The Distribution of 2-Selmer Ranks of Quadratic Twists of Elliptic Curves.

Zev Klagsbrun

partially joint with Karl Rubin and Barry Mazur

Department of Mathematics
University of Wisconsin - Madison

September 27, 2012

Theorem (Heath-Brown 1994, Swinnerton-Dyer 2008, Kane 2011)

Suppose $E/\mathbb{Q}$ is an elliptic curve with $E(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ that does not have a cyclic 4-isogeny over $\mathbb{Q}$. Then for $r \geq 2$,

$$\lim_{X\to\infty} \frac{\#\{d \text{ squarefree}, |d| < X : \dim_{\mathbb{F}_2} \mathrm{Sel}_2(E^d/\mathbb{Q}) = r\}}{\#\{d \text{ squarefree}, |d| < X\}} = \alpha_r$$

- $\alpha_r > 0$ *explicit constants with* $\sum \alpha_r = 1$.

Theorem (Heath-Brown 1994, Swinnerton-Dyer 2008, Kane 2011)

Suppose $E/\mathbb{Q}$ is an elliptic curve with $E(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ that does not have a cyclic 4-isogeny over $\mathbb{Q}$. Then for $r \geq 2$,

$$\lim_{X\to\infty} \frac{\#\{d \text{ squarefree}, |d| < X : \dim_{\mathbb{F}_2} \mathrm{Sel}_2(E^d/\mathbb{Q}) = r\}}{\#\{d \text{ squarefree}, |d| < X\}} = \alpha_r$$

- $\alpha_r > 0$ *explicit constants with* $\sum \alpha_r = 1$.
- $\alpha_0 \approx .21$, $\alpha_1 \approx .42$, $\alpha_2 \approx .21$

- $d_2(E/K) := \dim_{\mathbb{F}_2}\mathrm{Sel}_2(E/K) - \dim_{\mathbb{F}_2}E(K)[2]$ will be referred to as the *2-Selmer rank of E*.

- $E^F := E^d$, where $F = K(\sqrt{d})$

Theorem (Dokchitser & Dokchitser)

Suppose K is a totally complex number field and E/K has potential good reduction over an abelian extension of K. Then

$$d_2(E^F/K) \equiv d_2(E/K) \pmod 2$$

for every quadratic twist E^F of E.

Theorem (Kramer, 1981)

We have a natural map

$$\{F/K \text{ quadratic}\} = K^\times/(K^\times)^2 \to \prod_{v|2\Delta_E\infty} K_v^\times/(K_v^\times)^2$$

Theorem (Kramer, 1981)

We have a natural map

$$\{F/K \text{ quadratic}\} = K^\times/(K^\times)^2 \to \prod_{v|2\Delta_E\infty} K_v^\times/(K_v^\times)^2$$

- $d_2(E^F/K) \pmod 2$ *is determined entirely by the image of* F/K *under this map.*

Theorem (K., Mazur, Rubin)

Let

$$S(X) := \{F/K : \mathbf{N}_{K/\mathbb{Q}}\mathfrak{q} < X \ \forall \mathfrak{q} \textit{ ramified in } F/K\}.$$

Theorem (K., Mazur, Rubin)

Let

$$S(X) := \{F/K : \mathbf{N}_{K/\mathbb{Q}}\mathfrak{q} < X \ \forall \mathfrak{q} \text{ ramified in } F/K\}.$$

Then for sufficiently large X,

$$\frac{\#\{F/K \in S(X) : d_2(E^F/K) \text{ is even }\}}{\#S(X)} = \frac{1+\delta}{2}$$

- $\delta \in [-1,1] \cap \mathbb{Z}[\frac{1}{2}]$.
- $\delta = \prod_{v|2\Delta_E\infty} \delta_v$, *where the δ_v are explicit.*
- $\delta_v = 0$ *for all real places v, so $\delta = 0$ if K has a real embedding.*

Example

Let E be the curve given by

$$y^2 + xy + y = x^3 + x^2 - 3x + 1,$$

K a finite extension of $\mathbb{Q}(\sqrt{-2})$ that is unramified at primes above 5. Then

$$\delta = -1^{[K:\mathbb{Q}(\sqrt{-2})]} \prod_{v|2} (1 - 2^{[K_v:\mathbb{Q}_2]})$$

- δ is dense in $[-1, 1]$ as K varies.
- $\dfrac{\#\{F/K \in S(X) : d_2(E^F/K) \text{ is even } \}}{\#S(X)}$ is dense in $[0, 1]$ as K varies

Conjecture (Goldfeld's Conjecture)

If E an elliptic curve over $\mathbb{Q}$, then

- 50% *of all quadratic twists of E have rank* 0
- 50% *have rank* 1
- 0% *have rank* ≥ 2

Conjecture (Goldfeld's Conjecture for Number Fields)

If E an elliptic curve over K, then there is a computable factor $\delta \in [-1, 1]$ such that

- *The proportion of twists of E having rank 0 is* $\frac{1+\delta}{2}$.
- *The proportion of twists of E having rank 1 is* $\frac{1-\delta}{2}$.

Conjecture (Goldfeld's Conjecture)

If E an elliptic curve over $\mathbb{Q}$, then

- 50% *of all quadratic twists of E have rank* 0
- 50% *have rank* 1
- 0% *have rank* ≥ 2

Conjecture (Goldfeld's Conjecture for Number Fields)

If E an elliptic curve over K, then there is a computable factor $\delta \in [-1, 1]$ such that

- *The proportion of twists of E having rank 0 is $\frac{1+\delta}{2}$.*
- *The proportion of twists of E having rank 1 is $\frac{1-\delta}{2}$.*
- *δ may depend on how the twists are ordered.*

Theorem (K., Mazur, Rubin)

Suppose $E(K)[2] = 0$ *and* $\mathrm{Gal}(K(E[2])/K) \simeq \mathcal{S}_3$. *There exist "skew-boxes" boxes* $B_m(X)$ *for* $m \in \mathbb{N}$ *and* $X \in \mathbb{R}^+$ *with* $\bigcup_{m,X} B_m(X) = \{[F : K] = 2\}$ *such that*

$$\lim_{m\to\infty} \lim_{X\to\infty} \frac{\#\{F/K \in B_m(X) : d_2(E^F/K) = r\}}{\#B_m(X)}$$

$$= \begin{cases} (1+\delta)\alpha_r & \text{if } r \text{ is even} \\ (1-\delta)\alpha_r & \text{if } r \text{ is odd} \end{cases}$$

• $E[2]$ and $E^F[2]$ are G_K-isomorphic so we can view $H^1(K, E^F[2])$ and sitting inside of $H^1(K, E[2])$.

• For every F/K, the group $\mathrm{Sel}_2(E^F/K)$ is subgroup of $H^1(K, E[2])$ which is defined by local conditions in $H^1(K_v, E[2])$ for each v of K.

• The local conditions for E^F and E vary in a controlled manner, and we can understand how the subgroup of $H^1(K, E[2])$ changes as we change the local condition at a single prime from the local condition for E to the local condition for E^F.

• $E[2]$ and $E^F[2]$ are G_K-isomorphic so we can view $H^1(K, E^F[2])$ and sitting inside of $H^1(K, E[2])$.

• For every F/K, the group $\mathrm{Sel}_2(E^F/K)$ is subgroup of $H^1(K, E[2])$ which is defined by local conditions in $H^1(K_v, E[2])$ for each v of K.

• The local conditions for E^F and E vary in a controlled manner, and we can understand how the subgroup of $H^1(K, E[2])$ changes as we change the local condition at a single prime from the local condition for E to the local condition for E^F.

• We work our way from $\mathrm{Sel}(E/K)$ to $\mathrm{Sel}(E^F/K)$ by successively changing the local conditions at each prime ramified in F/K. This gives us a chain of intermediate subgroups $\mathcal{Z}_1, \mathcal{Z}_2, \ldots, \mathcal{Z}_m$ of $H^1(K, E[2])$ each defined by local conditions, where $\mathcal{Z}_i$ and $\mathcal{Z}_{i+1}$ differ by a single local condition and $\mathcal{Z}_m = \mathrm{Sel}_2(E/K)$.

• $E[2]$ and $E^F[2]$ are G_K-isomorphic so we can view $H^1(K, E^F[2])$ and sitting inside of $H^1(K, E[2])$.

• For every F/K, the group $\mathrm{Sel}_2(E^F/K)$ is subgroup of $H^1(K, E[2])$ which is defined by local conditions in $H^1(K_v, E[2])$ for each v of K.

• The local conditions for E^F and E vary in a controlled manner, and we can understand how the subgroup of $H^1(K, E[2])$ changes as we change the local condition at a single prime from the local condition for E to the local condition for E^F.

• We work our way from $\mathrm{Sel}(E/K)$ to $\mathrm{Sel}(E^F/K)$ by successively changing the local conditions at each prime ramified in F/K. This gives us a chain of intermediate subgroups $\mathcal{Z}_1, \mathcal{Z}_2, \ldots, \mathcal{Z}_m$ of $H^1(K, E[2])$ each defined by local conditions, where $\mathcal{Z}_i$ and $\mathcal{Z}_{i+1}$ differ by a single local condition and $\mathcal{Z}_m = \mathrm{Sel}_2(E/K)$.

• This process is a Markov process where the states are the ranks of the intermediate groups $\mathcal{Z}_i$ and the probabilities come from understanding what happens when we change a single local condition.

• The α_r are the stable distribution of this Markov process.

Example (K., 2011)

Let K be a number field and let E be the elliptic curve over K given by

$$E : y^2 = x^3 - 2(1 + 256n^2)x^2 + (1 + 256n^2)x$$

where $n \in \mathbb{N}$ with $1 + 256n^2 \notin (K^\times)^2$. Then $d_2(E^F/K) \geq r_2$ for every quadratic F/K where r_2 is the number of complex place of K.

Example (K., 2011)

Let K be a number field and let E be the elliptic curve over K given by

$$E : y^2 = x^3 - 2(1 + 256n^2)x^2 + (1 + 256n^2)x$$

where $n \in \mathbb{N}$ with $1 + 256n^2 \notin (K^\times)^2$. Then $d_2(E^F/K) \geq r_2$ for every quadratic F/K where r_2 is the number of complex place of K.

- E has a cyclic 4-isogeny defined over $K(E[2])$

Example (K., 2011)

Let K be a number field and let E be the elliptic curve over K given by

$$E : y^2 = x^3 - 2(1 + 256n^2)x^2 + (1 + 256n^2)x$$

where $n \in \mathbb{N}$ with $1 + 256n^2 \notin (K^\times)^2$. Then $d_2(E^F/K) \geq r_2$ for every quadratic F/K where r_2 is the number of complex place of K.

- E has a cyclic 4-isogeny defined over $K(E[2])$
- Impossible when E does not have a cyclic 4-isogeny defined over $K(E[2])$.

Theorem (K., 2012)

Suppose $E(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z}$ *and* E *does not have a cyclic 4-isogeny defined over* $\mathbb{Q}(E[2])$*. Then for any fixed* r*,*

$$\liminf_{X\to\infty} \frac{\#\{d \text{ squarefree}, |d| < X : d_2(E^d/\mathbb{Q}) \geq r\}}{\#\{d \text{ squarefree}, |d| < X\}}$$

Theorem (K., 2012)

Suppose $E(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z}$ *and* E *does not have a cyclic 4-isogeny defined over* $\mathbb{Q}(E[2])$*. Then for any fixed* r*,*

$$\liminf_{X\to\infty} \frac{\#\{d \text{ squarefree}, |d| < X : d_2(E^d/\mathbb{Q}) \geq r\}}{\#\{d \text{ squarefree}, |d| < X\}} \geq \frac{1}{2}$$

Theorem (K., 2012)

Suppose $E(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z}$ *and* E *does not have a cyclic 4-isogeny defined over* $\mathbb{Q}(E[2])$*. Then for any fixed* r*,*

$$\liminf_{X\to\infty} \frac{\#\{d \text{ squarefree}, |d| < X : d_2(E^d/\mathbb{Q}) \geq r\}}{\#\{d \text{ squarefree}, |d| < X\}} \geq \frac{1}{2}$$

- *At least* $\frac{1}{2}$ *of the twists of* E *have arbitrarily large 2-Selmer rank*
- *There is no distribution function on 2-Selmer ranks within the twist family of* E

We have a 2-isogeny $\phi : E \to E'$ with $C := \ker \phi = E(K)[2]$

We have a 2-isogeny $\phi : E \to E'$ with $C := \ker \phi = E(K)[2]$

$$\begin{array}{ccc} E'(K)/\phi(E(K)) & \xrightarrow{\kappa} & H^1(K, C) \\ \downarrow & & \downarrow res_v \\ E'(K_v)/\phi(E(K_v)) & \xrightarrow{\kappa_v} & H^1(K_v, C) \end{array}$$

We have a 2-isogeny $\phi : E \to E'$ with $C := \ker \phi = E(K)[2]$

$$\begin{array}{ccc} E'(K)/\phi(E(K)) & \xrightarrow{\kappa} & H^1(K, C) \\ \downarrow & & \downarrow res_v \\ E'(K_v)/\phi(E(K_v)) & \xrightarrow{\kappa_v} & H^1(K_v, C) \end{array}$$

- $H^1_\phi(K_v, C) = image\left(\kappa_v : E'(K_v)/\phi(E(K_v)) \to H^1(K_v, C)\right)$

We have a 2-isogeny $\phi : E \to E'$ with $C := \ker \phi = E(K)[2]$

$$\begin{array}{ccc} E'(K)/\phi(E(K)) & \xrightarrow{\kappa} & H^1(K, C) \\ \downarrow & & \downarrow res_v \\ E'(K_v)/\phi(E(K_v)) & \xrightarrow{\kappa_v} & H^1(K_v, C) \end{array}$$

- $H^1_\phi(K_v, C) = image\left(\kappa_v : E'(K_v)/\phi(E(K_v)) \to H^1(K_v, C)\right)$
- $\mathrm{Sel}_\phi(E/K) = \left\{ c \in H^1(K, C) : \begin{array}{c} res_v(c) \in H^1_\phi(K_v, C) \\ \text{for all } v \text{ of } K \end{array} \right\}$

- $0 \to E'(K)[2] \to Sel_{\phi}(E/K) \to Sel_2(E/K) \to \mathrm{Sel}_{\hat{\phi}}(E'/K)$

- $0 \to E'(K)[2] \to Sel_\phi(E/K) \to Sel_2(E/K) \to \mathrm{Sel}_{\hat{\phi}}(E'/K)$
- $\mathcal{T}(E/E') = \dfrac{\#\mathrm{Sel}_\phi(E/K)}{\#\mathrm{Sel}_{\hat{\phi}}(E'/K)}$

- $0 \to E'(K)[2] \to Sel_\phi(E/K) \to Sel_2(E/K) \to \mathrm{Sel}_{\hat{\phi}}(E'/K)$
- $\mathcal{T}(E/E') = \dfrac{\#\mathrm{Sel}_\phi(E/K)}{\#\mathrm{Sel}_{\hat{\phi}}(E'/K)}$
- $d_2(E/K) \geq \mathrm{ord}_2(\mathcal{T}(E/E'))$

- $0 \to E'(K)[2] \to Sel_\phi(E/K) \to Sel_2(E/K) \to \mathrm{Sel}_{\hat{\phi}}(E'/K)$
- $\mathcal{T}(E/E') = \dfrac{\#\mathrm{Sel}_\phi(E/K)}{\#\mathrm{Sel}_{\hat{\phi}}(E'/K)}$
- $d_2(E/K) \geq \mathrm{ord}_2(\mathcal{T}(E/E'))$
- $\mathcal{T}(E/E') = \displaystyle\prod_{v|2\Delta_E\infty} \frac{\#H^1_\phi(K_v, C)}{2}$

Let Δ be the discriminant of E and Δ' be the discriminant of E'.

Let Δ be the discriminant of E and Δ' be the discriminant of E'.

- There exists a constant $C = C(E)$ such that

$$\left| \mathrm{ord}_2 \mathcal{T}(E^d/E'^d) - \sum_{\substack{p \mid d \\ p \nmid 2\Delta_E}} \frac{\left(\frac{\Delta'}{p}\right) - \left(\frac{\Delta}{p}\right)}{2} \right| \leq C$$

Let Δ be the discriminant of E and Δ' be the discriminant of E'.

- There exists a constant $C = C(E)$ such that

$$\left| \mathrm{ord}_2 \mathcal{T}(E^d/E'^d) - \sum_{\substack{p \mid d \\ p \nmid 2\Delta_E}} \frac{\left(\frac{\Delta'}{p}\right) - \left(\frac{\Delta}{p}\right)}{2} \right| \leq C$$

- The Erdös-Kac Theorem shows that

$$\frac{\sum_{\substack{p \mid d \\ p \nmid 2\Delta_E}} \frac{\left(\frac{\Delta'}{p}\right) - \left(\frac{\Delta}{p}\right)}{2}}{\sqrt{\log \log d}}$$

has the standard normal distribution.

Let Δ be the discriminant of E and Δ' be the discriminant of E'.

- There exists a constant $C = C(E)$ such that

$$\left| \mathrm{ord}_2 \mathcal{T}(E^d/E'^d) - \sum_{\substack{p \mid d \\ p \nmid 2\Delta_E}} \frac{\left(\frac{\Delta'}{p}\right) - \left(\frac{\Delta}{p}\right)}{2} \right| \leq C$$

- The Erdös-Kac Theorem shows that

$$\frac{\sum_{\substack{p \mid d \\ p \nmid 2\Delta_E}} \frac{\left(\frac{\Delta'}{p}\right) - \left(\frac{\Delta}{p}\right)}{2}}{\sqrt{\log \log d}}$$

has the standard normal distribution.

- For any fixed r,

$$\mathrm{ord}_2 \mathcal{T}(E^d/E'^d) \geq r$$

for half of all squarefree d.