widehat{h}(P) \geq \frac{1}{c_1} \log|\Delta| - c_2,$$

where

$$|\Delta| = -16\ \left|4A^3 + 27B^2\right|$$

is minimal among all Weierstrass equations $y^2 = x^3 + Ax + B$ isomorphic to E with $A, B \in \mathbb{Z}$.

- Similar conjecture for number fields K, with c_1, c_2 depending only on K.
- Conjecture has consequences for:
  - rational points,
  - integer points,
  - elliptic divisibility sequences.

Minimal discriminants for function fields

Let k be a perfect field of characteristic $\notin \{2,3\}$ (for simplicity), let C/k be a curve and let $K = k(C)$, let E/K be an elliptic curve.

For every $v \in C(\overline{k})$, choose a Weierstrass equation

$$y^2 = x^3 + A_v x + B_v$$

with $\mathrm{ord}_v(A_v) \geq 0$, $\mathrm{ord}_v(B_v) \geq 0$, and $d_v := \mathrm{ord}_v(\Delta_v)$ minimal.

Define

$$\deg \Delta = \sum_{v \in C(\overline{k})} d_v \quad \in \mathbb{Z}_{\geq 0}.$$

Example

$k = \mathbb{F}_7$, $C = \mathbb{P}^1$,
$K = \mathbb{F}_7(t)$,
$C(\overline{k}) = \overline{k} \cup \{\infty\}$,
$E : y^2 = x^3 - t^3 x + t$.

Minimal at all $v \in \overline{k}$,
with $\Delta_v = t^2(t-5)^7$.
$v = 0 \quad \rightsquigarrow d_0 = 2$,
$v = 5 = \sqrt[7]{\frac{27}{4}} \rightsquigarrow d_5 = 7$.

$v = \infty \quad \rightsquigarrow$
$E : y^2 = x^3 - t^{-1} x + t^{-5}$,
$\Delta_\infty = t^{-3}(1 - 5t^{-1})^7$,
$d_\infty = 3$,
$\deg \Delta = 2 + 7 + 3 = 12$.

Let k be a field of characteristic 0 (for simplicity),
let C/k be a curve of genus g, and let $K = k(C)$,
let E/K be an elliptic curve with $j(E) \in K \setminus k$, let $P \in E(K)$ be a point of infinite order.

Theorem (Hindry-Silverman, 1988)

We have

$$\widehat{h}(P) \geq \frac{1}{c_1} \deg \Delta,$$

where $c_1 = 10^{12.6+23g}$.

Theorem (Elkies)

If $g \leq 1$, can take $c_1 = 25330$.

Theorem (Naskręcki-Streng)

If $g \geq 2$, can take $c_1 = 10^{8.4}(g-1)^3$. (Improved from exponential to cubic.)

Proofs, part 1. Black box: Néron local heights

If $Q \neq O$, then $\widehat{h}(Q) = \sum_{v \in C(\overline{k})} \widehat{h}_v(Q)$, where

$$\widehat{h}_v(Q) = \frac{1}{2} \max\left\{0, -\mathrm{ord}_v(x(Q))\right\} + c_v(Q) \geq c_v(Q).$$

Proofs, part 1. Black box: Néron local heights

If $Q \neq O$, then
$$\widehat{h}(Q) = \sum_{v \in C(\overline{k})} \widehat{h}_v(Q), \quad \text{where}$$
$$\widehat{h}_v(Q) = \frac{1}{2}\max\left\{0, -\mathrm{ord}_v(x(Q))\right\} + c_v(Q) \geq c_v(Q).$$

For simplicity, assume all fibres are good or split multiplicative. Then

$$c_v(Q) = \begin{cases} 0 & \text{if } d_v := \mathrm{ord}(\Delta_v) = 0, \\ & \end{cases}$$

Proofs, part 1. Black box: Néron local heights

If $Q \neq O$, then
$$\widehat{h}(Q) = \sum_{v \in C(\overline{k})} \widehat{h}_v(Q), \quad \text{where}$$
$$\widehat{h}_v(Q) = \frac{1}{2}\max\{0, -\mathrm{ord}_v(x(Q))\} + c_v(Q) \geq c_v(Q).$$

For simplicity, assume all fibres are good or split multiplicative. Then

$$c_v(Q) = \begin{cases} 0 & \text{if } d_v := \mathrm{ord}(\Delta_v) = 0, \\ \frac{1}{2} d_v B\left(\frac{\varphi_v(Q)}{d_v}\right) & \text{for some homomorphism } \varphi_v : E(K) \to \mathbb{Z}/d_v\mathbb{Z}, \text{ if } d_v > 0. \end{cases}$$

Periodic Bernoulli polynomial
$B(t) = \{t\}^2 - \{t\} + \frac{1}{6}$.

Proofs, part 1. Black box: Néron local heights

If $Q \neq O$, then

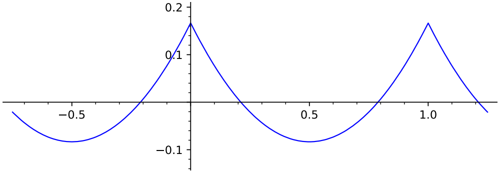
$$\widehat{h}(Q) = \sum_{v \in C(\overline{k})} \widehat{h}_v(Q), \quad \text{where}$$

$$\widehat{h}_v(Q) = \frac{1}{2}\max\{0, -\mathrm{ord}_v(x(Q))\} + c_v(Q) \geq c_v(Q).$$

For simplicity, assume all fibres are good or split multiplicative. Then

$$c_v(Q) = \begin{cases} 0 & \text{if } d_v := \mathrm{ord}(\Delta_v) = 0, \\ \frac{1}{2} d_v B\left(\frac{\varphi_v(Q)}{d_v}\right) & \text{for some homomorphism } \varphi_v : E(K) \to \mathbb{Z}/d_v\mathbb{Z}, \text{ if } d_v > 0. \end{cases}$$

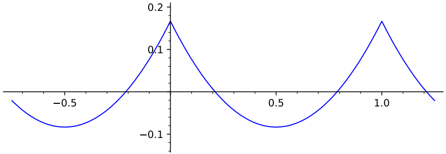
Periodic Bernoulli polynomial
$B(t) = \{t\}^2 - \{t\} + \frac{1}{6}$.



Proofs, part 1. Black box: Néron local heights – Example

$$c_v(Q) = \begin{cases} 0 & \text{if } d_v := \mathrm{ord}(\Delta_v) = 0, \\ \frac{1}{2} d_v B\left(\frac{\varphi_v(Q)}{d_v}\right) & \text{for some homomorphism } \varphi_v : E(K) \to \mathbb{Z}/d_v\mathbb{Z}, \text{ if } d_v > 0. \end{cases}$$

Periodic Bernoulli polynomial
$B(t) = \{t\}^2 - \{t\} + \frac{1}{6}$.



Example: $K = \mathbb{F}_7(t)$, $y^2 = x^3 - t^3x + t$, $P = (4t^2 + 5t + 4, (t+2)^3)$.

$$\left.\begin{array}{llll} d_0 = 2, & \varphi_0(P) = 0, & \widehat{h}_0(P) = & 0 + \frac{1}{6}, \\ d_5 = 7, & \varphi_5(P) = 3, & \widehat{h}_5(P) = & 0 + \frac{-23}{84}, \\ d_\infty = 3, & \varphi_\infty(P) = 0, & \widehat{h}_\infty(P) = & 0 + \frac{1}{4}, \end{array}\right\} \rightsquigarrow \quad \widehat{h}(P) = \frac{1}{6} + \frac{-23}{84} + \frac{1}{4} = \frac{1}{7}.$$

Overarching idea of all proofs (Hindry-Silverman)

For $N \in \mathbb{Z}_{\geq 1}$ and $\omega = (\omega_1, \omega_2, \ldots, \omega_N) \in \mathbb{R}^N_{\geq 0}$, consider

$$\left(\sum_n n^2 \omega_n\right) \widehat{h}(P) = \sum_{n=1}^{N} \omega_n \widehat{h}(nP)$$

$$\geq \sum_{\substack{v \\ \text{bad}}} \sum_n \omega_n c_v(nP)$$

Overarching idea of all proofs (Hindry-Silverman)

For $N \in \mathbb{Z}_{\geq 1}$ and $\omega = (\omega_1, \omega_2, \ldots, \omega_N) \in \mathbb{R}_{\geq 0}^N$, consider

Periodic Bernoulli polynomial
$B(t) = \{t\}^2 - \{t\} + \frac{1}{6}$,

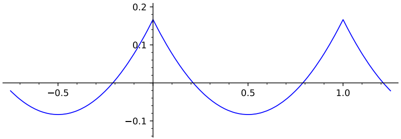
$$\begin{aligned}
\left(\sum_n n^2 \omega_n\right) \widehat{h}(P) &= \sum_{n=1}^{N} \omega_n \widehat{h}(nP) \\
&\geq \sum_{\substack{v \\ \text{bad}}} \sum_n \omega_n c_v(nP) \\
&\geq \frac{1}{2} \sum_{\substack{v \\ \text{bad}}} d_v \sum_n \omega_n B\left(n \, \frac{\varphi_v(P)}{d_v}\right) =: R.
\end{aligned}$$

Overarching idea of all proofs (Hindry-Silverman)

For $N \in \mathbb{Z}_{\geq 1}$ and $\omega = (\omega_1, \omega_2, \ldots, \omega_N) \in \mathbb{R}^N_{\geq 0}$, consider

$$\begin{aligned}\left(\sum_n n^2 \omega_n\right) \widehat{h}(P) &= \sum_{n=1}^{N} \omega_n \widehat{h}(nP) \\ &\geq \sum_{\substack{v \\ \text{bad}}} \sum_n \omega_n c_v(nP) \\ &\geq \frac{1}{2} \sum_{\substack{v \\ \text{bad}}} d_v \sum_n \omega_n B\left(n \frac{\varphi_v(P)}{d_v}\right) =: R.\end{aligned}$$

Periodic Bernoulli polynomial $B(t) = \{t\}^2 - \{t\} + \frac{1}{6}$,



Now try to minimize $c_1 := \sum_n n^2 \omega_n$ subject to $(R \geq \deg \Delta := \sum_v d_v$ for all E and $P)$.

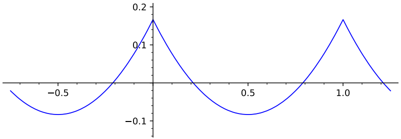
Overarching idea of all proofs (Hindry-Silverman)

For $N \in \mathbb{Z}_{\geq 1}$ and $\omega = (\omega_1, \omega_2, \ldots, \omega_N) \in \mathbb{R}_{\geq 0}^N$, consider

$$\begin{aligned}
\left(\sum_n n^2 \omega_n\right) \widehat{h}(P) &= \sum_{n=1}^{N} \omega_n \widehat{h}(nP) \\
&\geq \sum_{\substack{v \\ \text{bad}}} \sum_n \omega_n c_v(nP) \\
&\geq \frac{1}{2} \sum_{\substack{v \\ \text{bad}}} d_v \sum_n \omega_n B\left(n \, \frac{\varphi_v(P)}{d_v}\right) =: R.
\end{aligned}$$

Now try to minimize $c_1 := \sum_n n^2 \omega_n$ subject to ($R \geq \deg \Delta := \sum_v d_v$ for all E and P).

Periodic Bernoulli polynomial $B(t) = \{t\}^2 - \{t\} + \frac{1}{6}$,



Problem: "all E and P" is a lot, and where does $g = g(C)$ come in?

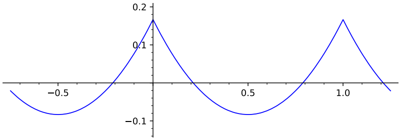
Overarching idea of all proofs (Hindry-Silverman)

For $N \in \mathbb{Z}_{\geq 1}$ and $\omega = (\omega_1, \omega_2, \ldots, \omega_N) \in \mathbb{R}^N_{\geq 0}$, consider

$$\begin{aligned}
\left(\sum_n n^2 \omega_n\right) \widehat{h}(P) &= \sum_{n=1}^{N} \omega_n \widehat{h}(nP) \\
&\geq \sum_{\substack{v \\ \text{bad}}} \sum_n \omega_n c_v(nP) \\
&\geq \frac{1}{2} \sum_{\substack{v \\ \text{bad}}} d_v \sum_n \omega_n B\left(n \, \frac{\varphi_v(P)}{d_v}\right) =: R.
\end{aligned}$$

Now try to minimize $c_1 := \sum_n n^2 \omega_n$ subject to ($R \geq \deg \Delta := \sum_v d_v$ for all E and P).

Periodic Bernoulli polynomial $B(t) = \{t\}^2 - \{t\} + \frac{1}{6}$,



Problem: "all E and P" is a lot, and where does $g = g(C)$ come in?

Let $\deg \mathfrak{N} = \#\{v \in C(\overline{k}) : d_v > 0\}$, $\sigma = \frac{\deg \Delta}{\deg \mathfrak{N}} = (\text{average } d_v)$. Then Mason-Stothers (abc) gives $\deg \Delta \leq 12(g-1) + 6 \deg \mathfrak{N}$, hence $\sigma \leq 6$ if $g \leq 1$, and $\sigma = O(g)$.

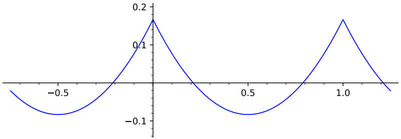
Overarching idea of all proofs (Hindry-Silverman)

For $N \in \mathbb{Z}_{\geq 1}$ and $\omega = (\omega_1, \omega_2, \ldots, \omega_N) \in \mathbb{R}^N_{\geq 0}$, consider

$$\begin{aligned}\left(\sum_n n^2\omega_n\right)\widehat{h}(P) &= \sum_{n=1}^{N}\omega_n\widehat{h}(nP)\\ &\geq \sum_{\substack{v\\ \text{bad}}}\sum_n \omega_n c_v(nP)\\ &\geq \frac{1}{2}\sum_{\substack{v\\ \text{bad}}} d_v \sum_n \omega_n B\left(n\,\frac{\varphi_v(P)}{d_v}\right) =: R.\end{aligned}$$

Now try to minimize $c_1 := \sum_n n^2\omega_n$ subject to ($R \geq \deg\Delta := \sum_v d_v$ for all E and P).

Periodic Bernoulli polynomial $B(t) = \{t\}^2 - \{t\} + \frac{1}{6}$,



Problem: "all E and P" is a lot, and where does $g = g(C)$ come in?

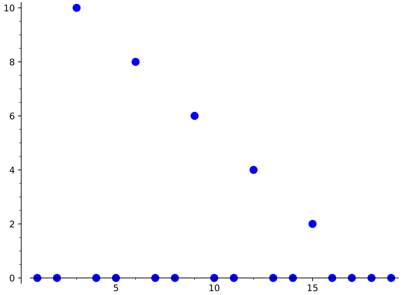
Let $\deg\mathfrak{N} = \#\{v \in C(\overline{k}) : d_v > 0\}$, $\sigma = \frac{\deg\Delta}{\deg\mathfrak{N}} = (\text{average } d_v)$.
Then Mason-Stothers (abc) gives $\deg\Delta \leq 12(g-1) + 6\deg\mathfrak{N}$, hence $\sigma \leq 6$ if $g \leq 1$, and $\sigma = O(g)$.

Hindry-Silverman's solution

$$c_1\,\widehat{h}(P) \geq R \quad \text{with } c_1 = \sum_n n^2\omega_n,\ R = \frac{1}{2}\sum_{\substack{v\\ \text{bad}}} d_v \sum_n \omega_n B\left(n\,\frac{\varphi_v(P)}{d_v}\right). \quad \text{Goal: } c_1 \text{ small } \&\ R \geq \deg\Delta.$$

For well-chosen $m, M \in \mathbb{Z}_{\geq 1}$, take

$$\omega_n = \begin{cases} 0 & \text{if } m \nmid n \text{ or } n \geq mM, \\ 12\left(1 - \frac{n}{m(M+1)}\right) & \text{otherwise.} \end{cases}$$



graph if $m = 3,\ M = 5$

Fourier analysis gives

$$\sum_n \omega_n B\,(nt) \geq -1 \quad \text{for all } t \in \mathbb{R}.$$

Elementary:

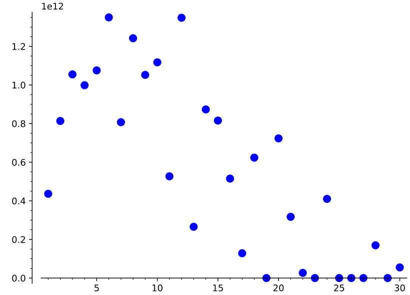
$$\sum_n \omega_n B\left(n\frac{a}{d_v}\right) = M \quad \text{if } d_v \mid m.$$

Elkies's solution

$$c_1\,\widehat{h}(P) \geq R \quad \text{with } c_1 = \sum_n n^2\omega_n,\ R = \frac{1}{2}\sum_{\substack{v\\ \text{bad}}} d_v \sum_n \omega_n B\left(n\,\frac{\varphi_v(P)}{d_v}\right). \quad \text{Goal: } c_1 \text{ small } \&\ R \geq \deg\Delta.$$

Elkies finds a simpler set of equations that imply $R \geq \deg\Delta$ for all $(d_v)_v$ and all $(\varphi_v(P))_v$ with $\sigma \leq 6$.

Then solves that using linear optimization (linear programming).

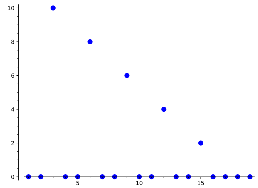


graph of $n \mapsto \omega_n$ for Elkies's ω

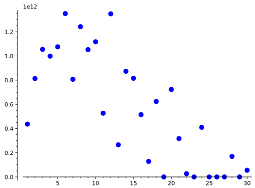
Our solution

$$c_1\,\widehat{h}(P) \geq R \quad \text{with } c_1 = \sum_n n^2\omega_n,\ R = \frac{1}{2}\sum_{\substack{v\\ \text{bad}}} d_v \sum_n \omega_n B\left(n\,\frac{\varphi_v(P)}{d_v}\right). \quad \text{Goal: } c_1 \text{ small } \&\ R \geq \deg\Delta.$$

Hindry-Silverman



Elkies



$\sigma \leq 6$

Naskręcki-Streng

We repeated Elkies's work for $\sigma \leq 7$, $\sigma \leq 8$, $\sigma \leq 9$, etcetera.

The ω look like linear combinations of Hindry-Silverman-type ω.

This inspired a new family of vectors ω, and to our surprise we could prove a polynomial bound!

Lower bounds on heights of points on elliptic curves over function fields

Let k be a field of characteristic 0 (for simplicity),
let C/k be a curve of genus g, and let $K = k(C)$,
let E/K be an elliptic curve with $j(E) \in K \setminus k$, let $P \in E(K)$ be a point of infinite order.

Theorem (Hindry-Silverman, 1988)

We have

$$\widehat{h}(P) \geq \frac{1}{c_1} \deg \Delta,$$

where $c_1 = 10^{12.6+23g}$.

Theorem (Elkies)

If $g \leq 1$, can take $c_1 = 25330$.

Theorem (Naskręcki-Streng)

If $g \geq 2$, can take $c_1 = 10^{8.4}(g-1)^3$. (Improved from exponential to cubic.)

Our work

Theorem (Naskręcki-Streng)

$$\widehat{h}(P) \geq \frac{1}{285\ \sigma^5} \deg(\Delta)$$

Proof.

$$\omega = \sum_{b=1}^{c} \left(\frac{\frac{1}{b} - \frac{1}{c+1}}{M_b + 1} \right) \tau(b, M_b), \quad \text{where}$$

$$c = \left\lfloor \frac{5}{2}\sigma \right\rfloor,$$

$$M_b = \lceil f b^{-2/3} \rceil - 1,$$

$$f \approx 4.14\ \sigma^{5/3}$$

plus estimates, plus work for arbitrary reduction types and base fields. □

Theorem (Naskręcki-Streng)

$$\widehat{h}(P) \geq \frac{1}{10^9\ (g-1)^3} \deg(\Delta) \quad \text{if } g \geq 2.$$

Proof.

$$\omega = \sum_{b \in \mathcal{B}} \left(\frac{1}{b(M_b + 1)} \right) \tau(b, M_b), \quad \text{where}$$

$$\mathcal{B} = \{d_v : v \text{ bad}\},$$

$$M_b = \lceil f b^{-2/3} \rceil - 1,$$

$$f \approx 2.25\ \sigma\ (\#\mathcal{B})^{2/3}.$$

plus estimates, plus work for arbitrary reduction types and base fields. □

Results

	$[K:\mathbb{Q}]=d$ $\widehat{h}(P) \geq \frac{\log(\mathrm{Norm}(\Delta))}{\dots}$	function field K $\widehat{h}(P) \geq \frac{\deg(\Delta)}{\dots}$
Hindry-Silverman (1988)	$(20\sigma)^{8d}10^{1.1+4\sigma}$	$10^{12.6+23g}$
Elkies		50656 if $\sigma \leq 6$ (e.g. if $g \leq 1$)
Naskręcki-Streng	?	$285\ \sigma^5$ and $10^9(g-1)^3$ if $g \geq 2$

$$\sigma = \frac{\deg(\Delta)}{\deg(N)} = O(g).$$

Results

	$[K:\mathbb{Q}]=d$ $\widehat{h}(P) \geq \frac{\log(\mathrm{Norm}(\Delta))}{\cdots}$	function field K $\widehat{h}(P) \geq \frac{\deg(\Delta)}{\cdots}$
Hindry-Silverman (1988)	$(20\sigma)^{8d}10^{1.1+4\sigma}$	$10^{12.6+23g}$
Elkies		50656 if $\sigma \leq 6$ (e.g. if $g \leq 1$)
Petsche (2006)	$O(d^3\sigma^6\log(d\sigma)^2)$	
Naskręcki-Streng	?	$285\ \sigma^5$ and $10^9(g-1)^3$ if $g \geq 2$

$$\sigma = \frac{\deg(\Delta)}{\deg(N)} = O(g).$$

Results

	$[K:\mathbb{Q}] = d$ $\widehat{h}(P) \geq \frac{\log(\mathrm{Norm}(\Delta))}{\ldots}$	function field K $\widehat{h}(P) \geq \frac{\deg(\Delta)}{\ldots}$
Hindry-Silverman (1988)	$(20\sigma)^{8d}10^{1.1+4\sigma}$	$10^{12.6+23g}$
Elkies		50656 if $\sigma \leq 6$ (e.g. if $g \leq 1$)
Petsche (2006)	$O(d^3\sigma^6\log(d\sigma)^2)$	would give $O(\sigma^6)$ and $O(g^6)$
Naskręcki-Streng	?	285 σ^5 and $10^9(g-1)^3$ if $g \geq 2$

$$\sigma = \frac{\deg(\Delta)}{\deg(N)} = O(g).$$

Results

	$[K:\mathbb{Q}] = d$ $\widehat{h}(P) \geq \frac{\log(\mathrm{Norm}(\Delta))}{\ldots}$	function field K $\widehat{h}(P) \geq \frac{\deg(\Delta)}{\ldots}$
Hindry-Silverman (1988)	$(20\sigma)^{8d}10^{1.1+4\sigma}$	$10^{12.6+23g}$
Elkies		50656 if $\sigma \leq 6$ (e.g. if $g \leq 1$)
Petsche (2006)	$O(d^3\sigma^6\log(d\sigma)^2)$	would give $O(\sigma^6)$ and $O(g^6)$
Naskręcki-Streng	?	$285\ \sigma^5$ and $10^9(g-1)^3$ if $g \geq 2$

$$\sigma = \frac{\deg(\Delta)}{\deg(N)} = O(g).$$

Second idea (Elkies)

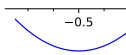
Suppose that $\omega \in \mathbb{R}^N_{\geq 0}$, , $s_1, s_2 \in \mathbb{R}_{\geq 0}$ are such that $\forall b \in \mathbb{Z}_{\geq 1}$ and $\forall a \in (\mathbb{Z}/b\mathbb{Z})$:

d_v

$$(\star) \qquad \frac{1}{2}\sum_n \omega_n B\left(n\frac{a}{d}\right) \geq \frac{s_2}{d} - s_1 .$$

$B(x)$

$$\left(\sum_n n^2\omega_n\right)\widehat{h}(P) \geq \frac{1}{2}\sum_{\substack{v\\ \text{bad}}} d_v \sum_n \omega_n B\left(n\,\frac{\varphi_v(P)}{d_v}\right)$$



Second idea (Elkies)

Suppose that $\omega \in \mathbb{R}_{\geq 0}^{N}$, , $s_1, s_2 \in \mathbb{R}_{\geq 0}$ are such that $\forall b \in \mathbb{Z}_{\geq 1}$ and $\forall a \in (\mathbb{Z}/b\mathbb{Z})$:

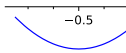
d_v

$B(x)$

$$(\star) \qquad \frac{1}{2}\sum_{n} \omega_n B\left(n\frac{a}{d}\right) \geq \frac{s_2}{d} - s_1.$$

Then

$$\left(\sum_n n^2\omega_n\right) \widehat{h}(P) \geq \frac{1}{2}\sum_{\substack{v\\ \text{bad}}} d_v \sum_n \omega_n B\left(n\,\frac{\varphi_v(P)}{d_v}\right) \geq \sum_{\substack{v\\ \text{bad}}} (s_2 - s_1 d_v)$$



Second idea (Elkies)

Suppose that $\omega \in \mathbb{R}_{\geq 0}^{N}$, , $s_1, s_2 \in \mathbb{R}_{\geq 0}$ are such that $\forall\, b \in \mathbb{Z}_{\geq 1}$ and $\forall\, a \in (\mathbb{Z}/b\mathbb{Z})$:

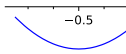
d_v

$$(\star) \qquad \frac{1}{2}\sum_n \omega_n B\left(n\frac{a}{d}\right) \geq \frac{s_2}{d} - s_1.$$

$B(x)$

Then

$$\left(\sum_n n^2\omega_n\right)\widehat{h}(P) \geq \frac{1}{2}\sum_{\substack{v\\ \text{bad}}} d_v \sum_n \omega_n B\left(n\,\frac{\varphi_v(P)}{d_v}\right) \geq \sum_{\substack{v\\ \text{bad}}} (s_2 - s_1 d_v)$$



$$= s_2 \deg(N) - s_1 \deg(\Delta)$$

Second idea (Elkies)

Suppose that $\omega \in \mathbb{R}_{\geq 0}^{N}$, , $s_1, s_2 \in \mathbb{R}_{\geq 0}$ are such that $\forall\, b \in \mathbb{Z}_{\geq 1}$ and $\forall\, a \in (\mathbb{Z}/b\mathbb{Z})$:

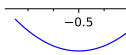
d_v

$$(\star) \qquad \frac{1}{2}\sum_n \omega_n B\left(n\frac{a}{d}\right) \geq \frac{s_2}{d} - s_1.$$

$B(x)$

Then

$$\left(\sum_n n^2\omega_n\right)\widehat{h}(P) \geq \frac{1}{2}\sum_{\substack{v\\ \text{bad}}} d_v \sum_n \omega_n B\left(n\,\frac{\varphi_v(P)}{d_v}\right) \geq \sum_{\substack{v\\ \text{bad}}} (s_2 - s_1 d_v)$$



$$= s_2 \deg(N) - s_1 \deg(\Delta)$$

$$= \left(\frac{s_2}{\sigma} - s_1\right)\deg(\Delta) \geq \left(\frac{s_2}{6} - s_1\right)\deg(\Delta) \quad \text{if } \sigma \leq 6.$$

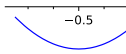
Second idea (Elkies)

Suppose that $\omega \in \mathbb{R}^{N}_{\geq 0}$, , $s_1, s_2 \in \mathbb{R}_{\geq 0}$ are such that $\forall\, b \in \mathbb{Z}_{\geq 1}$ and $\forall\, a \in (\mathbb{Z}/b\mathbb{Z})$:

d_v

$$(\star) \qquad \frac{1}{2}\sum_n \omega_n B\left(n\frac{a}{d}\right) \geq \frac{s_2}{d} - s_1.$$

$B(x)$



Then

$$\left(\sum_n n^2\omega_n\right)\widehat{h}(P) \geq \frac{1}{2}\sum_{\substack{v\\ \text{bad}}} d_v \sum_n \omega_n B\left(n\,\frac{\varphi_v(P)}{d_v}\right) \geq \sum_{\substack{v\\ \text{bad}}}(s_2 - s_1 d_v)$$

$$= s_2 \deg(N) - s_1 \deg(\Delta)$$

$$= \left(\frac{s_2}{\sigma} - s_1\right)\deg(\Delta) \geq \left(\frac{s_2}{6} - s_1\right)\deg(\Delta) \quad \text{if } \sigma \leq 6.$$

Elkies minimizes $(\sum_n n^2\omega_n)$ subject to:

$\omega \in \mathbb{R}^{30}_{\geq 0}$, $(\frac{1}{6}s_2 - s_1) = 1$, and $(\star)$ for all $a, d \leq 60$.

Second idea (Elkies)

Suppose that $\omega \in \mathbb{R}^N_{\geq 0}$, , $s_1, s_2 \in \mathbb{R}_{\geq 0}$ are such that $\forall b \in \mathbb{Z}_{\geq 1}$ and $\forall a \in (\mathbb{Z}/b\mathbb{Z})$:

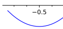
d_v

$$(\star) \qquad \frac{1}{2}\sum_n \omega_n B\left(n\frac{a}{d}\right) \geq \frac{s_2}{d} - s_1.$$

$B(x)$

Then

$$\left(\sum_n n^2\omega_n\right)\widehat{h}(P) \geq \frac{1}{2}\sum_{\substack{v\\ \text{bad}}} d_v \sum_n \omega_n B\left(n\,\frac{\varphi_v(P)}{d_v}\right) \geq \sum_{\substack{v\\ \text{bad}}}(s_2 - s_1 d_v)$$
$$= s_2 \deg(N) - s_1 \deg(\Delta)$$
$$= \left(\frac{s_2}{\sigma} - s_1\right)\deg(\Delta) \geq \left(\frac{s_2}{6} - s_1\right)\deg(\Delta) \quad \text{if } \sigma \leq 6.$$



Elkies minimizes $(\sum_n n^2\omega_n)$ subject to:
$\omega \in \mathbb{R}^{30}_{\geq 0}$, $(\frac{1}{6}s_2 - s_1) = 1$, and $(\star)$ for all $a, d \leq 60$.