Geometry of points over $\bar{\mathbb{Q}}$ of small height Part II

Matthew Baker

Georgia Institute of Technology

MSRI Introductory Workshop on Rational and Integral Points on Higher-dimensional Varieties
January 21, 2006

Lehmer's problem

In 1933, D. H. Lehmer asked the following question, which we phrase as a conjecture:

Conjecture (Lehmer)

There exists an absolute constant $C > 0$ such that if $\alpha \in \bar{\mathbb{Q}}^*$ is not a root of unity, then $h(\alpha) \geq \frac{C}{\deg(\alpha)}$.

- The dependence on $\deg(\alpha)$ is best possible, since $h(2^{1/n}) = \frac{\log 2}{n}$.
- The smallest known value of $m(\alpha) := \deg(\alpha)h(\alpha)$ was discovered by Lehmer: if α_{L} is the unique real root of

$$x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1 = 0$$

lying outside the unit circle, then $m(\alpha_{\mathrm{L}}) = \log(1.176280818\ldots) \approx 0.1623576\ldots$.

Mahler measure

- $m(\alpha) := \deg(\alpha)h(\alpha)$ is called the (logarithmic) Mahler measure of α.
- By Jensen's formula, if

$$f_\alpha(x) = a\prod_{j=1}^{d}(x-\alpha_j) \in \mathbb{Z}[x]$$

is the minimal polynomial of α, then

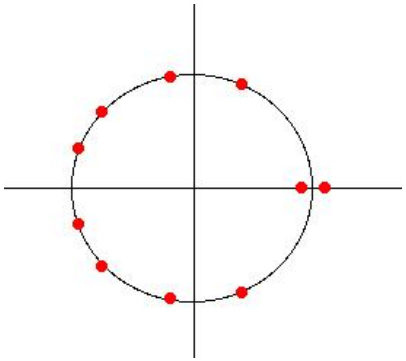
$$m(\alpha) = \int_0^1 \log|f_\alpha(e^{2\pi it})|\,dt \;=\; \log\left(|a|\prod_{j=1}^{d}\max\{1,|\alpha_j|\}\right) .$$

- In terms of Mahler measure, Lehmer's conjecture is that there exists an absolute constant $C > 0$ such that

$$m(\alpha) \geq C$$

for all $\alpha \in \bar{\mathbb{Q}}^*$ not equal to a root of unity.

Salem numbers



- α_{L} is an example of a Salem number, a real algebraic unit $\alpha > 1$ with exactly 2 complex conjugates (α and $1/\alpha$) not lying on the unit circle.
- If $\alpha > 1$ is a Salem number, then $m(\alpha) = \log \alpha$.
- A special case of Lehmer's problem is the following:

Conjecture

α_{L} is the smallest Salem number.

"Classical" results on Lehmer's problem

Theorem (Dobrowolski, 1979)

If α is an algebraic number of degree d which is not a root of unity, then

$$h(\alpha) \geq \frac{1}{1200d}\left(\frac{\log\log 3d}{\log 2d}\right)^3 .$$

The constant $\frac{1}{1200}$ was improved to $\frac{1}{4}$ by Voutier in 1996.

Theorem (Smyth, 1971)

If α is a non-reciprocal algebraic number of degree $d \geq 2$ which is not a root of unity, then

$$m(\alpha) \geq \log \theta_0 ,$$

where θ_0 is the real root of $x^3 - x - 1 = 0$. In particular, Lehmer's conjecture holds for non-reciprocal α.

The essential minimum

- Define the canonical height $\hat{h}$ on $\mathbf{G}_m^n(\bar{\mathbb{Q}})$ by

$$\hat{h}(\alpha_1, \ldots, \alpha_n) = h(\alpha_1) + \cdots + h(\alpha_n).$$

- Let V be a subvariety of $\mathbf{G}_m^n$ defined over $\bar{\mathbb{Q}}$. For $\theta > 0$, let

$$V_\theta = \{P \in V(\bar{\mathbb{Q}}) \ : \ \hat{h}(P) \leq \theta\},$$

and define the essential minimum $\hat{\mu}^{\mathrm{ess}}(V)$ as

$$\hat{\mu}^{\mathrm{ess}}(V) = \inf\{\theta > 0 \ : \ V_\theta \text{ is Zariski dense in } V\}.$$

- The generalized Bogomolov conjecture for subvarieties of tori asserts that $\hat{\mu}^{\mathrm{ess}}(V) = 0$ iff V is a torsion subvariety.
- If $V = \{P\}$ is a point, then $\hat{\mu}^{\mathrm{ess}}(\{P\}) = \hat{h}(P)$.

The canonical height of a subvariety

- We will be interested in lower bounds for the essential minimum $\hat{\mu}^{\mathrm{ess}}(V)$. A theorem of Zhang shows that this is essentially the same problem as finding lower bounds for the canonical height $\hat{h}(V)$ of V, in the sense of Arakelov theory.
- If $V/\mathbb{Q}$ is a hypersurface defined by a polynomial $F(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ having relatively prime integer coefficients, then

$$\hat{h}(V) = \int_0^1 \cdots \int_0^1 \log |F(e^{2\pi i t_1}, \ldots, e^{2\pi i t_n})| dt_1 \cdots dt_n$$

is just the multivariable logarithmic Mahler measure of F.

Comparison between $\hat{\mu}^{\mathrm{ess}}(V)$ and $\hat{h}(V)$

- The following is a special case of Zhang's "Theorem of the Successive Minima":

Theorem (Zhang)

If V is a subvariety of $\mathbf{G}_m^n$ defined over $\bar{\mathbb{Q}}$, then

$$\hat{\mu}^{\mathrm{ess}}(V) \leq \frac{\hat{h}(V)}{\deg(V)} \leq (\dim(V)+1)\hat{\mu}^{\mathrm{ess}}(V) \ .$$

- In particular, $\hat{\mu}^{\mathrm{ess}}(V) = 0$ iff $\hat{h}(V) = 0$.
- Zhang later proved a similar result for subvarieties of abelian varieties, which plays a crucial role in the proof of the Szpiro-Ullmo-Zhang equidistribution theorem.

The index of obstruction

- Let K be a field of characteristic zero, and let V be a subvariety of $\mathbf{G}_m^n$ defined over $\bar{\mathbb{Q}}$.
- Define the index of obstruction $\omega_K(V)$ to be the minimum degree of a nonzero polynomial $F \in K[x_1, \ldots, x_n]$ vanishing identically on V.
- Equivalently, $\omega_K(V)$ is the minimum degree of a hypersurface defined over K and containing V.
- **Examples:**
  - If $n = 1$ and $V = \{\alpha\}$, then $\omega_{\mathbb{Q}}(\{\alpha\}) = [\mathbb{Q}(\alpha) : \mathbb{Q}]$ and $\omega_{\bar{\mathbb{Q}}}(\{\alpha\}) = 1$.
  - More generally, if V is a hypersurface, then $\omega_{\bar{\mathbb{Q}}}(V) = \deg(V)$.

A higher-dimensional Lehmer conjecture

Conjecture ("Generalized Lehmer Conjecture", Amoroso-David, 1999)

Let V be a subvariety of $\mathbf{G}_m^n$, and assume that V is not contained in any torsion subvariety (i.e., a translate of a proper subgroup by a torsion point). Then there exists a constant $C(n) > 0$ such that

$$\hat{\mu}^{\mathrm{ess}}(V) \geq \frac{C(n)}{\omega_{\mathbb{Q}}(V)} \ .$$

Remarks:

- By Zhang's theorem of the successive minima, one can replace $\hat{\mu}^{\mathrm{ess}}(V)$ by $\hat{h}(V)/\deg(V)$ in any conjecture of this kind.
- A 0-dimensional subvariety $V = (\alpha_1, \ldots, \alpha_n)$ of $\mathbf{G}_m^n$ is contained in a torsion subvariety iff $\alpha_1, \ldots, \alpha_n$ are multiplicatively dependent.

A higher-dimensional Dobrowolski theorem

Theorem (Amoroso-David, 2001)

The Generalized Lehmer Conjecure is true up to an ϵ, in the sense that

$$\hat{\mu}^{\mathrm{ess}}(V) \geq \frac{C(n)}{\omega_{\mathbb{Q}}(V)} \left(\log 3\omega_{\mathbb{Q}}(V)\right)^{-\kappa(n)}$$

for some explicit constant $\kappa(n) > 0$.

Special case: There is a constant $C(n) > 0$ such that for every point $P \in \mathbf{G}_m^n(\bar{\mathbb{Q}})$ with multiplicatively independent coordinates, we have

$$\hat{h}(P) \geq \frac{C(n)}{\omega_{\mathbb{Q}}(P)} \left(\log 3\omega_{\mathbb{Q}}(V)\right)^{-\kappa(n)} \quad . \qquad (\heartsuit)$$

Application to Lehmer's original problem

Using Kummer theory, Amoroso and David deduce from (♡) that Lehmer's conjecture holds for Galois extensions of $\mathbb{Q}$:

Theorem (Amoroso-David, 1999)

There exists a constant $C > 0$ such that if α is an algebraic number of degree d which is not a root of unity, and if $\mathbb{Q}(\alpha)/\mathbb{Q}$ is a Galois extension, then

$$h(\alpha) \geq \frac{C}{d} \ .$$

A quantitative Bogomolov conjecture

Conjecture ("Effective Bogomolov Conjecture", Amoroso-David, 2003)

Let V be a subvariety of $\mathbf{G}_m^n$, and assume that V is not contained in any translate of a proper subgroup. Then there exists a constant $C(n) > 0$ such that

$$\hat{\mu}^{\mathrm{ess}}(V) \geq \frac{C(n)}{\omega_{\bar{\mathbb{Q}}}(V)} \ .$$

Remark: It is not enough to merely assume that V is not contained in a torsion subvariety. For example, the curve $V_n : xy = 2^{1/n}$ in $\mathbf{G}_m^2$ has $\hat{\mu}^{\mathrm{ess}}(V_n) \to 0$, but $\omega_{\bar{\mathbb{Q}}}(V_n) = 2$ for all n.

Effective Bogomolov up to an ϵ

Theorem (Amoroso-David, 2003)

The Effective Bogomolov Conjecure is true up to an ϵ, *in the sense that*

$$\hat{\mu}^{\mathrm{ess}}(V) \geq \frac{C(n)}{\omega_{\bar{\mathbb{Q}}}(V)} \left(\log 3\omega_{\bar{\mathbb{Q}}}(V)\right)^{-\kappa(n)}$$

for some constant $\kappa(n) > 0$.

Discussion of the Amoroso-David Conjectures

The effective Bogomolov and generalized Lehmer problems are closely related.

- One cannot hope for a simple lower bound for $\hat{\mu}^{\mathrm{ess}}(V)$ for all non-torsion subvarieties $V/\bar{\mathbb{Q}}$; it is necessary to make a supplementary hypothesis.
- One can either involve the field of definition of V, leading to the generalized Lehmer problem, or one can impose a stronger geometric restriction on V, leading to the effective Bogomolov problem.

Lehmer's problem for abelian varieties: Conjectures

Conjecture

Let A/K be an abelian variety defined over a number field K, and let L be a symmetric ample line bundle on A. Let V be a subvariety of A which is not contained in a torsion subvariety. Then there exists a constant $C(A/K, L) > 0$ such that

$$\hat{\mu}^{\mathrm{ess}}(V) \geq \frac{C(A/K, L)}{\omega_K(V)} \ . \qquad (\spadesuit)$$

Lehmer's problem for abelian varieties: Results

- David and Hindry (2000) have proved (♠) up to an ϵ when V has dimension zero and A has complex multiplication.
- This generalizes earlier work of Laurent (1983), who proved that if E/K is an elliptic curve with complex multiplication, then there exists a constant $C(E/K) > 0$ such that

$$\hat{h}(P) \geq \frac{C(E/K)}{d} \left(\frac{\log \log 3d}{\log 2d} \right)^3$$

  for every non-torsion point $P \in E(\bar{K})$ with $[K(P) : K] = d$.
- Conjecturally, Laurent's theorem holds without the log factors.
- Ratazzi (2004) used David-Hindry's theorem to prove (♠) up to an ϵ for V of any dimension, assuming that A has complex multiplication.

Heights in abelian extensions: algebraic tori

Over abelian extensions, something much stronger than Lehmer's conjecture holds:

Theorem (Amoroso-Dvornicich (2000), Amoroso-Zannier (2003))

Let K be a number field, and let K^{ab} be the maximal abelian extension of K. Then there exists a constant $C(K) > 0$ such that if $\alpha \in (K^{\mathrm{ab}})^*$ is not a root of unity, then

$$h(\alpha) \geq C(K) \ .$$

When $K = \mathbb{Q}$, this was proved in 2000 by Amoroso and Dvornicich, with $C(\mathbb{Q}) = \frac{\log 5}{12}$.

Application I: Class numbers of CM fields

A CM-field is an imaginary quadratic extension of a totally real number field.
Amoroso and Dvornicich used their results on heights in abelian extensions, together with the higher-dimensional Dobrowolski theorem of Amoroso-David, to prove the following result which had been conjectured by Louboutin:

Theorem (Amoroso-Dvornicich, 2003)

Assuming the Generalized Riemann Hypothesis, the exponent of the ideal class group of a CM-field goes to infinity with its absolute discriminant.

This had been proved earlier (by completely different methods) for quadratic fields independently by Boyd-Kisilevsky (1972) and Weinberger (1973)

Application II: Alternate proof of Smyth's theorem

Amoroso and Dvornicich also applied their results to give a new proof of Smyth's theorem that Lehmer's conjecture is true for all non-reciprocal algebraic numbers α. An outline of their argument is as follows.

- If γ is a nonzero algebraic integer in an abelian extension L of $\mathbb{Q}$, then all complex conjugates of $\overline{\gamma}/\gamma$ have absolute value 1, which implies that

$$\frac{1}{[L:\mathbb{Q}]} \log |N_{\mathbb{Q}}^{L}\gamma| \geq h(\overline{\gamma}/\gamma) \ .$$

- Applying this to $\gamma = f_\alpha(\zeta_p)$ for p a large prime, we obtain

$$\frac{1}{p-1} \log |N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_p)} f_\alpha(\zeta_p)| \geq h(\overline{\gamma}/\gamma) \ . \qquad (\diamondsuit)$$

- By Jensen's formula, the left-hand side of $(\diamondsuit)$ is approximately $m(\alpha)$.

Alternate proof of Smyth's theorem (continued)

- $f_\alpha(x)$ non-reciprocal is equivalent to the statement that for p sufficiently large, $\overline{\gamma}/\gamma$ is not a root of unity. [Recall that $\gamma = f_\alpha(\zeta_p)$.]
- Since $\gamma = f_\alpha(\zeta_p) \in \mathbb{Q}^{\mathrm{ab}}$, letting $p \to \infty$ gives

$$\begin{aligned} m(\alpha) &\approx \frac{1}{p-1} \log |N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_p)} f_\alpha(\zeta_p)| \\ &\geq h(\overline{\gamma}/\gamma) \\ &\geq \frac{\log 5}{12} . \end{aligned}$$

Heights in abelian extensions: abelian varieties

Theorem (Baker-Silverman, 2003)

Let A/K be an abelian variety defined over a number field K, and let L be a symmetric ample line bundle on A. Then there exists a constant $C(A/K, L) > 0$ such that

$$\hat{h}(P) \geq C(A/K, L) \quad \textit{for all nontorsion points } P \in A(K^{\mathrm{ab}}).$$

The proof relies upon a theorem of Zarhin about torsion points on abelian varieties which is deduced from Faltings' proof of the Mordell conjecture.

Lehmer's conjecture relative to abelian extensions

Conjecture

Let K be a number field. Then there exists a constant $C(K) > 0$ such that if $\alpha \in \bar{\mathbb{Q}}^*$ is not a root of unity, then

$$h(\alpha) \geq \frac{C(K)}{[K^{\mathrm{ab}}(\alpha) : K^{\mathrm{ab}}]} .$$

This conjecture was proved up to an ϵ by Amoroso and Zannier:

Theorem (Amoroso-Zannier)

There exists a constant $C(K) > 0$ such that if $\alpha \in \bar{\mathbb{Q}}^*$ is not a root of unity, then

$$h(\alpha) \geq \frac{C(K)}{D} \left(\frac{\log \log 5D}{\log 2D} \right)^{13} ,$$

where $D = [K^{\mathrm{ab}}(\alpha) : K^{\mathrm{ab}}]$.

Relative Lehmer problem for abelian varieties

Conjecture (David)

Let A/K be an abelian variety defined over a number field K, and let L be a symmetric ample line bundle on A. Then there exists a constant $C = C(A/K, L) > 0$ such that for every point $P \in A(\bar{K})$ which is not contained in a torsion subvariety of A, we have

$$\hat{h}_L(P) \geq \frac{C(A/K, L)}{\omega_{K^{\mathrm{ab}}}(P)} \ . \qquad (\clubsuit)$$

Results on David's conjecture

- David's conjecture has been proved up to an ϵ by Ratazzi (2004) when $A = E$ is an elliptic curve with complex multiplication.
- A proof of David's conjecture "up to an ϵ" for general A would have some interesting consequences.
- Amoroso and David have formulated a similar conjecture with A replaced by $\mathbf{G}_m^n$.

Intersecting with subgroups of codimension ≥ 2: Abelian varieties

If G is an algebraic group over $\bar{\mathbb{Q}}$, define

$$G^{[r]} := \cup_{\mathrm{codim}(H) \geq r} H(\bar{K}) \ ,$$

where the union is over all (not necessarily connected) algebraic subgroups H of codimension at least r in G.

Theorem (Rémond, 2003)

Let $A/\bar{\mathbb{Q}}$ be an abelian variety, and let $X \subset A$ be a curve which is not contained in any translate of a proper algebraic subgroup of A. If David's Conjecture (♣) holds up to an ϵ, then $X(\bar{\mathbb{Q}}) \cap A^{[2]}$ is finite.

Remark: If $\dim(A) = g$, then $A^{[g]} = A_{\mathrm{tors}}(\bar{\mathbb{Q}})$ is the torsion subgroup of A. Thus the conclusion of Rémond's theorem implies the Manin-Mumford conjecture.

Viada's theorem

An unconditional version of Rémond's theorem was proved by Viada when $A = E^n$ for E an elliptic curve having complex multiplication. More precisely:

Theorem (Viada, 2002)

Let K be a number field, E/K an elliptic curve, n a positive integer, and $A = E^n$. Let $X \subset A$ be a curve which is not contained in any translate of a proper algebraic subgroup of A. Then:

- *The intersection $X(\bar{K}) \cap A^{[1]}$ of $X(\bar{K})$ with the union of all proper algebraic subgroups of A has bounded height.*
- *The set $X(\bar{K}) \cap A^{[2+\frac{n}{2}]}$ is finite.*
- *If E has complex multiplication, then $X(\bar{K}) \cap A^{[2]}$ is finite.*

Intersecting with subgroups of codimension ≥ 2: Algebraic tori

The theorems of Rémond and Viada were motivated by a theorem of Bombieri, Masser, and Zannier which makes use of the higher-dimensional Dobrowolski theorem of Amoroso-Zannier.



Theorem (Bombieri-Masser-Zannier, 1999)

Let $X \subset \mathbf{G}_m^n$ be a curve defined over $\bar{\mathbb{Q}}$ which is not contained in any translate of a proper algebraic subgroup of $\mathbf{G}_m^n$. Then:

- $X(\bar{\mathbb{Q}}) \cap (\mathbf{G}_m^n)^{[2]}$ *is finite.*
- $X(\bar{\mathbb{Q}}) \cap (\mathbf{G}_m^n)^{[1]}$ *is a set of bounded height.*

Multiplicative dependence of α and $1-\alpha$

- The theorem of Bombieri-Masser-Zannier implies that the intersection of $X(\bar{\mathbb{Q}})$ with the union of all proper algebraic subgroups of $\mathbf{G}_m^n$ is a set of bounded height.
- This result was motivated by the following problem: Show that the set of algebraic numbers α for which α and $1-\alpha$ are multiplicatively dependent has bounded height.
- Equivalently: Show that the intersection of the curve $x+y=1$ in $\mathbf{G}_m^2$ with the union of all subgroups of the form $x^a y^b = 1$ with $a, b \in \mathbb{Z}$ forms a set of bounded height.
- Cohen and Zannier (1998) proved that if α and $1-\alpha$ are multiplicatively dependent, then $h(\alpha) \leq \log 2$.
- They also showed that there are exactly 34 algebraic numbers α for which there exist two independent multiplicative relations between $\alpha, 1-\alpha$, and $1+\alpha$.

A specialization theorem for $\mathbf{G}_m^n$

The Bombieri-Masser-Zannier theorem implies:

Corollary

Let $X/\bar{\mathbb{Q}}$ be a curve, and let $x_1, \ldots, x_n$ be nonzero rational functions on X which are multiplicatively independent modulo constants. Then the set of points $P \in X(\bar{\mathbb{Q}})$ for which $x_1(P), \ldots, x_n(P)$ are multiplicatively dependent has bounded height.

- This can be thought of as an analogue for $\mathbf{G}_m^n$ of the specialization theorems for abelian varieties due to Demjanenko-Manin and Silverman.
- The corollary is proved by considering the image X' of X in $\mathbf{G}_m^n$ under the map $P \mapsto (x_1(P), \ldots, x_n(P))$, and noting that the independence of $x_1, \ldots, x_n$ modulo constants is equivalent to the statement that X' is not contained in any translate of a proper subgroup of $\mathbf{G}_m^n$.

Application: Multiplicative dependence of complex numbers

In 2003, Bombieri-Masser-Zannier showed using a specialization argument that their result on intersecting curves with subgroups of codimension at least 2 remains true if $\bar{\mathbb{Q}}$ is replaced by any field of characteristic zero. As a sample application, they show:

Theorem (Bombieri-Masser-Zannier, 2003)

If $z_1, \ldots, z_n$ are distinct complex numbers, then there are only finitely many $z \in \mathbb{C}$ for which there are two independent multiplicative relations among $z - z_1, \ldots, z - z_n$, i.e., for which

$$(z - z_1)^{a_1} \cdots (z - z_n)^{a_n} = 1$$
$$(z - z_1)^{b_1} \cdots (z - z_n)^{b_n} = 1$$

for some linearly independent vectors $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in \mathbb{Z}^n$.

Possible generalizations

- So far, Bombieri-Masser-Zannier type theorems have been proved only for curves.
- It should be possible to formulate and prove an analogue of the Bombieri-Masser-Zannier theorem for varieties of any dimension contained in an arbitrary commutative algebraic group.