Torsion Points on Abelian Varieties

Matthew Baker

Georgia Institute of Technology

Modular Forms and Arithmetic
MSRI, July 2008

Outline

1. Almost rational torsion points
2. Torsion points over abelian extensions
3. Torsion points unramified at p

Outline

1. Almost rational torsion points
2. Torsion points over abelian extensions
3. Torsion points unramified at p

The Manin-Mumford Conjecture: Notation

- K: a number field

The Manin-Mumford Conjecture: Notation

- K: a number field
- X: a (complete, nonsingular, geometrically integral) algebraic curve of genus $g \geq 2$ defined over K

The Manin-Mumford Conjecture: Notation

- K: a number field
- X: a (complete, nonsingular, geometrically integral) algebraic curve of genus $g \geq 2$ defined over K
- J: the Jacobian of X

The Manin-Mumford Conjecture: Notation

- K: a number field
- X: a (complete, nonsingular, geometrically integral) algebraic curve of genus $g \geq 2$ defined over K
- J: the Jacobian of X
- We fix a base point $P_0 \in X(\bar{K})$ and identify $X(\bar{K})$ with its image in $J(\bar{K})$ under the Albanese embedding

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

The Manin-Mumford Conjecture: Statement

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 Manin-Mumford Conjecture: Statement

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.

- There are many different proofs of this theorem in the literature. We will present an elegant short proof due to Ken Ribet based on the notion of almost rational torsion points.

Almost rational torsion points

Definition

Let A/K be an abelian variety. A torsion point $P \in A(\bar{K})$ is called almost rational if $\sigma P + \tau P = 2P$ with $\sigma, \tau \in \mathrm{Gal}(\bar{K}/K)$ implies $\sigma P = \tau P = P$.

Almost rational torsion points

Definition

Let A/K be an abelian variety. A torsion point $P \in A(\bar{K})$ is called almost rational if $\sigma P + \tau P = 2P$ with $\sigma, \tau \in \mathrm{Gal}(\bar{K}/K)$ implies $\sigma P = \tau P = P$.

Theorem (Ribet)

If A is an abelian variety over a number field K, then the set of almost rational torsion points in $A(\bar{K})$ is finite.

Proof of Ribet's theorem (Sketch)

- Let $\rho : G_K = \mathrm{Gal}(\bar{K}/K) \to \mathrm{GL}_{2g}(\hat{\mathbb{Z}})$ be the Galois representation arising from the adelic Tate module of A, and let $\hat{\mathbb{Z}}^* \subset \mathrm{GL}_{2g}(\hat{\mathbb{Z}})$ be the subgroup of homotheties.

Proof of Ribet's theorem (Sketch)

- Let $\rho : G_K = \mathrm{Gal}(\bar{K}/K) \to \mathrm{GL}_{2g}(\hat{\mathbb{Z}})$ be the Galois representation arising from the adelic Tate module of A, and let $\hat{\mathbb{Z}}^* \subset \mathrm{GL}_{2g}(\hat{\mathbb{Z}})$ be the subgroup of homotheties.
- By a theorem of Serre, the group $\hat{\mathbb{Z}}^*/(\rho(G_K) \cap \hat{\mathbb{Z}}^*)$ has finite exponent e.

Proof of Ribet's theorem (Sketch)

- Let $\rho : G_K = \mathrm{Gal}(\bar{K}/K) \to \mathrm{GL}_{2g}(\hat{\mathbb{Z}})$ be the Galois representation arising from the adelic Tate module of A, and let $\hat{\mathbb{Z}}^* \subset \mathrm{GL}_{2g}(\hat{\mathbb{Z}})$ be the subgroup of homotheties.
- By a theorem of Serre, the group $\hat{\mathbb{Z}}^*/(\rho(G_K) \cap \hat{\mathbb{Z}}^*)$ has finite exponent e.
- Using the Weil bounds and Hensel's lemma, one shows that there is a constant $C(e)$ such that if $M > C(e)$, then there exist $x, y \in (\mathbb{Z}/M\mathbb{Z})^*$ such that $x^e + y^e = 2$ but $x^e, y^e \neq 1$.

Proof of Ribet's theorem (Sketch)

- Let $\rho : G_K = \mathrm{Gal}(\bar{K}/K) \to \mathrm{GL}_{2g}(\hat{\mathbb{Z}})$ be the Galois representation arising from the adelic Tate module of A, and let $\hat{\mathbb{Z}}^* \subset \mathrm{GL}_{2g}(\hat{\mathbb{Z}})$ be the subgroup of homotheties.
- By a theorem of Serre, the group $\hat{\mathbb{Z}}^*/(\rho(G_K) \cap \hat{\mathbb{Z}}^*)$ has finite exponent e.
- Using the Weil bounds and Hensel's lemma, one shows that there is a constant $C(e)$ such that if $M > C(e)$, then there exist $x, y \in (\mathbb{Z}/M\mathbb{Z})^*$ such that $x^e + y^e = 2$ but $x^e, y^e \neq 1$.
- If $P \in A(\bar{K})$ is a torsion point of order $M > C(e)$, then by Serre there exist $\sigma, \tau \in G_K$ such that $\sigma P = x^e P$ and $\tau P = y^e P$. But then $\sigma P + \tau P = 2P$ and $\sigma P, \tau P \neq P$, so P is not almost rational.

Ribet's proof of Manin-Mumford

Here is Ribet's short proof of the Manin-Mumford conjecture using the finiteness of the set of almost rational torsion points:

Ribet's proof of Manin-Mumford

Here is Ribet's short proof of the Manin-Mumford conjecture using the finiteness of the set of almost rational torsion points:

- If $P \in X(\bar{K}) \cap J(\bar{K})_{\mathrm{tors}}$ is not almost rational, then there exist $\sigma, \tau \in G_K$ such that $\sigma P + \tau P = 2P$ in $J(\bar{K})$ but $\sigma P, \tau P \neq P$.

Ribet's proof of Manin-Mumford

Here is Ribet's short proof of the Manin-Mumford conjecture using the finiteness of the set of almost rational torsion points:

- If $P \in X(\bar{K}) \cap J(\bar{K})_{\mathrm{tors}}$ is not almost rational, then there exist $\sigma, \tau \in G_K$ such that $\sigma P + \tau P = 2P$ in $J(\bar{K})$ but $\sigma P, \tau P \neq P$.
- Thus there is a degree 2 rational function f on X such that

$$(f) = (\sigma P) + (\tau P) - 2(P) \ ,$$

which means that X is hyperelliptic and P is a hyperelliptic branch point.

Ribet's proof of Manin-Mumford

Here is Ribet's short proof of the Manin-Mumford conjecture using the finiteness of the set of almost rational torsion points:

- If $P \in X(\bar{K}) \cap J(\bar{K})_{\text{tors}}$ is not almost rational, then there exist $\sigma, \tau \in G_K$ such that $\sigma P + \tau P = 2P$ in $J(\bar{K})$ but $\sigma P, \tau P \neq P$.
- Thus there is a degree 2 rational function f on X such that

$$(f) = (\sigma P) + (\tau P) - 2(P) \ ,$$

  which means that X is hyperelliptic and P is a hyperelliptic branch point.
- Thus $X(\bar{K}) \cap J(\bar{K})_{\text{tors}}$ is contained in the union of the finite set of almost rational torsion points and the (possibly empty) finite set of hyperelliptic branch points.

Explicit example: Torsion points on modular curves

- Let $N \geq 23$ be a prime number, and let $X = X_0(N)$ be the usual modular curve, embedded in its Jacobian $J_0(N)$ using the cusp ∞ as a base point.

Explicit example: Torsion points on modular curves

- Let $N \geq 23$ be a prime number, and let $X = X_0(N)$ be the usual modular curve, embedded in its Jacobian $J_0(N)$ using the cusp ∞ as a base point.
- There is another cusp called 0 on $X_0(N)$. Manin and Drinfeld proved that the difference $i_\infty(0) = [(0) - (\infty)]$ is always torsion in $J_0(N)$.

Explicit example: Torsion points on modular curves

- Let $N \geq 23$ be a prime number, and let $X = X_0(N)$ be the usual modular curve, embedded in its Jacobian $J_0(N)$ using the cusp ∞ as a base point.
- There is another cusp called 0 on $X_0(N)$. Manin and Drinfeld proved that the difference $i_\infty(0) = [(0) - (\infty)]$ is always torsion in $J_0(N)$.

Theorem (Baker, Tamagawa, 1999)

Let $S = \{23, 29, 31, 41, 47, 53, 71\}$ be the set of N for which $X_0^+(N)$ has genus 0. Let H be the set of hyperelliptic branch points on $X_0(N)$ when $X_0(N)$ is hyperelliptic (which happens iff $N \in S$ or $N = 37$). Then

$$X_0(N)(\bar{\mathbb{Q}}) \cap J_0(N)(\bar{\mathbb{Q}})_{\mathrm{tors}} =$$

Explicit example: Torsion points on modular curves

- Let $N \geq 23$ be a prime number, and let $X = X_0(N)$ be the usual modular curve, embedded in its Jacobian $J_0(N)$ using the cusp ∞ as a base point.
- There is another cusp called 0 on $X_0(N)$. Manin and Drinfeld proved that the difference $i_\infty(0) = [(0) - (\infty)]$ is always torsion in $J_0(N)$.

Theorem (Baker, Tamagawa, 1999)

Let $S = \{23, 29, 31, 41, 47, 53, 71\}$ be the set of N for which $X_0^+(N)$ has genus 0. Let H be the set of hyperelliptic branch points on $X_0(N)$ when $X_0(N)$ is hyperelliptic (which happens iff $N \in S$ or $N = 37$). Then

$$X_0(N)(\bar{\mathbb{Q}}) \cap J_0(N)(\bar{\mathbb{Q}})_{\text{tors}} = \begin{cases} \{0, \infty\} & \text{if } N \notin S \\ & \end{cases}$$

Explicit example: Torsion points on modular curves

- Let $N \geq 23$ be a prime number, and let $X = X_0(N)$ be the usual modular curve, embedded in its Jacobian $J_0(N)$ using the cusp ∞ as a base point.
- There is another cusp called 0 on $X_0(N)$. Manin and Drinfeld proved that the difference $i_\infty(0) = [(0) - (\infty)]$ is always torsion in $J_0(N)$.

Theorem (Baker, Tamagawa, 1999)

Let $S = \{23, 29, 31, 41, 47, 53, 71\}$ be the set of N for which $X_0^+(N)$ has genus 0. Let H be the set of hyperelliptic branch points on $X_0(N)$ when $X_0(N)$ is hyperelliptic (which happens iff $N \in S$ or $N = 37$). Then

$$X_0(N)(\bar{\mathbb{Q}}) \cap J_0(N)(\bar{\mathbb{Q}})_{\text{tors}} = \begin{cases} \{0, \infty\} & \text{if } N \notin S \\ \{0, \infty\} \cup H & \text{if } N \in S. \end{cases}$$

Modular curves (continued)

- Let C be the cuspidal subgroup of $J_0(N)$, the rational cyclic subgroup generated by $(0) - (\infty)$, and let Σ be the Shimura subgroup of $J_0(N)$.

Modular curves (continued)

- Let C be the cuspidal subgroup of $J_0(N)$, the rational cyclic subgroup generated by $(0) - (\infty)$, and let Σ be the Shimura subgroup of $J_0(N)$.
- The explicit determination of $X_0(N)(\bar{\mathbb{Q}}) \cap J_0(N)(\bar{\mathbb{Q}})_{\text{tors}}$ can be deduced from the following result due to Ribet:

Modular curves (continued)

- Let C be the cuspidal subgroup of $J_0(N)$, the rational cyclic subgroup generated by $(0) - (\infty)$, and let Σ be the Shimura subgroup of $J_0(N)$.
- The explicit determination of $X_0(N)(\bar{\mathbb{Q}}) \cap J_0(N)(\bar{\mathbb{Q}})_{\mathrm{tors}}$ can be deduced from the following result due to Ribet:

Theorem (Ribet)

The set of almost rational torsion points in $J_0(N)(\bar{\mathbb{Q}})$ is precisely $\Sigma[3] \oplus C$.

Torsion points on Fermat curves

- Let $p \geq 7$ be a prime number, let a be an integer with $1 \leq a \leq p-2$, and let $X = X_{a,p}$ be the Fermat quotient curve given in affine coordinates by

$$y(1-y)^a = x^p \; .$$

Torsion points on Fermat curves

- Let $p \geq 7$ be a prime number, let a be an integer with $1 \leq a \leq p-2$, and let $X = X_{a,p}$ be the Fermat quotient curve given in affine coordinates by

$$y(1-y)^a = x^p \ .$$

- The curve $X_{a,p}$ is a quotient of the Fermat curve F_p given by $x^p + y^p = 1$, and its genus is $g = \frac{p-1}{2}$.

Torsion points on Fermat curves

- Let $p \geq 7$ be a prime number, let a be an integer with $1 \leq a \leq p-2$, and let $X = X_{a,p}$ be the Fermat quotient curve given in affine coordinates by

$$y(1-y)^a = x^p \ .$$

- The curve $X_{a,p}$ is a quotient of the Fermat curve F_p given by $x^p + y^p = 1$, and its genus is $g = \frac{p-1}{2}$.
- The three rational points $(0,0), (0,1), \infty$ on X are called the cusps. We will view X as embedded in its Jacobian $J = J_{a,p}$ via the map i_∞. It is easy to see that $i_\infty(0,0)$ and $i_\infty(0,1)$ are torsion points of J.

Fermat curves (continued)

Theorem (Grant-Shaulis (2004), Tzermias (2007))

Let $S_p = \{1, \frac{p-1}{2}, p-2\}$ be the set of a for which $X = X_{a,p}$ is hyperelliptic. Let H be the set of hyperelliptic branch points on X when $a \in S_p$. Then

$$X_{a,p}(\bar{\mathbb{Q}}) \cap J_{a,p}(\bar{\mathbb{Q}})_{\text{tors}} =$$

Fermat curves (continued)

Theorem (Grant-Shaulis (2004), Tzermias (2007))

Let $S_p = \{1, \frac{p-1}{2}, p-2\}$ be the set of a for which $X = X_{a,p}$ is hyperelliptic. Let H be the set of hyperelliptic branch points on X when $a \in S_p$. Then

$$X_{a,p}(\bar{\mathbb{Q}}) \cap J_{a,p}(\bar{\mathbb{Q}})_{\mathrm{tors}} = \begin{cases} \{\text{cusps}\} & \text{if } a \notin S \\ \end{cases}$$

Fermat curves (continued)

Theorem (Grant-Shaulis (2004), Tzermias (2007))

Let $S_p = \{1, \frac{p-1}{2}, p-2\}$ be the set of a for which $X = X_{a,p}$ is hyperelliptic. Let H be the set of hyperelliptic branch points on X when $a \in S_p$. Then

$$X_{a,p}(\bar{\mathbb{Q}}) \cap J_{a,p}(\bar{\mathbb{Q}})_{\mathrm{tors}} = \begin{cases} \{\mathrm{cusps}\} & \text{if } a \notin S \\ \{\mathrm{cusps}\} \cup H & \text{if } a \in S. \end{cases}$$

Fermat curves (continued)

- The arguments of Grant-Shaulis (in the hyperelliptic case) and Tzermias (in the non-hyperelliptic case) both rely heavily on information about the almost rational torsion points on $J_{a,p}$ coming from the theory of complex multiplication.

Fermat curves (continued)

- The arguments of Grant-Shaulis (in the hyperelliptic case) and Tzermias (in the non-hyperelliptic case) both rely heavily on information about the almost rational torsion points on $J_{a,p}$ coming from the theory of complex multiplication.
- One easily deduces from the above result the earlier theorem of Coleman-Tamagawa-Tzermias, which says that the only torsion points on the Fermat curve F_p itself are the cusps (the points where one of the coordinates is zero, together with ∞).

Almost rational torsion points on semistable elliptic curves

- The following result due to Frank Calegari classifies the almost rational torsion points on semistable elliptic curves over $\mathbb{Q}$. Its proof makes use of Wiles' modularity theorem, Ribet's level-lowering theorem, and Mazur's explicit determination of the possibilities for $E(\mathbb{Q})_{\text{tors}}$:

Almost rational torsion points on semistable elliptic curves

- The following result due to Frank Calegari classifies the almost rational torsion points on semistable elliptic curves over $\mathbb{Q}$. Its proof makes use of Wiles' modularity theorem, Ribet's level-lowering theorem, and Mazur's explicit determination of the possibilities for $E(\mathbb{Q})_{\text{tors}}$:

Theorem (Calegari)

Let $E/\mathbb{Q}$ be a semistable elliptic curve. A point $P \in E(\bar{\mathbb{Q}})_{\text{tors}}$ is almost rational iff $P = Q + R + S$, where Q is a generator of a μ_3-subgroup of $E[3]$, $R \in E(\mathbb{Q})[9]$, and $S \in E(\mathbb{Q}(\mu_3))[16]$.

Outline

Ribet's theorem

Theorem (Ribet, 1981)

Let A be an abelian variety defined over a number field K, and let $K^{\mathrm{cycl}} = K(\mu_\infty)$ be the maximal cyclotomic extension of K. Then $A(K^{\mathrm{cycl}})_{\mathrm{tors}}$ is finite.

Ribet's theorem

Theorem (Ribet, 1981)

Let A be an abelian variety defined over a number field K, and let $K^{\mathrm{cycl}} = K(\mu_\infty)$ be the maximal cyclotomic extension of K. Then $A(K^{\mathrm{cycl}})_{\mathrm{tors}}$ is finite.

There are two steps in Ribet's argument:

Ribet's theorem

Theorem (Ribet, 1981)

Let A be an abelian variety defined over a number field K, and let $K^{\mathrm{cycl}} = K(\mu_\infty)$ be the maximal cyclotomic extension of K. Then $A(K^{\mathrm{cycl}})_{\mathrm{tors}}$ is finite.

There are two steps in Ribet's argument:

1. Ribet first proves that $A(K^{\mathrm{cycl}})[p] = 0$ for all but finitely many primes p using results about semistable reduction of abelian varieties and the Oort-Tate classification of finite flat group schemes of order p.

Ribet's theorem

Theorem (Ribet, 1981)

Let A be an abelian variety defined over a number field K, and let $K^{\mathrm{cycl}} = K(\mu_\infty)$ be the maximal cyclotomic extension of K. Then $A(K^{\mathrm{cycl}})_{\mathrm{tors}}$ is finite.

There are two steps in Ribet's argument:

1. Ribet first proves that $A(K^{\mathrm{cycl}})[p] = 0$ for all but finitely many primes p using results about semistable reduction of abelian varieties and the Oort-Tate classification of finite flat group schemes of order p.
2. He then proves that $A(K^{\mathrm{cycl}})[p^\infty]$ is finite for all primes p using Tate's results on p-divisible groups, Serre's results on locally algebraic representations of $\mathrm{Gal}(\bar{K}/K)$, and Weil's proof of the Riemann hypothesis for abelian varieties over finite fields.

Zhang's generalization via equidistribution

Using equidistribution methods, Shouwu Zhang proved a generalization of Ribet's theorem in which torsion points are replaced by points of "small" canonical height:

Zhang's generalization via equidistribution

Using equidistribution methods, Shouwu Zhang proved a generalization of Ribet's theorem in which torsion points are replaced by points of "small" canonical height:

Theorem (Zhang, 1998)

Let K be a number field, and let A/K be an abelian variety. Let L be a symmetric ample line bundle on A, and let $\hat{h}_L : A(\bar{K}) \to \mathbb{R}_{\geq 0}$ be the corresponding canonical height function. Then there exists $\varepsilon > 0$ such that the set

$$\{P \in A(K^{\text{cycl}}) \ : \ \hat{h}_L(P) < \varepsilon\}$$

is finite.

Zhang's generalization via equidistribution (continued)

When the field K is totally real, Zhang's method yields a similar result for points of small height over the maximal abelian extension K^{ab} of K:

Zhang's generalization via equidistribution (continued)

When the field K is totally real, Zhang's method yields a similar result for points of small height over the maximal abelian extension K^{ab} of K:

Theorem (Zhang, 1998)

Let K be a totally real number field, and let A/K be an abelian variety. Let L be a symmetric ample line bundle on A, and let $\hat{h}_L : A(\bar{K}) \to \mathbb{R}_{\geq 0}$ be the corresponding canonical height function. Then there exists $\varepsilon > 0$ such that the set

$$\{P \in A(K^{\mathrm{ab}}) \ : \ \hat{h}_L(P) < \varepsilon\}$$

is finite.

Idea of Zhang's proof

- The maximal totally real subfield $(K^{\mathrm{cycl}})^+$ of K^{cycl} has finite index, and when K is totally real, $(K^{\mathrm{ab}})^+$ has finite index in K^{ab} by Class Field Theory. By restriction of scalars, one can replace K^{cycl} by $(K^{\mathrm{cycl}})^+$ (resp. K^{ab} by $(K^{\mathrm{ab}})^+$) in the statement of Zhang's theorems.

Idea of Zhang's proof

- The maximal totally real subfield $(K^{\mathrm{cycl}})^+$ of K^{cycl} has finite index, and when K is totally real, $(K^{\mathrm{ab}})^+$ has finite index in K^{ab} by Class Field Theory. By restriction of scalars, one can replace K^{cycl} by $(K^{\mathrm{cycl}})^+$ (resp. K^{ab} by $(K^{\mathrm{ab}})^+$) in the statement of Zhang's theorems.
- Since points lying in $A(\mathbb{R})$ cannot be equidistributed with respect to Haar measure on $A(\mathbb{C})$, the results follow easily from the following equidistribution theorem, generalizing earlier work of Szpiro-Ullmo-Zhang:

Zhang's equidistribution theorem

Theorem (Zhang)

Let $\{P_n\}$ be a sequence of points in $A(\bar{K})$ such that $\hat{h}_L(P_n) \to 0$, and such that no subsequence is contained in a proper torsion subvariety of A. Let δ_n denote the discrete probability measure on $A(\mathbb{C})$ supported equally on the Galois conjugates of P_n. Then δ_n converges weakly to the Haar probability measure μ on $A(\mathbb{C})$.

Zarhin's generalization of Ribet's theorem

For arbitrary abelian extensions of K, one has the following result of Zarhin (as slightly strengthened by Ruppert):

Zarhin's generalization of Ribet's theorem

For arbitrary abelian extensions of K, one has the following result of Zarhin (as slightly strengthened by Ruppert):

Theorem (Zarhin)

Let A be an abelian variety defined over a number field K having no abelian subvariety with complex multiplication over K. Then $A(K^{ab})_{tors}$ is finite.

Zarhin's generalization of Ribet's theorem

For arbitrary abelian extensions of K, one has the following result of Zarhin (as slightly strengthened by Ruppert):

Theorem (Zarhin)

Let A be an abelian variety defined over a number field K having no abelian subvariety with complex multiplication over K. Then $A(K^{ab})_{tors}$ is finite.

The proof makes use of the methods pioneered by Faltings in his proof of Tate's isogeny conjecture.

Small points over abelian extensions

Theorem (Baker-Silverman, 2004)

Let A be an abelian variety defined over a number field K, and let L be a symmetric ample line bundle on A. Then:

Small points over abelian extensions

Theorem (Baker-Silverman, 2004)

Let A be an abelian variety defined over a number field K, and let L be a symmetric ample line bundle on A. Then:

1. *There exists $\varepsilon > 0$ such that $\hat{h}_L(P) \geq \varepsilon$ for all non-torsion points $P \in A(K^{\mathrm{ab}})$.*

Small points over abelian extensions

Theorem (Baker-Silverman, 2004)

Let A be an abelian variety defined over a number field K, and let L be a symmetric ample line bundle on A. Then:

1. *There exists $\varepsilon > 0$ such that $\hat{h}_L(P) \geq \varepsilon$ for all non-torsion points $P \in A(K^{\mathrm{ab}})$.*
2. *The set*
$$\{P \in A(K^{\mathrm{cycl}}) \ : \ \hat{h}_L(P) < \varepsilon\}$$
is finite.

Small points over abelian extensions

Theorem (Baker-Silverman, 2004)

Let A be an abelian variety defined over a number field K, and let L be a symmetric ample line bundle on A. Then:

1. *There exists $\varepsilon > 0$ such that $\hat{h}_L(P) \geq \varepsilon$ for all non-torsion points $P \in A(K^{\text{ab}})$.*
2. *The set*
$$\{P \in A(K^{\text{cycl}}) \ : \ \hat{h}_L(P) < \varepsilon\}$$
is finite.
3. *If A does not have complex multiplication over K, then*
$$\{P \in A(K^{\text{ab}}) \ : \ \hat{h}_L(P) < \varepsilon\}$$
is finite.

Some comments about the proof

- The proof of part (i) proceeds by induction on the local conductor of the abelian extension $K(P)/K$. The cases where A does or does not have CM are handled separately.

Some comments about the proof

- The proof of part (i) proceeds by induction on the local conductor of the abelian extension $K(P)/K$. The cases where A does or does not have CM are handled separately.
- The proof of the CM case is similar in spirit to the proof of the following earlier result concerning the multiplicative group $\mathbf{G}_m$:

Some comments about the proof

- The proof of part (i) proceeds by induction on the local conductor of the abelian extension $K(P)/K$. The cases where A does or does not have CM are handled separately.
- The proof of the CM case is similar in spirit to the proof of the following earlier result concerning the multiplicative group $\mathbf{G}_m$:

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

Let K be a number field. Then there exists $\varepsilon > 0$ such that $h(\alpha) \geq \varepsilon$ for every $\alpha \in K^{\mathrm{ab}}$ which is not a root of unity.

Explicit results for elliptic curves

When K is totally real and A is an elliptic curve over K, Zhang's generalization of Ribet's theorem can be made completely explicit using a quantitative version of the Szpiro-Ullmo-Zhang equidistribution theorem:

Explicit results for elliptic curves

When K is totally real and A is an elliptic curve over K, Zhang's generalization of Ribet's theorem can be made completely explicit using a quantitative version of the Szpiro-Ullmo-Zhang equidistribution theorem:

Theorem (Baker-Petsche, 2005)

Let K be a totally real number field, and let E/K be an elliptic curve. Then:

Explicit results for elliptic curves

When K is totally real and A is an elliptic curve over K, Zhang's generalization of Ribet's theorem can be made completely explicit using a quantitative version of the Szpiro-Ullmo-Zhang equidistribution theorem:

Theorem (Baker-Petsche, 2005)

Let K be a totally real number field, and let E/K be an elliptic curve. Then:

1. $$|E(K^{\mathrm{cycl}})_{\mathrm{tors}}| \leq 36(h(j_E) + 10)^4 \ .$$

Explicit results for elliptic curves

When K is totally real and A is an elliptic curve over K, Zhang's generalization of Ribet's theorem can be made completely explicit using a quantitative version of the Szpiro-Ullmo-Zhang equidistribution theorem:

Theorem (Baker-Petsche, 2005)

Let K be a totally real number field, and let E/K be an elliptic curve. Then:

1. $$|E(K^{\text{cycl}})_{\text{tors}}| \leq 36(h(j_E)+10)^4 \ .$$
2. *If $P \in E(K^{\text{cycl}})$ is non-torsion, then*
$$\hat{h}(P) \geq \frac{1}{864(h(j_E)+10)^5} \ .$$

Idea of the proof

- The proof of this quantitative result is based on a height-discrepancy inequality.

Idea of the proof

- The proof of this quantitative result is based on a height-discrepancy inequality.
- If v is a place of K and $Z = \{P_1, \ldots, P_N\}$ is a finite subset of $E(\bar{K})$, one defines the local discrepancy of Z to be

$$D_v(Z) = \frac{1}{N^2} \sum_{i,j} \lambda_v^*(P_i - P_j)$$

where λ_v^* is a certain nonnegative "smoothing" of the usual Néron canonical local height function λ_v.

Idea of the proof

- The proof of this quantitative result is based on a height-discrepancy inequality.
- If v is a place of K and $Z = \{P_1, \ldots, P_N\}$ is a finite subset of $E(\bar{K})$, one defines the local discrepancy of Z to be

$$D_v(Z) = \frac{1}{N^2} \sum_{i,j} \lambda_v^*(P_i - P_j)$$

where λ_v^* is a certain nonnegative "smoothing" of the usual Néron canonical local height function λ_v.
- The local discrepancy measures how far the points $P_1, \ldots, P_N$ are from being "v-adically equidistributed".

The Height-Discrepancy Inequality

- One defines the global discrepancy $D(Z)$ to be the sum of the local discrepancies, and the global canonical height $\hat{h}(Z)$ to be the average of the $\hat{h}(P_i)$'s.

The Height-Discrepancy Inequality

- One defines the global discrepancy $D(Z)$ to be the sum of the local discrepancies, and the global canonical height $\hat{h}(Z)$ to be the average of the $\hat{h}(P_i)$'s.

Theorem (Baker-Petsche, the "Height-Discrepancy Inequality")

Let $Z \subset E(\bar{K})$ have cardinality N. Then

$$D(Z) \leq 4\hat{h}(Z) + \frac{1}{N}\left(\frac{1}{2}\log N + \frac{1}{12}h(j_E) + \frac{16}{5}\right) .$$

Outline

1. Almost rational torsion points
2. Torsion points over abelian extensions
3. Torsion points unramified at p

Ribet's theorem for $J_0(N)$

- Let N be a prime number, let $\mathbf{T}$ be the Hecke algebra associated to $X_0(N)$, and let I be the Eisenstein ideal in $\mathbf{T}$.

Ribet's theorem for $J_0(N)$

- Let N be a prime number, let $\mathbf{T}$ be the Hecke algebra associated to $X_0(N)$, and let I be the Eisenstein ideal in $\mathbf{T}$.
- The kernel of the Eisenstein ideal is the Galois module $J_0(N)[I]$ consisting of all points of $J_0(N)(\bar{\mathbb{Q}})$ annihilated by I. It is a finite module of order n^2, where n is the numerator of the fraction $\frac{N-1}{12}$. When n is odd, $J_0(N)[I] = C \oplus \Sigma$.

Ribet's theorem for $J_0(N)$

- Let N be a prime number, let $\mathbf{T}$ be the Hecke algebra associated to $X_0(N)$, and let I be the Eisenstein ideal in $\mathbf{T}$.
- The kernel of the Eisenstein ideal is the Galois module $J_0(N)[I]$ consisting of all points of $J_0(N)(\bar{\mathbb{Q}})$ annihilated by I. It is a finite module of order n^2, where n is the numerator of the fraction $\frac{N-1}{12}$. When n is odd, $J_0(N)[I] = C \oplus \Sigma$.
- Given a maximal ideal $\mathfrak{p}$ in the ring of integers of a number field K, we let $K^{(\mathfrak{p})}$ denote the maximal algebraic extension of K unramified at all primes lying over $\mathfrak{p}$. By results of Mazur, one knows that all points of $J[I]$ are unramified above N, i.e., $J_0(N)[I] \subseteq J_0(N)(\mathbb{Q}^{(N)})$.

Ribet's theorem (continued)

The following result plays a crucial role in the determination of all torsion points of $J_0(N)$ which lie on $X_0(N)$ (and in Ribet's determination of the almost rational torsion points of $J_0(N)$):

Ribet's theorem (continued)

The following result plays a crucial role in the determination of all torsion points of $J_0(N)$ which lie on $X_0(N)$ (and in Ribet's determination of the almost rational torsion points of $J_0(N)$):

Theorem (Ribet, 1999)

The group of torsion points of $J_0(N)(\bar{\mathbb{Q}})$ unramified above N is precisely the kernel of the Eisenstein ideal:

$$J_0(N)(\mathbb{Q}^{(N)})_{\mathrm{tors}} = J_0(N)[I] \; .$$

Idea of the proof

- Let $P \in J_0(N)(\bar{\mathbb{Q}})$ be unramified at N. It suffices to show that the $\mathbf{T}[\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})]$ module M generated by P and $J_0(N)[I]$ is annihilated by I.

Idea of the proof

- Let $P \in J_0(N)(\bar{\mathbb{Q}})$ be unramified at N. It suffices to show that the $\mathbf{T}[\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})]$ module M generated by P and $J_0(N)[I]$ is annihilated by I.
- If V is any Jordan-Holder constituent of M, the annihilator of V is a maximal ideal $\mathfrak{m}$ of $\mathbf{T}$. Suppose $\mathfrak{m}$ is not Eisenstein. Then $V \cong \rho_{\mathfrak{m}}$, the standard two-dimensional irreducible representation of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ attached to $\mathfrak{m}$.

Idea of the proof

- Let $P \in J_0(N)(\bar{\mathbb{Q}})$ be unramified at N. It suffices to show that the $\mathbf{T}[\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})]$ module M generated by P and $J_0(N)[I]$ is annihilated by I.
- If V is any Jordan-Holder constituent of M, the annihilator of V is a maximal ideal $\mathfrak{m}$ of $\mathbf{T}$. Suppose $\mathfrak{m}$ is not Eisenstein. Then $V \cong \rho_{\mathfrak{m}}$, the standard two-dimensional irreducible representation of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ attached to $\mathfrak{m}$.
- If $\mathfrak{m} \nmid 2$, then since V is unramified at N, Ribet's level-lowering theorem shows that $\rho_{\mathfrak{m}}$ is modular of level 1, which is impossible.

Idea of the proof (continued)

- On the other hand, if $\mathfrak{m} \mid 2$, then $\rho_{\mathfrak{m}} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_2)$ is an irreducible representation which is unramified outside 2. But Tate proved that no such representation exists!

Idea of the proof (continued)

- On the other hand, if $\mathfrak{m} \mid 2$, then $\rho_{\mathfrak{m}} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_2)$ is an irreducible representation which is unramified outside 2. But Tate proved that no such representation exists!
- Thus $\mathfrak{m}$ is Eisenstein, from which it follows that every Jordan-Holder constituent of M is annihilated by I.

Idea of the proof (continued)

- On the other hand, if $\mathfrak{m} \mid 2$, then $\rho_{\mathfrak{m}} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_2)$ is an irreducible representation which is unramified outside 2. But Tate proved that no such representation exists!
- Thus $\mathfrak{m}$ is Eisenstein, from which it follows that every Jordan-Holder constituent of M is annihilated by I.
- To deduce the *a priori* stronger fact that M itself is annihilated by I, one applies various results of Mazur, especially the local principality of the Eisenstein ideal.

Gubler's theorem

- By the work of Deligne-Rapoport, the abelian variety $J_0(N)$ is totally degenerate at N (i.e., it admits a non-archimedean uniformization in the sense of Mumford).

Gubler's theorem

- By the work of Deligne-Rapoport, the abelian variety $J_0(N)$ is totally degenerate at N (i.e., it admits a non-archimedean uniformization in the sense of Mumford).
- Recently, Walter Gubler has shown that the finiteness of $J_0(N)(\mathbb{Q}^{(N)})_{\text{tors}}$ is a general phenomenon occurring for totally degenerate abelian varieties, and it extends to points of small canonical height:

Gubler's theorem (continued)

Theorem (Gubler, 2007)

Let $\mathfrak{p}$ be a maximal ideal in the ring of integers of a number field K, and let A/K be an abelian variety which is totally degenerate at $\mathfrak{p}$. Then the set $A(K^{(\mathfrak{p})})_{\mathrm{tors}}$ of torsion points of A which are unramified above $\mathfrak{p}$ is finite. More generally, for any symmetric ample line bundle L on A, there exists $\varepsilon > 0$ such that the set

$$\{P \in A(K^{(\mathfrak{p})}) \ : \ \hat{h}_L(P) < \varepsilon\}$$

is finite.

Non-archimedean equidistribution

- The proof of Gubler's theorem is based on a non-archimedean analogue, for totally degenerate abelian varieties, of the Szpiro-Ullmo-Zhang and Zhang equidistribution theorems.

Non-archimedean equidistribution

- The proof of Gubler's theorem is based on a non-archimedean analogue, for totally degenerate abelian varieties, of the Szpiro-Ullmo-Zhang and Zhang equidistribution theorems.
- Let $\mathbb{C}_p$ be the completion of the algebraic closure of $K_{\mathfrak{p}}$, and let A^{an} denote the Berkovich analytic space associated to $A_{\mathbb{C}_p}$, which is a canonically defined compact Hausdorff space containing $A(\mathbb{C}_p)$ as a dense subspace.

Non-archimedean equidistribution

- The proof of Gubler's theorem is based on a non-archimedean analogue, for totally degenerate abelian varieties, of the Szpiro-Ullmo-Zhang and Zhang equidistribution theorems.
- Let $\mathbb{C}_p$ be the completion of the algebraic closure of $K_{\mathfrak{p}}$, and let A^{an} denote the Berkovich analytic space associated to $A_{\mathbb{C}_p}$, which is a canonically defined compact Hausdorff space containing $A(\mathbb{C}_p)$ as a dense subspace.
- Berkovich has constructed a canonical subset Σ of A^{an}, called the *skeleton* of A^{an}, together with a deformation retraction $r : A^{\mathrm{an}} \to \Sigma$. To say that A is totally degenerate is equivalent to saying that Σ is homeomorphic to a g-dimensinal real torus $\mathbb{R}^g/\Lambda$.

Non-archimedean equidistribution (continued)

The one-dimensional (elliptic curve) case of following theorem was proved earlier by Chambert-Loir:

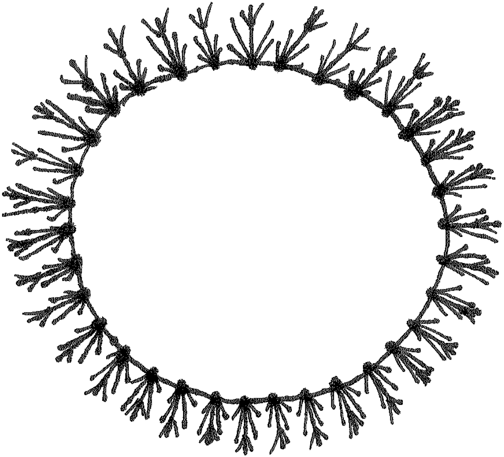
Non-archimedean equidistribution (continued)

The one-dimensional (elliptic curve) case of following theorem was proved earlier by Chambert-Loir:

Theorem (Gubler, 2007)

With notation and hypotheses as above, let $\{P_n\}$ be a sequence of points in $A(\bar{K})$ such that $\hat{h}_L(P_n) \to 0$, and such that no subsequence is contained in a proper torsion subvariety of A. Let δ_n denote the discrete probability measure on Σ supported equally on $r(P_n^\sigma)$, where P_n^σ runs through the Galois conjugates of P_n. Then δ_n converges weakly to the Haar probability measure μ on Σ.

The Berkovich analytic space associated to an elliptic curve with multiplicative reduction



Explicit results for elliptic curves

- For elliptic curves, one can deduce from the height-discrepancy inequality an explicit quantitative version of the results of Chambert-Loir and Gubler.

Explicit results for elliptic curves

- For elliptic curves, one can deduce from the height-discrepancy inequality an explicit quantitative version of the results of Chambert-Loir and Gubler.
- For simplicity, we assume that $K = \mathbb{Q}$, but there is a similar result over any number field K.

Explicit results for elliptic curves (continued)

Theorem (Baker-Petsche, 2005)

Let p be a prime number, and let $E/\mathbb{Q}$ be an elliptic curve with split multiplicative reduction at p. Let $M = -12 \operatorname{ord}_p(j_E)$. Then:

Explicit results for elliptic curves (continued)

Theorem (Baker-Petsche, 2005)

Let p be a prime number, and let $E/\mathbb{Q}$ be an elliptic curve with split multiplicative reduction at p. Let $M = -12\,\mathrm{ord}_p(j_E)$. Then:

1.
$$|E(\mathbb{Q}^{(p)})_{\mathrm{tors}}| \leq \frac{8M}{5\log p}(\log Mp^2 + \frac{1}{6}h(j_E) + \frac{32}{5}) .$$

Explicit results for elliptic curves (continued)

Theorem (Baker-Petsche, 2005)

Let p be a prime number, and let $E/\mathbb{Q}$ be an elliptic curve with split multiplicative reduction at p. Let $M = -12\,\mathrm{ord}_p(j_E)$. Then:

1. $$|E(\mathbb{Q}^{(p)})_{\mathrm{tors}}| \leq \frac{8M}{5\log p}(\log Mp^2 + \frac{1}{6}h(j_E) + \frac{32}{5})\ .$$

2. *If $P \in E(\mathbb{Q}^{(p)})$ is non-torsion, then*

$$\hat{h}(P) \geq \frac{25}{512}(\frac{\log p}{M})^3(\log Mp^2 + +\frac{1}{6}h(j_E) + \frac{32}{5})\ .$$