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

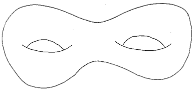
Matthew Baker

Georgia Institute of Technology

MSRI Introductory Workshop on Rational and Integral Points on Higher-dimensional Varieties
January 19, 2006

Notation

- K: a field of characteristic zero
- X: an algebraic curve of genus $g \geq 1$ defined over K
  We assume X is complete, nonsingular, and absolutely irreducible.



The Jacobian

- The Jacobian J of X is an abelian variety of dimension g with the property that

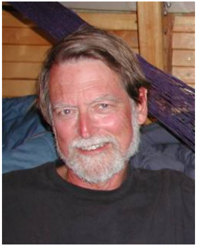
$$J(\bar{K}) = \mathrm{Div}^0(X)/\,\mathrm{Prin}(X).$$

- By choosing a base point $P_0 \in X(\bar{K})$, one obtains an embedding

$$\begin{aligned} i_0 : X(\bar{K}) &\hookrightarrow J(\bar{K}) \\ P &\mapsto [(P) - (P_0)] \end{aligned}$$

- From now on, we fix a base point $P_0 \in X(\bar{K})$ and identify $X(\bar{K})$ with its image in $J(\bar{K})$.

The Manin-Mumford conjecture

Theorem (Manin-Mumford Conjecture, proved by Raynaud in 1983)

Let X/K be a curve of genus $g \geq 2$. Then $X(\bar{K}) \cap J(\bar{K})_{\text{tors}}$ is finite.

The Mordell conjecture

The Manin-Mumford conjecture should be compared with the Mordell conjecture:

Theorem (Mordell Conjecture, proved by Faltings in 1983)

Suppose K is a number field, and let X/K be a curve of genus $g \geq 2$. Then $X(\bar{K}) \cap J(K)$ is finite.

Generalized Manin-Mumford and Mordell conjectures

If A/K is an abelian variety, a torsion subvariety of A is a translate by a torsion point of an abelian subvariety of A.

Theorem (Generalized Manin-Mumford Conjecture, proved by Raynaud in 1983)

Let V be an algebraic subvariety of an abelian variety A/K which is not a torsion subvariety. Then the intersection $V(\bar{K}) \cap J(\bar{K})_{\mathrm{tors}}$ is not Zariski-dense in V.

Theorem (Generalized Mordell Conjecture, proved by Faltings in 1991)

Let K be a number field, and let V be an algebraic subvariety of an abelian variety A/K which is not a translate of an abelian subvariety. Then the intersection $V(\bar{K}) \cap J(K)$ is not Zariski-dense in V.

Proofs of the Manin-Mumford conjecture

A brief history of some proofs of the Manin-Mumford and generalized Manin-Mumford conjectures:

- Raynaud (1983): Based on reduction mod p^2 and action of Galois on torsion points of J.
- Coleman (1987): Uses p-adic integration to analyze which primes can ramify in the field generated by torsion points on X.
- Buium (1996): Based on p-adic jet spaces; uses one of Coleman's results.
- Hrushovsky (1996): Uses model theory (mathematical logic).
- Pink-Rössler (2002): Translation of Hrushovsky's proof into classical algebraic geometry.

Mordell-Lang Conjecture

- An abelian group Γ has finite rank if there is a finitely generated subgroup $\Gamma_0 \subset \Gamma$ such that for every $P \in \Gamma$, there exists $n \geq 1$ for which $nP \in \Gamma_0$.
- Equivalently, Γ has finite rank iff $\Gamma \otimes \mathbb{Q}$ is a finite-dimensional $\mathbb{Q}$-vector space.

The following result synthesizes the Mordell and generalized Manin-Mumford conjectures:

Theorem (Mordell-Lang Conjecture, due to Faltings, Vojta, & Raynaud)

Let K be a number field, and let V be an algebraic subvariety of an abelian variety A/K which is not a translate of an abelian subvariety. Finally, let Γ be a finite rank subgroup of $A(\bar{K})$. Then the intersection $V(\bar{K}) \cap \Gamma$ is not Zariski-dense in V.

Applications of Mordell-Lang to curves

- A curve X is hyperelliptic if there is a degree 2 map from X to $\mathbb{P}^1$, and bielliptic if there is a degree 2 map from X to an elliptic curve.
- If X is hyperelliptic, the hyperelliptic branch points are the points of X where the degree 2 map from X to $\mathbb{P}^1$ is ramified.

Theorem (Faltings + Silverman-Abramovich-Harris, 1991)

Let K be a number field, and let X/K be a curve of genus $g \geq 2$. Then there exists a finite extension K'/K such that $\cup_{[L:K']=2} X(L)$ is infinite iff X is either hyperelliptic or bielliptic.

Theorem (Raynaud + Baker-Poonen, 2001)

Let X/K be a curve of genus $g \geq 2$. Then there are infinitely many pairs (P, Q) of distinct points in $X(\bar{K})$ with $(P) - (Q)$ torsion in $J(\bar{K})$ iff $g = 2$, or $g = 3$ and X is both hyperelliptic and bielliptic.

Torsion points on Fermat curves

- Let $N \geq 4$ be an integer.
- Let F_N be the Fermat curve $F_N : X^N + Y^N = Z^N$.
- A cusp is a point of $F_N(\bar{\mathbb{Q}})$ satisfying $XYZ = 0$.
- Embed F_N into its Jacobian J_N using a cusp as a base point.
- Rohrlich (1977) proved that the difference of two cusps is always torsion in J_N.

Theorem (Coleman-Tamagawa-Tzermias, 1998)

$$X_N(\bar{\mathbb{Q}}) \cap J_N(\bar{\mathbb{Q}})_{\text{tors}} = \{\text{cusps}\}.$$

Torsion points on modular curves

- Let $p \geq 23$ be a prime number.
- Let $Y_0(p)$ be the modular curve parametrizing elliptic curves together with a cyclic subgroup of order p, and let $X_0(p)$ be its two-point compactification obtained by adding the cusps 0 and ∞.
- Embed $X_0(p)$ into its Jacobian $J_0(p)$ using a cusp as a base point.
- Manin and Drinfeld proved that the difference $[(0) - (\infty)]$ is always torsion as an element of $J_0(p)$.

Theorem (Baker, Tamagawa, 1999)

Let H be the set of hyperelliptic branch points on $X_0(p)$ when X is hyperelliptic and $p \neq 37$, and otherwise let $H = \emptyset$. Then

$$X_0(p)(\bar{\mathbb{Q}}) \cap J_0(p)(\bar{\mathbb{Q}})_{\mathrm{tors}} = \{0, \infty\} \cup H.$$

Torsion points on higher-dimensional varieties

There are few nontrivial examples where we can explicitly determine all torsion points lying on a higher-dimensional subvariety of an abelian variety. One known result is the following:

Theorem (Baker, 1999)

Let $V \subset J_0(p)$ be the (2-dimensional) image of the map $X_0(p)^2 \to J_0(p)$ given by $(P, Q) \mapsto [(P) - (Q)]$. Let $c = [(0) - (\infty)] \in J_0(p)(\mathbb{Q})_{\mathrm{tors}}$. If $p > 311$, then

$$V(\bar{\mathbb{Q}}) \cap J_0(p)(\bar{\mathbb{Q}})_{\mathrm{tors}} = \{0, \pm c\} .$$

- Equivalently, the cusps 0 and ∞ are the only distinct points of $X_0(p)(\bar{\mathbb{Q}})$ whose difference has finite order in $J_0(p)$.
- Anderson, Grant, and Simon have some partial results describing the torsion points lying on the theta divisor of certain Fermat quotient curves.

Computing torsion points on curves

- Poonen (2001) developed an algorithm to compute the torsion points on an arbitrary curve.
- The algorithm is based on Buium's approach.
- Poonen implemented the algorithm on a computer in the special case where $K = \mathbb{Q}$, $g = 2$, and the base point P_0 is a hyperelliptic branch point.
- It would be interesting to develop an algorithm to compute the torsion points on higher-dimensional subvarieties of abelian varieties.

Open question

Question

Fix an integer $g \geq 2$. Is there a uniform bound for the number of torsion points lying on a curve X of genus g?

Remarks:

- For $g = 2$, the record is 22 torsion points.
- If we fix X and vary the base point P_0 used to embed X in its Jacobian, the number of torsion points remains bounded (Baker-Poonen, 2001).

Mordell-Lang Conjecture for subvarieties of algebraic tori and semiabelian varieties

- An algebraic torus is an affine group variety of the form $\mathbf{G}_m^n$ for some $n \geq 1$, where $\mathbf{G}_m = \mathbb{A}^1 - \{0\}$ is the *multiplicative group* over $\mathbb{Q}$. We have $\mathbf{G}_m^n(\mathbb{C}) = (\mathbb{C}^*)^n$.
- A semiabelian variety G is an extension of an abelian variety by a torus:

$$1 \to \mathbf{G}_m^n \to G \to A \to 0.$$

- A torsion subvariety of G is a translate by a torsion point of an algebraic subgroup of G.

Remark: The torsion subvarieties of $\mathbf{G}_m^n$ are those defined by one or more equations of the form $X_1^{a_1} X_2^{a_2} \cdots X_n^{a_n} = \zeta$, where $a_i \in \mathbb{Z}$ and ζ is a root of unity.

Theorem (Mordell-Lang Conjecture for semiabelian varieties, proved by McQuillan in 1995)

Let K be a number field, let G be a semiabelian variety, and let V be an algebraic subvariety of G which is not a translate of an algebraic subgroup. Finally, let Γ be a finite rank subgroup of $G(\bar{K})$. Then the intersection $V(\bar{K}) \cap \Gamma$ is not Zariski-dense in V.

Remarks:

- The special case where $G = \mathbf{G}_m^n$ ("Mordell-Lang conjecture for algebraic tori") was proved in 1984 by Laurent.
- The Manin-Mumford conjecture for semiabelian varieties was proved by Hindry in 1988, following earlier work of Serre and Ribet.

Application: $X + Y = 1$ and integral points on elliptic curves

- Let K be a number field, and let $S \subset M_K$ be a finite set of places. By Dirichlet's theorem, the group $\mathcal{O}_S^*$ of S-units in K^* is finitely generated.
- The "Mordell" part of Mordell-Lang in the special case of

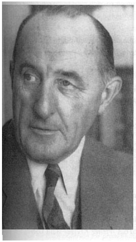
$$\{(X, Y) \ : \ X + Y = 1\} \subset \mathbf{G}_m \times \mathbf{G}_m$$

implies:

Theorem (Finiteness of solutions to the S-unit equation)

There are only finitely many S-units $\alpha \in K^*$ such that $1 - \alpha$ is also an S-unit.

A well-known argument shows that finiteness of solutions to the S-unit equation implies:



Corollary (Siegel's Theorem)

Let K be a number field, let $S \subset M_K$ be a finite set of places, and let E/K be an elliptic curve. Then the set of S-integral points on E is finite.

Application: The Ailon-Rudnick conjecture for polynomials

Conjecture (Ailon-Rudnick)

If $a, b \neq \pm 1$ are multiplicatively independent non-zero integers with $\gcd(a-1, b-1) = 1$, then there are infinitely many integers $k \geq 1$ such that

$$\gcd(a^k - 1, b^k - 1) = 1 \ .$$

For complex polynomials, something even stronger is known:

Theorem (Ailon-Rudnick)

If $f, g \in \mathbb{C}[t]$ are multiplicatively independent non-constant polynomials with $\gcd(f-1, g-1) = 1$, then there is a finite union $\mathcal{P}$ of proper arithmetic progressions such that for all $k \in \mathbb{N} \backslash \mathcal{P}$,

$$\gcd(f^k - 1, g^k - 1) = 1 \ .$$

Proof of the Ailon-Rudnick theorem

- By the Manin-Mumford conjecture for curves in $\mathbf{G}_m^2$ (proved originally by Ihara, Serre, and Tate), the intersection of a non-torsion curve in $\mathbb{C}^* \times \mathbb{C}^*$ with $\mu_\infty \times \mu_\infty$ is finite.
- Applying this to the curve $\{(f(t), g(t)) \ : \ t \in \mathbb{C}\}$, there are only finitely many t for which both $f(t)$ and $g(t)$ are roots of unity when f, g are multiplicatively independent.
- Thus there are only finitely many possible linear factors $(t - \alpha_1), \ldots, (t - \alpha_m)$ of $\gcd(f^k - 1, g^k - 1)$.
- For each $i = 1, \ldots, m$, let k_i be the smallest positive integer such that $(t - \alpha_i) \mid \gcd(f(t)^{k_i} - 1, g(t)^{k_i} - 1)$.
- We must have $k_i > 1$, and for $k \notin k_i\mathbb{N}$, $(t - \alpha_i) \nmid \gcd(f(t)^{k_i} - 1, g(t)^{k_i} - 1)$.
- $\cup_i k_i\mathbb{N}$ is the required union of arithmetic progressions.

The Mordell-Lang conjecture over function fields

- The Mordell-Lang conjecture has been extended to function fields of arbitrary transcendence degree by Buium (in characteristic 0) and Hrushovski (in any characteristic).
- The statement of Hrushovski's theorem is slightly complicated, as one has to take into account issues arising from isotrivial varieties and inseparable extensions.
- The proofs yield explicit quantitative bounds.
- Hrushovski's method of proof involves mathematical logic, in particular the model theory of difference fields.

Application: Tame fundamental groups of curves

Akio Tamagawa used one of Hrushovski's theorems (the "Manin-Mumford conjecture in characteristic p") to prove the following result about tame fundamental groups of curves in characteristic p (as defined by Grothendieck):

Theorem (Tamagawa,2004)

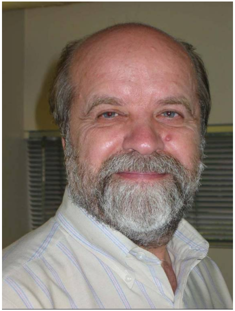
There are only finitely many isomorphism classes of curves of genus $g \geq 2$ over $\overline{\mathbb{F}}_p$ having the same tame fundamental group.

The result is striking because in characteristic zero, every curve of genus g (for fixed g) has the same fundamental group!

Idea of the proof of Tamagawa's theorem

- The key idea in the proof of Tamagawa's theorem is to consider the theta divisor Θ' of $X' = F^*(X)$ in $J' = F^*(J)$, where X is a curve over $\overline{\mathbb{F}}_p$, J is its Jacobian, and F is the Frobenius map.
- As observed by Raynaud, the intersection $\Theta'(\overline{\mathbb{F}}_p) \cap J'(\overline{\mathbb{F}}_p)_{\mathrm{tors}}$ contains a great deal of information about cyclic étale covers of X.
- Tamagawa's finiteness theorem follows by applying Hrushovski's theorem.

Bogomolov asked the following question:



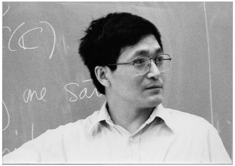
Question

Let K be a number field. Given a curve X/K of genus $g \geq 2$ embedded in its Jacobian J, does there exist $\varepsilon > 0$ such that the set

$$\{P \in X(\bar{K}) \ : \ \hat{h}(P) < \varepsilon\}$$

is finite?

The generalized Bogomolov Conjecture



- Ullmo (1998) answered Bogomolov's question in the affirmative. Shortly after, Zhang generalized Ullmo's result to higher dimensions.

- Zhang's theorem includes as a special case the Generalized Manin-Mumford Conjecture.

Theorem (Generalized Bogomolov Conjecture, proved by Zhang in 1998)

Let K be a number field, and let V be an algebraic subvariety of an abelian variety A/K which is not a torsion subvariety. Then there exists $\varepsilon > 0$ such that

$$\{P \in V(\bar{K}) \ : \ \hat{h}(P) < \varepsilon\}$$

is not Zariski-dense in V.

Proofs of the generalized Bogomolov conjecture

A brief history of some proofs of the generalized Bogomolov conjecture:

- Zhang (1992): Proved the analogous result for subvarieties of algebraic tori.
- Ullmo (1998), Zhang (1998): Used a 1997 theorem of Spziro-Ullmo-Zhang on equidistribution of small points.
- Bilu (1997): Proved equidistribution of small points for $\mathbf{G}_m^n$ and deduced generalized Bogomolov for subvarieties of algebraic tori.
- Schmidt (1993), Bombieri-Zannier (1995): Gave elementary effective proofs of the generalized Bogomolov conjecture for subvarieties of algebraic tori.
- David-Philippon (1998–2000): Gave a new effective proof of the generalized Bogomolov conjecture, first for subvarieties of algebraic tori, then for abelian varieties, and finally for semiabelian varieties.

Equidistribution of small points

- Let $\{P_n\}$ be a sequence of points in $A(\bar{K})$.
- Let δ_n denote the discrete probability measure on $A(\mathbb{C})$ supported equally on the Galois conjugates of P_n.
- We say $\{P_n\}$ is generic if no subsequence is contained in a proper subvariety of A, and strict if no subsequence is contained in a proper torsion subvariety of A.

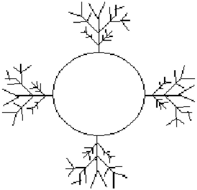
Theorem (Szpiro-Ullmo-Zhang, 1997)

If $\hat{h}(P_n) \to 0$ and the sequence $\{P_n\}$ is generic, then δ_n converges weakly to the unit Haar measure on $A(\mathbb{C})$.

Remark: Zhang proved that this remains true if "generic" is replaced by "strict", which implies the Bogomolov conjecture.

Equidistribution of small points: open problems

- Generalize the Szpiro-Ullmo-Zhang equidistribution theorem to semiabelian varieties.
- Prove a non-archimedean version of the Szpiro-Ullmo-Zhang equidistribution theorem. This has recently been done using Berkovich spaces in some special cases:



  - Abelian varieties with good reduction (Chambert-Loir)
  - Elliptic curves (Chambert-Loir, Baker-Petsche)
- Formulate and prove higher-dimensional equidistribution theorems for points of small height with respect to a dynamical system. This has recently been done for dynamical systems on $\mathbb{P}^1$ by Baker-Hsia-Rumely, Favre-Rivera–Letelier, and Autissier-Chambert–Loir.

Mordell-Lang plus Bogomolov

- Let K be a number field, and let G/K be a semiabelian variety.
- If $\Gamma \subset G(\bar{K})$, define

$$\Gamma_\varepsilon := \{\gamma + P \ : \gamma \in \Gamma \ , \ P \in A(\bar{K}) \ , \ \hat{h}(P) \leq \varepsilon\}.$$

Theorem (Mordell-Lang + Bogomolov, proved by Poonen (1999), Zhang (2000), Rémond (2003))

Let $\Gamma \subset G(\bar{K})$ be a finite rank subgroup, and let V be an algebraic subvariety of G which is not a translate of an algebraic subgroup. Then there exists $\varepsilon > 0$ such that $V(\bar{K}) \cap \Gamma_\varepsilon$ is not Zariski dense in V.

Remarks:

- Poonen and Zhang proved the Mordell-Lang + Bogomolov result for "almost split" semiabelian varieties, and Rémond established the general case.
- The almost split hypothesis came from Chambert-Loir's extension of the Szpiro-Ullmo-Zhang equidistribution theorem to semiabelian varieties, which is limited to this case. Rémond's proof does not use equidistribution.

Example: $X + Y = 1$

- It follows from the Bogomolov conjecture for curves in $\mathbf{G}_m^2$ that there exists $\varepsilon > 0$ such that the set

$$\{\alpha \in \bar{\mathbb{Q}} \ : \ h(\alpha) + h(1-\alpha) < \varepsilon\}$$

  is finite.

- Zagier proved the following more precise result:

Theorem (Zagier, 1993)

For all algebraic numbers $\alpha \neq 0, 1, (1 \pm \sqrt{-3})/2$, *we have*

$$h(\alpha) + h(1-\alpha) \geq \frac{1}{2} \log \frac{1+\sqrt{5}}{2},$$

with equality if and only if α *or* $1 - \alpha$ *is a primitive 10th root of unity.*

Application: Uniform bounds for the S-unit equation

Theorem (Beukers-Schlickewei, 1996)

If $\Gamma \subset (\bar{\mathbb{Q}}^*)^2$ is a subgroup of rank r, then

$$\#\{(x,y) \in \Gamma \ : \ x + y = 1\} \leq 256^{r+1}.$$

- The proof breaks into three cases:
  - Small height solutions, which are estimated using the Bogomolov discreteness property and sphere-packing bounds.
  - Medium height solutions, which are counted using a *gap principle*.
  - Large height solutions, which are ruled out by diophantine approximation.
- Except for the particular constants involved, this generalizes a famous result of Evertse (1984) on solutions to $x + y = 1$ in S-units.

Remark: Rémond (2003) has vastly generalized this kind of result, proving explicit bounds of the above type, depending only on $r, \deg(V)$, and $\dim(G)$, when $\{x + y = 1\} \subset \mathbf{G}_m^2$ is replaced by an arbitrary subvariety V of a semiabelian variety G.

Ih's conjecture

Ih's conjecture is a finiteness statement about torsion points which does not extend to small points.

Conjecture (Ih)

Let K be a number field, and let A/K be an abelian variety. Let D be an effective ample divisor on A, at least one of whose irreducible components is not a torsion subvariety of A. Then the set of all torsion points of $A(\bar{K})$ which are integral with respect to D is not Zariski dense in A.

Remarks:

- A torsion point P in $A(\bar{K})$ is integral with respect to D if its Zariski closure $\overline{P}$ in a fixed model $\mathcal{A}$ is disjoint from $\overline{D}$.
- The validity of the conjecture is independent of the choice of model.
- One can formulate an analogous conjecture for subvarieties of $\mathbf{G}_m^n$, and for dynamical systems.

Ih's conjecture: Results

Ih's conjecture has been proved for $\mathbf{G}_m$ and for elliptic curves. The statement for elliptic curves is the following:

Theorem (Baker-Ih-Rumely, 2005)

Let K be a number field, let E/K be an elliptic curve, and let $P \in E(\bar{K})$ be a non-torsion point. Then the set of all torsion points of $E(\bar{K})$ which are integral with respect to P is finite.

Remarks:

- The theorem holds more generally with "integral" replaced by "S-integral".
- Examples show that the theorem fails if P is torsion, or if torsion points are replaced by points of small height.
- The theorem is proved using properties of local canonical heights, David's results on linear forms in elliptic logarithms, and a strong version of the Szpiro-Ullmo-Zhang equidistribution theorem for torsion points on elliptic curves.

In its simplest form, the conjecture for $\mathbf{G}_m$ states:

Theorem (Baker-Ih-Rumely, 2005)

Fix an algebraic number $\alpha \in \bar{\mathbb{Q}}^*$ which is not a root of unity. Then the set of all roots of unity which are integral with respect to α is finite.

If α is an algebraic integer, the theorem says that there are only finitely many roots of unity $\zeta \in \bar{\mathbb{Q}}^*$ such that $\alpha - \zeta$ is an algebraic unit.

Remarks:

- The hypothesis $h(\alpha) > 0$ is necessary: taking $\alpha = 1$, we recall that $1 - \zeta$ is a unit for each root of unity ζ of composite order.
- Finiteness for roots of unity cannot be strengthened to finiteness for small points. For example, take $\alpha = 2$ and let β_n be a root of the polynomial $f_n(x) = x^{2^n}(x-2) - 1$. Then $h(\beta_n) \to 0$ and $2 - \beta_n$ is a unit for all $n \geq 1$.

Motivation for Ih's conjecture

The motivation for Ih's conjecture is the following philosophical picture:

Type of variety	$\mathcal{O}_K$	$\bar{\mathbb{Z}}$
Projective	Generalized Mordell Conjecture	Manin-Mumford Conjecture
Affine	Lang's Integrality Conjecture	Ih's Conjecture

Remark: Lang's integrality conjecture (proved by Faltings) is the statement that if D is an effective ample divisor on A, then the set of $\mathcal{O}_K$-integral points of A not meeting $\text{Supp}(D)$ is finite.