Explicit 2-descent and the average size of the 2-Selmer group of the Jacobians of odd hyperelliptic curves

Manjul Bhargava
Princeton University

September 25, 2012

(Joint work with Dick Gross)

Odd hyperelliptic curves

Odd hyperelliptic curves

A hyperelliptic curve C of genus $n \geq 1$ over $\mathbb{Q}$ with a marked rational Weierstrass point O has an affine equation of the form

$$y^2 = x^{2n+1} + c_2 x^{2n-1} + c_3 x^{2n-2} + \ldots + c_{2n+1} = f(x) \qquad (1)$$

with rational coefficients c_m.

Odd hyperelliptic curves

A hyperelliptic curve C of genus $n \geq 1$ over $\mathbb{Q}$ with a marked rational Weierstrass point O has an affine equation of the form

$$y^2 = x^{2n+1} + c_2 x^{2n-1} + c_3 x^{2n-2} + \ldots + c_{2n+1} = f(x) \qquad (1)$$

with rational coefficients c_m. (The point O lies above $x = \infty$, and $f(x)$ is separable.)

Odd hyperelliptic curves

A hyperelliptic curve C of genus $n \geq 1$ over $\mathbb{Q}$ with a marked rational Weierstrass point O has an affine equation of the form

$$y^2 = x^{2n+1} + c_2 x^{2n-1} + c_3 x^{2n-2} + \ldots + c_{2n+1} = f(x) \qquad (1)$$

with rational coefficients c_m. (The point O lies above $x = \infty$, and $f(x)$ is separable.)

Such curves are called odd hyperelliptic curves.

Odd hyperelliptic curves

A hyperelliptic curve C of genus $n \geq 1$ over $\mathbb{Q}$ with a marked rational Weierstrass point O has an affine equation of the form

$$y^2 = x^{2n+1} + c_2 x^{2n-1} + c_3 x^{2n-2} + \ldots + c_{2n+1} = f(x) \quad (1)$$

with rational coefficients c_m. (The point O lies above $x = \infty$, and $f(x)$ is separable.)

Such curves are called odd hyperelliptic curves.

The change of variable $x' = u^2 x,\ y' = u^{2n+1} y$ results in a change in the coefficients: $c'_m = u^{2m} c_m$.

Odd hyperelliptic curves

A hyperelliptic curve C of genus $n \geq 1$ over $\mathbb{Q}$ with a marked rational Weierstrass point O has an affine equation of the form

$$y^2 = x^{2n+1} + c_2 x^{2n-1} + c_3 x^{2n-2} + \ldots + c_{2n+1} = f(x) \quad (1)$$

with rational coefficients c_m. (The point O lies above $x = \infty$, and $f(x)$ is separable.)

Such curves are called odd hyperelliptic curves.

The change of variable $x' = u^2 x,\ y' = u^{2n+1} y$ results in a change in the coefficients: $c'_m = u^{2m} c_m$. Hence we may assume all coefficients are integers.

Odd hyperelliptic curves

A hyperelliptic curve C of genus $n \geq 1$ over $\mathbb{Q}$ with a marked rational Weierstrass point O has an affine equation of the form

$$y^2 = x^{2n+1} + c_2 x^{2n-1} + c_3 x^{2n-2} + \ldots + c_{2n+1} = f(x) \qquad (1)$$

with rational coefficients c_m. (The point O lies above $x = \infty$, and $f(x)$ is separable.)

Such curves are called odd hyperelliptic curves.

The change of variable $x' = u^2 x,\ y' = u^{2n+1} y$ results in a change in the coefficients: $c'_m = u^{2m} c_m$. Hence we may assume all coefficients are integers.

These integers are unique if we assume further that, for every prime p, the integral coefficients c_m are not all divisible by p^{2m}.

Odd hyperelliptic curves

A hyperelliptic curve C of genus $n \geq 1$ over $\mathbb{Q}$ with a marked rational Weierstrass point O has an affine equation of the form

$$y^2 = x^{2n+1} + c_2x^{2n-1} + c_3x^{2n-2} + \ldots + c_{2n+1} = f(x) \quad (1)$$

with rational coefficients c_m. (The point O lies above $x = \infty$, and $f(x)$ is separable.)

Such curves are called odd hyperelliptic curves.

The change of variable $x' = u^2x,\ y' = u^{2n+1}y$ results in a change in the coefficients: $c'_m = u^{2m}c_m$. Hence we may assume all coefficients are integers.

These integers are unique if we assume further that, for every prime p, the integral coefficients c_m are not all divisible by p^{2m}. In this case we say the coefficients are indivisible.

Heights of minimal equations

We assume now that the odd hyperelliptic curve C is given by its unique equation with indivisible integral coefficients.

Heights of minimal equations

We assume now that the odd hyperelliptic curve C is given by its unique equation with indivisible integral coefficients.

The discriminant of $f(x)$ is a polynomial $D(c_2, c_3, \ldots, c_{2n+1})$ of weighted homogeneous degree $2n(2n+1)$ in the coefficients c_m, where c_m has degree m.

Heights of minimal equations

We assume now that the odd hyperelliptic curve C is given by its unique equation with indivisible integral coefficients.

The discriminant of $f(x)$ is a polynomial $D(c_2, c_3, \ldots, c_{2n+1})$ of weighted homogeneous degree $2n(2n+1)$ in the coefficients c_m, where c_m has degree m.

We define the *discriminant* Δ of the curve C by the formula

$$\Delta(C) := 4^{2n} D(c_2, c_3, \ldots, c_{2n+1}),$$

Heights of minimal equations

We assume now that the odd hyperelliptic curve C is given by its unique equation with indivisible integral coefficients.

The discriminant of $f(x)$ is a polynomial $D(c_2, c_3, \ldots, c_{2n+1})$ of weighted homogeneous degree $2n(2n+1)$ in the coefficients c_m, where c_m has degree m.

We define the *discriminant* Δ of the curve C by the formula

$$\Delta(C) := 4^{2n} D(c_2, c_3, \ldots, c_{2n+1}),$$

and the (naive) *height* H of the curve C by

$$H(C) := \max\{|c_k|^{2n(2n+1)/k}\}_{k=2}^{2n+1}.$$

Heights of minimal equations

We assume now that the odd hyperelliptic curve C is given by its unique equation with indivisible integral coefficients.

The discriminant of $f(x)$ is a polynomial $D(c_2, c_3, \ldots, c_{2n+1})$ of weighted homogeneous degree $2n(2n+1)$ in the coefficients c_m, where c_m has degree m.

We define the *discriminant* Δ of the curve C by the formula

$$\Delta(C) := 4^{2n} D(c_2, c_3, \ldots, c_{2n+1}),$$

and the (naive) *height* H of the curve C by

$$H(C) := \max\{|c_k|^{2n(2n+1)/k}\}_{k=2}^{2n+1}.$$

We include the expression $2n(2n+1)$ in the definition so that the weighted homogeneous degree of H and Δ are the same.

Heights of minimal equations

We assume now that the odd hyperelliptic curve C is given by its unique equation with indivisible integral coefficients.

The discriminant of $f(x)$ is a polynomial $D(c_2, c_3, \ldots, c_{2n+1})$ of weighted homogeneous degree $2n(2n+1)$ in the coefficients c_m, where c_m has degree m.

We define the *discriminant* Δ of the curve C by the formula

$$\Delta(C) := 4^{2n} D(c_2, c_3, \ldots, c_{2n+1}),$$

and the (naive) *height* H of the curve C by

$$H(C) := \max\{|c_k|^{2n(2n+1)/k}\}_{k=2}^{2n+1}.$$

We include the expression $2n(2n+1)$ in the definition so that the weighted homogeneous degree of H and Δ are the same.

The height $H(C)$ gives a concrete way to enumerate all odd hyperelliptic curves over $\mathbb{Q}$ of a fixed genus: for any real number $X > 0$ there are clearly only finitely many curves with $H(C) < X$.

Genus one

Genus one

The discriminant and height for odd hyperelliptic curves extend naturally the classical notions in the case of elliptic curves (which is the case $n = 1$):

Genus one

The discriminant and height for odd hyperelliptic curves extend naturally the classical notions in the case of elliptic curves (which is the case $n = 1$):

Any elliptic curve E over $\mathbb{Q}$ is given by a unique equation of the form $y^2 = x^3 + c_2x + c_3$, where $c_2, c_3 \in \mathbb{Z}$ and for all primes p: $p^6 \nmid c_3$ whenever $p^4 \mid c_2$.

Genus one

The discriminant and height for odd hyperelliptic curves extend naturally the classical notions in the case of elliptic curves (which is the case $n = 1$):

Any elliptic curve E over $\mathbb{Q}$ is given by a unique equation of the form $y^2 = x^3 + c_2x + c_3$, where $c_2, c_3 \in \mathbb{Z}$ and for all primes p: $p^6 \nmid c_3$ whenever $p^4 \mid c_2$.

The discriminant is then defined by the formula

$$\Delta(E) := 2^4(-4c_2^3 - 27c_3^2),$$

Genus one

The discriminant and height for odd hyperelliptic curves extend naturally the classical notions in the case of elliptic curves (which is the case $n = 1$):

Any elliptic curve E over $\mathbb{Q}$ is given by a unique equation of the form $y^2 = x^3 + c_2x + c_3$, where $c_2, c_3 \in \mathbb{Z}$ and for all primes p: $p^6 \nmid c_3$ whenever $p^4 \mid c_2$.

The discriminant is then defined by the formula

$$\Delta(E) := 2^4(-4c_2^3 - 27c_3^2),$$

and the naive height by

$$H(E) := \max\{|c_2|^3, |c_3|^2\}.$$

The average size of the 2-Selmer group

Recall that the 2-Selmer group $S_2(J)$ of the Jacobian $J = \mathrm{Jac}(C)$ of C is a finite subgroup of the Galois cohomology group $H^1(\mathbb{Q}, J[2])$, which is defined by local conditions and fits into an exact sequence

$$0 \to J(\mathbb{Q})/2J(\mathbb{Q}) \to S_2(J) \to Ш_J[2] \to 0,$$

where $Ш_J$ denotes the Tate-Shafarevich group of J over $\mathbb{Q}$.

The average size of the 2-Selmer group

Recall that the 2-Selmer group $S_2(J)$ of the Jacobian $J = \mathrm{Jac}(C)$ of C is a finite subgroup of the Galois cohomology group $H^1(\mathbb{Q}, J[2])$, which is defined by local conditions and fits into an exact sequence

$$0 \to J(\mathbb{Q})/2J(\mathbb{Q}) \to S_2(J) \to Ш_J[2] \to 0,$$

where $Ш_J$ denotes the Tate-Shafarevich group of J over $\mathbb{Q}$.

Then our main theorem is

Recall that the 2-Selmer group $S_2(J)$ of the Jacobian $J = \mathrm{Jac}(C)$ of C is a finite subgroup of the Galois cohomology group $H^1(\mathbb{Q}, J[2])$, which is defined by local conditions and fits into an exact sequence

$$0 \to J(\mathbb{Q})/2J(\mathbb{Q}) \to S_2(J) \to Ш_J[2] \to 0,$$

where $Ш_J$ denotes the Tate-Shafarevich group of J over $\mathbb{Q}$.

Then our main theorem is

Theorem 1 (joint w/Dick Gross). *When all odd hyperelliptic curves of any fixed genus $n \geq 1$ over $\mathbb{Q}$ are ordered by height, the average size of the 2-Selmer groups of their Jacobians is equal to 3.*

Recall that the 2-Selmer group $S_2(J)$ of the Jacobian $J = \mathrm{Jac}(C)$ of C is a finite subgroup of the Galois cohomology group $H^1(\mathbb{Q}, J[2])$, which is defined by local conditions and fits into an exact sequence

$$0 \to J(\mathbb{Q})/2J(\mathbb{Q}) \to S_2(J) \to Ш_J[2] \to 0,$$

where $Ш_J$ denotes the Tate-Shafarevich group of J over $\mathbb{Q}$.

Then our main theorem is

Theorem 1 (joint w/Dick Gross). *When all odd hyperelliptic curves of any fixed genus $n \geq 1$ over $\mathbb{Q}$ are ordered by height, the average size of the 2-Selmer groups of their Jacobians is equal to 3.*

We actually prove something stronger, namely:

The average size of the 2-Selmer group

Recall that the 2-Selmer group $S_2(J)$ of the Jacobian $J = \mathrm{Jac}(C)$ of C is a finite subgroup of the Galois cohomology group $H^1(\mathbb{Q}, J[2])$, which is defined by local conditions and fits into an exact sequence

$$0 \to J(\mathbb{Q})/2J(\mathbb{Q}) \to S_2(J) \to Ш_J[2] \to 0,$$

where $Ш_J$ denotes the Tate-Shafarevich group of J over $\mathbb{Q}$.

Then our main theorem is

Theorem 1 (joint w/Dick Gross). *When all odd hyperelliptic curves of any fixed genus $n \geq 1$ over $\mathbb{Q}$ are ordered by height, the average size of the 2-Selmer groups of their Jacobians is equal to 3.*

We actually prove something stronger, namely:

Theorem 1' (joint w/Dick Gross). *When all odd hyperelliptic curves of any fixed genus $n \geq 1$ in any family defined by finitely many conguence conditions are ordered by height, the average size of the 2-Selmer groups of their Jacobians is equal to 3.*

The case of genus $n = 1$: elliptic curves

The case of genus $n = 1$: elliptic curves

The fact that the average size of the 2-Selmer group is 3 for elliptic curves was proven last year in joint work with Arul Shankar.

The case of genus $n = 1$: elliptic curves

The fact that the average size of the 2-Selmer group is 3 for elliptic curves was proven last year in joint work with Arul Shankar.

To get a hold of 2-Selmer groups of elliptic curves, we used a correspondence between 2-Selmer elements and integral binary quartic forms, which was first introduced and used in the original computations of Birch and Swinnerton-Dyer.

The case of genus $n = 1$: elliptic curves

The fact that the average size of the 2-Selmer group is 3 for elliptic curves was proven last year in joint work with Arul Shankar.

To get a hold of 2-Selmer groups of elliptic curves, we used a correspondence between 2-Selmer elements and integral binary quartic forms, which was first introduced and used in the original computations of Birch and Swinnerton-Dyer.

The 2-Selmer group of E can be thought of as the group of locally soluble 2-coverings of E.

The case of genus $n = 1$: elliptic curves

The fact that the average size of the 2-Selmer group is 3 for elliptic curves was proven last year in joint work with Arul Shankar.

To get a hold of 2-Selmer groups of elliptic curves, we used a correspondence between 2-Selmer elements and integral binary quartic forms, which was first introduced and used in the original computations of Birch and Swinnerton-Dyer.

The 2-Selmer group of E can be thought of as the group of locally soluble 2-coverings of E.

A 2-covering of E is a genus one curve C that fits into a commutative diagram

$$\begin{tikzcd} E \arrow[r, "{[2]}"] & E \\ C \arrow[u, "\cong/\mathbb{C}"] \arrow[ur, "/\mathbb{Q}"'] & \end{tikzcd}$$

The case of genus $n = 1$: elliptic curves

The fact that the average size of the 2-Selmer group is 3 for elliptic curves was proven last year in joint work with Arul Shankar.

To get a hold of 2-Selmer groups of elliptic curves, we used a correspondence between 2-Selmer elements and integral binary quartic forms, which was first introduced and used in the original computations of Birch and Swinnerton-Dyer.

The 2-Selmer group of E can be thought of as the group of locally soluble 2-coverings of E.

A 2-covering of E is a genus one curve C that fits into a commutative diagram

$$\begin{tikzcd} E \arrow[r, "{[2]}"] & E \\ C \arrow[u, "\cong/\mathbb{C}"] \arrow[ur, "/\mathbb{Q}"'] & \end{tikzcd}$$

The 2-covering C is called soluble if it has a rational point;

The case of genus $n = 1$: elliptic curves

The fact that the average size of the 2-Selmer group is 3 for elliptic curves was proven last year in joint work with Arul Shankar.

To get a hold of 2-Selmer groups of elliptic curves, we used a correspondence between 2-Selmer elements and integral binary quartic forms, which was first introduced and used in the original computations of Birch and Swinnerton-Dyer.

The 2-Selmer group of E can be thought of as the group of locally soluble 2-coverings of E.

A 2-covering of E is a genus one curve C that fits into a commutative diagram

$$\begin{tikzcd} E \arrow[r, "{[2]}"] & E \\ C \arrow[u, "\cong/\mathbb{C}"] \arrow[ur, "/\mathbb{Q}"'] & \end{tikzcd}$$

The 2-covering C is called soluble if it has a rational point; locally soluble if it has a $\mathbb{Q}_p$-point for all p and an $\mathbb{R}$-point.

How do binary quartics come in?

How do binary quartics come in?

$$\{\text{soluble 2-coverings}\} \cong E(\mathbb{Q})/2E(\mathbb{Q});$$

How do binary quartics come in?

$$\{\text{soluble 2-coverings}\} \cong E(\mathbb{Q})/2E(\mathbb{Q});$$

$$\{\text{locally soluble 2-coverings}\} \cong S^{(2)}(E).$$

$$\{\text{soluble 2-coverings}\} \cong E(\mathbb{Q})/2E(\mathbb{Q});$$

$$\{\text{locally soluble 2-coverings}\} \cong S^{(2)}(E).$$

Lemma. (Cassels) If C is a locally soluble 2-covering of E, then C has a positive rational divisor of degree 2 (i.e., it has a degree 2 map to $\mathbb{P}^1$).

How do binary quartics come in?

$$\{\text{soluble 2-coverings}\} \cong E(\mathbb{Q})/2E(\mathbb{Q});$$

$$\{\text{locally soluble 2-coverings}\} \cong S^{(2)}(E).$$

Lemma. (Cassels) If C is a locally soluble 2-covering of E, then C has a positive rational divisor of degree 2 (i.e., it has a degree 2 map to $\mathbb{P}^1$).

Proof: We have a natural map $C \times C \to E$, via $(x, y) \mapsto x + y$.

How do binary quartics come in?

$$\{\text{soluble 2-coverings}\} \cong E(\mathbb{Q})/2E(\mathbb{Q});$$

$$\{\text{locally soluble 2-coverings}\} \cong S^{(2)}(E).$$

Lemma. (Cassels) If C is a locally soluble 2-covering of E, then C has a positive rational divisor of degree 2 (i.e., it has a degree 2 map to $\mathbb{P}^1$).

Proof: We have a natural map $C \times C \to E$, via $(x, y) \mapsto x + y$. The inverse image of O is a set of linearly equivalent divisors, giving a map to a curve Z of genus 0 over $\mathbb{Q}$.

How do binary quartics come in?

$$\{\text{soluble 2-coverings}\} \cong E(\mathbb{Q})/2E(\mathbb{Q});$$

$$\{\text{locally soluble 2-coverings}\} \cong S^{(2)}(E).$$

Lemma. (Cassels) If C is a locally soluble 2-covering of E, then C has a positive rational divisor of degree 2 (i.e., it has a degree 2 map to $\mathbb{P}^1$).

Proof: We have a natural map $C \times C \to E$, via $(x, y) \mapsto x + y$. The inverse image of O is a set of linearly equivalent divisors, giving a map to a curve Z of genus 0 over $\mathbb{Q}$. If (x, y) is in this inverse image, then x and y are defined over the same field.

How do binary quartics come in?

$$\{\text{soluble 2-coverings}\} \cong E(\mathbb{Q})/2E(\mathbb{Q});$$

$$\{\text{locally soluble 2-coverings}\} \cong S^{(2)}(E).$$

Lemma. (Cassels) If C is a locally soluble 2-covering of E, then C has a positive rational divisor of degree 2 (i.e., it has a degree 2 map to $\mathbb{P}^1$).

Proof: We have a natural map $C \times C \to E$, via $(x, y) \mapsto x + y$. The inverse image of O is a set of linearly equivalent divisors, giving a map to a curve Z of genus 0 over $\mathbb{Q}$. If (x, y) is in this inverse image, then x and y are defined over the same field.

Now C has an $\mathbb{R}$-point and $\mathbb{Q}_p$-point for every p, implying that Z has an $\mathbb{R}$-point and $\mathbb{Q}_p$-point for every p.

How do binary quartics come in?

$$\{\text{soluble 2-coverings}\} \cong E(\mathbb{Q})/2E(\mathbb{Q});$$

$$\{\text{locally soluble 2-coverings}\} \cong S^{(2)}(E).$$

Lemma. (Cassels) If C is a locally soluble 2-covering of E, then C has a positive rational divisor of degree 2 (i.e., it has a degree 2 map to $\mathbb{P}^1$).

Proof: We have a natural map $C \times C \to E$, via $(x, y) \mapsto x + y$. The inverse image of O is a set of linearly equivalent divisors, giving a map to a curve Z of genus 0 over $\mathbb{Q}$. If (x, y) is in this inverse image, then x and y are defined over the same field.

Now C has an $\mathbb{R}$-point and $\mathbb{Q}_p$-point for every p, implying that Z has an $\mathbb{R}$-point and $\mathbb{Q}_p$-point for every p. So $Z \cong \mathbb{P}^1\ /\mathbb{Q} \Rightarrow C$ is a double cover of $\mathbb{P}^1/\mathbb{Q}$.

How do binary quartics come in?

$$\{\text{soluble 2-coverings}\} \cong E(\mathbb{Q})/2E(\mathbb{Q});$$

$$\{\text{locally soluble 2-coverings}\} \cong S^{(2)}(E).$$

Lemma. (Cassels) If C is a locally soluble 2-covering of E, then C has a positive rational divisor of degree 2 (i.e., it has a degree 2 map to $\mathbb{P}^1$).

Proof: We have a natural map $C \times C \to E$, via $(x, y) \mapsto x + y$. The inverse image of O is a set of linearly equivalent divisors, giving a map to a curve Z of genus 0 over $\mathbb{Q}$. If (x, y) is in this inverse image, then x and y are defined over the same field.

Now C has an $\mathbb{R}$-point and $\mathbb{Q}_p$-point for every p, implying that Z has an $\mathbb{R}$-point and $\mathbb{Q}_p$-point for every p. So $Z \cong \mathbb{P}^1\ /\mathbb{Q} \Rightarrow C$ is a double cover of $\mathbb{P}^1/\mathbb{Q}$. $\square$

Four points in $\mathbb{P}^1$

So if C is a locally soluble 2-covering of E, then it is a double cover of $\mathbb{P}^1$, ramified at 4 points.

Four points in $\mathbb{P}^1$

So if C is a locally soluble 2-covering of E, then it is a double cover of $\mathbb{P}^1$, ramified at 4 points. This gives a binary quartic form over $\mathbb{Q}$,

Four points in $\mathbb{P}^1$

So if C is a locally soluble 2-covering of E, then it is a double cover of $\mathbb{P}^1$, ramified at 4 points. This gives a binary quartic form over $\mathbb{Q}$, well-defined up to $\mathrm{GL}_2(\mathbb{Q})$-equivalence.

Four points in $\mathbb{P}^1$

So if C is a locally soluble 2-covering of E, then it is a double cover of $\mathbb{P}^1$, ramified at 4 points. This gives a binary quartic form over $\mathbb{Q}$, well-defined up to $\mathrm{GL}_2(\mathbb{Q})$-equivalence.

To prove the main theorem, about the average size of the 2-Selmer group of elliptic curves being 3:

Four points in $\mathbb{P}^1$

So if C is a locally soluble 2-covering of E, then it is a double cover of $\mathbb{P}^1$, ramified at 4 points. This gives a binary quartic form over $\mathbb{Q}$, well-defined up to $\mathrm{GL}_2(\mathbb{Q})$-equivalence.

To prove the main theorem, about the average size of the 2-Selmer group of elliptic curves being 3:

- Given an elliptic curve $E_{A,B} : y^2 = x^3 + Ax + B$ with indivisible coefficients, choose an integral binary quartic form f for each element of $S^{(2)}(E_{A,B})$, such that

Four points in $\mathbb{P}^1$

So if C is a locally soluble 2-covering of E, then it is a double cover of $\mathbb{P}^1$, ramified at 4 points. This gives a binary quartic form over $\mathbb{Q}$, well-defined up to $\mathrm{GL}_2(\mathbb{Q})$-equivalence.

To prove the main theorem, about the average size of the 2-Selmer group of elliptic curves being 3:

- Given an elliptic curve $E_{A,B} : y^2 = x^3 + Ax + B$ with indivisible coefficients, choose an integral binary quartic form f for each element of $S^{(2)}(E_{A,B})$, such that
  - $y^2 = f(x)$ gives the desired 2-covering over $\mathbb{Q}$;

Four points in $\mathbb{P}^1$

So if C is a locally soluble 2-covering of E, then it is a double cover of $\mathbb{P}^1$, ramified at 4 points. This gives a binary quartic form over $\mathbb{Q}$, well-defined up to $\mathrm{GL}_2(\mathbb{Q})$-equivalence.

To prove the main theorem, about the average size of the 2-Selmer group of elliptic curves being 3:

- Given an elliptic curve $E_{A,B} : y^2 = x^3 + Ax + B$ with indivisible coefficients, choose an integral binary quartic form f for each element of $S^{(2)}(E_{A,B})$, such that
    - $y^2 = f(x)$ gives the desired 2-covering over $\mathbb{Q}$;
    - the SL_2-invariants $(I(f), J(f))$ of the binary quartic form agree with the invariants (A, B) of the elliptic curve (at least away from 2 and 3);

Four points in $\mathbb{P}^1$

So if C is a locally soluble 2-covering of E, then it is a double cover of $\mathbb{P}^1$, ramified at 4 points. This gives a binary quartic form over $\mathbb{Q}$, well-defined up to $\mathrm{GL}_2(\mathbb{Q})$-equivalence.

To prove the main theorem, about the average size of the 2-Selmer group of elliptic curves being 3:

- Given an elliptic curve $E_{A,B} : y^2 = x^3 + Ax + B$ with indivisible coefficients, choose an integral binary quartic form f for each element of $S^{(2)}(E_{A,B})$, such that
  - $y^2 = f(x)$ gives the desired 2-covering over $\mathbb{Q}$;
  - the SL_2-invariants $(I(f), J(f))$ of the binary quartic form agree with the invariants (A, B) of the elliptic curve (at least away from 2 and 3);
- Count these $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of integral binary quartic forms having bounded height via geometry-of-numbers arguments.

Four points in $\mathbb{P}^1$

So if C is a locally soluble 2-covering of E, then it is a double cover of $\mathbb{P}^1$, ramified at 4 points. This gives a binary quartic form over $\mathbb{Q}$, well-defined up to $\mathrm{GL}_2(\mathbb{Q})$-equivalence.

To prove the main theorem, about the average size of the 2-Selmer group of elliptic curves being 3:

- Given an elliptic curve $E_{A,B} : y^2 = x^3 + Ax + B$ with indivisible coefficients, choose an integral binary quartic form f for each element of $S^{(2)}(E_{A,B})$, such that
  - $y^2 = f(x)$ gives the desired 2-covering over $\mathbb{Q}$;
  - the SL_2-invariants $(I(f), J(f))$ of the binary quartic form agree with the invariants (A, B) of the elliptic curve (at least away from 2 and 3);
- Count these $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of integral binary quartic forms having bounded height via geometry-of-numbers arguments. The binary quartic forms corresponding to 2-Selmer elements are defined by infinitely many congruence conditions, so a sieve has to be performed.

How to generalize to higher genus?

How to generalize to higher genus?

The key algebraic ingredient in the proof was the parametrization of 2-Selmer elements of elliptic curves by binary quartic forms.

How to generalize to higher genus?

The key algebraic ingredient in the proof was the parametrization of 2-Selmer elements of elliptic curves by binary quartic forms.

The analogues of binary quartic forms for higher descent on elliptic curves have been studied by Cassels, Cremona–Fisher–Stoll, and Fisher.

How to generalize to higher genus?

The key algebraic ingredient in the proof was the parametrization of 2-Selmer elements of elliptic curves by binary quartic forms.

The analogues of binary quartic forms for higher descent on elliptic curves have been studied by Cassels, Cremona–Fisher–Stoll, and Fisher. For further generalizations, see also Wei Ho's talk later this week.

How to generalize to higher genus?

The key algebraic ingredient in the proof was the parametrization of 2-Selmer elements of elliptic curves by binary quartic forms.

The analogues of binary quartic forms for higher descent on elliptic curves have been studied by Cassels, Cremona–Fisher–Stoll, and Fisher. For further generalizations, see also Wei Ho's talk later this week.

What is the analogue of binary quartic forms for odd hyperelliptic curves of higher genus?

How to generalize to higher genus?

The key algebraic ingredient in the proof was the parametrization of 2-Selmer elements of elliptic curves by binary quartic forms.

The analogues of binary quartic forms for higher descent on elliptic curves have been studied by Cassels, Cremona–Fisher–Stoll, and Fisher. For further generalizations, see also Wei Ho's talk later this week.

What is the analogue of binary quartic forms for odd hyperelliptic curves of higher genus?

First try: binary $(2n+2)$-ic forms!

How to generalize to higher genus?

The key algebraic ingredient in the proof was the parametrization of 2-Selmer elements of elliptic curves by binary quartic forms.

The analogues of binary quartic forms for higher descent on elliptic curves have been studied by Cassels, Cremona–Fisher–Stoll, and Fisher. For further generalizations, see also Wei Ho's talk later this week.

What is the analogue of binary quartic forms for odd hyperelliptic curves of higher genus?

First try: binary $(2n+2)$-ic forms! This doesn't work.

How to generalize to higher genus?

The key algebraic ingredient in the proof was the parametrization of 2-Selmer elements of elliptic curves by binary quartic forms.

The analogues of binary quartic forms for higher descent on elliptic curves have been studied by Cassels, Cremona–Fisher–Stoll, and Fisher. For further generalizations, see also Wei Ho's talk later this week.

What is the analogue of binary quartic forms for odd hyperelliptic curves of higher genus?

First try: binary $(2n+2)$-ic forms! This doesn't work. (Such forms basically give even hyperelliptic curves, not (2-Selmer) homogeneous spaces for the Jacobians of odd hyperelliptic curves.)

How to generalize to higher genus? (cont'd)

How to generalize to higher genus? (cont'd)

Note that SL_2 (or rather PSL_2) may be thought of as SO_3;

How to generalize to higher genus? (cont'd)

Note that SL_2 (or rather PSL_2) may be thought of as SO_3; this is because when SL_2 acts on binary quadratic forms $ax^2 + bxy + cy^2$, it fixes the discriminant $A_0 = b^2 - 4ac$ (a ternary quadratic form!).

How to generalize to higher genus? (cont'd)

Note that SL_2 (or rather PSL_2) may be thought of as SO_3; this is because when SL_2 acts on binary quadratic forms $ax^2 + bxy + cy^2$, it fixes the discriminant $A_0 = b^2 - 4ac$ (a ternary quadratic form!).

Consider the action of SO_3 on the space of all ternary quadratic forms (i.e., on the symmetric square of its standard representation).

How to generalize to higher genus? (cont'd)

Note that SL_2 (or rather PSL_2) may be thought of as SO_3; this is because when SL_2 acts on binary quadratic forms $ax^2 + bxy + cy^2$, it fixes the discriminant $A_0 = b^2 - 4ac$ (a ternary quadratic form!).

Consider the action of SO_3 on the space of all ternary quadratic forms (i.e., on the symmetric square of its standard representation). This representation is six-dimensional.

How to generalize to higher genus? (cont'd)

Note that SL_2 (or rather PSL_2) may be thought of as SO_3; this is because when SL_2 acts on binary quadratic forms $ax^2 + bxy + cy^2$, it fixes the discriminant $A_0 = b^2 - 4ac$ (a ternary quadratic form!).

Consider the action of SO_3 on the space of all ternary quadratic forms (i.e., on the symmetric square of its standard representation). This representation is six-dimensional. However, it is not irreducible, since the quadratic form A_0 is fixed!

How to generalize to higher genus? (cont'd)

Note that SL_2 (or rather PSL_2) may be thought of as SO_3; this is because when SL_2 acts on binary quadratic forms $ax^2 + bxy + cy^2$, it fixes the discriminant $A_0 = b^2 - 4ac$ (a ternary quadratic form!).

Consider the action of SO_3 on the space of all ternary quadratic forms (i.e., on the symmetric square of its standard representation). This representation is six-dimensional. However, it is not irreducible, since the quadratic form A_0 is fixed!

The complementary 5-dimensional representation is irreducible,

How to generalize to higher genus? (cont'd)

Note that SL_2 (or rather PSL_2) may be thought of as SO_3; this is because when SL_2 acts on binary quadratic forms $ax^2 + bxy + cy^2$, it fixes the discriminant $A_0 = b^2 - 4ac$ (a ternary quadratic form!).

Consider the action of SO_3 on the space of all ternary quadratic forms (i.e., on the symmetric square of its standard representation). This representation is six-dimensional. However, it is not irreducible, since the quadratic form A_0 is fixed!

The complementary 5-dimensional representation is irreducible, and indeed this is the representation on binary quartic forms (when viewing the group as SL_2 rather than SO_3).

How to generalize to higher genus? (cont'd)

How to generalize to higher genus? (cont'd)

In general, let us consider the split quadratic form

How to generalize to higher genus? (cont'd)

In general, let us consider the split quadratic form

$$A = \begin{bmatrix} & & & & 1 \\ & & & 1 & \\ & & \iddots & & \\ & 1 & & & \\ 1 & & & & \end{bmatrix}.$$

in $2n+1$ variables.

How to generalize to higher genus? (cont'd)

In general, let us consider the split quadratic form

$$A = \begin{bmatrix} & & & & 1 \\ & & & 1 & \\ & & \iddots & & \\ & 1 & & & \\ 1 & & & & \end{bmatrix}.$$

in $2n+1$ variables.

Let SO_{2n+1} denote the orthogonal group of this quadratic form, and consider its action on the symmetric square of its standard representation W.

How to generalize to higher genus? (cont'd)

In general, let us consider the split quadratic form

$$A = \begin{bmatrix} & & & & 1 \\ & & & 1 & \\ & & \iddots & & \\ & 1 & & & \\ 1 & & & & \end{bmatrix}.$$

in $2n+1$ variables.

Let SO_{2n+1} denote the orthogonal group of this quadratic form, and consider its action on the symmetric square of its standard representation W. The quadratic form A is again fixed, and the complementary representation V (of dimension $n(2n+3)$) is irreducible.

In general, let us consider the split quadratic form

$$A = \begin{bmatrix} & & & & 1 \\ & & & 1 & \\ & & \iddots & & \\ & 1 & & & \\ 1 & & & & \end{bmatrix}.$$

in $2n+1$ variables.

Let SO_{2n+1} denote the orthogonal group of this quadratic form, and consider its action on the symmetric square of its standard representation W. The quadratic form A is again fixed, and the complementary representation V (of dimension $n(2n+3)$) is irreducible.

The elements B of V (quadratic forms in $2n+1$ variables, modulo translation by A) yield the desired generalization of binary quartic forms.

Invariant theory and Fano varieties of pencils of quadrics

Invariant theory and Fano varieties of pencils of quadrics

The action of SO_{2n+1} on V has $2n$ independent invariants, given by the coefficients of the polynomial $f(x)$ given by

$$f(x) = (-1)^n \det(xA - B) = x^{2n+1} + c_2 x^{2n-1} + \cdots + c_{2n+1}.$$

Invariant theory and Fano varieties of pencils of quadrics

The action of SO_{2n+1} on V has $2n$ independent invariants, given by the coefficients of the polynomial $f(x)$ given by

$$f(x) = (-1)^n \det(xA - B) = x^{2n+1} + c_2 x^{2n-1} + \cdots + c_{2n+1}.$$

(We say B is nondegenerate if $\mathrm{Disc}(f) \neq 0$, which we always assume.)

The action of SO_{2n+1} on V has $2n$ independent invariants, given by the coefficients of the polynomial $f(x)$ given by

$$f(x) = (-1)^n \det(xA - B) = x^{2n+1} + c_2 x^{2n-1} + \cdots + c_{2n+1}.$$

(We say B is nondegenerate if $\mathrm{Disc}(f) \neq 0$, which we always assume.)

Meanwhile, on the geometric side, we may associate to the element B in $V(\mathbb{Q})$ a pencil of quadrics in projective space $\mathbb{P}(W \oplus \mathbb{Q}) = \mathbb{P}^{2n+1}$:

Invariant theory and Fano varieties of pencils of quadrics

The action of SO_{2n+1} on V has $2n$ independent invariants, given by the coefficients of the polynomial $f(x)$ given by

$$f(x) = (-1)^n \det(xA - B) = x^{2n+1} + c_2 x^{2n-1} + \cdots + c_{2n+1}.$$

(We say B is nondegenerate if $\mathrm{Disc}(f) \neq 0$, which we always assume.)

Meanwhile, on the geometric side, we may associate to the element B in $V(\mathbb{Q})$ a pencil of quadrics in projective space $\mathbb{P}(W \oplus \mathbb{Q}) = \mathbb{P}^{2n+1}$: two quadrics generating this pencil are

$$A' = A \oplus 0 \quad \text{and} \quad B' = B \oplus z^2.$$

Invariant theory and Fano varieties of pencils of quadrics

The action of SO_{2n+1} on V has $2n$ independent invariants, given by the coefficients of the polynomial $f(x)$ given by

$$f(x) = (-1)^n \det(xA - B) = x^{2n+1} + c_2 x^{2n-1} + \cdots + c_{2n+1}.$$

(We say B is nondegenerate if $\mathrm{Disc}(f) \neq 0$, which we always assume.)

Meanwhile, on the geometric side, we may associate to the element B in $V(\mathbb{Q})$ a pencil of quadrics in projective space $\mathbb{P}(W \oplus \mathbb{Q}) = \mathbb{P}^{2n+1}$: two quadrics generating this pencil are

$$A' = A \oplus 0 \text{ and } B' = B \oplus z^2.$$

The discriminant locus $\mathrm{Disc}(xA' - yB')$ of this pencil is a homogeneous polynomial $g(x, y)$ of degree $2n+2$ satisfying $g(1, 0) = 0$ and $g(x, 1) = f(x)$.

The action of SO_{2n+1} on V has $2n$ independent invariants, given by the coefficients of the polynomial $f(x)$ given by

$$f(x) = (-1)^n \det(xA - B) = x^{2n+1} + c_2 x^{2n-1} + \cdots + c_{2n+1}.$$

(We say B is nondegenerate if $\mathrm{Disc}(f) \neq 0$, which we always assume.)

Meanwhile, on the geometric side, we may associate to the element B in $V(\mathbb{Q})$ a pencil of quadrics in projective space $\mathbb{P}(W \oplus \mathbb{Q}) = \mathbb{P}^{2n+1}$: two quadrics generating this pencil are

$$A' = A \oplus 0 \quad \text{and} \quad B' = B \oplus z^2.$$

The discriminant locus $\mathrm{Disc}(xA' - yB')$ of this pencil is a homogeneous polynomial $g(x, y)$ of degree $2n+2$ satisfying $g(1, 0) = 0$ and $g(x, 1) = f(x)$.

The Fano variety F_B of maximal linear isotropic subspaces of the base locus is smooth of dimension n over $\mathbb{Q}$, and forms [a principal homogeneous space for] the Jacobian J of the curve $C : y^2 = f(x)$ (Donagi, others).

Fano varieties associated to elements of V

Which homogeneous spaces arise over a non–algebraically closed field like $\mathbb{Q}$?

Fano varieties associated to elements of V

Which homogeneous spaces arise over a non–algebraically closed field like $\mathbb{Q}$? They are all of order 2.

Fano varieties associated to elements of V

Which homogeneous spaces arise over a non–algebraically closed field like $\mathbb{Q}$? They are all of order 2.

In fact, we prove that there is an injective map from the set of orbits of $\mathrm{SO}_{2n+1}(\mathbb{Q})$ on $V(\mathbb{Q})$ having characteristic polynomial $f(x)$ to the set of elements in the Galois cohomology group $H^1(\mathbb{Q}, J[2])$.

Fano varieties associated to elements of V

Which homogeneous spaces arise over a non–algebraically closed field like $\mathbb{Q}$? They are all of order 2.

In fact, we prove that there is an injective map from the set of orbits of $\mathrm{SO}_{2n+1}(\mathbb{Q})$ on $V(\mathbb{Q})$ having characteristic polynomial $f(x)$ to the set of elements in the Galois cohomology group $H^1(\mathbb{Q}, J[2])$. So this is a good place to look for 2-Selmer elements of J!

Fano varieties associated to elements of V

Which homogeneous spaces arise over a non–algebraically closed field like $\mathbb{Q}$? They are all of order 2.

In fact, we prove that there is an injective map from the set of orbits of $\mathrm{SO}_{2n+1}(\mathbb{Q})$ on $V(\mathbb{Q})$ having characteristic polynomial $f(x)$ to the set of elements in the Galois cohomology group $H^1(\mathbb{Q}, J[2])$. So this is a good place to look for 2-Selmer elements of J!

Let us say that B is locally soluble if the associated Fano variety F_B has points over $\mathbb{Q}_v$ for all places v.

Fano varieties associated to elements of V

Which homogeneous spaces arise over a non–algebraically closed field like $\mathbb{Q}$? They are all of order 2.

In fact, we prove that there is an injective map from the set of orbits of $\mathrm{SO}_{2n+1}(\mathbb{Q})$ on $V(\mathbb{Q})$ having characteristic polynomial $f(x)$ to the set of elements in the Galois cohomology group $H^1(\mathbb{Q}, J[2])$. So this is a good place to look for 2-Selmer elements of J!

Let us say that B is locally soluble if the associated Fano variety F_B has points over $\mathbb{Q}_v$ for all places v. Then we prove:

Fano varieties associated to elements of V

Which homogeneous spaces arise over a non–algebraically closed field like $\mathbb{Q}$? They are all of order 2.

In fact, we prove that there is an injective map from the set of orbits of $\mathrm{SO}_{2n+1}(\mathbb{Q})$ on $V(\mathbb{Q})$ having characteristic polynomial $f(x)$ to the set of elements in the Galois cohomology group $H^1(\mathbb{Q}, J[2])$. So this is a good place to look for 2-Selmer elements of J!

Let us say that B is locally soluble if the associated Fano variety F_B has points over $\mathbb{Q}_v$ for all places v. Then we prove:

Theorem. *Let $C : y^2 = f(x)$ be an odd hyperelliptic curve of genus n. Then the classes in the 2-Selmer group of the Jacobian J of C over $\mathbb{Q}$ correspond bijectively to the $\mathrm{SO}_{2n+1}(\mathbb{Q})$-orbits of locally soluble elements in $V(\mathbb{Q})$ having characteristic polynomial $f(x)$.*

Which homogeneous spaces arise over a non–algebraically closed field like $\mathbb{Q}$? They are all of order 2.

In fact, we prove that there is an injective map from the set of orbits of $\mathrm{SO}_{2n+1}(\mathbb{Q})$ on $V(\mathbb{Q})$ having characteristic polynomial $f(x)$ to the set of elements in the Galois cohomology group $H^1(\mathbb{Q}, J[2])$. So this is a good place to look for 2-Selmer elements of J!

Let us say that B is locally soluble if the associated Fano variety F_B has points over $\mathbb{Q}_v$ for all places v. Then we prove:

Theorem. *Let $C : y^2 = f(x)$ be an odd hyperelliptic curve of genus n. Then the classes in the 2-Selmer group of the Jacobian J of C over $\mathbb{Q}$ correspond bijectively to the $\mathrm{SO}_{2n+1}(\mathbb{Q})$-orbits of locally soluble elements in $V(\mathbb{Q})$ having characteristic polynomial $f(x)$.*

When $n = 1$, this recovers the classical correspondence of Birch and Swinnerton-Dyer between 2-Selmer elements of elliptic curves and locally soluble binary quartic forms over $\mathbb{Q}$.

How to construct an orbit in $V(\mathbb{Q})$ from a 2-Selmer element

How to construct an orbit in $V(\mathbb{Q})$ from a 2-Selmer element

Given an odd hyperelliptic curve $C : y^2 = f(x)$ of genus n over $\mathbb{Q}$ with Jacobian J, define the $\mathbb{Q}$-algebra $L := \mathbb{Q}[x]/(f(x))$, and let β denote the image of x in L.

How to construct an orbit in $V(\mathbb{Q})$ from a 2-Selmer element

Given an odd hyperelliptic curve $C : y^2 = f(x)$ of genus n over $\mathbb{Q}$ with Jacobian J, define the $\mathbb{Q}$-algebra $L := \mathbb{Q}[x]/(f(x))$, and let β denote the image of x in L.

We use $(L^*/L^{*2})_{N\equiv 1}$ to denote the kernel of the norm map from L^*/L^{*2} to $\mathbb{Q}^*/\mathbb{Q}^{*2}$.

How to construct an orbit in $V(\mathbb{Q})$ from a 2-Selmer element

Given an odd hyperelliptic curve $C : y^2 = f(x)$ of genus n over $\mathbb{Q}$ with Jacobian J, define the $\mathbb{Q}$-algebra $L := \mathbb{Q}[x]/(f(x))$, and let β denote the image of x in L.

We use $(L^*/L^{*2})_{N\equiv 1}$ to denote the kernel of the norm map from L^*/L^{*2} to $\mathbb{Q}^*/\mathbb{Q}^{*2}$.

Theorem (Schaefer). *There is a natural isomorphism*

$$H^1(\mathbb{Q}, J[2]) \cong (L^*/L^{*2})_{N\equiv 1}.$$

How to construct an orbit in $V(\mathbb{Q})$ from a 2-Selmer element (cont'd)

Given an element of $\alpha \in (L^*/L^{*2})_{N\equiv 1} \cong H^1(\mathbb{Q}, J[2])$,

How to construct an orbit in $V(\mathbb{Q})$ from a 2-Selmer element (cont'd)

Given an element of $\alpha \in (L^*/L^{*2})_{N\equiv 1} \cong H^1(\mathbb{Q}, J[2])$, we can construct a pencil of quadrics on $\mathbb{P}(L) \cong \mathbb{P}^{2n}$ generated by

$$A_\alpha = \mathrm{Tr}(\alpha\lambda^2/f'(\beta)) \text{ and } B_\alpha = \mathrm{Tr}(\alpha\beta\lambda^2/f'(\beta))$$

How to construct an orbit in $V(\mathbb{Q})$ from a 2-Selmer element (cont'd)

Given an element of $\alpha \in (L^*/L^{*2})_{N\equiv 1} \cong H^1(\mathbb{Q}, J[2])$, we can construct a pencil of quadrics on $\mathbb{P}(L) \cong \mathbb{P}^{2n}$ generated by

$$A_\alpha = \mathrm{Tr}(\alpha\lambda^2/f'(\beta)) \text{ and } B_\alpha = \mathrm{Tr}(\alpha\beta\lambda^2/f'(\beta))$$

leading to a pencil of quadrics on $\mathbb{P}(L \oplus \mathbb{Q}) \cong \mathbb{P}^{2n+1}$ generated by

$$A'_\alpha = \mathrm{Tr}(\alpha\lambda^2/f'(\beta)) \oplus 0 \text{ and } B'_\alpha = \mathrm{Tr}(\alpha\beta\lambda^2/f'(\beta)) \oplus z^2.$$

How to construct an orbit in $V(\mathbb{Q})$ from a 2-Selmer element (cont'd)

Given an element of $\alpha \in (L^*/L^{*2})_{N\equiv 1} \cong H^1(\mathbb{Q}, J[2])$, we can construct a pencil of quadrics on $\mathbb{P}(L) \cong \mathbb{P}^{2n}$ generated by

$$A_\alpha = \mathrm{Tr}(\alpha\lambda^2/f'(\beta)) \text{ and } B_\alpha = \mathrm{Tr}(\alpha\beta\lambda^2/f'(\beta))$$

leading to a pencil of quadrics on $\mathbb{P}(L \oplus \mathbb{Q}) \cong \mathbb{P}^{2n+1}$ generated by

$$A'_\alpha = \mathrm{Tr}(\alpha\lambda^2/f'(\beta)) \oplus 0 \text{ and } B'_\alpha = \mathrm{Tr}(\alpha\beta\lambda^2/f'(\beta)) \oplus z^2.$$

Then $g(x, y) = \det(xA'_\alpha - yB'_\alpha)$ has the property that $g(1, 0) = 0$ and $g(x, 1) = f(x)$.

How to construct an orbit in $V(\mathbb{Q})$ from a 2-Selmer element (cont'd)

Given an element of $\alpha \in (L^*/L^{*2})_{N\equiv 1} \cong H^1(\mathbb{Q}, J[2])$, we can construct a pencil of quadrics on $\mathbb{P}(L) \cong \mathbb{P}^{2n}$ generated by

$$A_\alpha = \mathrm{Tr}(\alpha\lambda^2/f'(\beta)) \text{ and } B_\alpha = \mathrm{Tr}(\alpha\beta\lambda^2/f'(\beta))$$

leading to a pencil of quadrics on $\mathbb{P}(L \oplus \mathbb{Q}) \cong \mathbb{P}^{2n+1}$ generated by

$$A'_\alpha = \mathrm{Tr}(\alpha\lambda^2/f'(\beta)) \oplus 0 \text{ and } B'_\alpha = \mathrm{Tr}(\alpha\beta\lambda^2/f'(\beta)) \oplus z^2.$$

Then $g(x, y) = \det(xA'_\alpha - yB'_\alpha)$ has the property that $g(1, 0) = 0$ and $g(x, 1) = f(x)$.

Let F_α be the variety of n-dimensional subspaces of $L \oplus \mathbb{Q}$ which are isotropic for all elements in the pencil $xA'_\alpha - yB'_\alpha$.

How to construct an orbit in $V(\mathbb{Q})$ from a 2-Selmer element (cont'd)

Given an element of $\alpha \in (L^*/L^{*2})_{N\equiv 1} \cong H^1(\mathbb{Q}, J[2])$, we can construct a pencil of quadrics on $\mathbb{P}(L) \cong \mathbb{P}^{2n}$ generated by

$$A_\alpha = \mathrm{Tr}(\alpha\lambda^2/f'(\beta)) \text{ and } B_\alpha = \mathrm{Tr}(\alpha\beta\lambda^2/f'(\beta))$$

leading to a pencil of quadrics on $\mathbb{P}(L \oplus \mathbb{Q}) \cong \mathbb{P}^{2n+1}$ generated by

$$A'_\alpha = \mathrm{Tr}(\alpha\lambda^2/f'(\beta)) \oplus 0 \text{ and } B'_\alpha = \mathrm{Tr}(\alpha\beta\lambda^2/f'(\beta)) \oplus z^2.$$

Then $g(x, y) = \det(xA'_\alpha - yB'_\alpha)$ has the property that $g(1, 0) = 0$ and $g(x, 1) = f(x)$.

Let F_α be the variety of n-dimensional subspaces of $L \oplus \mathbb{Q}$ which are isotropic for all elements in the pencil $xA'_\alpha - yB'_\alpha$. The variety F_α has an involution τ induced from the involution $\tau(\lambda, z) = (\lambda, -z)$ of $L \oplus \mathbb{Q}$.

How to construct an orbit in $V(\mathbb{Q})$ from a 2-Selmer element (cont'd)

Given an element of $\alpha \in (L^*/L^{*2})_{N\equiv 1} \cong H^1(\mathbb{Q}, J[2])$, we can construct a pencil of quadrics on $\mathbb{P}(L) \cong \mathbb{P}^{2n}$ generated by

$$A_\alpha = \mathrm{Tr}(\alpha\lambda^2/f'(\beta)) \text{ and } B_\alpha = \mathrm{Tr}(\alpha\beta\lambda^2/f'(\beta))$$

leading to a pencil of quadrics on $\mathbb{P}(L \oplus \mathbb{Q}) \cong \mathbb{P}^{2n+1}$ generated by

$$A'_\alpha = \mathrm{Tr}(\alpha\lambda^2/f'(\beta)) \oplus 0 \text{ and } B'_\alpha = \mathrm{Tr}(\alpha\beta\lambda^2/f'(\beta)) \oplus z^2.$$

Then $g(x,y) = \det(xA'_\alpha - yB'_\alpha)$ has the property that $g(1,0) = 0$ and $g(x,1) = f(x)$.

Let F_α be the variety of n-dimensional subspaces of $L \oplus \mathbb{Q}$ which are isotropic for all elements in the pencil $xA'_\alpha - yB'_\alpha$. The variety F_α has an involution τ induced from the involution $\tau(\lambda, z) = (\lambda, -z)$ of $L \oplus \mathbb{Q}$. The variety F_α is a principal homogeneous space for J, and the finite set of points F fixed by the involution forms a principal homogeneous space for $J[2]$.

How to construct an orbit in $V(\mathbb{Q})$ from a 2-Selmer element (cont'd)

If F_α is a trivial principal homogeneous space over $\mathbb{Q}_p$,

How to construct an orbit in $V(\mathbb{Q})$ from a 2-Selmer element (cont'd)

If F_α is a trivial principal homogeneous space over $\mathbb{Q}_p$, so it has a $\mathbb{Q}_p$-rational point,

How to construct an orbit in $V(\mathbb{Q})$ from a 2-Selmer element (cont'd)

If F_α is a trivial principal homogeneous space over $\mathbb{Q}_p$, so it has a $\mathbb{Q}_p$-rational point, then this $\mathbb{Q}_p$-point corresponds to an n-dimensional subspace Y in $(L \oplus \mathbb{Q}) \otimes \mathbb{Q}_p$ which is isotropic for both A'_α and B'_α when viewed as quadrics over $\mathbb{Q}_p$.

How to construct an orbit in $V(\mathbb{Q})$ from a 2-Selmer element (cont'd)

If F_α is a trivial principal homogeneous space over $\mathbb{Q}_p$, so it has a $\mathbb{Q}_p$-rational point, then this $\mathbb{Q}_p$-point corresponds to an n-dimensional subspace Y in $(L \oplus \mathbb{Q}) \otimes \mathbb{Q}_p$ which is isotropic for both A'_α and B'_α when viewed as quadrics over $\mathbb{Q}_p$. The projection X of Y is isotropic for A_α and has dimension n over $\mathbb{Q}_p$.

How to construct an orbit in $V(\mathbb{Q})$ from a 2-Selmer element (cont'd)

If F_α is a trivial principal homogeneous space over $\mathbb{Q}_p$, so it has a $\mathbb{Q}_p$-rational point, then this $\mathbb{Q}_p$-point corresponds to an n-dimensional subspace Y in $(L \oplus \mathbb{Q}) \otimes \mathbb{Q}_p$ which is isotropic for both A'_α and B'_α when viewed as quadrics over $\mathbb{Q}_p$. The projection X of Y is isotropic for A_α and has dimension n over $\mathbb{Q}_p$.

Hence A_α defines a split quadratic space over $\mathbb{Q}_p$. If this is true for all p,

How to construct an orbit in $V(\mathbb{Q})$ from a 2-Selmer element (cont'd)

If F_α is a trivial principal homogeneous space over $\mathbb{Q}_p$, so it has a $\mathbb{Q}_p$-rational point, then this $\mathbb{Q}_p$-point corresponds to an n-dimensional subspace Y in $(L \oplus \mathbb{Q}) \otimes \mathbb{Q}_p$ which is isotropic for both A'_α and B'_α when viewed as quadrics over $\mathbb{Q}_p$. The projection X of Y is isotropic for A_α and has dimension n over $\mathbb{Q}_p$.

Hence A_α defines a split quadratic space over $\mathbb{Q}_p$. If this is true for all p, then A_α defines a split quadratic space over $\mathbb{Q}$.

How to construct an orbit in $V(\mathbb{Q})$ from a 2-Selmer element (cont'd)

If F_α is a trivial principal homogeneous space over $\mathbb{Q}_p$, so it has a $\mathbb{Q}_p$-rational point, then this $\mathbb{Q}_p$-point corresponds to an n-dimensional subspace Y in $(L \oplus \mathbb{Q}) \otimes \mathbb{Q}_p$ which is isotropic for both A'_α and B'_α when viewed as quadrics over $\mathbb{Q}_p$. The projection X of Y is isotropic for A_α and has dimension n over $\mathbb{Q}_p$.

Hence A_α defines a split quadratic space over $\mathbb{Q}_p$. If this is true for all p, then A_α defines a split quadratic space over $\mathbb{Q}$.

Therefore, by a simultaneous rational change of basis on A_α and B_α, we can make A_α equal to A and then the resulting B_α yields the desired element of $V(\mathbb{Q})$ whose orbit corresponds to the 2-Selmer class α.

How to construct an orbit in $V(\mathbb{Q})$ from a 2-Selmer element (cont'd)

If F_α is a trivial principal homogeneous space over $\mathbb{Q}_p$, so it has a $\mathbb{Q}_p$-rational point, then this $\mathbb{Q}_p$-point corresponds to an n-dimensional subspace Y in $(L \oplus \mathbb{Q}) \otimes \mathbb{Q}_p$ which is isotropic for both A'_α and B'_α when viewed as quadrics over $\mathbb{Q}_p$. The projection X of Y is isotropic for A_α and has dimension n over $\mathbb{Q}_p$.

Hence A_α defines a split quadratic space over $\mathbb{Q}_p$. If this is true for all p, then A_α defines a split quadratic space over $\mathbb{Q}$.

Therefore, by a simultaneous rational change of basis on A_α and B_α, we can make A_α equal to A and then the resulting B_α yields the desired element of $V(\mathbb{Q})$ whose orbit corresponds to the 2-Selmer class α.

This gives an explicit correspondence between 2-Selmer classes of the Jacobian J of $C : y^2 = f(x)$ and locally soluble $\mathrm{SO}_{2n+1}(\mathbb{Q})$-orbits on $V(\mathbb{Q})$ having characteristic polynomial $f(x)$.

Integral theory

We have seen that if $f(x) \in \mathbb{Z}[x]$ is a polynomial of degree $2n+1$ with nonzero discriminant, then the 2-Selmer elements of the Jacobian J of $C : y^2 = f(x)$ can be represented as locally soluble $\mathrm{SO}_{2n+1}(\mathbb{Q})$-orbits on $V(\mathbb{Q})$ having characteristic polynomial $f(x)$.

Integral theory

We have seen that if $f(x) \in \mathbb{Z}[x]$ is a polynomial of degree $2n+1$ with nonzero discriminant, then the 2-Selmer elements of the Jacobian J of $C : y^2 = f(x)$ can be represented as locally soluble $\mathrm{SO}_{2n+1}(\mathbb{Q})$-orbits on $V(\mathbb{Q})$ having characteristic polynomial $f(x)$.

In each such orbit corresponding to a 2-Selmer element, can we always find an integral point, i.e., a locally soluble $\mathrm{SO}_{2n+1}(\mathbb{Z})$-orbit on $V(\mathbb{Z})$ with characteristic polynomial $f(x)$?

Integral theory

We have seen that if $f(x) \in \mathbb{Z}[x]$ is a polynomial of degree $2n+1$ with nonzero discriminant, then the 2-Selmer elements of the Jacobian J of $C : y^2 = f(x)$ can be represented as locally soluble $\mathrm{SO}_{2n+1}(\mathbb{Q})$-orbits on $V(\mathbb{Q})$ having characteristic polynomial $f(x)$.

In each such orbit corresponding to a 2-Selmer element, can we always find an integral point, i.e., a locally soluble $\mathrm{SO}_{2n+1}(\mathbb{Z})$-orbit on $V(\mathbb{Z})$ with characteristic polynomial $f(x)$?

Yes! (except possibly at the prime 2)

Integral theory

We have seen that if $f(x) \in \mathbb{Z}[x]$ is a polynomial of degree $2n+1$ with nonzero discriminant, then the 2-Selmer elements of the Jacobian J of $C : y^2 = f(x)$ can be represented as locally soluble $\mathrm{SO}_{2n+1}(\mathbb{Q})$-orbits on $V(\mathbb{Q})$ having characteristic polynomial $f(x)$.

In each such orbit corresponding to a 2-Selmer element, can we always find an integral point, i.e., a locally soluble $\mathrm{SO}_{2n+1}(\mathbb{Z})$-orbit on $V(\mathbb{Z})$ with characteristic polynomial $f(x)$?

Yes! (except possibly at the prime 2)

Proof involves classifying integral orbits in terms of suitable ideal classes in the order $\mathbb{Z}[x]/(f(x))$, and then playing with Newton polygons to produce such integral orbits locally from local points.

Counting integral orbits of bounded height

Once we know the existence of integral orbits, we can count how many there are up to bounded height using geometry-of-numbers arguments.

Counting integral orbits of bounded height

Once we know the existence of integral orbits, we can count how many there are up to bounded height using geometry-of-numbers arguments.

Namely, we construct suitable fundamental domains for the action of $\mathrm{SO}_{2n+1}(\mathbb{Z})$ on $V(\mathbb{R})$, and enumerate the number lattice points in these regions having bounded invariants.

Counting integral orbits of bounded height

Once we know the existence of integral orbits, we can count how many there are up to bounded height using geometry-of-numbers arguments.

Namely, we construct suitable fundamental domains for the action of $\mathrm{SO}_{2n+1}(\mathbb{Z})$ on $V(\mathbb{R})$, and enumerate the number lattice points in these regions having bounded invariants.

The primary obstacle in this counting, as in representations encountered previously, is that the fundamental region in which one has to count points is not compact but instead has a rather complex system of cusps going off to infinity.

Counting integral orbits of bounded height

Once we know the existence of integral orbits, we can count how many there are up to bounded height using geometry-of-numbers arguments.

Namely, we construct suitable fundamental domains for the action of $\mathrm{SO}_{2n+1}(\mathbb{Z})$ on $V(\mathbb{R})$, and enumerate the number lattice points in these regions having bounded invariants.

The primary obstacle in this counting, as in representations encountered previously, is that the fundamental region in which one has to count points is not compact but instead has a rather complex system of cusps going off to infinity. A priori, it could be difficult to obtain exact counts of points of bounded height in the cusps of these fundamental regions.

Counting integral orbits of bounded height

Once we know the existence of integral orbits, we can count how many there are up to bounded height using geometry-of-numbers arguments.

Namely, we construct suitable fundamental domains for the action of $\mathrm{SO}_{2n+1}(\mathbb{Z})$ on $V(\mathbb{R})$, and enumerate the number lattice points in these regions having bounded invariants.

The primary obstacle in this counting, as in representations encountered previously, is that the fundamental region in which one has to count points is not compact but instead has a rather complex system of cusps going off to infinity. A priori, it could be difficult to obtain exact counts of points of bounded height in the cusps of these fundamental regions. We show however that, for all n, most of the integer points in the cusps are points corresponding to the identity element of the 2-Selmer group; meanwhile, most of the points in the main bodies of these fundamental regions correspond to non-identity elements.

Sieve

Sieve

We are interested in counting not all integral orbits, but only those which are locally soluble,

Sieve

We are interested in counting not all integral orbits, but only those which are locally soluble, and we only want to count one integral orbit for each locally soluble rational orbit.

Sieve

We are interested in counting not all integral orbits, but only those which are locally soluble, and we only want to count one integral orbit for each locally soluble rational orbit.

The orbits we wish to count are determined by infinitely many congruence conditions,

Sieve

We are interested in counting not all integral orbits, but only those which are locally soluble, and we only want to count one integral orbit for each locally soluble rational orbit.

The orbits we wish to count are determined by infinitely many congruence conditions, and a sieve is required to obtain a correct asymptotic count of exactly those points.

Sieve

We are interested in counting not all integral orbits, but only those which are locally soluble, and we only want to count one integral orbit for each locally soluble rational orbit.

The orbits we wish to count are determined by infinitely many congruence conditions, and a sieve is required to obtain a correct asymptotic count of exactly those points.

In the end, we find that the average occurring in Theorem 1 arises naturally as the sum of two contributions.

Sieve

We are interested in counting not all integral orbits, but only those which are locally soluble, and we only want to count one integral orbit for each locally soluble rational orbit.

The orbits we wish to count are determined by infinitely many congruence conditions, and a sieve is required to obtain a correct asymptotic count of exactly those points.

In the end, we find that the average occurring in Theorem 1 arises naturally as the sum of two contributions. One comes from the main body of the fundamental region,

Sieve

We are interested in counting not all integral orbits, but only those which are locally soluble, and we only want to count one integral orbit for each locally soluble rational orbit.

The orbits we wish to count are determined by infinitely many congruence conditions, and a sieve is required to obtain a correct asymptotic count of exactly those points.

In the end, we find that the average occurring in Theorem 1 arises naturally as the sum of two contributions. One comes from the main body of the fundamental region, which corresponds to the average number of non-identity elements in the 2-Selmer group

Sieve

We are interested in counting not all integral orbits, but only those which are locally soluble, and we only want to count one integral orbit for each locally soluble rational orbit.

The orbits we wish to count are determined by infinitely many congruence conditions, and a sieve is required to obtain a correct asymptotic count of exactly those points.

In the end, we find that the average occurring in Theorem 1 arises naturally as the sum of two contributions. One comes from the main body of the fundamental region, which corresponds to the average number of non-identity elements in the 2-Selmer group and which we show is given by the Tamagawa number ($= 2$) of the group $\mathrm{SO}(W)$ over $\mathbb{Q}$.

Sieve

We are interested in counting not all integral orbits, but only those which are locally soluble, and we only want to count one integral orbit for each locally soluble rational orbit.

The orbits we wish to count are determined by infinitely many congruence conditions, and a sieve is required to obtain a correct asymptotic count of exactly those points.

In the end, we find that the average occurring in Theorem 1 arises naturally as the sum of two contributions. One comes from the main body of the fundamental region, which corresponds to the average number of non-identity elements in the 2-Selmer group and which we show is given by the Tamagawa number ($= 2$) of the group $\mathrm{SO}(W)$ over $\mathbb{Q}$. The other comes from the cusp of the fundamental region,

Sieve

We are interested in counting not all integral orbits, but only those which are locally soluble, and we only want to count one integral orbit for each locally soluble rational orbit.

The orbits we wish to count are determined by infinitely many congruence conditions, and a sieve is required to obtain a correct asymptotic count of exactly those points.

In the end, we find that the average occurring in Theorem 1 arises naturally as the sum of two contributions. One comes from the main body of the fundamental region, which corresponds to the average number of non-identity elements in the 2-Selmer group and which we show is given by the Tamagawa number $(= 2)$ of the group $\mathrm{SO}(W)$ over $\mathbb{Q}$. The other comes from the cusp of the fundamental region,which counts the average number $(= 1)$ of identity elements in the 2-Selmer group.

Sieve

We are interested in counting not all integral orbits, but only those which are locally soluble, and we only want to count one integral orbit for each locally soluble rational orbit.

The orbits we wish to count are determined by infinitely many congruence conditions, and a sieve is required to obtain a correct asymptotic count of exactly those points.

In the end, we find that the average occurring in Theorem 1 arises naturally as the sum of two contributions. One comes from the main body of the fundamental region, which corresponds to the average number of non-identity elements in the 2-Selmer group and which we show is given by the Tamagawa number ($= 2$) of the group $\mathrm{SO}(W)$ over $\mathbb{Q}$. The other comes from the cusp of the fundamental region,which counts the average number ($= 1$) of identity elements in the 2-Selmer group.

The sum $2 + 1 = 3$ then gives us the average size of the 2-Selmer group, as stated in Theorem 1.

The same arguments work also in any congruence family of odd hyperelliptic curves.

The average size of the 2-Selmer group

The same arguments work also in any congruence family of odd hyperelliptic curves. Thus we obtain

The same arguments work also in any congruence family of odd hyperelliptic curves. Thus we obtain

Theorem 1'. *When all odd hyperelliptic curves of any fixed genus* $n \geq 1$ *in any family defined by finitely many conguence conditions are ordered by height, the average size of the* 2*-Selmer groups of their Jacobians is equal to* 3*.*

Some consequences for the average rank

Some consequences for the average rank

Corollary. *When all odd hyperelliptic curves of genus n (in any congruence family) are ordered by height, the average rank of their Jacobians is bounded*

Some consequences for the average rank

Corollary. *When all odd hyperelliptic curves of genus n (in any congruence family) are ordered by height, the average rank of their Jacobians is bounded by* 1.5.

Corollary. *When all odd hyperelliptic curves of genus n (in any congruence family) are ordered by height, the average rank of their Jacobians is bounded by* 1.5.

Some consequences for the average rank

Corollary. *When all odd hyperelliptic curves of genus n (in any congruence family) are ordered by height, the average rank of their Jacobians is bounded by 1.5.*

Proof:

Corollary. *When all odd hyperelliptic curves of genus n (in any congruence family) are ordered by height, the average rank of their Jacobians is bounded by* 1.5*.*

Proof: Since the rank of the Mordell-Weil group $J(\mathbb{Q})$ is at most the 2-rank $r_2(S_2(J))$ of the 2-Selmer group of the Jacobian J, and since

Some consequences for the average rank

Corollary. *When all odd hyperelliptic curves of genus n (in any congruence family) are ordered by height, the average rank of their Jacobians is bounded by 1.5.*

Proof: Since the rank of the Mordell-Weil group $J(\mathbb{Q})$ is at most the 2-rank $r_2(S_2(J))$ of the 2-Selmer group of the Jacobian J, and since $2r_2(S_2(J)) \leq 2^{r_2(S_2(J))} = \#S_2(J)$, by taking averages we obtain that twice the average rank is at most 3, as desired.

Corollary. *When all odd hyperelliptic curves of genus n (in any congruence family) are ordered by height, the average rank of their Jacobians is bounded by* 1.5.

Proof: Since the rank of the Mordell-Weil group $J(\mathbb{Q})$ is at most the 2-rank $r_2(S_2(J))$ of the 2-Selmer group of the Jacobian J, and since $2r_2(S_2(J)) \leq 2^{r_2(S_2(J))} = \#S_2(J)$, by taking averages we obtain that twice the average rank is at most 3, as desired. $\square$

Some consequences for the average rank

Corollary. *When all odd hyperelliptic curves of genus n (in any congruence family) are ordered by height, the average rank of their Jacobians is bounded by 1.5.*

Proof: Since the rank of the Mordell-Weil group $J(\mathbb{Q})$ is at most the 2-rank $r_2(S_2(J))$ of the 2-Selmer group of the Jacobian J, and since $2r_2(S_2(J)) \leq 2^{r_2(S_2(J))} = \#S_2(J)$, by taking averages we obtain that twice the average rank is at most 3, as desired. $\square$

Note that the average rank is bounded by 1.5,

Corollary. *When all odd hyperelliptic curves of genus n (in any congruence family) are ordered by height, the average rank of their Jacobians is bounded by* 1.5.

Proof: Since the rank of the Mordell-Weil group $J(\mathbb{Q})$ is at most the 2-rank $r_2(S_2(J))$ of the 2-Selmer group of the Jacobian J, and since $2r_2(S_2(J)) \leq 2^{r_2(S_2(J))} = \#S_2(J)$, by taking averages we obtain that twice the average rank is at most 3, as desired. $\square$

Note that the average rank is bounded by 1.5, independent of the genus.

Some consequences for the average rank

Corollary. *When all odd hyperelliptic curves of genus n (in any congruence family) are ordered by height, the average rank of their Jacobians is bounded by* 1.5*.*

Proof: Since the rank of the Mordell-Weil group $J(\mathbb{Q})$ is at most the 2-rank $r_2(S_2(J))$ of the 2-Selmer group of the Jacobian J, and since $2r_2(S_2(J)) \leq 2^{r_2(S_2(J))} = \#S_2(J)$, by taking averages we obtain that twice the average rank is at most 3, as desired. $\square$

Note that the average rank is bounded by 1.5, independent of the genus.

(The same is true also for the average size of $Ш_J[2]$.)

Chabauty–Coleman's p-adic method

Chabauty–Coleman's p-adic method

Recall that the method of Chabauty, as refined by Coleman, yields a finite and effective bound on the number of rational points on a curve over $\mathbb{Q}$ whenever its genus is greater than the rank of its Jacobian.

Chabauty–Coleman's p-adic method

Recall that the method of Chabauty, as refined by Coleman, yields a finite and effective bound on the number of rational points on a curve over $\mathbb{Q}$ whenever its genus is greater than the rank of its Jacobian. Theorem 1 thus implies

Recall that the method of Chabauty, as refined by Coleman, yields a finite and effective bound on the number of rational points on a curve over $\mathbb{Q}$ whenever its genus is greater than the rank of its Jacobian. Theorem 1 thus implies

Corollary. *Let δ_n denote the lower density of odd hyperelliptic curves of genus n satisfying Chabauty's condition.*

Chabauty–Coleman's p-adic method

Recall that the method of Chabauty, as refined by Coleman, yields a finite and effective bound on the number of rational points on a curve over $\mathbb{Q}$ whenever its genus is greater than the rank of its Jacobian. Theorem 1 thus implies

Corollary. *Let δ_n denote the lower density of odd hyperelliptic curves of genus n satisfying Chabauty's condition. Then $\delta_n \to 1$ as $n \to \infty$.*

Recall that the method of Chabauty, as refined by Coleman, yields a finite and effective bound on the number of rational points on a curve over $\mathbb{Q}$ whenever its genus is greater than the rank of its Jacobian. Theorem 1 thus implies

Corollary. *Let δ_n denote the lower density of odd hyperelliptic curves of genus n satisfying Chabauty's condition. Then $\delta_n \to 1$ as $n \to \infty$.*

That is, for an asymptotic density of 1 of odd hyperelliptic curves, one can effectively bound the number of rational points.

Chabauty–Coleman's p-adic method (cont'd)

Chabauty–Coleman's p-adic method (cont'd)

As an explicit consequence, we may use the main Theorem 1, together with Chabauty–Coleman's method as in Stoll's treatment, to prove the following explicit bounds on the number of rational points on odd hyperelliptic curves:

Chabauty–Coleman's p-adic method (cont'd)

As an explicit consequence, we may use the main Theorem 1, together with Chabauty–Coleman's method as in Stoll's treatment, to prove the following explicit bounds on the number of rational points on odd hyperelliptic curves:

Corollary.

(a) *For any $n \geq 2$, a positive proportion of odd hyperelliptic curves of genus n have at most 3 rational points.*

Chabauty–Coleman's p-adic method (cont'd)

As an explicit consequence, we may use the main Theorem 1, together with Chabauty–Coleman's method as in Stoll's treatment, to prove the following explicit bounds on the number of rational points on odd hyperelliptic curves:

Corollary.

(a) *For any $n \geq 2$, a positive proportion of odd hyperelliptic curves of genus n have at most 3 rational points.*

(b) *For any $n \geq 3$, a majority (i.e., a proportion of $> 50\%$) of all odd hyperelliptic curves of genus n have less than 20 rational points.*

Chabauty–Coleman's p-adic method (cont'd)

As an explicit consequence, we may use the main Theorem 1, together with Chabauty–Coleman's method as in Stoll's treatment, to prove the following explicit bounds on the number of rational points on odd hyperelliptic curves:

Corollary.

(a) *For any $n \geq 2$, a positive proportion of odd hyperelliptic curves of genus n have at most 3 rational points.*

(b) *For any $n \geq 3$, a majority (i.e., a proportion of $> 50\%$) of all odd hyperelliptic curves of genus n have less than 20 rational points.*

The numbers in the Corollary can certainly be improved with a more careful analysis.

As an explicit consequence, we may use the main Theorem 1, together with Chabauty–Coleman's method as in Stoll's treatment, to prove the following explicit bounds on the number of rational points on odd hyperelliptic curves:

Corollary.

(a) *For any $n \geq 2$, a positive proportion of odd hyperelliptic curves of genus n have at most 3 rational points.*

(b) *For any $n \geq 3$, a majority (i.e., a proportion of $> 50\%$) of all odd hyperelliptic curves of genus n have less than 20 rational points.*

The numbers in the Corollary can certainly be improved with a more careful analysis. Bjorn Poonen and Michael Stoll have recently shown us arguments that use Theorem 1 with more refined Chabauty–Coleman–style arguments to improve the numbers in (a) and (b) (provided $n \geq 3$) to 1 and 8 respectively.

Chabauty–Coleman's p-adic method (cont'd)

As an explicit consequence, we may use the main Theorem 1, together with Chabauty–Coleman's method as in Stoll's treatment, to prove the following explicit bounds on the number of rational points on odd hyperelliptic curves:

Corollary.

(a) *For any $n \geq 2$, a positive proportion of odd hyperelliptic curves of genus n have at most 3 rational points.*

(b) *For any $n \geq 3$, a majority (i.e., a proportion of $> 50\%$) of all odd hyperelliptic curves of genus n have less than 20 rational points.*

The numbers in the Corollary can certainly be improved with a more careful analysis. Bjorn Poonen and Michael Stoll have recently shown us arguments that use Theorem 1 with more refined Chabauty–Coleman–style arguments to improve the numbers in (a) and (b) (provided $n \geq 3$) to 1 and 8 respectively. For the latest, see the next talk!

Even hyperelliptic curves

Even hyperelliptic curves

The odd case was a good and important preparation for the general even case.

Even hyperelliptic curves

The odd case was a good and important preparation for the general even case.

Next time: *Most general (even) hyperelliptic curves have* **no** *rational points!*