2-Selmer groups and Heegner points

Chao Li

Department of Mathematics
Harvard University

May 24, 2014 / FRG Workshop in Cambridge
BSD Conjecture

Let $E/\mathbb{Q}$ be an elliptic curve.

- (Rank Conjecture)

$$\text{rank } E(\mathbb{Q}) \overset{?}{=} \text{ord}_{s=1} L(E/\mathbb{Q}, s).$$
BSD Conjecture

Let $E/\mathbb{Q}$ be an elliptic curve.

- (Rank Conjecture)

  \[
  \text{rank } E(\mathbb{Q}) = \text{ord}_{s=1} L(E/\mathbb{Q}, s).
  \]

- Known when $\text{ord}_{s=1} L(E/\mathbb{Q}, s) \leq 1$ (Gross-Zagier, Kolyvagin, ...)

(Refined BSD formula)

\[
\frac{L^{(r)}(E/Q, 1)}{r!} \overset{?}{=} \int_{E(\mathbb{R})} \omega \cdot \prod_p c_p \cdot |\Sha(E/Q)| \cdot \frac{\det(\langle P_i, P_j \rangle^r_{i,j=1})}{|E(Q)_{\text{tor}}|^2}.
\]
BSD Conjecture

- (Refined BSD formula)

\[
\frac{L^{(r)}(E/\mathbb{Q}, 1)}{r!} \overset{?}{=} \int_{E(\mathbb{R})} \omega \cdot \prod_p c_p \cdot |\text{III}(E/\mathbb{Q})| \cdot \frac{\det(\langle P_i, P_j \rangle^r_{i,j=1})}{|E(\mathbb{Q})_{\text{tor}}|^2}.
\]

Or,

\[
\frac{L^{(r)}(E/\mathbb{Q}, 1)}{r!\Omega(E/\mathbb{Q})R(E/\mathbb{Q})} \overset{?}{=} \prod_p c_p \cdot |\text{III}(E/\mathbb{Q})| \cdot \frac{\omega}{|E(\mathbb{Q})_{\text{tor}}|^2}.
\]
BSD Conjecture

- (Refined BSD formula)

\[ \frac{L^{(r)}(E/\mathbb{Q}, 1)}{r!} \overset{?}{=} \int_{E(\mathbb{R})} \omega \cdot \prod_p c_p \cdot |\Sha(E/\mathbb{Q})| \cdot \frac{\det(\langle P_i, P_j \rangle^r_{i,j=1})}{|E(\mathbb{Q})_{\text{tor}}|^2}. \]

Or,

\[ \frac{L^{(r)}(E/\mathbb{Q}, 1)}{r! \Omega(E/\mathbb{Q}) R(E/\mathbb{Q})} \overset{?}{=} \prod_p c_p \cdot |\Sha(E/\mathbb{Q})| \cdot \frac{1}{|E(\mathbb{Q})_{\text{tor}}|^2}. \]

- Known cases of \( p \)-part of BSD formula (under mild assumptions)
BSD Conjecture

- (Refined BSD formula)

\[ \frac{L^{(r)}(E/\mathbb{Q}, 1)}{r!} = \int_{E(\mathbb{R})} \omega \cdot \prod_p c_p \cdot |\Sha(E/\mathbb{Q})| \cdot \frac{\det(\langle P_i, P_j \rangle)_{i,j=1}^r}{|E(\mathbb{Q})_{\text{tor}}|^2}. \]

Or,

\[ \frac{L^{(r)}(E/\mathbb{Q}, 1)}{r! \Omega(E/\mathbb{Q}) R(E/\mathbb{Q})} = \prod_p c_p \cdot |\Sha(E/\mathbb{Q})| \cdot \frac{1}{|E(\mathbb{Q})_{\text{tor}}|^2}. \]

- Known cases of \( p \)-part of BSD formula (under mild assumptions)
  - \( p \geq 3 \) when \( \text{ord}_{s=1} L(E/\mathbb{Q}, s) = 0 \) (Skinner-Urban, Kato, ...)

Chao Li (Harvard) 2-Selmer groups and Heegner points FRG 2014
BSD Conjecture

- (Refined BSD formula)

\[
\frac{L^{(r)}(E/\mathbb{Q}, 1)}{r!} = \int_{E(\mathbb{R})} \omega \cdot \prod_p c_p \cdot |\Sha(E/\mathbb{Q})| \cdot \frac{\det(\langle P_i, P_j \rangle_{i,j=1}^r)}{|E(\mathbb{Q})_{\text{tor}}|^2}.
\]

Or,

\[
\frac{L^{(r)}(E/\mathbb{Q}, 1)}{r! \Omega(E/\mathbb{Q}) R(E/\mathbb{Q})} = \prod_p c_p \cdot |\Sha(E/\mathbb{Q})| \cdot \frac{1}{|E(\mathbb{Q})_{\text{tor}}|^2}.
\]

- Known cases of \(p\)-part of BSD formula (under mild assumptions)
  - \(p \geq 3\) when \(\text{ord}_{s=1} L(E/\mathbb{Q}, s) = 0\) (Skinner-Urban, Kato, ...)
  - \(p \geq 5\) when \(\text{ord}_{s=1} L(E/\mathbb{Q}, s) = 1\) (Wei Zhang, ...)
BSD Conjecture

- (Refined BSD formula)

\[
\frac{L(r)(E/\mathbb{Q}, 1)}{r!} = \frac{1}{r!} \int_{E(\mathbb{R})} \omega \cdot \prod_p c_p \cdot |\Sha(E/\mathbb{Q})| \cdot \frac{\det(\langle P_i, P_j \rangle^r_{i,j=1})}{|E(\mathbb{Q})_{\text{tor}}|^2}.
\]

Or,

\[
\frac{L(r)(E/\mathbb{Q}, 1)}{r! \Omega(E/\mathbb{Q}) R(E/\mathbb{Q})} = \frac{1}{r! \Omega(E/\mathbb{Q}) R(E/\mathbb{Q})} \prod_p c_p \cdot |\Sha(E/\mathbb{Q})| \cdot \frac{\det(\langle P_i, P_j \rangle^r_{i,j=1})}{|E(\mathbb{Q})_{\text{tor}}|^2}.
\]

- Known cases of $p$-part of BSD formula (under mild assumptions)
  - $p \geq 3$ when \(\text{ord}_{s=1} L(E/\mathbb{Q}, s) = 0\) (Skinner-Urban, Kato, ...)
  - $p \geq 5$ when \(\text{ord}_{s=1} L(E/\mathbb{Q}, s) = 1\) (Wei Zhang, ...)
  - $p = 2$ ?
BSD Conjecture

- (Refined BSD formula)

\[
\frac{L^{(r)}(E/Q, 1)}{r!} \overset{?}{=} \int_{E(\mathbb{R})} \omega \cdot \prod_{p} c_p \cdot |\Sha(E/Q)| \cdot \frac{\det(\langle P_i, P_j \rangle_{i,j=1}^r)}{|E(Q)_{tor}|^2}.
\]

Or,

\[
\frac{L^{(r)}(E/Q, 1)}{r!\Omega(E/Q)R(E/Q)} \overset{?}{=} \prod_{p} c_p \cdot |\Sha(E/Q)| \frac{1}{|E(Q)_{tor}|^2}.
\]

- Known cases of \(p\)-part of BSD formula (under mild assumptions)
  - \(p \geq 3\) when \(\text{ord}_{s=1} L(E/Q, s) = 0\) (Skinner-Urban, Kato, ...)
  - \(p \geq 5\) when \(\text{ord}_{s=1} L(E/Q, s) = 1\) (Wei Zhang, ...)

- \(p = 2\) ? Why \(p = 2\)?
### BSD formula

<table>
<thead>
<tr>
<th>Curve</th>
<th>$r$</th>
<th>$\Omega$</th>
<th>$L^{(r)}(1) / r!$</th>
<th>$R$</th>
<th>$L^{(r)}(1) / r! \Omega R$</th>
</tr>
</thead>
<tbody>
<tr>
<td>676 C</td>
<td>0</td>
<td>0.4150660384</td>
<td>0.4150660384</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>676 D</td>
<td>0</td>
<td>2.9442542341</td>
<td>2.9442542341</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>676 E</td>
<td>0</td>
<td>0.8165892007</td>
<td>2.4497676021</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>677 A</td>
<td>1</td>
<td>2.8368146928</td>
<td>1.2893981935</td>
<td>0.4545232358</td>
<td>1.0000000000</td>
</tr>
<tr>
<td>678 A</td>
<td>1</td>
<td>4.8406123729</td>
<td>1.5171515354</td>
<td>0.1567107030</td>
<td>2.0000000000</td>
</tr>
<tr>
<td>678 B</td>
<td>1</td>
<td>1.5883609701</td>
<td>1.7574538605</td>
<td>0.1844095783</td>
<td>6.0000000000</td>
</tr>
<tr>
<td>678 C</td>
<td>1</td>
<td>1.4205258825</td>
<td>2.4773594939</td>
<td>0.2491390713</td>
<td>7.0000000000</td>
</tr>
<tr>
<td>678 D</td>
<td>0</td>
<td>1.3970457314</td>
<td>2.7940914629</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>678 E</td>
<td>0</td>
<td>3.1622103101</td>
<td>3.1622103101</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>678 F</td>
<td>0</td>
<td>1.2858801950</td>
<td>2.5717603900</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>680 A</td>
<td>1</td>
<td>3.2750305235</td>
<td>2.0532909813</td>
<td>1.2539064699</td>
<td>0.5000000000</td>
</tr>
<tr>
<td>680 B</td>
<td>0</td>
<td>1.4663778907</td>
<td>1.4663778907</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>680 C</td>
<td>0</td>
<td>0.6189257201</td>
<td>2.4757028802</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>681 A</td>
<td>1</td>
<td>3.8078769894</td>
<td>1.7148309965</td>
<td>0.2251689066</td>
<td>2.0000000000</td>
</tr>
<tr>
<td>681 B</td>
<td>0</td>
<td>0.8199176894</td>
<td>1.8448152061</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>681 C</td>
<td>2</td>
<td>3.7708461685</td>
<td>1.0262711474</td>
<td>0.1360796890</td>
<td>2.0000000000</td>
</tr>
<tr>
<td>681 D</td>
<td>0</td>
<td>0.5238009112</td>
<td>2.0952036450</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>681 E</td>
<td>1</td>
<td>2.2367233352</td>
<td>2.0523231219</td>
<td>0.0917557880</td>
<td>10.0000000000</td>
</tr>
<tr>
<td>682 A</td>
<td>1</td>
<td>3.1826703234</td>
<td>2.2812508906</td>
<td>0.7167725770</td>
<td>57.0000000000</td>
</tr>
<tr>
<td>682 B</td>
<td>1</td>
<td>0.6115533121</td>
<td>2.6265637235</td>
<td>0.0753492204</td>
<td>6.0000000000</td>
</tr>
<tr>
<td>684 A</td>
<td>1</td>
<td>2.5117117855</td>
<td>2.1232510164</td>
<td>0.1408900408</td>
<td>6.0000000000</td>
</tr>
<tr>
<td>684 B</td>
<td>1</td>
<td>0.8914338511</td>
<td>2.0174937497</td>
<td>0.3772001230</td>
<td>2.0000000000</td>
</tr>
<tr>
<td>684 C</td>
<td>0</td>
<td>1.0106719472</td>
<td>2.0213438944</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>685 A</td>
<td>1</td>
<td>5.0493985695</td>
<td>2.5294065402</td>
<td>0.5009322408</td>
<td>1.0000000000</td>
</tr>
<tr>
<td>688 A</td>
<td>1</td>
<td>2.1361539012</td>
<td>2.0384041307</td>
<td>0.954202959</td>
<td>1.0000000000</td>
</tr>
<tr>
<td>688 B</td>
<td>0</td>
<td>1.2461451514</td>
<td>2.4922903027</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>688 C</td>
<td>1</td>
<td>1.3631824182</td>
<td>2.3637294196</td>
<td>1.7339788043</td>
<td>1.0000000000</td>
</tr>
<tr>
<td>689 A</td>
<td>1</td>
<td>5.1047223290</td>
<td>1.0333048176</td>
<td>0.8096854253</td>
<td>0.2500000000</td>
</tr>
<tr>
<td>690 A</td>
<td>1</td>
<td>0.7448541864</td>
<td>1.3963979050</td>
<td>0.9373629565</td>
<td>2.0000000000</td>
</tr>
</tbody>
</table>

Chao Li (Harvard)  
2-Selmer groups and Heegner points  
FRG 2014
Our strategy: study the 2-Selmer group

\[ \text{Sel}_2(E/\mathbb{Q}) \subseteq H^1(\mathbb{Q}, E[2]) \]

via level raising of modular forms (mod 2).
Our strategy: study the $2$-Selmer group

$$\text{Sel}_2(E/\mathbb{Q}) \subseteq H^1(\mathbb{Q}, E[2])$$

via level raising of modular forms (mod 2).

Inspired by W. Zhang’s recent work.
- $E/\mathbb{Q}$: elliptic curve of odd conductor $N$. 
- $E/\mathbb{Q}$: elliptic curve of odd conductor $N$.
- $\bar{\rho} = \bar{\rho}_{E,2} : G_{\mathbb{Q}} \to \text{Aut}(E[2]) \cong GL_2(\mathbb{F}_2)$
- $E/\mathbb{Q}$: elliptic curve of odd conductor $N$.
- $\bar{\rho} = \bar{\rho}_{E,2}: G_{\mathbb{Q}} \to \text{Aut}(E[2]) \cong GL_2(\mathbb{F}_2)$

Assume (throughout this talk) the following mild hypothesis:

1. (surj) $\bar{\rho}$ is surjective
- $E/\mathbb{Q}$: elliptic curve of odd conductor $N$.
- $\bar{\rho} = \bar{\rho}_{E,2} : G_{\mathbb{Q}} \to \text{Aut}(E[2]) \cong GL_2(\mathbb{F}_2)$

Assume (throughout this talk) the following mild hypothesis:

1. (surj) $\bar{\rho}$ is surjective

2. (ram) Serre conductor $N(\bar{\rho}) = N$
\( E/\mathbb{Q} \): elliptic curve of odd conductor \( N \).

\[ \bar{\rho} = \bar{\rho}_{E,2} : G_{\mathbb{Q}} \to \text{Aut}(E[2]) \cong GL_2(\mathbb{F}_2) \]

Assume (throughout this talk) the following mild hypothesis:

1. \((\text{surj})\) \( \bar{\rho} \) is surjective

2. \((\text{ram})\) Serre conductor \( N(\bar{\rho}) = N \)

3. \((\text{nontrivial at 2})\) \( \bar{\rho}|_{G_{\mathbb{Q}_2}} \) is nontrivial
- $E/\mathbb{Q}$: elliptic curve of odd conductor $N$.
- $\bar{\rho} = \bar{\rho}_{E,2}: G_{\mathbb{Q}} \to \text{Aut}(E[2]) \cong GL_2(\mathbb{F}_2)$

Assume (throughout this talk) the following mild hypothesis:

1. (surj) $\mathbb{Q}(E[2])/\mathbb{Q}$ is a $GL_2(\mathbb{F}_2) \cong S_3$-extension ($\iff E[2](\mathbb{Q}) = 0$).
2. (ram) Serre conductor $N(\bar{\rho}) = N$
3. (nontrivial at 2) $\bar{\rho}|_{G_{\mathbb{Q}_2}}$ is nontrivial
$E/\mathbb{Q}$: elliptic curve of odd conductor $N$.

$\bar{\rho} = \bar{\rho}_{E,2} : G_{\mathbb{Q}} \to \text{Aut}(E[2]) \cong GL_2(\mathbb{F}_2)$

Assume (throughout this talk) the following mild hypothesis:

1. (surj) $\mathbb{Q}(E[2])/\mathbb{Q}$ is a $GL_2(\mathbb{F}_2) \cong S_3$-extension ($\implies E[2](\mathbb{Q}) = 0$).

2. (ram) the order of component group of the Neron model of $E$ is odd at any $p | N$ ($\implies 2 \nmid \prod_p c_p$).

3. (nontrivial at 2) $\bar{\rho}|_{G_{\mathbb{Q}_2}}$ is nontrivial
\(E/\mathbb{Q}\): elliptic curve of odd conductor \(N\).

\(\bar{\rho} = \bar{\rho}_{E,2}: G_\mathbb{Q} \to \text{Aut}(E[2]) \cong GL_2(\mathbb{F}_2)\)

Assume (throughout this talk) the following mild hypothesis:

1. (surj) \(\mathbb{Q}(E[2])/\mathbb{Q}\) is a \(GL_2(\mathbb{F}_2) \cong S_3\)-extension \(\implies E[2](\mathbb{Q}) = 0\).

2. (ram) the order of component group of the Neron model of \(E\) is odd at any \(p \mid N\) \(\implies 2 \nmid \prod_p c_p\).

3. (nontrivial at 2) 2 does not split in \(\mathbb{Q}(E[2])/\mathbb{Q}\)
Under these assumptions,

\[ E[2] \text{ (as } G_{\mathbb{Q}}\text{-module)} + \text{ knowledge of reduction type at } p \]

pins down the local condition for \( \text{Sel}_2(E/\mathbb{Q}) \) at \( p \).
Under these assumptions,

\[ E[2] \text{ (as } G_{\mathbb{Q}}\text{-module}) + \text{ knowledge of reduction type at } p \]

pins down the local condition for \( \text{Sel}_2(E/\mathbb{Q}) \) at \( p \)

Keep \( E[2] \), but at a prime \( q \nmid 2N \) of choice,

\[ \text{good reduction at } q \leadsto \text{ multiplicative reduction at } q \]
Under these assumptions,

\[ E[2] \text{ (as } G_{\mathbb{Q}}\text{-module}) + \text{knowledge of reduction type at } p \]

pins down the local condition for \( \text{Sel}_2(E/\mathbb{Q}) \) at \( p \)

Keep \( E[2] \), but at a prime \( q \nmid 2N \) of choice,

good reduction at \( q \leadsto \) multiplicative reduction at \( q \)

Necessarily:

\[ \bar{\rho}(\text{Frob}_q) = \left( \begin{array}{cc} q & * \\ 0 & 1 \end{array} \right) \text{ (mod } 2) \]
Under these assumptions,

\[ E[2] \text{ (as } G_\mathbb{Q}\text{-module}) + \text{ knowledge of reduction type at } p \]

pins down the local condition for \( \text{Sel}_2(E/\mathbb{Q}) \) at \( p \)

Keep \( E[2] \), but at a prime \( q \nmid 2N \) of choice,

good reduction at \( q \) \( \rightsquigarrow \) multiplicative reduction at \( q \)

Necessarily:

\[
\bar{\rho}(\text{Frob}_q) = \begin{pmatrix} q^* & 0 \\ 0 & 1 \end{pmatrix} \pmod{2}
\]

In \( GL_2(\mathbb{F}_2) \cong S_3 \),
Under these assumptions, 

\[ E[2] \text{ (as } G_\mathbb{Q}\text{-module}) + \text{ knowledge of reduction type at } p \]

does pin down the local condition for \( Sel_2(E/\mathbb{Q}) \) at \( p \).

Keep \( E[2] \), but at a prime \( q \nmid 2N \) of choice,

- good reduction at \( q \Leftrightarrow \) multiplicative reduction at \( q \)

Necessarily:

\[ \bar{\rho}(\text{Frob}_q) = \begin{pmatrix} q^* \\ 0 \end{pmatrix} \pmod{2} \]

\( \text{In } GL_2(\mathbb{F}_2) \cong S_3 \),

- \( \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \) (trivial)
Under these assumptions,

\[ E[2] \text{ (as } G_\mathbb{Q}\text{-module) + knowledge of reduction type at } p \]

pins down the local condition for \( \text{Sel}_2(E/\mathbb{Q}) \) at \( p \)

Keep \( E[2] \), but at a prime \( q \nmid 2N \) of choice,

good reduction at \( q \) \( \rightsquigarrow \) multiplicative reduction at \( q \)

Necessarily:

\[ \bar{\rho}(\text{Frob}_q) = \begin{pmatrix} q^* & \ast \\ 0 & 1 \end{pmatrix} \pmod{2} \]

In \( GL_2(\mathbb{F}_2) \cong S_3 \),

\( \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \) (trivial)
\( \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \) (order 2)
Under these assumptions,
\[ E[2] \text{ (as } G_Q\text{-module)} + \text{ knowledge of reduction type at } p \]
pins down the local condition for \( \text{Sel}_2(E/\mathbb{Q}) \) at \( p \)

Keep \( E[2] \), but at a prime \( q \nmid 2N \) of choice,
\[
\text{good reduction at } q \Rightarrow \text{ multiplicative reduction at } q
\]

Necessarily:
\[
\bar{\rho}(\text{Frob}_q) = \begin{pmatrix} q^* & 0 \\ 0 & 1 \end{pmatrix} \pmod{2}
\]

In \( GL_2(\mathbb{F}_2) \cong S_3 \),
\[
\begin{align*}
\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \text{ (trivial)} \\
\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & \text{ (order 2)} \\
\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} & \text{ (order 3)}
\end{align*}
\]
Under these assumptions,

\[ E[2] \text{ (as } G_\mathbb{Q}\text{-module)} + \text{knowledge of reduction type at } p \]

pins down the local condition for \( \text{Sel}_2(E/\mathbb{Q}) \) at \( p \)

Keep \( E[2] \), but at a prime \( q \nmid 2N \) of choice,

good reduction at \( q \leadsto \text{multiplicative reduction at } q \)

Necessarily:

\[ \bar{\rho}(\text{Frob}_q) = \left( \begin{array}{cc} q^* & 0 \\ 0 & 1 \end{array} \right) \pmod{2} \]

In \( GL_2(\mathbb{F}_2) \cong S_3 \),

\[ \begin{array}{c}
\left( \begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right) \text{ (trivial)} \\
\left( \begin{array}{cc} 1 & 1 \\ 0 & 1 \end{array} \right) \text{ (order 2)} \\
\left( \begin{array}{cc} 1 & 1 \\ 1 & 0 \end{array} \right) \text{ (order 3)} \\
\end{array} \]
Under these assumptions,

\[ E[2] \text{ (as } G_{\mathbb{Q}}\text{-module)} + \text{knowledge of reduction type at } p \]
pins down the local condition for \( \text{Sel}_2(E/\mathbb{Q}) \) at \( p \)

Keep \( E[2] \), but at a prime \( q \nmid 2N \) of choice,

good reduction at \( q \rightarrow \) multiplicative reduction at \( q \)

Necessarily:

\[ \bar{\rho}(\text{Frob}_q) = \begin{pmatrix} q^* & 1 \\ 0 & 1 \end{pmatrix} \pmod{2} \]

In \( \text{GL}_2(\mathbb{F}_2) \cong S_3 \),

- \( \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \) (trivial)
- \( \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \) (order 2)
- \( \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \) (order 3)

**Theorem (Ribet’s level raising)**

*Let \( q \nmid 2N \) be a prime. Suppose \( \bar{\rho}(\text{Frob}_q) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \) or \( \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \), then \( \bar{\rho} \)
comes from a weight 2 newform of level \( Nq \).*
\[ E/\mathbb{Q} \rightsquigarrow f = \sum_{n \geq 1} a_n q^n \in S_2(N)^{\text{new}}. \]
\[ E/\mathbb{Q} \rightsquigarrow f = \sum_{n \geq 1} a_n q^n \in S_2(N)^{\text{new}}. \]
\[ \bar{\rho}(\text{Frob}_q) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ or } \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \iff 2 \mid a_q. \]
\( E/\mathbb{Q} \rightsquigarrow f = \sum_{n \geq 1} a_n q^n \in S_2(N)^{\text{new}}. \)

\( \bar{\rho}(\text{Frob}_q) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ or } \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \iff 2 \mid a_q. \)

\( 2 \mid a_q \rightsquigarrow g = \sum_{n \geq 1} b_n q^n \in S_2(Nq)^{\text{new}} \) such that

\[ f \equiv g \pmod{2}. \]
\( E / \mathbb{Q} \leadsto f = \sum_{n \geq 1} a_n q^n \in S_2(N)^\text{new} \).

\[ \bar{\rho}(\text{Frob}_q) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ or } \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \iff 2 \mid a_q. \]

\( 2 \mid a_q \leadsto g = \sum_{n \geq 1} b_n q^n \in S_2(Nq)^\text{new} \) such that

\[ f \equiv g \pmod{2}. \]

More precisely,
- \( E/\mathbb{Q} \sim f = \sum_{n \geq 1} a_n q^n \in S_2(N)^{\text{new}} \).
- \( \bar{\rho}(\text{Frob}_q) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \) or \( \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \) \( \iff \) \( 2 \mid a_q \).
- \( 2 \mid a_q \leadsto g = \sum_{n \geq 1} b_n q^n \in S_2(Nq)^{\text{new}} \) such that
  \[
  f \equiv g \pmod{2}.
  \]
- More precisely,
  - \( F = \mathbb{Q}(g) \) (totally real) with ring of integers \( \mathcal{O} = \mathcal{O}_F \).

Chao Li (Harvard) 2-Selmer groups and Heegner points FRG 2014
\[ E/\mathbb{Q} \sim f = \sum_{n \geq 1} a_n q^n \in S_2(N)^{\text{new}}. \]

\[ \bar{\rho}(\text{Frob}_q) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ or } \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \iff 2 \mid a_q. \]

\[ 2 \mid a_q \sim g = \sum_{n \geq 1} b_n q^n \in S_2(Nq)^{\text{new}} \] such that

\[ f \equiv g \pmod{2}. \]

More precisely,

\[ F = \mathbb{Q}(g) \text{ (totally real) with ring of integers } \mathcal{O} = \mathcal{O}_F. \]

\[ \exists \lambda \mid 2 \text{ a prime of } \mathcal{O} \text{ such that for any } p \neq q, \]

\[ a_p \equiv b_p \pmod{\lambda} \]

\[ \sum_{n \geq 1} a_n q^n \in S_2(N)^{\text{new}}. \]
\( E / \mathbb{Q} \rightsquigarrow f = \sum_{n \geq 1} a_n q^n \in S_2(N)^{\text{new}}. \)

\( \bar{\rho}(\text{Frob}_q) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ or } \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \iff 2 \mid a_q. \)

\( 2 \mid a_q \rightsquigarrow g = \sum_{n \geq 1} b_n q^n \in S_2(Nq)^{\text{new}} \) such that

\[ f \equiv g \pmod{2}. \]

More precisely,

\( F = \mathbb{Q}(g) \) (totally real) with ring of integers \( \mathcal{O} = \mathcal{O}_F. \)

\( \exists \lambda \mid 2 \) a prime of \( \mathcal{O} \) such that for any \( p \neq q, \)

\[ a_p \equiv b_p \pmod{\lambda}. \]

\( g \rightsquigarrow A / \mathbb{Q} \) an abelian variety up to isogeny, of dimension \([F : \mathbb{Q}]\) with real multiplication by \( F. \)
\( E / \mathbb{Q} \sim f = \sum_{n \geq 1} a_n q^n \in S_2(N)^{\text{new}}. \)

\( \bar{\rho}(\text{Frob}_q) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ or } \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \iff 2 \mid a_q. \)

\( 2 \mid a_q \sim g = \sum_{n \geq 1} b_n q^n \in S_2(Nq)^{\text{new}} \) such that

\[ f \equiv g \pmod{2}. \]

More precisely,

- \( F = \mathbb{Q}(g) \) (totally real) with ring of integers \( \mathcal{O} = \mathcal{O}_F. \)
- \( \exists \lambda \mid 2 \) a prime of \( \mathcal{O} \) such that for any \( p \neq q, \)

\[ a_p \equiv b_p \pmod{\lambda} \]

\( g \sim A / \mathbb{Q} \) an abelian variety up to isogeny, of dimension \([F : \mathbb{Q}]\) with real multiplication by \( F. \)

Choose \( A \) in the isogeny class so that \( \mathcal{O} \hookrightarrow \text{End}(A) \). It is unique up to prime-to-\( \lambda \) isogenies.
Definition

Such $q$ is called a *level raising prime* for $E$. We say that $A$ is obtained from $E$ *via level raising at $q$*; $A$ and $E$ are congruent mod 2.

Remark

There are a lot of level raising primes!

Example

$E = X_0(11)$:

$$y^2 + y = x^3 - x^2 - 10x - 20.$$ 

$q = 7$ is a level raising prime. 

There are three (isogeny classes of) elliptic curves of conductor 77. Two of them are congruent to $E$ mod 2.
Definition
Such $q$ is called a *level raising prime* for $E$. We say that $A$ is obtained from $E$ *via level raising at $q$*; $A$ and $E$ are congruent mod 2.

Remark
There are a lot of level raising primes!
Definition
Such $q$ is called a \textit{level raising prime} for $E$. We say that $A$ is obtained from $E$ \textit{via level raising at} $q$; $A$ and $E$ are \textit{congruent mod 2}.

Remark
There are a lot of level raising primes!

Example
$E = X_0(11) : y^2 + y = x^3 - x^2 - 10x - 20$.

<table>
<thead>
<tr>
<th>$a_p$</th>
<th>2</th>
<th>3</th>
<th>5</th>
<th>7</th>
<th>11</th>
<th>13</th>
<th>17</th>
<th>19</th>
</tr>
</thead>
<tbody>
<tr>
<td>11a</td>
<td>-2</td>
<td>-1</td>
<td>1</td>
<td>-2</td>
<td>1</td>
<td>4</td>
<td>2</td>
<td>0</td>
</tr>
</tbody>
</table>
Definition

Such $q$ is called a \textit{level raising prime} for $E$. We say that $A$ is obtained from $E$ \textit{via level raising at} $q$; $A$ and $E$ are \textit{congruent mod 2}.

Remark

There are a lot of level raising primes!

Example

$E = X_0(11) : y^2 + y = x^3 - x^2 - 10x - 20$. $q = 7$ is a level raising prime. There are three (isogeny classes of) elliptic curves of conductor 77.

<table>
<thead>
<tr>
<th>$a_p$</th>
<th>2</th>
<th>3</th>
<th>5</th>
<th>7</th>
<th>11</th>
<th>13</th>
<th>17</th>
<th>19</th>
</tr>
</thead>
<tbody>
<tr>
<td>11a</td>
<td>-2</td>
<td>-1</td>
<td>1</td>
<td>-2</td>
<td>1</td>
<td>4</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>77a</td>
<td>0</td>
<td>-3</td>
<td>-1</td>
<td>-1</td>
<td>-1</td>
<td>-4</td>
<td>2</td>
<td>-6</td>
</tr>
<tr>
<td>77b</td>
<td>0</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>-1</td>
<td>-4</td>
<td>-6</td>
<td>2</td>
</tr>
<tr>
<td>77c</td>
<td>1</td>
<td>2</td>
<td>-2</td>
<td>-1</td>
<td>1</td>
<td>4</td>
<td>4</td>
<td>0</td>
</tr>
</tbody>
</table>
Definition
Such \( q \) is called a level raising prime for \( E \). We say that \( A \) is obtained from \( E \) via level raising at \( q \); \( A \) and \( E \) are congruent mod 2.

Remark
There are a lot of level raising primes!

Example
\( E = X_0(11) : y^2 + y = x^3 - x^2 - 10x - 20 \). \( q = 7 \) is a level raising prime. There are three (isogeny classes of) elliptic curves of conductor 77. Two of them are congruent to \( E \) mod 2.

<table>
<thead>
<tr>
<th>( a_p )</th>
<th>2</th>
<th>3</th>
<th>5</th>
<th>7</th>
<th>11</th>
<th>13</th>
<th>17</th>
<th>19</th>
</tr>
</thead>
<tbody>
<tr>
<td>11a</td>
<td>-2</td>
<td>-1</td>
<td>1</td>
<td>-2</td>
<td>1</td>
<td>4</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>77a</td>
<td>0</td>
<td>-3</td>
<td>-1</td>
<td>-1</td>
<td>-1</td>
<td>-4</td>
<td>2</td>
<td>-6</td>
</tr>
<tr>
<td>77b</td>
<td>0</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>-1</td>
<td>-4</td>
<td>-6</td>
<td>2</td>
</tr>
<tr>
<td>77c</td>
<td>1</td>
<td>2</td>
<td>-2</td>
<td>-1</td>
<td>1</td>
<td>4</td>
<td>4</td>
<td>0</td>
</tr>
</tbody>
</table>
Let $k = \mathcal{O}/\lambda$. Then

$$E[2] \otimes_{F_2} k \cong A[\lambda].$$
Let $k = \mathcal{O}/\lambda$. Then

$$E[2] \otimes_{F_2} k \cong A[\lambda].$$

2-descent:

$$0 \to E(\mathbb{Q}) \otimes_{\mathbb{Z}} F_2 \to \text{Sel}_2(E/\mathbb{Q}) \to \text{III}(E/\mathbb{Q})[2] \to 0,$$
Let $k = \mathcal{O}/\lambda$. Then

$$E[2] \otimes_{F_2} k \simeq A[\lambda].$$

2-descent:

$$0 \to E(\mathbb{Q}) \otimes_{\mathbb{Z}} F_2 \to \text{Sel}_2(E/\mathbb{Q}) \to \Sha(E/\mathbb{Q})[2] \to 0,$$

$\lambda$-descent:

$$0 \to A(\mathbb{Q}) \otimes_{\mathcal{O}} k \to \text{Sel}_\lambda(A/\mathbb{Q}) \to \Sha(A/\mathbb{Q})[\lambda] \to 0.$$
Let $k = \mathcal{O}/\lambda$. Then
\[ E[2] \otimes_{F_2} k \cong A[\lambda]. \]

2-descent:
\[ 0 \to E(\mathbb{Q}) \otimes_{\mathbb{Z}} F_2 \to \text{Sel}_2(E/\mathbb{Q}) \to \Sha(E/\mathbb{Q})[2] \to 0, \]

$\lambda$-descent:
\[ 0 \to A(\mathbb{Q}) \otimes_{\mathcal{O}} k \to \text{Sel}_\lambda(A/\mathbb{Q}) \to \Sha(A/\mathbb{Q})[\lambda] \to 0. \]

Can compare the Selmer groups of $E$ and $A$,
\[ \text{Sel}_2(E/\mathbb{Q}) \otimes k \quad \text{Sel}_\lambda(A/\mathbb{Q}) \]
\[ H^1(\mathbb{Q}, E[2]) \otimes k \quad H^1(\mathbb{Q}, A[\lambda]). \]
Let \( k = \mathcal{O}/\lambda \). Then
\[
E[2] \otimes_{F_2} k \cong A[\lambda].
\]

2-descent:
\[
0 \to E(\mathbb{Q}) \otimes_{\mathbb{Z}} F_2 \to \text{Sel}_2(E/\mathbb{Q}) \to \Sha(E/\mathbb{Q})[2] \to 0,
\]
\lambda\text{-descent:}
\[
0 \to A(\mathbb{Q}) \otimes \mathcal{O} k \to \text{Sel}_\lambda(A/\mathbb{Q}) \to \Sha(A/\mathbb{Q})[\lambda] \to 0.
\]
Can compare the Selmer groups of \( E \) and \( A \),
\[
\text{Sel}_2(E/\mathbb{Q}) \otimes k \xrightarrow{\cong} \text{Sel}_\lambda(A/\mathbb{Q})
\]
\[
H^1(\mathbb{Q}, E[2]) \otimes k \xrightarrow{\cong} H^1(\mathbb{Q}, A[\lambda]).
\]
Parity conjecture

- Assume $K$ is an imaginary quadratic field such that $d_K \neq -4, -3$ satisfying the Heegner hypothesis:
  
  $$p \mid N \implies p \text{ is split in } K.$$
Assume $K$ is an imaginary quadratic field such that $d_K \neq -4, -3$ satisfying the Heegner hypothesis:

$$p \mid N \implies p \text{ is split in } K.$$

Then $K/\mathbb{Q}$ is disjoint with $\mathbb{Q}(E[2])/\mathbb{Q}$ ($\implies E[2](K) = 0$ and $2 \nmid \prod_{v|N} c_v$).
Assume $K$ is an imaginary quadratic field such that $d_K \neq -4, -3$ satisfying the Heegner hypothesis:

$$p \mid N \implies p \text{ is split in } K.$$

Then $K/\mathbb{Q}$ is disjoint with $\mathbb{Q}(E[2])/\mathbb{Q}$ ($\iff E[2](K) = 0$ and $2 \nmid \prod_{v|N} c_v$).

Half of the level raising primes $q$ are inert in $K$. Choose such $q$ henceforth, then

$$\epsilon(f/K) = -\epsilon(g/K).$$
Parity conjecture

- Assume $K$ is an imaginary quadratic field such that $d_K \neq -4, -3$ satisfying the Heegner hypothesis:
  \[ p \mid N \implies p \text{ is split in } K. \]
- Then $K/\mathbb{Q}$ is disjoint with $\mathbb{Q}(E[2])/\mathbb{Q} \iff E[2](K) = 0$ and $2 \nmid \prod_{v | N} c_v$.
- Half of the level raising primes $q$ are inert in $K$. Choose such $q$ henceforth, then
  \[ \varepsilon(f/K) = -\varepsilon(g/K). \]
- BSD $\implies$ rank $E(K)$ and rank$_F A(K)$ have different parity.
Assume $K$ is an imaginary quadratic field such that $d_K \neq -4, -3$ satisfying the Heegner hypothesis:

\[ p | N \implies p \text{ is split in } K. \]

Then $K/\mathbb{Q}$ is disjoint with $\mathbb{Q}(E[2])/\mathbb{Q}$ ($\implies E[2](K) = 0$ and $2 \nmid \prod_{v \mid N} c_v$).

Half of the level raising primes $q$ are inert in $K$. Choose such $q$ henceforth, then

\[ \varepsilon(f/K) = -\varepsilon(g/K). \]

BSD $\implies$ rank $E(K)$ and rank$_F A(K)$ have different parity.

$\dim_{\mathbb{F}_2} \Sha(E/K)[2]$ and $\dim_k \Sha(A/K)[\lambda]$ should be even.
BSD predicts that

**Parity Conjecture**

$\dim_{F_2} \text{Sel}_2(E/K)$ and $\dim_k \text{Sel}_\lambda(A/K)$ have different parity.
BSD predicts that

**Parity Conjecture**

\[ \dim_{\mathbb{F}_2} \text{Sel}_2(E/K) \text{ and } \dim_k \text{Sel}_\lambda(A/K) \text{ have different parity.} \]

**Theorem A (–)**

When \( \overline{\rho}(\text{Frob}_q) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \),

\[ \dim_{\mathbb{F}_2} \text{Sel}_2(E/K) = \dim_k \text{Sel}_\lambda(A/K) \pm 1. \]
BSD predicts that

**Parity Conjecture**

\( \dim_{F_2} \mathrm{Sel}_2(E/K) \) and \( \dim_k \mathrm{Sel}_\lambda(A/K) \) have different parity.

**Theorem A (−)**

When \( \bar{\rho}(\text{Frob}_q) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \),

\[
\dim_{F_2} \mathrm{Sel}_2(E/K) = \dim_k \mathrm{Sel}_\lambda(A/K) \pm 1.
\]
Remark
The conclusion of the theorem may fail when \((\text{nontrivial at } 2)\) is not satisfied due to the uncertainty of the local condition at 2.
Remark
The conclusion of the theorem may fail when (nontrivial at 2) is not satisfied due to the uncertainty of the local condition at 2.

Example
The elliptic curve

\[ E = 2351a1 : y^2 + xy + y = x^3 - 5x - 5 \]

has trivial \( \overline{\rho} |_{G_{\mathbb{Q}_2}} \).
Remark
The conclusion of the theorem may fail when (nontrivial at 2) is not satisfied due to the uncertainty of the local condition at 2.

Example
The elliptic curve

\[ E = 2351a1 : y^2 + xy + y = x^3 - 5x - 5 \]

has trivial \( \bar{\rho}|_{G_{\mathbb{Q}_2}} \). The elliptic curve

\[ A = 25861i1 : y^2 + xy + y = x^3 + x^2 - 17x + 30 \]

is obtained from \( E \) via level raising at \( q = 11 \).
Remark
The conclusion of the theorem may fail when (nontrivial at 2) is not satisfied due to the uncertainty of the local condition at 2.

Example
The elliptic curve

$$E = 2351a1 : y^2 + xy + y = x^3 - 5x - 5$$

has trivial $\bar{\rho}|_{G_{\mathbb{Q}_2}}$. The elliptic curve

$$A = 25861i1 : y^2 + xy + y = x^3 + x^2 - 17x + 30$$

is obtained from $E$ via level raising at $q = 11$. For $K = \mathbb{Q}(\sqrt{-111})$,

$$\text{rank } E(K) = \dim_{\mathbb{F}_2} \text{Sel}_2(E/K) = 1,$$

$$\text{rank } A(K) = \dim_{\mathbb{F}_2} \text{Sel}_2(A/K) = 4.$$
Remark
\[ \dim_k \Sha(A/\mathbb{Q})[\lambda] \] is not necessarily even. No parity prediction for 2-Selmer groups over \( \mathbb{Q} \)!
Remark
\( \dim_k \Sha(A/\mathbb{Q})[\lambda] \) is not necessarily even. No parity prediction for 2-Selmer groups over \( \mathbb{Q} \! \). 

Remark
When \( A \) has an odd degree polarization, Poonen-Stoll constructed \( c \in \Sha(A/\mathbb{Q})[2] \) with Cassels-Tate pairing \( \langle c, c \rangle = 0 \) or \( 1/2 \in \mathbb{Q}/\mathbb{Z} \) so that \( \langle , \rangle \) on \( \Sha(A/\mathbb{Q})[2] \) is alternating if and only if \( \langle c, c \rangle = 0 \). A quadratic base change \( K/\mathbb{Q} \) kills this obstruction.
Heegner points

Corollary

If \( \dim \text{Sel}_2(E/K) = 1 \), then \( \dim_k \text{Sel}_\lambda(A/K) = 0 \) or 2.
Heegner points

Corollary

If \( \dim \text{Sel}_2(E/K) = 1 \), then \( \dim_k \text{Sel}_\chi(A/K) = 0 \) or 2.

Theorem B (−)

Suppose \( \dim \text{Sel}_2(E/K) = 1 \). Let \( y_K \in E(K) \) be a Heegner point. Suppose \( \bar{\rho}(\text{Frob}_q) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \) and \( \# \ker(J_0(N) \to J_1(N)) \) is odd. For simplicity assume \( \dim A = 1 \).
Heegner points

Corollary

If \( \dim \text{Sel}_2(E/K) = 1 \), then \( \dim_k \text{Sel}_\lambda(A/K) = 0 \) or 2.

Theorem B (–)

Suppose \( \dim \text{Sel}_2(E/K) = 1 \). Let \( y_K \in E(K) \) be a Heegner point. Suppose \( \bar{\rho}(\text{Frob}_q) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \) and \( \# \ker(J_0(N) \to J_1(N)) \) is odd. For simplicity assume \( \dim A = 1 \).

If the 2-part of BSD formula is true for \( A/K \). Then

\[
\text{Sel}_2(A/K) = 0 \iff y_K \mod q \not\in 2E(F_{q^2}) + E(F_q).
\]
Heegner points

Corollary
If \( \dim \text{Sel}_2(E/K) = 1 \), then \( \dim_k \text{Sel}_\lambda(A/K) = 0 \) or 2.

Theorem B (–)
Suppose \( \dim \text{Sel}_2(E/K) = 1 \). Let \( y_K \in E(K) \) be a Heegner point. Suppose \( \overline{\rho}(\text{Frob}_q) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \) and \( \# \ker(J_0(N) \to J_1(N)) \) is odd. For simplicity assume \( \dim A = 1 \).
If the 2-part of BSD formula is true for \( A/K \). Then

\[
\text{Sel}_2(A/K) = 0 \iff y_K \mod q \notin 2E(F_{q^2}) + E(F_q).
\]
(The latter is an index 2 subgroup of \( E(F_{q^2}) \)).
Heegner points

Corollary

If \( \dim \text{Sel}_2(E/K) = 1 \), then \( \dim_k \text{Sel}_\lambda(A/K) = 0 \) or 2.

Theorem B (\(-\))

Suppose \( \dim \text{Sel}_2(E/K) = 1 \). Let \( y_K \in E(K) \) be a Heegner point. Suppose \( \bar{\rho}(\text{Frob}_q) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \) and \( \# \ker(J_0(N) \to J_1(N)) \) is odd. For simplicity assume \( \dim A = 1 \).

If the 2-part of BSD formula is true for \( A/K \). Then

\[
\text{Sel}_2(A/K) = 0 \iff y_K \mod q \not\in 2E(F_{q^2}) + E(F_q).
\]

(The latter is an index 2 subgroup of \( E(F_{q^2}) \)).

Remark
Heegner points

Corollary

If \( \dim \text{Sel}_2(E/K) = 1 \), then \( \dim_k \text{Sel}_\lambda(A/K) = 0 \) or 2.

Theorem B (–)

Suppose \( \dim \text{Sel}_2(E/K) = 1 \). Let \( y_K \in E(K) \) be a Heegner point. Suppose \( \bar{\rho}(\text{Frob}_q) = (1 \ 1 \\ 0 \ 1) \) and \( \# \ker(J_0(N) \to J_1(N)) \) is odd. For simplicity assume \( \dim A = 1 \). If the 2-part of BSD formula is true for \( A/K \). Then

\[
\text{Sel}_2(A/K) = 0 \iff y_K \mod q \not\in 2E(\mathbb{F}_{q^2}) + E(\mathbb{F}_q).
\]

(The latter is an index 2 subgroup of \( E(\mathbb{F}_{q^2}) \)).

Remark

Establish an instance of “Jochnowitz congruences” in the terminology of Bertolini-Darmon: \( f \equiv g \leadsto L'(f/K, 1) \equiv L(g/K, 1) \).
Heegner points

Corollary

If \( \dim \text{Sel}_2(E/K) = 1 \), then \( \dim_k \text{Sel}_\lambda(A/K) = 0 \) or 2.

Theorem B (–)

Suppose \( \dim \text{Sel}_2(E/K) = 1 \). Let \( y_K \in E(K) \) be a Heegner point. Suppose \( \bar{\rho}(\text{Frob}_q) = \left( \begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix} \right) \) and \( \# \ker(J_0(N) \to J_1(N)) \) is odd. For simplicity assume \( \dim A = 1 \).

If the 2-part of BSD formula is true for \( A/K \). Then

\[
\text{Sel}_2(A/K) = 0 \iff y_K \mod q \not\in 2E(F_{q^2}) + E(F_q).
\]

(The latter is an index 2 subgroup of \( E(F_{q^2}) \)).

Remark

Establish an instance of “Jochnowitz congruences” in the terminology of Bertolini-Darmon: \( f \equiv g \leadsto L'(f/K, 1) \equiv L(g/K, 1) \). This level raising process tells us about Heegner points!
When \( \dim \text{Sel}_2(E/K) = 1 \), BSD predicts that

\[
\text{rank}(E(K)) = 1, \quad \Sha(E/K)[2] = 0.
\]
When \( \dim \text{Sel}_2(E/K) = 1 \), BSD predicts that
\[
\text{rank}(E(K)) = 1, \quad \Sha(E/K)[2] = 0.
\]

By Gross-Zagier formula,
\[
\text{BSD formula for } E/K \iff \#\Sha(E/K) = \left( \frac{[E(K) : \mathbb{Z}y_K]}{\prod_{v|N} c_v} \right)^2.
\]
When \( \dim \text{Sel}_2(E/K) = 1 \), BSD predicts that

\[
\text{rank}(E(K)) = 1, \quad \Sha(E/K)[2] = 0.
\]

By Gross-Zagier formula,

\[
\text{BSD formula for } E/K \iff \#\Sha(E/K) = \left( \frac{[E(K) : \mathbb{Z}y_K]}{\prod_{v|N} c_v} \right)^2.
\]

Conjecture (2-part of BSD formula)

\[ y_K \not\in 2E(K). \]
When \( \dim \text{Sel}_2(E/K) = 1 \), BSD predicts that

\[
\operatorname{rank}(E(K)) = 1, \quad \Sha(E/K)[2] = 0.
\]

By Gross-Zagier formula,

\[
\text{BSD formula for } E/K \iff \#\Sha(E/K) = \left( \frac{[E(K):\mathbb{Z}y_K]}{\prod_{v|N} c_v} \right)^2.
\]

Conjecture (2-part of BSD formula)

\[ y_K \notin 2E(K). \]

Corollary

If \( \text{Sel}_2(A/K) = 0 \), then

\[ 2\text{-part of BSD for } A/K \implies 2\text{-part of BSD for } E/K. \]
Question

\[ y_K \mod q \not\in 2E(\mathbb{F}_{q^2}) + E(\mathbb{F}_q) \] for some \( q \)?
Question

\[ y_K \mod q \not\in 2E(F_{q^2}) + E(F_q) \text{ for some } q? \]

Answer

No.
Question

\[ y_K \mod q \not\in 2E(\mathbb{F}_{q^2}) + E(\mathbb{F}_q) \text{ for some } q? \]

Answer

No.

\[ E(K)/2E(K) \cong \mathbb{Z}/2\mathbb{Z}. \]
Question

\[ y_K \ mod \ q \not\in 2E(\mathbb{F}_{q^2}) + E(\mathbb{F}_q) \text{ for some } q? \]

Answer

No.

\[ E(K)/2E(K) \cong \mathbb{Z}/2\mathbb{Z}. \text{ Gal}(K/\mathbb{Q}) \text{ always acts } \textit{trivially} \text{ on } \mathbb{Z}/2\mathbb{Z}. \]
Question

\[ y_K \mod q \notin 2E(\mathbb{F}_{q^2}) + E(\mathbb{F}_q) \text{ for some } q? \]

Answer

No.

\[ E(K)/2E(K) \cong \mathbb{Z}/2\mathbb{Z}. \text{ Gal}(K/\mathbb{Q}) \text{ always acts } trivially \text{ on } \mathbb{Z}/2\mathbb{Z}. \text{ So} \]

\[ y_K \mod q \in E(\mathbb{F}_{q^2})/2E(\mathbb{F}_{q^2}) \]

is invariant under Frob\(_q\).
Question

\[ y_K \mod q \notin 2E(\mathbb{F}_{q^2}) + E(\mathbb{F}_q) \text{ for some } q? \]

Answer

No.

\[ E(K)/2E(K) \cong \mathbb{Z}/2\mathbb{Z}. \text{ Gal}(K/\mathbb{Q}) \text{ always acts trivially on } \mathbb{Z}/2\mathbb{Z}. \text{ So} \]

\[ y_K \mod q \in \frac{E(\mathbb{F}_{q^2})}{2E(\mathbb{F}_{q^2})} \]

is invariant under Frob\(_q\). When \( \bar{\rho}(\text{Frob}_q) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \), the invariant subspace is exactly the image of

\[ \mathbb{Z}/2\mathbb{Z} \cong \frac{E(\mathbb{F}_q)}{2E(\mathbb{F}_q)} \hookrightarrow \frac{E(\mathbb{F}_{q^2})}{2E(\mathbb{F}_{q^2})} \cong (\mathbb{Z}/2\mathbb{Z})^2. \]
Question

\[ y_K \mod q \not\in 2E(\mathbb{F}_{q^2}) + E(\mathbb{F}_q) \] for some \( q \)?

Answer

No.

\[ E(K)/2E(K) \cong \mathbb{Z}/2\mathbb{Z}. \text{ Gal}(K/\mathbb{Q}) \text{ always acts trivially on } \mathbb{Z}/2\mathbb{Z}. \text{ So } \]

\[ y_K \mod q \in E(\mathbb{F}_{q^2})/2E(\mathbb{F}_{q^2}) \]

is invariant under Frob\(_q\). When \( \bar{\rho}(\text{Frob}_q) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \), the invariant subspace is exactly the image of

\[ \mathbb{Z}/2\mathbb{Z} \cong E(\mathbb{F}_q)/2E(\mathbb{F}_q) \hookrightarrow E(\mathbb{F}_{q^2})/2E(\mathbb{F}_{q^2}) \cong (\mathbb{Z}/2\mathbb{Z})^2. \]

Thus always

\[ y_K \mod q \in 2E(\mathbb{F}_{q^2}) + E(\mathbb{F}_q). \]
Obstruction for rank lowering

Theorem C (–)
Suppose $\bar{\rho}(\text{Frob}_q) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. If $\dim \text{Sel}_2(E/K) = 1$, then

$$\dim_k \text{Sel}_\lambda(A/K) = 2.$$
Obstruction for rank lowering

Theorem C (–)
Suppose $\bar{\rho}(\text{Frob}_q) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. If $\dim \text{Sel}_2(E/K) = 1$, then

$$\dim_k \text{Sel}_\lambda(A/K) = 2.$$ 

Over $K$, there is an intrinsic reason forcing the 2-Selmer rank to go up.
Obstruction for rank lowering

Theorem C (−)
Suppose $\bar{\rho}(\text{Frob}_q) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. If $\dim \text{Sel}_2(E/K) = 1$, then

$$\dim_k \text{Sel}_\lambda(A/K) = 2.$$ 

Over $K$, there is an intrinsic reason forcing the 2-Selmer rank to go up.
Example

\[ E = X_0(11). \]

<table>
<thead>
<tr>
<th>( q )</th>
<th>( A )</th>
<th>( d_K )</th>
<th>rank ( A(K) )</th>
<th>dim ( \text{III}(A/K)[2] )</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>77a</td>
<td>-8</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>77b</td>
<td>-8</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>13</td>
<td>143a</td>
<td>-7</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>13</td>
<td>143a</td>
<td>-8</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>17</td>
<td>187a</td>
<td>-7</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>17</td>
<td>187a</td>
<td>-24</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>19</td>
<td>209a</td>
<td>-7</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>19</td>
<td>209a</td>
<td>-19</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>29</td>
<td>319a</td>
<td>-8</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>29</td>
<td>319a</td>
<td>-19</td>
<td>0</td>
<td>2</td>
</tr>
</tbody>
</table>
Example

$E = X_0(11)$.  

<table>
<thead>
<tr>
<th>$q$</th>
<th>$A$</th>
<th>$d_K$</th>
<th>rank $A(K)$</th>
<th>dim $\Sha(A/K)[2]$</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>77a</td>
<td>-8</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>77b</td>
<td>-8</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>13</td>
<td>143a</td>
<td>-7</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>13</td>
<td>143a</td>
<td>-8</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>17</td>
<td>187a</td>
<td>-7</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>17</td>
<td>187a</td>
<td>-24</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>19</td>
<td>209a</td>
<td>-7</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>19</td>
<td>209a</td>
<td>-19</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>29</td>
<td>319a</td>
<td>-8</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>29</td>
<td>319a</td>
<td>-19</td>
<td>0</td>
<td>2</td>
</tr>
</tbody>
</table>

This never happens for $\Sha(A/K)[p]$ when $p$ is odd!
In contrast to the situation over $\mathbb{Q}$

In the joint work (in progress) with Bao Le Hung, we enhance Ribet’s level raising theorem (mod 2). One curious consequence:
In contrast to the situation over $\mathbb{Q}$

In the joint work (in progress) with Bao Le Hung, we enhance Ribet’s level raising theorem (mod 2). One curious consequence:

**Theorem D (Le Hung, −)**

Suppose $E/\mathbb{Q}$ satisfies our assumptions in the beginning and that $E$ has negative discriminant. Then for any given $r \geq 0$, there exists an abelian variety $A/\mathbb{Q}$ obtained from $E/\mathbb{Q}$ via a sequence of level raising, such that

$$\dim_k \text{Sel}_\lambda(A/\mathbb{Q}) = r.$$
In contrast to the situation over \( \mathbb{Q} \)

In the joint work (in progress) with Bao Le Hung, we enhance Ribet’s level raising theorem (mod 2). One curious consequence:

**Theorem D (Le Hung, –)**

Suppose \( E/\mathbb{Q} \) satisfies our assumptions in the beginning and that \( E \) has negative discriminant. Then for any given \( r \geq 0 \), there exists an abelian variety \( A/\mathbb{Q} \) obtained from \( E/\mathbb{Q} \) via a sequence of level raising, such that

\[
\dim_k \text{Sel}_\lambda(A/\mathbb{Q}) = r.
\]

Thanks!