Distribution of ranks of elliptic curves

Frank Thorne

University of Wisconsin - Madison

February 12, 2007

Goldfeld's Conjecture

Conjecture (Goldfeld)

Half of all elliptic curves have rank 0, half have rank 1, and the rest have rank ≥ 2.

Goldfeld's Conjecture

Conjecture (Goldfeld)

Half of all elliptic curves have rank 0, half have rank 1, and the rest have rank ≥ 2.

Questions:

Goldfeld's Conjecture

Conjecture (Goldfeld)

Half of all elliptic curves have rank 0, half have rank 1, and the rest have rank ≥ 2.

Questions:

- What are "half of all elliptic curves?"

Goldfeld's Conjecture

Conjecture (Goldfeld)

Half of all elliptic curves have rank 0, half have rank 1, and the rest have rank ≥ 2.

Questions:

- What are "half of all elliptic curves?"
- Why would we believe such a claim?

Ranks in families

- Understand distribution of ranks of elliptic curves.

Ranks in families

- Understand distribution of ranks of elliptic curves.
- If we write down some list $E_1, E_2, \ldots,$ we want to show

$$\sum_{i \leq X} \mathrm{rk}\ E_i \sim f(X)$$

$$\{i \leq X : \mathrm{rk}\ E_i = r\} \sim g(X)$$

for suitable functions f, g.

Natural Questions

- How should we order such a list?

Natural Questions

- How should we order such a list?
- What do we expect, and what can we prove?

Natural Questions

- How should we order such a list?
- What do we expect, and what can we prove?
- What about quantities related to the rank?

(i.e., analytic rank, the parity, Selmer ranks, etc.)

Families of curves: quadratic twists

Let

$$E: \ y^2 = x^3 + ax + b$$

be an elliptic curve. The *D-quadratic twist of E* is

$$E(D): \ Dy^2 = x^3 + ax + b$$

where D is a fundamental discriminant. This family...

Families of curves: quadratic twists

Let

$$E: \; y^2 = x^3 + ax + b$$

be an elliptic curve. The *D-quadratic twist of E* is

$$E(D): \; Dy^2 = x^3 + ax + b$$

where D is a fundamental discriminant. This family...

- will not include all elliptic curves, but...

Families of curves: quadratic twists

Let

$$E: \; y^2 = x^3 + ax + b$$

be an elliptic curve. The *D-quadratic twist of E* is

$$E(D): \; Dy^2 = x^3 + ax + b$$

where D is a fundamental discriminant. This family...

- will not include all elliptic curves, but...
- is accessible for reasons we'll see.

Height and conductor

The *height* of $E: \ y^2 = x^3 + ax + b$ is

$$\max(|a|^3, |b|^2).$$

With an appropriate minimality condition, every elliptic curve occurs exactly once.

Height and conductor

The *height* of $E: \ y^2 = x^3 + ax + b$ is

$$\max(|a|^3, |b|^2).$$

With an appropriate minimality condition, every elliptic curve occurs exactly once.
Can we prove results ordering by height or conductor?

Height and conductor

The *height* of $E: \; y^2 = x^3 + ax + b$ is

$$\max(|a|^3, |b|^2).$$

With an appropriate minimality condition, every elliptic curve occurs exactly once.
Can we prove results ordering by height or conductor?
Some anyway... (we won't concentrate on these)

Algebraic families

Let $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Z}[t]$. Consider

$$y^2 + a_1(t)xy + a_3(t)y = x^3 + a_2(t)x^2 + a_4(t)x + a_6(t).$$

This defines an *algebraic family* : for almost all $t \in \mathbb{Z}$ this defines an elliptic curve.

Algebraic families

Let $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Z}[t]$. Consider

$$y^2 + a_1(t)xy + a_3(t)y = x^3 + a_2(t)x^2 + a_4(t)x + a_6(t).$$

This defines an *algebraic family* : for almost all $t \in \mathbb{Z}$ this defines an elliptic curve.

If you know a lot of algebraic geometry, you can get results.

Basic principles: related quantities

Often quantities related to the rank are easier to study, such as:

Basic principles: related quantities

Often quantities related to the rank are easier to study, such as:

- Analytic ranks and parity

Basic principles: related quantities

Often quantities related to the rank are easier to study, such as:

- Analytic ranks and parity
- p-ranks and Selmer groups.

Analytic rank

Definition

If E is an elliptic curve over $\mathbb{Q}$ and $L(E,s)$ is the associated L-function, then the *analytic rank* of E is

$$\mathrm{ord}_{s=1}\, L(E,s).$$

Analytic rank

Definition

If E is an elliptic curve over $\mathbb{Q}$ and $L(E, s)$ is the associated L-function, then the *analytic rank* of E is

$$\mathrm{ord}_{s=1}\ L(E, s).$$

Conjecture (Birch and Swinnerton-Dyer)

$$\mathrm{rk}\ E = \mathrm{ord}_{s=1}\ L(E, s).$$

Parities of analytic ranks

Theorem

Given an elliptic curve E with conductor $N(E)$. Assume D is a fundamental discriminant. Then the analytic ranks of E and $E(D)$ have the same parity if and only if $\left(\frac{D}{-N}\right) = 1$.

Analytic ranks and parity

Proof:

If the L-series of E is

$$L(E, s) = \sum_n a_n n^{-s},$$

then we have

$$L(E(D), s) = \sum_n a_n \left(\frac{D}{n} \right) n^{-s}.$$

Analytic ranks and parity

Proof:

If the L-series of E is

$$L(E, s) = \sum_n a_n n^{-s},$$

then we have

$$L(E(D), s) = \sum_n a_n \left(\frac{D}{n}\right) n^{-s}.$$

Why? Look at

$$E : y^2 = x^3 + ax + b$$

$$E(D) : Dy^2 = x^3 + ax + b.$$

Analytic ranks and parity

Proof:

If the L-series of E is

$$L(E, s) = \sum_{n} a_n n^{-s},$$

then we have

$$L(E(D), s) = \sum_{n} a_n \left(\frac{D}{n}\right) n^{-s}.$$

Why? Look at

$$E : y^2 = x^3 + ax + b$$

$$E(D) : Dy^2 = x^3 + ax + b.$$

How to compute a_p? Look for solutions in $\mathbb{F}_p$.

Analytic ranks and parity

Proof:

If the L-series of E is

$$L(E, s) = \sum_n a_n n^{-s},$$

then we have

$$L(E(D), s) = \sum_n a_n \left(\frac{D}{n}\right) n^{-s}.$$

Why? Look at

$$E : y^2 = x^3 + ax + b$$

$$E(D) : Dy^2 = x^3 + ax + b.$$

How to compute a_p? Look for solutions in $\mathbb{F}_p$.

Is D is a square in $\mathbb{F}_p$?

The root number

Our L-series have functional equations: Write

$$\Lambda(E,s) = L(E,s)(\sqrt{N}/2\pi)^{-s}\Gamma(s)$$

then

$$\Lambda(E,s) = \Lambda(E,2-s)\omega(E).$$

The *root number* $\omega(E) = \pm 1$ determines the parity.

The root number

Our L-series have functional equations: Write

$$\Lambda(E,s) = L(E,s)(\sqrt{N}/2\pi)^{-s}\Gamma(s)$$

then

$$\Lambda(E,s) = \Lambda(E,2-s)\omega(E).$$

The *root number* $\omega(E) = \pm 1$ determines the parity.
By the theory of modular forms,

$$\omega(E) = \omega(E(D))\left(\frac{D}{-N}\right).$$

So, quadratic twists are split evenly between even and odd analytic rank.

The Kummer exact sequence

The *Kummer exact sequence* is

$$0 \to E/pE \to S_p(E) \to Sha[p] \to 0.$$

The Kummer exact sequence

The *Kummer exact sequence* is

$$0 \to E/pE \to S_p(E) \to Sha[p] \to 0.$$

- E/pE is the p-rank of E,

The Kummer exact sequence

The *Kummer exact sequence* is

$$0 \to E/pE \to S_p(E) \to Sha[p] \to 0.$$

- E/pE is the p-rank of E,
- $S_p(E)$ is the p-Selmer group,

The Kummer exact sequence

The *Kummer exact sequence* is

$$0 \to E/pE \to S_p(E) \to Sha[p] \to 0.$$

- E/pE is the p-rank of E,
- $S_p(E)$ is the p-Selmer group,
- $Sha[p]$, defined by this exact sequence, is the p-part of the Shafarevich-Tate group.

The Kummer exact sequence

The *Kummer exact sequence* is

$$0 \to E/pE \to S_p(E) \to Sha[p] \to 0.$$

- E/pE is the p-rank of E,
- $S_p(E)$ is the p-Selmer group,
- $Sha[p]$, defined by this exact sequence, is the p-part of the Shafarevich-Tate group.

So

$$\mathrm{rk}(E) + \mathrm{rk}_p(\mathrm{Tor}(E)) = rk_p S_p(E) - rk_p Sha[p].$$

The Kummer exact sequence (cont.)

Theorem

(Mazur). E doesn't have much p-torsion, and if $p \geq 11$ *it has none at all.*

The Kummer exact sequence (cont.)

Theorem

(Mazur). E doesn't have much p-torsion, and if $p \geq 11$ *it has none at all.*

Theorem

(Cassels, Tate [AEC X.4.14]) If the Shafarevich-Tate group is finite then its order is a square.

The Katz-Sarnak Philosophy

The object is to study the distribution of objects such as

- Zeroes of individual zeta and L-functions.

The Katz-Sarnak Philosophy

The object is to study the distribution of objects such as

- Zeroes of individual zeta and L-functions.
- Critical values of families of L-functions.

The Katz-Sarnak Philosophy

The object is to study the distribution of objects such as

- Zeroes of individual zeta and L-functions.
- Critical values of families of L-functions.

Big Idea: These distributions can be modeled by the theory of random matrices.

What is a random matrix?

Example: $SO(N)$.

What is a random matrix?

Example: $SO(N)$.
It is a *compact Lie group*,

What is a random matrix?

Example: $SO(N)$.
It is a *compact Lie group*, and therefore it has a *Haar measure* μ satisfying

What is a random matrix?

Example: $SO(N)$.
It is a *compact Lie group*, and therefore it has a *Haar measure* μ satisfying

- $\mu(SO(N)) = 1$,

What is a random matrix?

Example: $SO(N)$.
It is a *compact Lie group*, and therefore it has a *Haar measure* μ satisfying

- $\mu(SO(N)) = 1$,
- $\mu(X) = \mu(gX) = \mu(Xg)$ for any subset X and element g.

We think of μ as a *probability measure* on $SO(N)$.

A probability measure on $SO(N)$

A probability measure on $O(N)$ ($U(N)$, $Sp(N)$, etc.) lets us talk about:

- Expected distribution of eigenvalues on the unit circle

A probability measure on $SO(N)$

A probability measure on $O(N)$ ($U(N)$, $Sp(N)$, etc.) lets us talk about:

- Expected distribution of eigenvalues on the unit circle
- Moments of characteristic polynomials

A probability measure on $SO(N)$

A probability measure on $O(N)$ ($U(N)$, $Sp(N)$, etc.) lets us talk about:

- Expected distribution of eigenvalues on the unit circle
- Moments of characteristic polynomials
- Etc.

Why random matrices?

Analogy between number fields and function fields.

Why random matrices?

Analogy between number fields and function fields.

Theorem

For function fields, the Riemann Hypothesis is true.

Why random matrices?

Analogy between number fields and function fields.

Theorem

For function fields, the Riemann Hypothesis is true.

Proof: Give a *spectral interpretation* to the zeroes, in terms of eigenvalues of Frobenius acting on l-adic cohomology.

Why random matrices?

Analogy between number fields and function fields.

Theorem

For function fields, the Riemann Hypothesis is true.

Proof: Give a *spectral interpretation* to the zeroes, in terms of eigenvalues of Frobenius acting on l-adic cohomology.
This involves Galois representations into $GL(N)$ for appropriate N; the images are *monodromy groups* and are often nice: $SO(N), Sp(N), \ldots$

Why random matrices?

Analogy between number fields and function fields.

Theorem

For function fields, the Riemann Hypothesis is true.

Proof: Give a *spectral interpretation* to the zeroes, in terms of eigenvalues of Frobenius acting on l-adic cohomology.
This involves Galois representations into $GL(N)$ for appropriate N; the images are *monodromy groups* and are often nice:
$SO(N), Sp(N), \ldots$
These monodromy groups are related to statistics of the zeta functions.

Why random matrices?

Wild Speculation

All of the above is true for number fields too.

Why random matrices?

Wild Speculation

All of the above is true for number fields too.

Work of Katz-Sarnak, Rubinstein, and others uses this assumption to make predictions.

Ranks of elliptic curves

Conjecture

The values of $L(E(D), 1)$ as D varies are given by an orthogonal distribution.

In particular the L-values shouldn't be zero more often than they have to be.

Goldfeld's Conjecture

Conjecture (Goldfeld)

Fix any elliptic curve $E/\mathbb{Q}$. Then the sets of fundamental discriminants D for which the rank of $E(D)$ is 0 and 1 have density 1/2 each.

In other words, elliptic curves usually have the smallest rank possible.

Goldfeld's Conjecture

Conjecture (Goldfeld)

Fix any elliptic curve $E/\mathbb{Q}$. Then the sets of fundamental discriminants D for which the rank of $E(D)$ is 0 and 1 have density $1/2$ each.

In other words, elliptic curves usually have the smallest rank possible.

Is it true? See some data to the contrary compiled by Bektemirov, Mazur, Stein, and Watkins.

Conjecture for rank 2

Let

$$N_E(X) = \#\{|D| \leq X : \mathrm{rk}\ E(D) \geq 2, even\}.$$

$$N'_E(X) = \#\{|p| \leq X : \mathrm{rk}\ E(p) \geq 2, even\}.$$

Conjecture for rank 2

Let

$$N_E(X) = \#\{|D| \leq X : \mathrm{rk}\ E(D) \geq 2, even\}.$$

$$N'_E(X) = \#\{|p| \leq X : \mathrm{rk}\ E(p) \geq 2, even\}.$$

Conjecture (Conrey, Keating, Rubinstein, Snaith)

$$N'_E(X) \sim C_E X^{3/4} \log^{-5/8} X.$$

The power of log is complicated. So let's get the 3/4.

Derivation of $X^{3/4}$

Restrict to curves with even analytic rank. (Half of them)

Derivation of $X^{3/4}$

Restrict to curves with even analytic rank. (Half of them)
Katz-Sarnak philosophy says, the values $L(E(D), 1)$ follow an orthogonal distribution. But,

Derivation of $X^{3/4}$

Restrict to curves with even analytic rank. (Half of them)
Katz-Sarnak philosophy says, the values $L(E(D), 1)$ follow an orthogonal distribution. But, they are discretized!

Derivation of $X^{3/4}$

Restrict to curves with even analytic rank. (Half of them) Katz-Sarnak philosophy says, the values $L(E(D), 1)$ follow an orthogonal distribution. But, they are discretized!

Theorem (Waldspurger, Shimura, Kohnen-Zagier)

$$L(E(D), 1) = \kappa_E c_E(|D|)^2/\sqrt{D},$$

where the c_E are the *integer valued* coefficients of a certain half-integral weight modular form.

Ramanujan conjecture: $c_E(|D|) \ll |D|^{1/4+\epsilon}$.

Derivation of $X^{3/4}$

$L(E(D), 1)$ vanishes iff the Fourier coefficient $c_E(|D|)$ does.

Derivation of $X^{3/4}$

$L(E(D), 1)$ vanishes iff the Fourier coefficient $c_E(|D|)$ does.
If $c_E(|D|)$ can be as large as $|D|^{1/4}$, assume roughly equal distribution.

Derivation of $X^{3/4}$

$L(E(D), 1)$ vanishes iff the Fourier coefficient $c_E(|D|)$ does.
If $c_E(|D|)$ can be as large as $|D|^{1/4}$, assume roughly equal distribution.
Then approximately $X^{3/4}$ of the $c_E(|D|)$ will be zero.

The congruent number curve

The *congruent number elliptic curve* is

$$E : y^2 = x^3 - x$$

and its D-quadratic twist is

$$E(D) : y^2 = x^3 - D^2 x.$$

The congruent number curve

The *congruent number elliptic curve* is

$$E : y^2 = x^3 - x$$

and its D-quadratic twist is

$$E(D) : y^2 = x^3 - D^2 x.$$

For Heath-Brown's theorem, restrict to odd D.

Notation for Heath-Brown's theorem

Idea: study distribution of 2-Selmer ranks.

Notation for Heath-Brown's theorem

Idea: study distribution of 2-Selmer ranks.
The 2-*Selmer rank* $s(D)$ is defined by

$$2^{2+s(D)} = \#|S_2(E(D))|.$$

Notation for Heath-Brown's theorem

Idea: study distribution of 2-Selmer ranks.
The 2-*Selmer rank* $s(D)$ is defined by

$$2^{2+s(D)} = \#|S_2(E(D))|.$$

Here

- $S_2(E(D))$ is the 2-Selmer group,

Notation for Heath-Brown's theorem

Idea: study distribution of 2-Selmer ranks.
The 2-*Selmer rank* $s(D)$ is defined by

$$2^{2+s(D)} = \#|S_2(E(D))|.$$

Here

- $S_2(E(D))$ is the 2-Selmer group,
- We add 2 to $s(D)$ because of the 2-torsion.

Heath-Brown's Theorem

Theorem

For any integer $r \geq 0$, the set of quadratic twists $E(D)$ with D odd and $s(D) = r$ has density

$$2^r \delta(r, D) \prod_{n \geq 0} (1 - 2^{-2n-1}) \prod_{j=1}^{r} (2^j - 1)^{-1}.$$

Heath-Brown's Theorem

Theorem

For any integer $r \geq 0$, the set of quadratic twists $E(D)$ with D odd and $s(D) = r$ has density

$$2^r \delta(r, D) \prod_{n \geq 0} (1 - 2^{-2n-1}) \prod_{j=1}^{r} (2^j - 1)^{-1}.$$

$\delta(r, D)$ is 1 for r even and $D \equiv 1, 3 \mod 8$, or for r odd and $D \equiv 5, 7 \mod 8$, and $\delta(r, D) = 0$ otherwise.

Heath-Brown's Theorem (cont.)

Corollary

The density of curves considered with rank r has the above upper bound.

Heath-Brown's Theorem (cont.)

Corollary

The density of curves considered with rank r has the above upper bound.

The proof of the theorem follows by computing

$$\sum_D 2^{s(D)}$$

and (for $k \geq 2$)

$$\sum_D 2^{ks(D)}.$$

Heath-Brown's Theorem (cont.)

Corollary

The density of curves considered with rank r has the above upper bound.

The proof of the theorem follows by computing

$$\sum_D 2^{s(D)}$$

and (for $k \geq 2$)

$$\sum_D 2^{ks(D)}.$$

Remember, $2^{s(D)} = \frac{1}{4}\#|S_2(E(D))|$.

Computation of $\sum_D 2^{s(d)}$

By classical 2-descent theory, rational points on $E(D)$ correspond to systems

$$D_1 X^2 + D_4 W^2 = D_2 Y^2, \quad D_1 X^2 - D_4 W^2 = D_3 Z^2$$

with integer solutions.

Computation of $\sum_D 2^{s(d)}$

By classical 2-descent theory, rational points on $E(D)$ correspond to systems

$$D_1X^2 + D_4W^2 = D_2Y^2, \quad D_1X^2 - D_4W^2 = D_3Z^2$$

with integer solutions.
By definition, the 2-Selmer group is the number of such systems with p-adic solutions for all p.

Computation of $\sum_D 2^{s(d)}$

By classical 2-descent theory, rational points on $E(D)$ correspond to systems

$$D_1 X^2 + D_4 W^2 = D_2 Y^2, \quad D_1 X^2 - D_4 W^2 = D_3 Z^2$$

with integer solutions.

By definition, the 2-Selmer group is the number of such systems with p-adic solutions for all p.

This depends on whether certain quantities are squares mod p or not.

Computation of $\sum_D 2^{s(d)}$

By classical 2-descent theory, rational points on $E(D)$ correspond to systems

$$D_1 X^2 + D_4 W^2 = D_2 Y^2, \quad D_1 X^2 - D_4 W^2 = D_3 Z^2$$

with integer solutions.

By definition, the 2-Selmer group is the number of such systems with p-adic solutions for all p.

This depends on whether certain quantities are squares mod p or not. So we get to estimate character sums!

A character sum

We have

$$2^{s(D)} = \sum_{F} g(F)$$

A character sum

We have

$$2^{s(D)} = \sum_{F} g(F)$$

where F ranges over factorizations

$$D = \prod_{\substack{1 \leq i \leq 4, 0 \leq j \leq 4 \\ i \neq j}} D_{ij},$$

A character sum

We have

$$2^{s(D)} = \sum_F g(F)$$

where F ranges over factorizations

$$D = \prod_{\substack{1 \leq i \leq 4, 0 \leq j \leq 4 \\ i \neq j}} D_{ij},$$

$$g(F) := \left(\frac{-1}{D_{12} D_{14} D_{23} D_{21}} \right) \left(\frac{2}{D_{24} D_{21} D_{34} D_{41}} \right) \prod_{\substack{i; j \neq 0 \\ k \neq i, j; l}} 4^{-\omega(D_{i0}) - \omega(D_{ij})} \left(\frac{D_{kl}}{D_{ij}} \right).$$

Another character sum

The sum $\sum_D 2^{ks(D)}$ is even worse.

Constructive results

The idea: prove lower bounds by constructing a family of curves of a certain rank.

A Lower Bound for Rank 2

As before let

$$N_E(X) = \#\{|D| \leq X : \mathrm{rk}\ E(D) \geq 2, even\}.$$

A Lower Bound for Rank 2

As before let

$$N_E(X) = \#\{|D| \leq X : \mathrm{rk}\ E(D) \geq 2, even\}.$$

Theorem (Gouvêa-Mazur)

For any $E/\mathbb{Q}$,

$$N_E(X) \gg X^{1/2-\epsilon}.$$

Proof of Gouvêa-Mazur

If our curve is

$$E : y^2 = ax^3 + bx^2 + cx + d$$

write

$$F(u, v) = v(u^3 + au^2v + buv^2 + cv^3).$$

Proof of Gouvêa-Mazur

If our curve is

$$E : y^2 = ax^3 + bx^2 + cx + d$$

write

$$F(u, v) = v(u^3 + au^2v + buv^2 + cv^3).$$

By construction,

$$(u/v, 1/v^2) \in E(F(u, v))(\mathbb{Q}).$$

Proof of Gouvêa-Mazur

If our curve is

$$E : y^2 = ax^3 + bx^2 + cx + d$$

write

$$F(u, v) = v(u^3 + au^2v + buv^2 + cv^3).$$

By construction,

$$(u/v, 1/v^2) \in E(F(u, v))(\mathbb{Q}).$$

With only finitely many exceptions, *not a torsion point!*

Proof of Gouvêa-Mazur, cont.

Recall the parity principle as applied to root numbers:

$$\omega(E) = \omega(E(D))\left(\frac{D}{-N}\right).$$

By work of Cassels, etc., the parities of the algebraic ranks will be even in this case too.

Proof of Gouvêa-Mazur, continued

Thus, $E(D)$ will have even rank ≥ 2 whenever

- $\left(\frac{D}{-N}\right) = 1$ (or -1 in case E has even rank)

Proof of Gouvêa-Mazur, continued

Thus, $E(D)$ will have even rank ≥ 2 whenever

- $\left(\frac{D}{-N}\right) = 1$ (or -1 in case E has even rank)
- D is squarefree

Proof of Gouvêa-Mazur, continued

Thus, $E(D)$ will have even rank ≥ 2 whenever

- $\left(\frac{D}{-N}\right) = 1$ (or -1 in case E has even rank)
- D is squarefree
- $D = F(u, v)$ for some u and v.

The result follows by sieve methods.

Ono-Skinner's lower bound for rank 0

Write

$$N_{0,E}(X) = \#\{|D| \le X : \mathrm{rk}\ E(D) = 0\}.$$

Ono-Skinner's lower bound for rank 0

Write

$$N_{0,E}(X) = \#\{|D| \leq X : \mathrm{rk}\ E(D) = 0\}.$$

Theorem (Ono-Skinner)

We have

$$N_{0,E}(X) \gg X/\log X.$$

There are additional related results due to Ono.

Sketch proof of Ono-Skinner

Recall the formula of Waldspurger:

$$L(E(D), 1) = \kappa_E c_E(|D|)^2/\sqrt{D}$$

The c_E are Fourier coefficients of a weight $3/2$ modular form.

Sketch proof of Ono-Skinner

Recall the formula of Waldspurger:

$$L(E(D),1) = \kappa_E c_E(|D|)^2/\sqrt{D}$$

The c_E are Fourier coefficients of a weight $3/2$ modular form. We know that

$$L(E(D),1) \neq 0 \rightarrow \mathrm{rk}\ E = 0$$

and so can look for nonvanishing Fourier coefficients.

Sketch proof of Ono-Skinner (cont.)

- Multiply by an appropriate theta function to get an integer weight modular form F.

Sketch proof of Ono-Skinner (cont.)

- Multiply by an appropriate theta function to get an integer weight modular form F.
- Associate a Galois representation ρ to F using work of Deligne and Serre.

Sketch proof of Ono-Skinner (cont.)

- Multiply by an appropriate theta function to get an integer weight modular form F.
- Associate a Galois representation ρ to F using work of Deligne and Serre.
- Find *some* nonzero Fourier coefficient using work of Friedberg and Hoffstein.

Sketch proof of Ono-Skinner (cont.)

- Multiply by an appropriate theta function to get an integer weight modular form F.
- Associate a Galois representation ρ to F using work of Deligne and Serre.
- Find *some* nonzero Fourier coefficient using work of Friedberg and Hoffstein.
- Use surjectivity properties of ρ and Chebotarev Density to prove a lower bound for nonvanishing modulo a prime.