The average rank of elliptic curves

Manjul Bhargava
Princeton University

Conference on the BSD Conjecture
DPMMS, Cambridge

May 4, 2011

Average rank?

Q: What is the rank of elliptic curves on average?

Average rank?

Q: What is the rank of elliptic curves on average?

In order to ask this question more precisely, we need a natural way to measure the size of elliptic curves, so that we can order them by size.

Q: What is the rank of elliptic curves on average?

In order to ask this question more precisely, we need a natural way to measure the size of elliptic curves, so that we can order them by size.

We use the simplest such measure, called the naive height, which is basically a measure of the size of the coefficients of the defining equation of the elliptic curve.

A canonical representation of rational elliptic curves

To define the naive height, we use the following

A canonical representation of rational elliptic curves

To define the naive height, we use the following

Fact: Any elliptic curve E over $\mathbb{Q}$ is isomorphic to a cubic curve in the plane of the form

$$E_{A,B} : y^2 = x^3 + Ax + B.$$

A canonical representation of rational elliptic curves

To define the naive height, we use the following

Fact: Any elliptic curve E over $\mathbb{Q}$ is isomorphic to a cubic curve in the plane of the form

$$E_{A,B} : y^2 = x^3 + Ax + B.$$

In fact, any $E/\mathbb{Q}$ is isomorphic to a *unique* $E_{A,B}$ such that

$$\text{for all primes } p,\ \ p^4 \mid A \ \Rightarrow\ p^6 \nmid B.$$

A canonical representation of rational elliptic curves

To define the naive height, we use the following

Fact: Any elliptic curve E over $\mathbb{Q}$ is isomorphic to a cubic curve in the plane of the form

$$E_{A,B} : y^2 = x^3 + Ax + B.$$

In fact, any $E/\mathbb{Q}$ is isomorphic to a *unique* $E_{A,B}$ such that

$$\text{for all primes } p,\ \ p^4 \mid A \ \Rightarrow\ p^6 \nmid B.$$

The reason is:

A canonical representation of rational elliptic curves

To define the naive height, we use the following

Fact: Any elliptic curve E over $\mathbb{Q}$ is isomorphic to a cubic curve in the plane of the form

$$E_{A,B} : y^2 = x^3 + Ax + B.$$

In fact, any $E/\mathbb{Q}$ is isomorphic to a *unique* $E_{A,B}$ such that

$$\text{for all primes } p,\ p^4 \mid A \Rightarrow p^6 \nmid B.$$

The reason is: if $p^4 \mid A$ and $p^6 \mid B$,

A canonical representation of rational elliptic curves

To define the naive height, we use the following

Fact: Any elliptic curve E over $\mathbb{Q}$ is isomorphic to a cubic curve in the plane of the form

$$E_{A,B} : y^2 = x^3 + Ax + B.$$

In fact, any $E/\mathbb{Q}$ is isomorphic to a *unique* $E_{A,B}$ such that

$$\text{for all primes } p,\ \ p^4 \mid A \ \Rightarrow\ p^6 \nmid B.$$

The reason is: if $p^4 \mid A$ and $p^6 \mid B$, then $E_{A,B} \cong E_{A/p^4, B/p^6}$

A canonical representation of rational elliptic curves

To define the naive height, we use the following

Fact: Any elliptic curve E over $\mathbb{Q}$ is isomorphic to a cubic curve in the plane of the form

$$E_{A,B} : y^2 = x^3 + Ax + B.$$

In fact, any $E/\mathbb{Q}$ is isomorphic to a *unique* $E_{A,B}$ such that

$$\text{for all primes } p,\ \ p^4 \mid A \ \Rightarrow\ p^6 \nmid B.$$

The reason is: if $p^4 \mid A$ and $p^6 \mid B$, then $E_{A,B} \cong E_{A/p^4,B/p^6}$ via $x \mapsto p^2x'$ and $y \mapsto p^3y'$.

The height of an elliptic curve

Thus we have a canonical representation of any $E/\mathbb{Q}$ as

$$E_{A,B} : y^2 = x^3 + Ax + B.$$

Thus we have a canonical representation of any $E/\mathbb{Q}$ as

$$E_{A,B} : y^2 = x^3 + Ax + B.$$

We may thus define the height of E by the size of the coefficients of the defining equation.

The height of an elliptic curve

Thus we have a canonical representation of any $E/\mathbb{Q}$ as

$$E_{A,B} : y^2 = x^3 + Ax + B.$$

We may thus define the height of E by the size of the coefficients of the defining equation.

If $E = E_{A,B}$, then $H(E_{A,B}) := \max\{4|A|^3, 27B^2\}$.

The height of an elliptic curve

Thus we have a canonical representation of any $E/\mathbb{Q}$ as

$$E_{A,B} : y^2 = x^3 + Ax + B.$$

We may thus define the height of E by the size of the coefficients of the defining equation.

If $E = E_{A,B}$, then $H(E_{A,B}) := \max\{4|A|^3, 27B^2\}$. This is called the (naive) height of E.

The height of an elliptic curve

Thus we have a canonical representation of any $E/\mathbb{Q}$ as

$$E_{A,B} : y^2 = x^3 + Ax + B.$$

We may thus define the height of E by the size of the coefficients of the defining equation.

If $E = E_{A,B}$, then $H(E_{A,B}) := \max\{4|A|^3, 27B^2\}$. This is called the (naive) height of E.

The naive height is essentially the exponential of what is called the "Faltings height".

The height of an elliptic curve

Thus we have a canonical representation of any $E/\mathbb{Q}$ as

$$E_{A,B} : y^2 = x^3 + Ax + B.$$

We may thus define the height of E by the size of the coefficients of the defining equation.

If $E = E_{A,B}$, then $H(E_{A,B}) := \max\{4|A|^3, 27B^2\}$. This is called the (naive) height of E.

The naive height is essentially the exponential of what is called the "Faltings height".

Another related measure of the size of $E_{A,B}$ is called the discriminant $\Delta(E_{A,B}) := -4A^3 - 27B^2$.

Thus we have a canonical representation of any $E/\mathbb{Q}$ as

$$E_{A,B} : y^2 = x^3 + Ax + B.$$

We may thus define the height of E by the size of the coefficients of the defining equation.

If $E = E_{A,B}$, then $H(E_{A,B}) := \max\{4|A|^3, 27B^2\}$. This is called the (naive) height of E.

The naive height is essentially the exponential of what is called the "Faltings height".

Another related measure of the size of $E_{A,B}$ is called the discriminant $\Delta(E_{A,B}) := -4A^3 - 27B^2$.

Finally, there is a measure of size called the conductor $N(E)$ of E.

The height of an elliptic curve

Thus we have a canonical representation of any $E/\mathbb{Q}$ as

$$E_{A,B} : y^2 = x^3 + Ax + B.$$

We may thus define the height of E by the size of the coefficients of the defining equation.

If $E = E_{A,B}$, then $H(E_{A,B}) := \max\{4|A|^3, 27B^2\}$. This is called the (naive) height of E.

The naive height is essentially the exponential of what is called the "Faltings height".

Another related measure of the size of $E_{A,B}$ is called the discriminant $\Delta(E_{A,B}) := -4A^3 - 27B^2$.

Finally, there is a measure of size called the conductor $N(E)$ of E.

These various measures are conjectured to be about the same order of magnitude for all but a negligible proportion of elliptic curves!

Average rank

Average rank

Q: If all elliptic curves over $\mathbb{Q}$ are ordered by their heights (or discriminants, etc.), what is the average size of the rank?

Average rank

Q: If all elliptic curves over $\mathbb{Q}$ are ordered by their heights (or discriminants, etc.), what is the average size of the rank?

Conjecture (Goldfeld, Katz-Sarnak): $1/2$.

Average rank

Q: If all elliptic curves over $\mathbb{Q}$ are ordered by their heights (or discriminants, etc.), what is the average size of the rank?

Conjecture (Goldfeld, Katz-Sarnak): $1/2$. (*More precisely, one expects* 50% *of curves to have rank* 0, *and* 50% *to have rank* 1.)

Average rank

Q: If all elliptic curves over $\mathbb{Q}$ are ordered by their heights (or discriminants, etc.), what is the average size of the rank?

Conjecture (Goldfeld, Katz-Sarnak): $1/2$. (*More precisely, one expects* 50% *of curves to have rank* 0, *and* 50% *to have rank* 1.)

However, previously this average has not even been known to be finite (let alone $1/2$)!

Average rank

Q: If all elliptic curves over $\mathbb{Q}$ are ordered by their heights (or discriminants, etc.), what is the average size of the rank?

Conjecture (Goldfeld, Katz-Sarnak): 1/2. (*More precisely, one expects* 50% *of curves to have rank* 0*, and* 50% *to have rank* 1*.*)

However, previously this average has not even been known to be finite (let alone 1/2)! (at least not unconditionally!)

Average rank

Q: If all elliptic curves over $\mathbb{Q}$ are ordered by their heights (or discriminants, etc.), what is the average size of the rank?

Conjecture (Goldfeld, Katz-Sarnak): 1/2. (*More precisely, one expects* 50% *of curves to have rank* 0, *and* 50% *to have rank* 1.)

However, previously this average has not even been known to be finite (let alone 1/2)! (at least not unconditionally!)

Computations do not currently give much support to the conjecture either.

Average rank

Q: If all elliptic curves over $\mathbb{Q}$ are ordered by their heights (or discriminants, etc.), what is the average size of the rank?

Conjecture (Goldfeld, Katz-Sarnak): $1/2$. (*More precisely, one expects* 50% *of curves to have rank* 0, *and* 50% *to have rank* 1.)

However, previously this average has not even been known to be finite (let alone $1/2$)! (at least not unconditionally!)

Computations do not currently give much support to the conjecture either.

It was observed by Brumer and McGuinness in their 1990 computations that rank 2 curves seem to occur surprisingly often, and with *increasing* frequency!

Average rank

Q: If all elliptic curves over $\mathbb{Q}$ are ordered by their heights (or discriminants, etc.), what is the average size of the rank?

Conjecture (Goldfeld, Katz-Sarnak): $1/2$. (*More precisely, one expects* 50% *of curves to have rank* 0, *and* 50% *to have rank* 1.)

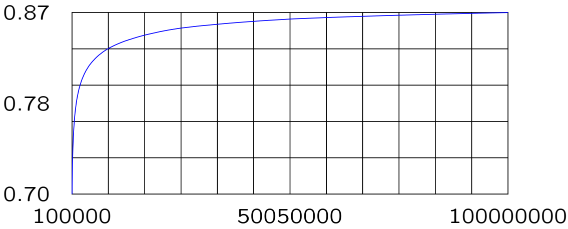
However, previously this average has not even been known to be finite (let alone $1/2$)! (at least not unconditionally!)

Computations do not currently give much support to the conjecture either.

It was observed by Brumer and McGuinness in their 1990 computations that rank 2 curves seem to occur surprisingly often, and with *increasing* frequency! These computations were extended recently by Bektemirov, Stein, and Watkins:

All Curves Ordered By Conductor

The average rank of all curves of conductor $\leq 10^8$ is $0.8664\ldots$.
A graph of the average rank as a function:



We created this graph by computing the average rank of curves of conductor up to $n \cdot 10^5$ for $1 \leq n \leq 1000$.

GRH + BSD

GRH + BSD

The first theoretical result towards the boundedness of average rank are due to Brumer.

GRH + BSD

The first theoretical result towards the boundedness of average rank are due to Brumer.

In 1992, Brumer showed that the Generalized Riemann Hypothesis (GRH) and the Birch and Swinnerton-Dyer Conjecture (BSD) together imply that the average rank is bounded.

GRH + BSD

The first theoretical result towards the boundedness of average rank are due to Brumer.

In 1992, Brumer showed that the Generalized Riemann Hypothesis (GRH) and the Birch and Swinnerton-Dyer Conjecture (BSD) together imply that the average rank is bounded. (in fact, bounded by 2.3.)

GRH + BSD

The first theoretical result towards the boundedness of average rank are due to Brumer.

In 1992, Brumer showed that the Generalized Riemann Hypothesis (GRH) and the Birch and Swinnerton-Dyer Conjecture (BSD) together imply that the average rank is bounded. (in fact, bounded by 2.3.)

In 2004, Heath-Brown (still assuming GRH + BSD) improved this to average rank ≤ 2.0.

GRH + BSD

The first theoretical result towards the boundedness of average rank are due to Brumer.

In 1992, Brumer showed that the Generalized Riemann Hypothesis (GRH) and the Birch and Swinnerton-Dyer Conjecture (BSD) together imply that the average rank is bounded. (in fact, bounded by 2.3.)

In 2004, Heath-Brown (still assuming GRH + BSD) improved this to average rank ≤ 2.0.

In 2009, Young further improved this (again assuming GRH + BSD) to $\leq \frac{25}{14} \approx 1.79$.

GRH + BSD

The first theoretical result towards the boundedness of average rank are due to Brumer.

In 1992, Brumer showed that the Generalized Riemann Hypothesis (GRH) and the Birch and Swinnerton-Dyer Conjecture (BSD) together imply that the average rank is bounded. (in fact, bounded by 2.3.)

In 2004, Heath-Brown (still assuming GRH + BSD) improved this to average rank ≤ 2.0.

In 2009, Young further improved this (again assuming GRH + BSD) to $\leq \frac{25}{14} \approx 1.79$.

The main theorem

The main theorem

Theorem. *When elliptic curves $E/\mathbb{Q}$ are ordered by height, the average rank is bounded;*

The main theorem

Theorem. *When elliptic curves* $E/\mathbb{Q}$ *are ordered by height, the average rank is bounded; in fact, it is bounded by* 1.5.

The main theorem

Theorem. *When elliptic curves $E/\mathbb{Q}$ are ordered by height, the average rank is bounded; in fact, it is bounded by* 1.5.

We prove something stronger, namely:

The main theorem

Theorem. *When elliptic curves $E/\mathbb{Q}$ are ordered by height, the average rank is bounded; in fact, it is bounded by* 1.5*.*

We prove something stronger, namely:

Theorem. *The same is true for the 2-Selmer rank, i.e., the average 2-Selmer rank is bounded by* 1.5*.*

The main theorem

Theorem. *When elliptic curves $E/\mathbb{Q}$ are ordered by height, the average rank is bounded; in fact, it is bounded by* 1.5.

We prove something stronger, namely:

Theorem. *The same is true for the 2-Selmer rank, i.e., the average 2-Selmer rank is bounded by* 1.5.

Recall that the 2-Selmer group $S^{(2)}(E)$ of an elliptic curve $E/\mathbb{Q}$ fits into an exact sequence

The main theorem

Theorem. *When elliptic curves $E/\mathbb{Q}$ are ordered by height, the average rank is bounded; in fact, it is bounded by* 1.5.

We prove something stronger, namely:

Theorem. *The same is true for the 2-Selmer rank, i.e., the average 2-Selmer rank is bounded by* 1.5.

Recall that the 2-Selmer group $S^{(2)}(E)$ of an elliptic curve $E/\mathbb{Q}$ fits into an exact sequence

$$0 \to E(\mathbb{Q})/2E(\mathbb{Q}) \to S^{(2)}(E) \to \text{Ш}_E[2] \to 0.$$

The main theorem

Theorem. *When elliptic curves $E/\mathbb{Q}$ are ordered by height, the average rank is bounded; in fact, it is bounded by* 1.5.

We prove something stronger, namely:

Theorem. *The same is true for the 2-Selmer rank, i.e., the average 2-Selmer rank is bounded by* 1.5.

Recall that the 2-Selmer group $S^{(2)}(E)$ of an elliptic curve $E/\mathbb{Q}$ fits into an exact sequence

$$0 \to E(\mathbb{Q})/2E(\mathbb{Q}) \to S^{(2)}(E) \to Ш_E[2] \to 0.$$

So $r_2(S^{(2)}(E)) = r_2(E(\mathbb{Q})[2]) + r_2(Ш_E[2]) + r(E) \leq 1.5$ on average.

The main theorem

Theorem. *When elliptic curves $E/\mathbb{Q}$ are ordered by height, the average rank is bounded; in fact, it is bounded by* 1.5*.*

We prove something stronger, namely:

Theorem. *The same is true for the 2-Selmer rank, i.e., the average 2-Selmer rank is bounded by* 1.5*.*

Recall that the 2-Selmer group $S^{(2)}(E)$ of an elliptic curve $E/\mathbb{Q}$ fits into an exact sequence

$$0 \to E(\mathbb{Q})/2E(\mathbb{Q}) \to S^{(2)}(E) \to \text{Ш}_E[2] \to 0.$$

So $r_2(S^{(2)}(E)) = r_2(E(\mathbb{Q})[2]) + r_2(\text{Ш}_E[2]) + r(E) \leq 1.5$ on average.

We actually prove something even stronger, namely:

The main theorem

Theorem. *When elliptic curves $E/\mathbb{Q}$ are ordered by height, the average rank is bounded; in fact, it is bounded by* 1.5.

We prove something stronger, namely:

Theorem. *The same is true for the 2-Selmer rank, i.e., the average 2-Selmer rank is bounded by* 1.5.

Recall that the 2-Selmer group $S^{(2)}(E)$ of an elliptic curve $E/\mathbb{Q}$ fits into an exact sequence

$$0 \to E(\mathbb{Q})/2E(\mathbb{Q}) \to S^{(2)}(E) \to \text{Ш}_E[2] \to 0.$$

So $r_2(S^{(2)}(E)) = r_2(E(\mathbb{Q})[2]) + r_2(\text{Ш}_E[2]) + r(E) \leq 1.5$ on average.

We actually prove something even stronger, namely:

Theorem. *When elliptic curves $E/\mathbb{Q}$ are ordered by height, the average size of the 2-Selmer group $S^{(2)}(E)$ is exactly* 3.

The main theorem

Theorem. *When elliptic curves $E/\mathbb{Q}$ are ordered by height, the average rank is bounded; in fact, it is bounded by* 1.5*.*

We prove something stronger, namely:

Theorem. *The same is true for the 2-Selmer rank, i.e., the average 2-Selmer rank is bounded by* 1.5*.*

Recall that the 2-Selmer group $S^{(2)}(E)$ of an elliptic curve $E/\mathbb{Q}$ fits into an exact sequence

$$0 \to E(\mathbb{Q})/2E(\mathbb{Q}) \to S^{(2)}(E) \to \text{Ш}_E[2] \to 0.$$

So $r_2(S^{(2)}(E)) = r_2(E(\mathbb{Q})[2]) + r_2(\text{Ш}_E[2]) + r(E) \leq 1.5$ on average.

We actually prove something even stronger, namely:

Theorem. *When all elliptic curves $E/\mathbb{Q}$ in any family defined by finitely many congruence conditions are ordered by height, the average size of the 2-Selmer group $S^{(2)}(E)$ is exactly* 3*.*

Proof of theorem

Proof of theorem

To get a hold of 2-Selmer groups of elliptic curves, we use 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.

Proof of theorem

To get a hold of 2-Selmer groups of elliptic curves, we use 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.

To state the result, recall that the action of $\mathrm{GL}_2(\mathbb{Z})$ on binary quartic forms, by linear substitution of variable, has two independent polynomial invariants, traditionally denoted I and J, respectively.

Proof of theorem

To get a hold of 2-Selmer groups of elliptic curves, we use 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.

To state the result, recall that the action of $\mathrm{GL}_2(\mathbb{Z})$ on binary quartic forms, by linear substitution of variable, has two independent polynomial invariants, traditionally denoted I and J, respectively. The invariant I has degree 2 and the invariant J has degree 3 in the coefficients of the binary quartic form.

To get a hold of 2-Selmer groups of elliptic curves, we use 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.

To state the result, recall that the action of $\mathrm{GL}_2(\mathbb{Z})$ on binary quartic forms, by linear substitution of variable, has two independent polynomial invariants, traditionally denoted I and J, respectively. The invariant I has degree 2 and the invariant J has degree 3 in the coefficients of the binary quartic form.

Theorem. (Birch & Swinnerton-Dyer)

Proof of theorem

To get a hold of 2-Selmer groups of elliptic curves, we use 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.

To state the result, recall that the action of $\mathrm{GL}_2(\mathbb{Z})$ on binary quartic forms, by linear substitution of variable, has two independent polynomial invariants, traditionally denoted I and J, respectively. The invariant I has degree 2 and the invariant J has degree 3 in the coefficients of the binary quartic form.

Theorem. (Birch & Swinnerton-Dyer) *There is an injective map from $S^{(2)}(E_{A,B})$ to the set of $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of integral binary quartic forms having invariants $I = -2^4 \cdot 3 \cdot A$ and $J = -2^4 \cdot 3 \cdot B$.*

Proof of theorem

To get a hold of 2-Selmer groups of elliptic curves, we use 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.

To state the result, recall that the action of $\mathrm{GL}_2(\mathbb{Z})$ on binary quartic forms, by linear substitution of variable, has two independent polynomial invariants, traditionally denoted I and J, respectively. The invariant I has degree 2 and the invariant J has degree 3 in the coefficients of the binary quartic form.

Theorem. (Birch & Swinnerton-Dyer) *There is an injective map from $S^{(2)}(E_{A,B})$ to the set of $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of integral binary quartic forms having invariants $I = -2^4 \cdot 3 \cdot A$ and $J = -2^4 \cdot 3 \cdot B$.*

BSD's theorem yields an efficient method for rank computations of elliptic curves.

Proof of theorem

To get a hold of 2-Selmer groups of elliptic curves, we use 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.

To state the result, recall that the action of $\mathrm{GL}_2(\mathbb{Z})$ on binary quartic forms, by linear substitution of variable, has two independent polynomial invariants, traditionally denoted I and J, respectively. The invariant I has degree 2 and the invariant J has degree 3 in the coefficients of the binary quartic form.

Theorem. (Birch & Swinnerton-Dyer) *There is an injective map from $S^{(2)}(E_{A,B})$ to the set of $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of integral binary quartic forms having invariants $I = -2^4 \cdot 3 \cdot A$ and $J = -2^4 \cdot 3 \cdot B$.*

BSD's theorem yields an efficient method for rank computations of elliptic curves. This method has been further refined by Cremona, and implemented in his well-known `mwrank` program.

Counting binary forms

Disquisitiones Arithmeticae (1801)

Binary quadratic form:

Counting binary forms

Disquisitiones Arithmeticae (1801)

Binary quadratic form:

$$Q(x, y) = ax^2 + bxy + cy^2 \ (a, b, c \in \mathbb{Z})$$

Counting binary forms

Disquisitiones Arithmeticae (1801)

Binary quadratic form:

$$Q(x, y) = ax^2 + bxy + cy^2 \ (a, b, c \in \mathbb{Z})$$

$\mathrm{SL}_2(\mathbb{Z})$ acts on the set of binary quadratic forms (by linear substitution).

Counting binary forms

Disquisitiones Arithmeticae (1801)

Binary quadratic form:

$$Q(x, y) = ax^2 + bxy + cy^2 \ (a, b, c \in \mathbb{Z})$$

$\mathrm{SL}_2(\mathbb{Z})$ acts on the set of binary quadratic forms (by linear substitution).

$$\mathrm{Disc}(Q) = b^2 - 4ac.$$

Counting binary forms

Disquisitiones Arithmeticae (1801)

Binary quadratic form:

$$Q(x, y) = ax^2 + bxy + cy^2 \ (a, b, c \in \mathbb{Z})$$

$\mathrm{SL}_2(\mathbb{Z})$ acts on the set of binary quadratic forms (by linear substitution).

$\mathrm{Disc}(Q) = b^2 - 4ac$. (unique SL_2-polynomial invariant)

Counting binary forms

Disquisitiones Arithmeticae (1801)

Binary quadratic form:

$$Q(x,y) = ax^2 + bxy + cy^2 \ (a,b,c \in \mathbb{Z})$$

$\mathrm{SL}_2(\mathbb{Z})$ acts on the set of binary quadratic forms (by linear substitution).

$\mathrm{Disc}(Q) = b^2 - 4ac$. (unique SL_2-polynomial invariant)

It is known that there are only finitely many $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of binary quadratic forms with given value of discriminant D.

Counting binary forms

Disquisitiones Arithmeticae (1801)

Binary quadratic form:

$$Q(x,y) = ax^2 + bxy + cy^2 \ (a,b,c \in \mathbb{Z})$$

$\mathrm{SL}_2(\mathbb{Z})$ acts on the set of binary quadratic forms (by linear substitution).

$\mathrm{Disc}(Q) = b^2 - 4ac$. (unique SL_2-polynomial invariant)

It is known that there are only finitely many $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of binary quadratic forms with given value of discriminant D.

How many classes h_D are there with discriminant D, or with D at most X?

Disquisitiones Arithmeticae (1801)

Binary quadratic form:

$$Q(x,y) = ax^2 + bxy + cy^2 \ (a,b,c \in \mathbb{Z})$$

$\mathrm{SL}_2(\mathbb{Z})$ acts on the set of binary quadratic forms (by linear substitution).

$$\mathrm{Disc}(Q) = b^2 - 4ac. \text{ (unique } \mathrm{SL}_2\text{-polynomial invariant)}$$

It is known that there are only finitely many $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of binary quadratic forms with given value of discriminant D.

How many classes h_D are there with discriminant D, or with D at most X?

Theorem. (Gauss 1801/Mertens 1874/Siegel 1944)

$$\sum_{-X<D<0} h_D \sim \frac{\pi}{18} \cdot X^{3/2}; \qquad \sum_{0<D<X} h_D \log \epsilon_D \sim \frac{\pi^2}{18} \cdot X^{3/2}.$$

Counting binary forms: cubic forms

Counting binary forms: cubic forms

The next natural case is that of binary cubic forms $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$, $a, b, c, d \in \mathbb{Z}$.

Counting binary forms: cubic forms

The next natural case is that of binary cubic forms $f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$, $a,b,c,d \in \mathbb{Z}$.

$\mathrm{GL}_2(\mathbb{Z})$ acts naturally on such forms.

Counting binary forms: cubic forms

The next natural case is that of binary cubic forms $f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$, $a, b, c, d \in \mathbb{Z}$.

$\mathrm{GL}_2(\mathbb{Z})$ acts naturally on such forms.

There is again just one polynomial invariant for this action,

Counting binary forms: cubic forms

The next natural case is that of binary cubic forms $f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$, $a,b,c,d \in \mathbb{Z}$.

$\mathrm{GL}_2(\mathbb{Z})$ acts naturally on such forms.

There is again just one polynomial invariant for this action, namely the discriminant $\mathrm{Disc}(f)$ of f, given by

Counting binary forms: cubic forms

The next natural case is that of binary cubic forms $f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$, $a,b,c,d \in \mathbb{Z}$.

$\mathrm{GL}_2(\mathbb{Z})$ acts naturally on such forms.

There is again just one polynomial invariant for this action, namely the discriminant $\mathrm{Disc}(f)$ of f, given by

$$\mathrm{Disc}(f) = b^2c^2 + 18abcd - 4ac^3 - 4b^3d - 27a^2d^2.$$

Counting binary forms: cubic forms

The next natural case is that of binary cubic forms $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$, $a, b, c, d \in \mathbb{Z}$.

$\mathrm{GL}_2(\mathbb{Z})$ acts naturally on such forms.

There is again just one polynomial invariant for this action, namely the discriminant $\mathrm{Disc}(f)$ of f, given by

$$\mathrm{Disc}(f) = b^2c^2 + 18abcd - 4ac^3 - 4b^3d - 27a^2d^2.$$

As before there exist only finitely many $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of binary cubic forms with given value of discriminant D.

Counting binary forms: cubic forms

The next natural case is that of binary cubic forms $f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$, $a,b,c,d \in \mathbb{Z}$.

$\mathrm{GL}_2(\mathbb{Z})$ acts naturally on such forms.

There is again just one polynomial invariant for this action, namely the discriminant $\mathrm{Disc}(f)$ of f, given by

$$\mathrm{Disc}(f) = b^2c^2 + 18abcd - 4ac^3 - 4b^3d - 27a^2d^2.$$

As before there exist only finitely many $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of binary cubic forms with given value of discriminant D.

How many classes $h(D)$ of irreducible binary cubic forms are there with discriminant D, or with D at most X?

Counting binary forms: cubic forms

The next natural case is that of binary cubic forms $f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$, $a, b, c, d \in \mathbb{Z}$.

$\mathrm{GL}_2(\mathbb{Z})$ acts naturally on such forms.

There is again just one polynomial invariant for this action, namely the discriminant $\mathrm{Disc}(f)$ of f, given by

$$\mathrm{Disc}(f) = b^2c^2 + 18abcd - 4ac^3 - 4b^3d - 27a^2d^2.$$

As before there exist only finitely many $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of binary cubic forms with given value of discriminant D.

How many classes $h(D)$ of irreducible binary cubic forms are there with discriminant D, or with D at most X?

Theorem. (Davenport 1951)

$$\sum_{-X<D<0} h(D) \sim \frac{\pi^2}{24} \cdot X; \qquad \sum_{0<D<X} h(D) \sim \frac{\pi^2}{72} \cdot X.$$

The next natural case is that of binary quartic forms $f(x, y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4, \;\; a, b, c, d, e \in \mathbb{Z}$.

Counting binary forms: quartic forms

The next natural case is that of binary quartic forms $f(x,y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4$, $a,b,c,d,e \in \mathbb{Z}$.

$\mathrm{GL}_2(\mathbb{Z})$ again acts on these forms by linear substitution.

Counting binary forms: quartic forms

The next natural case is that of binary quartic forms $f(x,y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4$, $a,b,c,d,e \in \mathbb{Z}$.

$\mathrm{GL}_2(\mathbb{Z})$ again acts on these forms by linear substitution.

There are now two polynomial invariants for this action, traditionally denoted I and J, where:

Counting binary forms: quartic forms

The next natural case is that of binary quartic forms $f(x,y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4$, $a,b,c,d,e \in \mathbb{Z}$.

$\mathrm{GL}_2(\mathbb{Z})$ again acts on these forms by linear substitution.

There are now two polynomial invariants for this action, traditionally denoted I and J, where:

$$I(f) = 12ae - 3bd + c^2,$$

Counting binary forms: quartic forms

The next natural case is that of binary quartic forms $f(x,y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4$, $a,b,c,d,e \in \mathbb{Z}$.

$\mathrm{GL}_2(\mathbb{Z})$ again acts on these forms by linear substitution.

There are now two polynomial invariants for this action, traditionally denoted I and J, where:

$$I(f) = 12ae - 3bd + c^2,$$

$$J(f) = 72ace + 9bcd - 27ad^2 - 27eb^2 - 2c^3.$$

Counting binary forms: quartic forms

The next natural case is that of binary quartic forms $f(x,y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4$, $a,b,c,d,e \in \mathbb{Z}$.

$\mathrm{GL}_2(\mathbb{Z})$ again acts on these forms by linear substitution.

There are now two polynomial invariants for this action, traditionally denoted I and J, where:

$$I(f) = 12ae - 3bd + c^2,$$

$$J(f) = 72ace + 9bcd - 27ad^2 - 27eb^2 - 2c^3.$$

Again, if you fix both I and J, then there exist only finitely many $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of integral binary quartic forms having this value of (I, J).

Counting binary forms: quartic forms

The next natural case is that of binary quartic forms $f(x,y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4$, $a,b,c,d,e \in \mathbb{Z}$.

$\mathrm{GL}_2(\mathbb{Z})$ again acts on these forms by linear substitution.

There are now two polynomial invariants for this action, traditionally denoted I and J, where:

$$I(f) = 12ae - 3bd + c^2,$$

$$J(f) = 72ace + 9bcd - 27ad^2 - 27eb^2 - 2c^3.$$

Again, if you fix both I and J, then there exist only finitely many $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of integral binary quartic forms having this value of (I, J).

On average, how many classes $h_{I,J}$ of irreducible binary quartic forms are there having given invariants I and J?

Counting binary forms: quartic forms

The next natural case is that of binary quartic forms $f(x,y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4, \;\; a,b,c,d,e \in \mathbb{Z}$.

$\mathrm{GL}_2(\mathbb{Z})$ again acts on these forms by linear substitution.

There are now two polynomial invariants for this action, traditionally denoted I and J, where:

$$I(f) = 12ae - 3bd + c^2,$$

$$J(f) = 72ace + 9bcd - 27ad^2 - 27eb^2 - 2c^3.$$

Again, if you fix both I and J, then there exist only finitely many $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of integral binary quartic forms having this value of (I,J).

On average, how many classes $h_{I,J}$ of irreducible binary quartic forms are there having given invariants I and J? Equivalently, how many equivalence classes of binary quartic forms are there having bounded I and J?

Counting binary quartic forms

We define the height $H(f)$ of a binary quartic form f by:

$$H(f) := H(I, J) := \max\{|I^3|, J^2/4\}$$

Counting binary quartic forms

We define the height $H(f)$ of a binary quartic form f by:

$$H(f) := H(I, J) := \max\{|I^3|, J^2/4\}$$

How many equivalence classes of quartics f have $H(f) < X$?

Counting binary quartic forms

We define the height $H(f)$ of a binary quartic form f by:

$$H(f) := H(I,J) := \max\{|I^3|, J^2/4\}$$

How many equivalence classes of quartics f have $H(f) < X$?

Works of Julia, Cremona, Stoll, Yukie, Yang each imply that this number is $O(X^{5/6+\epsilon})$.

Counting binary quartic forms

We define the height $H(f)$ of a binary quartic form f by:

$$H(f) := H(I, J) := \max\{|I^3|, J^2/4\}$$

How many equivalence classes of quartics f have $H(f) < X$?

Works of Julia, Cremona, Stoll, Yukie, Yang each imply that this number is $O(X^{5/6+\epsilon})$. Almost any reduction theory method implies this immediately.

Counting binary quartic forms

We define the height $H(f)$ of a binary quartic form f by:

$$H(f) := H(I,J) := \max\{|I^3|, J^2/4\}$$

How many equivalence classes of quartics f have $H(f) < X$?

Works of Julia, Cremona, Stoll, Yukie, Yang each imply that this number is $O(X^{5/6+\epsilon})$. Almost any reduction theory method implies this immediately.

Theorem.

(a) $$\sum_{\substack{H(I,J)<X \\ \mathrm{Disc}(I,J)>0}} h(I,J) \sim \frac{12}{135}\zeta(2) \cdot X^{5/6};$$

Counting binary quartic forms

We define the height $H(f)$ of a binary quartic form f by:

$$H(f) := H(I,J) := \max\{|I^3|, J^2/4\}$$

How many equivalence classes of quartics f have $H(f) < X$?

Works of Julia, Cremona, Stoll, Yukie, Yang each imply that this number is $O(X^{5/6+\epsilon})$. Almost any reduction theory method implies this immediately.

Theorem.

(a) $$\sum_{\substack{H(I,J)<X \\ \mathrm{Disc}(I,J)>0}} h(I,J) \sim \frac{12}{135}\zeta(2)\cdot X^{5/6};$$

(b) $$\sum_{\substack{H(I,J)<X \\ \mathrm{Disc}(I,J)<0}} h(I,J) \sim \frac{32}{135}\zeta(2)\cdot X^{5/6}.$$

Counting binary quartic forms

We define the height $H(f)$ of a binary quartic form f by:

$$H(f) := H(I,J) := \max\{|I^3|, J^2/4\}$$

How many equivalence classes of quartics f have $H(f) < X$?

Works of Julia, Cremona, Stoll, Yukie, Yang each imply that this number is $O(X^{5/6+\epsilon})$. Almost any reduction theory method implies this immediately.

Theorem.

(a) $$\sum_{\substack{H(I,J)<X \\ \mathrm{Disc}(I,J)>0}} h(I,J) \sim \frac{12}{135}\zeta(2)\cdot X^{5/6};$$

(b) $$\sum_{\substack{H(I,J)<X \\ \mathrm{Disc}(I,J)<0}} h(I,J) \sim \frac{32}{135}\zeta(2)\cdot X^{5/6}.$$

How many classes do we get per (I,J)?

Eligible (I, J)

Eligible (I, J)

We say that a pair $(I, J) \in \mathbb{Z} \times \mathbb{Z}$ is eligible if it occurs as the invariants of some integer binary quartic form.

Eligible (I, J)

We say that a pair $(I, J) \in \mathbb{Z} \times \mathbb{Z}$ is eligible if it occurs as the invariants of some integer binary quartic form. In fact, the set of eligible (I, J) is defined purely by congruences.

Eligible (I, J)

We say that a pair $(I, J) \in \mathbb{Z} \times \mathbb{Z}$ is eligible if it occurs as the invariants of some integer binary quartic form. In fact, the set of eligible (I, J) is defined purely by congruences.

These congruence conditions are:

(a) $I \equiv 0 \pmod 3$ and $J \equiv 0 \pmod{27}$,

(b) $I \equiv 1 \pmod 9$ and $J \equiv \pm 2 \pmod{27}$,

(c) $I \equiv 4 \pmod 9$ and $J \equiv \pm 16 \pmod{27}$,

(d) $I \equiv 7 \pmod 9$ and $J \equiv \pm 7 \pmod{27}$.

Eligible (I, J)

We say that a pair $(I, J) \in \mathbb{Z} \times \mathbb{Z}$ is eligible if it occurs as the invariants of some integer binary quartic form. In fact, the set of eligible (I, J) is defined purely by congruences.

These congruence conditions are:

(a) $I \equiv 0 \pmod 3$ and $J \equiv 0 \pmod{27}$,

(b) $I \equiv 1 \pmod 9$ and $J \equiv \pm 2 \pmod{27}$,

(c) $I \equiv 4 \pmod 9$ and $J \equiv \pm 16 \pmod{27}$,

(d) $I \equiv 7 \pmod 9$ and $J \equiv \pm 7 \pmod{27}$.

The number of eligible (I, J) having height less than X is thus a constant times $X^{5/6}$.

Eligible (I, J)

We say that a pair $(I, J) \in \mathbb{Z} \times \mathbb{Z}$ is eligible if it occurs as the invariants of some integer binary quartic form. In fact, the set of eligible (I, J) is defined purely by congruences.

These congruence conditions are:

(a) $I \equiv 0 \pmod 3$ and $J \equiv 0 \pmod{27}$,

(b) $I \equiv 1 \pmod 9$ and $J \equiv \pm 2 \pmod{27}$,

(c) $I \equiv 4 \pmod 9$ and $J \equiv \pm 16 \pmod{27}$,

(d) $I \equiv 7 \pmod 9$ and $J \equiv \pm 7 \pmod{27}$.

The number of eligible (I, J) having height less than X is thus a constant times $X^{5/6}$. (In fact, $\frac{8}{27} \cdot X^{5/6}$.)

The average number of binary quartic forms per (I, J)

We may thus average the number of $\mathrm{GL}_2(\mathbb{Z})$-orbits of binary quartics over eligible pairs (I, J).

We may thus average the number of $\mathrm{GL}_2(\mathbb{Z})$-orbits of binary quartics over eligible pairs (I, J).

Theorem.

(a) The average number of positive discriminant binary quartic forms per eligible (I, J) is $3\zeta(2)/2$.

We may thus average the number of $\mathrm{GL}_2(\mathbb{Z})$-orbits of binary quartics over eligible pairs (I, J).

Theorem.

(a) The average number of positive discriminant binary quartic forms per eligible (I, J) is $3\zeta(2)/2$.

(b) The average number of negative discriminant binary quartic forms per eligible (I, J) is $\zeta(2)$.

We may thus average the number of $\mathrm{GL}_2(\mathbb{Z})$-orbits of binary quartics over eligible pairs (I, J).

Theorem.

(a) The average number of positive discriminant binary quartic forms per eligible (I, J) is $3\zeta(2)/2$.

(b) The average number of negative discriminant binary quartic forms per eligible (I, J) is $\zeta(2)$.

The analogous theorems can be proven for equivalence classes of binary quartic forms satisfying any desired finite set of congruence conditions.

Back to elliptic curves!

Back to elliptic curves!

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

Back to elliptic curves!

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

- Given $A, B \in \mathbb{Z}$, choose an integral binary quartic form f for each element of $S^{(2)}(E_{A,B})$, such that

Back to elliptic curves!

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

- Given $A, B \in \mathbb{Z}$, 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 $\mathbb{Q}$;

Back to elliptic curves!

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

- Given $A, B \in \mathbb{Z}$, 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 invariants $(I(f), J(f))$ agree with the invariants (A, B) of the elliptic curve (at least away from 2 and 3);

Back to elliptic curves!

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

- Given $A, B \in \mathbb{Z}$, 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 invariants $(I(f), J(f))$ agree with the invariants (A, B) of the elliptic curve (at least away from 2 and 3);

  The construction of such a set of binary quartic forms follows from the work of Birch and Swinnerton-Dyer.

Back to elliptic curves!

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

- Given $A, B \in \mathbb{Z}$, 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 invariants $(I(f), J(f))$ agree with the invariants (A, B) of the elliptic curve (at least away from 2 and 3);

  The construction of such a set of binary quartic forms follows from the work of Birch and Swinnerton-Dyer.

- Count these integral binary quartic forms.

Back to elliptic curves!

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

- Given $A, B \in \mathbb{Z}$, 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 invariants $(I(f), J(f))$ agree with the invariants (A, B) of the elliptic curve (at least away from 2 and 3);

  The construction of such a set of binary quartic forms follows from the work of Birch and Swinnerton-Dyer.

- Count these integral binary quartic forms. These are defined by infinitely many congruence conditions, so a sieve has to be performed.

Back to elliptic curves!

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

- Given $A, B \in \mathbb{Z}$, 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 invariants $(I(f), J(f))$ agree with the invariants (A, B) of the elliptic curve (at least away from 2 and 3);

  The construction of such a set of binary quartic forms follows from the work of Birch and Swinnerton-Dyer.

- Count these integral binary quartic forms. These are defined by infinitely many congruence conditions, so a sieve has to be performed. A uniformity estimate must be proven to perform this sieve, and that is by far the most technical part of this work.

Back to elliptic curves!

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

- Given $A, B \in \mathbb{Z}$, 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 invariants $(I(f), J(f))$ agree with the invariants (A, B) of the elliptic curve (at least away from 2 and 3);

  The construction of such a set of binary quartic forms follows from the work of Birch and Swinnerton-Dyer.

- Count these integral binary quartic forms. These are defined by infinitely many congruence conditions, so a sieve has to be performed. A uniformity estimate must be proven to perform this sieve, and that is by far the most technical part of this work. It involves counting integral points in much bigger spaces than binary quartic forms!

In particular, we must count points of bounded invariants in a certain nonreductive coregular space of dimension 12.

Average Size of 2-Selmer

In particular, we must count points of bounded invariants in a certain nonreductive coregular space of dimension 12.

Once this count is performed, the uniformity estimate proven, and then the sieve carried out, we finally obtain:

In particular, we must count points of bounded invariants in a certain nonreductive coregular space of dimension 12.

Once this count is performed, the uniformity estimate proven, and then the sieve carried out, we finally obtain:

Theorem. *When all elliptic curves $E/\mathbb{Q}$ (in any family defined by finitely many congruence conditions) are ordered by height, the average size of the* 2*-Selmer group* $S^{(2)}(E)$ *is* 3*.*

Average Size of 2-Selmer

In particular, we must count points of bounded invariants in a certain nonreductive coregular space of dimension 12.

Once this count is performed, the uniformity estimate proven, and then the sieve carried out, we finally obtain:

Theorem. *When all elliptic curves $E/\mathbb{Q}$ (in any family defined by finitely many congruence conditions) are ordered by height, the average size of the 2-Selmer group $S^{(2)}(E)$ is 3.*

Corollary. *When all elliptic curves $E/\mathbb{Q}$ (in any family defined by finitely many congruence conditions) are ordered by height, the average rank is at most 1.5.*

What about 3-Selmer?

We may also determine the average size of the 3-Selmer group of elliptic curves!

What about 3-Selmer?

We may also determine the average size of the 3-Selmer group of elliptic curves!

The set of 3-Selmer elements of elliptic curves is parametrized by 3-coverings, which may in turn be parametrized by appropriate $\mathrm{GL}_3(\mathbb{Q})$-orbits of integer ternary cubic forms.

What about 3-Selmer?

We may also determine the average size of the 3-Selmer group of elliptic curves!

The set of 3-Selmer elements of elliptic curves is parametrized by 3-coverings, which may in turn be parametrized by appropriate $\mathrm{GL}_3(\mathbb{Q})$-orbits of integer ternary cubic forms. (This follows from a result of Cassels.)

What about 3-Selmer?

We may also determine the average size of the 3-Selmer group of elliptic curves!

The set of 3-Selmer elements of elliptic curves is parametrized by 3-coverings, which may in turn be parametrized by appropriate $\mathrm{GL}_3(\mathbb{Q})$-orbits of integer ternary cubic forms. (This follows from a result of Cassels.)

The analogous "minimization" results of BSD over the integers have been proven by Cremona, Fisher, and Stoll in this case.

What about 3-Selmer?

We may also determine the average size of the 3-Selmer group of elliptic curves!

The set of 3-Selmer elements of elliptic curves is parametrized by 3-coverings, which may in turn be parametrized by appropriate $\mathrm{GL}_3(\mathbb{Q})$-orbits of integer ternary cubic forms. (This follows from a result of Cassels.)

The analogous "minimization" results of BSD over the integers have been proven by Cremona, Fisher, and Stoll in this case.

Proceeding in an analogous way (though now the dimension of the basic space is much bigger!), we show:

What about 3-Selmer?

We may also determine the average size of the 3-Selmer group of elliptic curves!

The set of 3-Selmer elements of elliptic curves is parametrized by 3-coverings, which may in turn be parametrized by appropriate $\mathrm{GL}_3(\mathbb{Q})$-orbits of integer ternary cubic forms. (This follows from a result of Cassels.)

The analogous "minimization" results of BSD over the integers have been proven by Cremona, Fisher, and Stoll in this case.

Proceeding in an analogous way (though now the dimension of the basic space is much bigger!), we show:

Theorem. *When all elliptic curves $E/\mathbb{Q}$ (in any family defined by finitely many congruence conditions) are ordered by height, the mean size of $S^{(3)}(E)$ is 4.*

What about 3-Selmer?

We may also determine the average size of the 3-Selmer group of elliptic curves!

The set of 3-Selmer elements of elliptic curves is parametrized by 3-coverings, which may in turn be parametrized by appropriate $\mathrm{GL}_3(\mathbb{Q})$-orbits of integer ternary cubic forms. (This follows from a result of Cassels.)

The analogous "minimization" results of BSD over the integers have been proven by Cremona, Fisher, and Stoll in this case.

Proceeding in an analogous way (though now the dimension of the basic space is much bigger!), we show:

Theorem. *When all elliptic curves $E/\mathbb{Q}$ (in any family defined by finitely many congruence conditions) are ordered by height, the mean size of $S^{(3)}(E)$ is 4.*

Corollary. *When all elliptic curves $E/\mathbb{Q}$ (in any family defined by finitely many congruence conditions) are ordered by height, the average rank is less than 1.17.*

Some consequences

Consider the family $\mathcal{F}$ of elliptic curves E that satisfy the following mild conditions.

Some consequences

Consider the family $\mathcal{F}$ of elliptic curves E that satisfy the following mild conditions.

- The curve E and its twist by -1 both have additive reduction at 2.
- The j-invariant of the curve E is a 2-adic unit.
- The curve E has good ordinary reduction at 3.
- The odd part of the discriminant of E is squarefree and congruent to 1 mod 4.

Some consequences

Consider the family $\mathcal{F}$ of elliptic curves E that satisfy the following mild conditions.

- The curve E and its twist by -1 both have additive reduction at 2.
- The j-invariant of the curve E is a 2-adic unit.
- The curve E has good ordinary reduction at 3.
- The odd part of the discriminant of E is squarefree and congruent to 1 mod 4.

It is easy to show that curves satisfying these conditions consist of a positive proportion of all elliptic curves.

Some consequences

Consider the family $\mathcal{F}$ of elliptic curves E that satisfy the following mild conditions.

- The curve E and its twist by -1 both have additive reduction at 2.
- The j-invariant of the curve E is a 2-adic unit.
- The curve E has good ordinary reduction at 3.
- The odd part of the discriminant of E is squarefree and congruent to 1 mod 4.

It is easy to show that curves satisfying these conditions consist of a positive proportion of all elliptic curves.

Furthermore, our results about 3-Selmer also apply to this family.

Some consequences

Consider the family $\mathcal{F}$ of elliptic curves E that satisfy the following mild conditions.

- The curve E and its twist by -1 both have additive reduction at 2.
- The j-invariant of the curve E is a 2-adic unit.
- The curve E has good ordinary reduction at 3.
- The odd part of the discriminant of E is squarefree and congruent to 1 mod 4.

It is easy to show that curves satisfying these conditions consist of a positive proportion of all elliptic curves.

Furthermore, our results about 3-Selmer also apply to this family.

Suppose $E \in \mathcal{F}$. Then E twisted by -1 is also in $\mathcal{F}$,

Some consequences

Consider the family $\mathcal{F}$ of elliptic curves E that satisfy the following mild conditions.

- The curve E and its twist by -1 both have additive reduction at 2.
- The j-invariant of the curve E is a 2-adic unit.
- The curve E has good ordinary reduction at 3.
- The odd part of the discriminant of E is squarefree and congruent to 1 mod 4.

It is easy to show that curves satisfying these conditions consist of a positive proportion of all elliptic curves.

Furthermore, our results about 3-Selmer also apply to this family.

Suppose $E \in \mathcal{F}$. Then E twisted by -1 is also in $\mathcal{F}$, and furthermore, the analytic root numbers of E and its twist by -1 are different.

Some consequences

Consider the family $\mathcal{F}$ of elliptic curves E that satisfy the following mild conditions.

- The curve E and its twist by -1 both have additive reduction at 2.
- The j-invariant of the curve E is a 2-adic unit.
- The curve E has good ordinary reduction at 3.
- The odd part of the discriminant of E is squarefree and congruent to 1 mod 4.

It is easy to show that curves satisfying these conditions consist of a positive proportion of all elliptic curves.

Furthermore, our results about 3-Selmer also apply to this family.

Suppose $E \in \mathcal{F}$. Then E twisted by -1 is also in $\mathcal{F}$, and furthermore, the analytic root numbers of E and its twist by -1 are different. Therefore, exactly half the root numbers of curves in $\mathcal{F}$ are $+1$.

Parity of p-Selmer rank

A recent result of Tim and Vladimir Dokchitser states that the parity of the p-Selmer rank of E is even iff the root number of E is $+1$!

Parity of p-Selmer rank

A recent result of Tim and Vladimir Dokchitser states that the parity of the p-Selmer rank of E is even iff the root number of E is $+1$!

Combining this with the fact that the 3-Selmer average is at most 4 in any family (e.g., $\mathcal{F}$), we are able to prove:

A recent result of Tim and Vladimir Dokchitser states that the parity of the p-Selmer rank of E is even iff the root number of E is $+1$!

Combining this with the fact that the 3-Selmer average is at most 4 in any family (e.g., $\mathcal{F}$), we are able to prove:

Theorem. *When all elliptic curves $E/\mathbb{Q}$ are ordered by height, a positive proportion of them have rank* 0*.*

Parity of p-Selmer rank

A recent result of Tim and Vladimir Dokchitser states that the parity of the p-Selmer rank of E is even iff the root number of E is $+1$!

Combining this with the fact that the 3-Selmer average is at most 4 in any family (e.g., $\mathcal{F}$), we are able to prove:

Theorem. *When all elliptic curves $E/\mathbb{Q}$ are ordered by height, a positive proportion of them have rank* 0.

Indeed, as the average number of 3-Selmer elements of curves in $\mathcal{F}$ is at most 4, it is not possible for all the curves with even 2-Selmer rank to have rank greater than 0.

Parity of p-Selmer rank

A recent result of Tim and Vladimir Dokchitser states that the parity of the p-Selmer rank of E is even iff the root number of E is $+1$!

Combining this with the fact that the 3-Selmer average is at most 4 in any family (e.g., $\mathcal{F}$), we are able to prove:

Theorem. *When all elliptic curves $E/\mathbb{Q}$ are ordered by height, a positive proportion of them have rank* 0.

Indeed, as the average number of 3-Selmer elements of curves in $\mathcal{F}$ is at most 4, it is not possible for all the curves with even 2-Selmer rank to have rank greater than 0. At least half of them must have rank 0!

Parity of p-Selmer rank

A recent result of Tim and Vladimir Dokchitser states that the parity of the p-Selmer rank of E is even iff the root number of E is $+1$!

Combining this with the fact that the 3-Selmer average is at most 4 in any family (e.g., $\mathcal{F}$), we are able to prove:

Theorem. *When all elliptic curves $E/\mathbb{Q}$ are ordered by height, a positive proportion of them have rank* 0*.*

Indeed, as the average number of 3-Selmer elements of curves in $\mathcal{F}$ is at most 4, it is not possible for all the curves with even 2-Selmer rank to have rank greater than 0. At least half of them must have rank 0!

A similar argument gives:

Parity of p-Selmer rank

A recent result of Tim and Vladimir Dokchitser states that the parity of the p-Selmer rank of E is even iff the root number of E is $+1$!

Combining this with the fact that the 3-Selmer average is at most 4 in any family (e.g., $\mathcal{F}$), we are able to prove:

Theorem. *When all elliptic curves $E/\mathbb{Q}$ are ordered by height, a positive proportion of them have rank* 0.

Indeed, as the average number of 3-Selmer elements of curves in $\mathcal{F}$ is at most 4, it is not possible for all the curves with even 2-Selmer rank to have rank greater than 0. At least half of them must have rank 0!

A similar argument gives:

Theorem. *Assume $Ш(E)$ is finite for all E. When all elliptic curves $E/\mathbb{Q}$ are ordered by height, a positive proportion of them have rank* 1.

Nonvanishing of elliptic curve L-functions

What about analytic rank?

What about analytic rank?

A recent result of Skinner–Urban states that if the L-function of an elliptic curve E vanishes at $s = 1$ and E has good ordinary reduction at 3, then the 3-Selmer group of E is nontrivial.

Nonvanishing of elliptic curve L-functions

What about analytic rank?

A recent result of Skinner–Urban states that if the L-function of an elliptic curve E vanishes at $s = 1$ and E has good ordinary reduction at 3, then the 3-Selmer group of E is nontrivial.

Combining this with the fact that the 3-Selmer average is at most 4 in any family (e.g., $\mathcal{F}$), we are able to prove:

Nonvanishing of elliptic curve L-functions

What about analytic rank?

A recent result of Skinner–Urban states that if the L-function of an elliptic curve E vanishes at $s = 1$ and E has good ordinary reduction at 3, then the 3-Selmer group of E is nontrivial.

Combining this with the fact that the 3-Selmer average is at most 4 in any family (e.g., $\mathcal{F}$), we are able to prove:

Theorem. *When all elliptic curves $E/\mathbb{Q}$ are ordered by height, a positive proportion of them have* analytic rank 0*;*

Nonvanishing of elliptic curve L-functions

What about analytic rank?

A recent result of Skinner–Urban states that if the L-function of an elliptic curve E vanishes at $s = 1$ and E has good ordinary reduction at 3, then the 3-Selmer group of E is nontrivial.

Combining this with the fact that the 3-Selmer average is at most 4 in any family (e.g., $\mathcal{F}$), we are able to prove:

Theorem. *When all elliptic curves $E/\mathbb{Q}$ are ordered by height, a positive proportion of them have* analytic rank 0*; that is, a positive proportion of elliptic curves have nonvanishing L-function at $s = 1$.*

Nonvanishing of elliptic curve L-functions

What about analytic rank?

A recent result of Skinner–Urban states that if the L-function of an elliptic curve E vanishes at $s = 1$ and E has good ordinary reduction at 3, then the 3-Selmer group of E is nontrivial.

Combining this with the fact that the 3-Selmer average is at most 4 in any family (e.g., $\mathcal{F}$), we are able to prove:

Theorem. *When all elliptic curves $E/\mathbb{Q}$ are ordered by height, a positive proportion of them have* analytic rank 0*; that is, a positive proportion of elliptic curves have nonvanishing L-function at $s = 1$.*

Corollary. *A positive proportion of elliptic curves satisfy the BSD rank conjecture.*

What about 4-Selmer and 5-Selmer?

What about 4-Selmer and 5-Selmer?

Elements in 4-Selmer and 5-Selmer groups of elliptic curves can be mapped to integer points, up to equivalence, having the corresponding invariants in the spaces

$$\mathbb{Z}^2 \otimes \mathrm{Sym}^2(\mathbb{Z}^4) \;\text{ and }\; \mathbb{Z}^5 \otimes \wedge^2\mathbb{Z}^5,$$

respectively.

What about 4-Selmer and 5-Selmer?

Elements in 4-Selmer and 5-Selmer groups of elliptic curves can be mapped to integer points, up to equivalence, having the corresponding invariants in the spaces

$$\mathbb{Z}^2 \otimes \mathrm{Sym}^2(\mathbb{Z}^4) \ \text{ and } \ \mathbb{Z}^5 \otimes \wedge^2\mathbb{Z}^5,$$

respectively. (This again can be deduced from work of Cassels, Cremona–Fisher–Stoll, and Fisher.)

What about 4-Selmer and 5-Selmer?

Elements in 4-Selmer and 5-Selmer groups of elliptic curves can be mapped to integer points, up to equivalence, having the corresponding invariants in the spaces

$$\mathbb{Z}^2 \otimes \mathrm{Sym}^2(\mathbb{Z}^4) \text{ and } \mathbb{Z}^5 \otimes \wedge^2\mathbb{Z}^5,$$

respectively. (This again can be deduced from work of Cassels, Cremona–Fisher–Stoll, and Fisher.)

Counting points in these spaces should thus similarly lead to the analogous results for 4-Selmer and 5-Selmer.

What about 4-Selmer and 5-Selmer?

Elements in 4-Selmer and 5-Selmer groups of elliptic curves can be mapped to integer points, up to equivalence, having the corresponding invariants in the spaces

$$\mathbb{Z}^2 \otimes \mathrm{Sym}^2(\mathbb{Z}^4) \text{ and } \mathbb{Z}^5 \otimes \wedge^2\mathbb{Z}^5,$$

respectively. (This again can be deduced from work of Cassels, Cremona–Fisher–Stoll, and Fisher.)

Counting points in these spaces should thus similarly lead to the analogous results for 4-Selmer and 5-Selmer. However, cusps are extremely complicated.

What about 4-Selmer and 5-Selmer?

Elements in 4-Selmer and 5-Selmer groups of elliptic curves can be mapped to integer points, up to equivalence, having the corresponding invariants in the spaces

$$\mathbb{Z}^2 \otimes \mathrm{Sym}^2(\mathbb{Z}^4) \text{ and } \mathbb{Z}^5 \otimes \wedge^2\mathbb{Z}^5,$$

respectively. (This again can be deduced from work of Cassels, Cremona–Fisher–Stoll, and Fisher.)

Counting points in these spaces should thus similarly lead to the analogous results for 4-Selmer and 5-Selmer. However, cusps are extremely complicated. (These spaces are 20- and 50-dimensional, respectively, with about 1000 cuspidal regions to deal with!)

What about 4-Selmer and 5-Selmer?

Elements in 4-Selmer and 5-Selmer groups of elliptic curves can be mapped to integer points, up to equivalence, having the corresponding invariants in the spaces

$$\mathbb{Z}^2 \otimes \mathrm{Sym}^2(\mathbb{Z}^4) \text{ and } \mathbb{Z}^5 \otimes \wedge^2\mathbb{Z}^5,$$

respectively. (This again can be deduced from work of Cassels, Cremona–Fisher–Stoll, and Fisher.)

Counting points in these spaces should thus similarly lead to the analogous results for 4-Selmer and 5-Selmer. However, cusps are extremely complicated. (These spaces are 20- and 50-dimensional, respectively, with about 1000 cuspidal regions to deal with!)

What about 4-Selmer and 5-Selmer?

Dealing with these issues, we are finally able to prove:

What about 4-Selmer and 5-Selmer?

Dealing with these issues, we are finally able to prove:

Theorem. *When all elliptic curves* $E/\mathbb{Q}$ *(in any family defined by finitely many congruence conditions) are ordered by height, the mean size of* $S^{(4)}(E)$ *is* 7.

What about 4-Selmer and 5-Selmer?

Dealing with these issues, we are finally able to prove:

Theorem. *When all elliptic curves $E/\mathbb{Q}$ (in any family defined by finitely many congruence conditions) are ordered by height, the mean size of $S^{(4)}(E)$ is 7.*

Theorem. *When all elliptic curves $E/\mathbb{Q}$ (in any family defined by finitely many congruence conditions) are ordered by height, the mean size of $S^{(5)}(E)$ is 6.*

What about 4-Selmer and 5-Selmer?

Dealing with these issues, we are finally able to prove:

Theorem. *When all elliptic curves $E/\mathbb{Q}$ (in any family defined by finitely many congruence conditions) are ordered by height, the mean size of $S^{(4)}(E)$ is 7.*

Theorem. *When all elliptic curves $E/\mathbb{Q}$ (in any family defined by finitely many congruence conditions) are ordered by height, the mean size of $S^{(5)}(E)$ is 6.*

Using the last theorem, together with a more careful analysis of changing of root numbers under twisting, we can now prove:

What about 4-Selmer and 5-Selmer?

Dealing with these issues, we are finally able to prove:

Theorem. *When all elliptic curves $E/\mathbb{Q}$ (in any family defined by finitely many congruence conditions) are ordered by height, the mean size of $S^{(4)}(E)$ is 7.*

Theorem. *When all elliptic curves $E/\mathbb{Q}$ (in any family defined by finitely many congruence conditions) are ordered by height, the mean size of $S^{(5)}(E)$ is 6.*

Using the last theorem, together with a more careful analysis of changing of root numbers under twisting, we can now prove:

Corollary. *When all elliptic curves $E/\mathbb{Q}$ are ordered by height, the average rank is less than 1.*

Some final remarks

Similar counting techniques applied to various other (coregular) spaces should eventually lead to densities of other data associated to elliptic curves and related algebraic and geometric objects.

Some final remarks

Similar counting techniques applied to various other (coregular) spaces should eventually lead to densities of other data associated to elliptic curves and related algebraic and geometric objects.

There are about 50 such spaces that parametrize genus one curves

Some final remarks

Similar counting techniques applied to various other (coregular) spaces should eventually lead to densities of other data associated to elliptic curves and related algebraic and geometric objects.

There are about 50 such spaces that parametrize genus one curves with extra data (joint work with Wei Ho).

Some final remarks

Similar counting techniques applied to various other (coregular) spaces should eventually lead to densities of other data associated to elliptic curves and related algebraic and geometric objects.

There are about 50 such spaces that parametrize genus one curves with extra data (joint work with Wei Ho).

There are several such spaces that parametrize various data corresponding to higher genus curves (Dick Gross, Wei Ho, Sam Stevens, Jack Thorne, . . .).