Computing the image of Galois representations attached to an elliptic curve

Andrew V. Sutherland (MIT)

December 1, 2009

joint work with Nicholas Katz (Princeton)
Definitions

For an elliptic curve $E/K$ and a prime $\ell \neq \text{char}(K)$, the group $\text{Gal}(\bar{K}/K)$ acts on the $\ell$-adic Tate module

$$T_\ell(E) = \lim_{\leftarrow n} E[\ell^n].$$

This yields a group representation

$$\rho_{E,\ell} : \text{Gal}(\bar{K}/K) \to \text{Aut}(T_\ell(E)) \cong \text{GL}_2(\mathbb{Z}_\ell).$$

For this talk $K = \mathbb{Q}$. 
Surjectivity of $\rho_{E,\ell}$

For $E$ without complex multiplication, $\rho_{E,\ell}$ is usually surjective.

Theorem (Serre)
Let $K$ be a number field and assume $E/K$ does not have CM.
1. The image of $\rho_{E,\ell}$ has finite index in $\text{GL}_2(\mathbb{Z}_\ell)$ for all $\ell$.
2. There exists $\ell_0$ such that $\text{im} \rho_{E,\ell} = \text{GL}_2(\mathbb{Z}_\ell)$ for all $\ell > \ell_0$.

Conjecturally, there is an $\ell_0$ that depends only on $K$. For $K = \mathbb{Q}$, it is believed that $\ell_0 = 37$.

For this talk $E$ does not have CM.
Reduction modulo $\ell$

We will restrict our attention to $\bar{\rho}_{E,\ell} : \text{Gal}(\bar{K}/K) \to \text{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

**Theorem (Serre)**

*For $K = \mathbb{Q}$ and $\ell > 3$, the map $\rho_{E,\ell}$ is surjective iff $\bar{\rho}_{E,\ell}$ is.*

Conjecturally, $\text{im} \bar{\rho}_{E,\ell}$ determines $\text{im} \rho_{E,\ell}$ for all $\ell > 3$.

The theorem fails for $\ell = 2$ and $\ell = 3$ [Elkies], but it then suffices to consider $\rho_{E,\ell} \mod \ell^k$ for small $k$ (empirically $k \leq 3$).
When is $\bar{\rho}_{E,\ell}$ non-surjective?

If $E[\ell](\mathbb{Q})$ is non-trivial, then $\bar{\rho}_{E,\ell}$ cannot be surjective. This occurs for $\ell \leq 7$ (and no others [Mazur]).

If $E/\mathbb{Q}$ admits a rational $\ell$-isogeny then $\bar{\rho}_{E,\ell}$ is not surjective. This occurs for $\ell \leq 17$ and $\ell = 37$ (and no others, without CM).

However, $\bar{\rho}_{E,\ell}$ may be non-surjective even when $E/\mathbb{Q}$ has no rational $\ell$-isogenies, and $\text{im} \bar{\rho}_{E,\ell}$ may vary in any case.
When is $\bar{\rho}_{E,\ell}$ non-surjective?

If $E[\ell](\mathbb{Q})$ is non-trivial, then $\bar{\rho}_{E,\ell}$ cannot be surjective. This occurs for $\ell \leq 7$ (and no others [Mazur]).

If $E/\mathbb{Q}$ admits a rational $\ell$-isogeny then $\bar{\rho}_{E,\ell}$ is not surjective. This occurs for $\ell \leq 17$ and $\ell = 37$ (and no others, without CM).

However, $\bar{\rho}_{E,\ell}$ may be non-surjective even when $E/\mathbb{Q}$ has no rational $\ell$-isogenies, and $\text{im} \bar{\rho}_{E,\ell}$ may vary in any case.

Classifying the possibilities for $\text{im} \bar{\rho}_{E,\ell} \subseteq \text{GL}_2[\mathbb{Z}/\ell\mathbb{Z}]$ may be viewed as a generalization of Mazur’s Theorem.
Distribution of Frobenius traces

For primes $p$ of good reduction, let $a_p = p + 1 - \#E(\mathbb{F}_p)$.

The Čebotarev density theorem implies that for $c \in \mathbb{Z}/\ell\mathbb{Z}$,

$$\text{dens}(a_p \equiv c \mod \ell) = \frac{\# \{ A : \text{tr} A = c, A \in \text{im} \bar{\rho}_{E,\ell} \}}{\# \text{im} \bar{\rho}_{E,\ell}}.$$

When $\text{im} \bar{\rho}_{E,\ell}$ is small, these densities can become highly non-uniform (even zero).

The constants appearing in both the Lang-Trotter conjecture and Koblitz’ conjecture depend on $\text{dens}(a_p \equiv c \mod m)$. 
Main results

An algorithm to compute $\text{im} \, \bar{\rho}_{E,\ell}$ for small $\ell$ (up to isomorphism). If $\bar{\rho}_{E,\ell}$ is surjective, the algorithm proves this unconditionally. Otherwise its output is heuristically correct with high probability (in principle, this can also be made unconditional).
Main results

An algorithm to compute $\text{im} \hat{\rho}_{E,\ell}$ for small $\ell$ (up to isomorphism). If $\hat{\rho}_{E,\ell}$ is surjective, the algorithm proves this unconditionally. Otherwise its output is heuristically correct with high probability (in principle, this can also be made unconditional).

- Very fast, usually well under a millisecond per curve.
- We have computed $\hat{\rho}_{E,\ell}$ for every $E$ in the Stein-Watkins database (over 100 million curves), for primes $\ell < 60$. 
Main results

An algorithm to compute $\text{im} \tilde{\rho}_{E,\ell}$ for small $\ell$ (up to isomorphism). If $\tilde{\rho}_{E,\ell}$ is surjective, the algorithm proves this unconditionally. Otherwise its output is heuristically correct with high probability (in principle, this can also be made unconditional).

- Very fast, usually well under a millisecond per curve.
- We have computed $\tilde{\rho}_{E,\ell}$ for every $E$ in the Stein-Watkins database (over 100 million curves), for primes $\ell < 60$.

Previous work addressed curves of conductor up to 200 [Reverter-Vila], with partial results up to 30000 [Stein].
A probabilistic approach

The action of the Frobenius endomorphism on $E[\ell](\overline{\mathbb{F}}_p)$ corresponds to a matrix $A_p \in \text{im} \bar{\rho}_\ell \subseteq \text{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

We have $\text{tr} A_p = a_p \mod \ell$ and $\det A_p = p \mod \ell$, hence we know the characteristic polynomial $\lambda^2 - a_p \lambda + p \mod \ell$.

By varying $p$, we can “randomly” sample $\text{im} \bar{\rho}_{E,\ell}$. The Čebotarev density theorem implies equidistribution.
A probabilistic approach

The action of the Frobenius endomorphism on $E[\ell](\overline{\mathbb{F}_p})$ corresponds to a matrix $A_p \in \text{im} \bar{\rho}_\ell \subseteq \text{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

We have $\text{tr} A_p = a_p \mod \ell$ and $\det A_p = p \mod \ell$, hence we know the characteristic polynomial $\lambda^2 - a_p \lambda + p \mod \ell$.

By varying $p$, we can “randomly” sample $\text{im} \bar{\rho}_{E,\ell}$. The Čebotarev density theorem implies equidistribution.

Unfortunately, this does not give enough information.
The case $\ell = 2$

$\text{GL}_2(\mathbb{Z}/2\mathbb{Z}) \cong S_3$ has 6 subgroups in 4 conjugacy classes.

For $H \subseteq \text{GL}_2(\mathbb{Z}/2\mathbb{Z})$, let $t_i(H) = \#\{A \in H : \text{tr} A = i\}$. We consider the possible vectors $t(H) = (t_0(H), t_1(H))$.

1. For $H = \text{GL}_2(\mathbb{Z}/2\mathbb{Z})$ we have $t(H) = (4, 2)$.
2. The subgroup $H \cong \mathbb{Z}/3\mathbb{Z}$ has $t(H) = (1, 2)$.
3. Three conjugate $H \cong \mathbb{Z}/2\mathbb{Z}$ have $t(H) = (2, 0)$
4. The trivial $H$ has $t(H) = (1, 0)$.

1-2 are distinguished from 3-4 by a trace 1 element (easy). We can distinguish 1 from 2 by comparing frequencies (harder). We can’t distinguish 3 from 4 (impossible).
Using the fixspace of $A_p$

The Frobenius endomorphism fixes $E(F_p)[\ell]$, hence we have

$$\text{cok}(A_p - I) \cong E(F_p)[\ell],$$

when viewed as submodules of $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$.

We can easily compute $E(F_p)[\ell]$, and this yields additional information about $A_p$ that cannot be derived from $a_p$.

We can now easily distinguish all 4 subgroups when $\ell = 2$. This generalizes nicely.
Signatures in $GL_2(\mathbb{Z}/\ell\mathbb{Z})$

For each subgroup $H$ of $GL_2(\mathbb{Z}/\ell\mathbb{Z})$, we define the extended signature of $H$ as the multiset

$$S_H = \{(\det A, \text{tr} A, \text{cok}(A - I)) : A \in H\}.$$ 

The signature $s_H$ is simply the set $S_H$, ignoring multiplicities. Note that $s_H$ and $S_H$ are invariant under conjugation.
Signatures in $\text{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$

For each subgroup $H$ of $\text{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, we define the \textit{extended signature} of $H$ as the multiset

$$S_H = \{ (\det A, \text{tr} A, \text{cok}(A - I)) : A \in H \}.$$ 

The \textit{signature} $s_H$ is simply the set $S_H$, ignoring multiplicities. Note that $s_H$ and $S_H$ are invariant under conjugation.

\textbf{Lemma}

\textit{Let} $\ell < 60$ \textit{be prime and let} $G$ \textit{and} $H$ \textit{be subgroups of} $\text{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ \textit{for which the determinant map is surjective.}

1. $s_G = s_H$ $\iff$ $S_G = S_H$
2. $S_G = S_H$ $\implies$ $G \cong H$. 
The lattice of conjugacy classes in $\text{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$

Up to conjugacy, we may determine $\text{im} \bar{\rho}_{E,\ell}$ identifying its location in the lattice of conjugacy classes of $\text{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

We may restrict our attention to the (upwardly closed) subset of classes $C_\ell$ for which the determinant map is surjective.

For any signature set $s$ and $H \in C_\ell$, we say $s_H$ minimally covers $s$ if $s \subset s_H$ and for each $G \in C_\ell$ we have $s \subset s_G \implies s_H \subset s_G$.

Note that if $s$ minimally covered by $s_G$ and $s_H$, then $s_G = s_H$ and therefore $G \cong H$ (by the lemma).
The algorithm

Given an elliptic curve $E/\mathbb{Q}$, a prime $\ell$, and $\epsilon > 0$, set $s \leftarrow \emptyset$, $k \leftarrow 0$ and for each good prime $p \neq \ell$:

1. Compute $E(\mathbb{F}_p)$ to obtain $a_p$ and $V_p = E(\mathbb{F}_p)[\ell]$.
2. Set $s \leftarrow s \cup (p \mod \ell, a_p \mod \ell, V_p)$, and increment $k$.
3. If $s$ is minimally covered by $s_H$ for some $H \in \mathcal{C}_\ell$ and we have $\delta^k_H < \epsilon$, then output $H$ and terminate.
The algorithm

Given an elliptic curve $E/\mathbb{Q}$, a prime $\ell$, and $\epsilon > 0$, set $s \leftarrow \emptyset$, $k \leftarrow 0$ and for each good prime $p \neq \ell$:

1. Compute $E(\mathbb{F}_p)$ to obtain $a_p$ and $V_p = E(\mathbb{F}_p)[\ell]$.
2. Set $s \leftarrow s \cup (p \mod \ell, a_p \mod \ell, V_p)$, and increment $k$.
3. If $s$ is minimally covered by $s_H$ for some $H \in C_\ell$ and we have $\delta_H^k < \epsilon$, then output $H$ and terminate.

Here $\delta_H$ is the maximum over $G \supseteq H$ of the probability that the signature of a random element of $G$ lies in $s_H$, which we take to be zero when $H = \text{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

The values of $s_H$ and $\delta_H$ for all $H \in C_\ell$ are precomputed.
Efficient implementation

If $\overline{\rho}_{E,\ell}$ is surjective, we expect the algorithm to terminate in $O(\log \ell)$ iterations (around ten). Otherwise, for $\epsilon = 2^{-n}$, we typically need $O(n)$ iterations (a few hundred).
If $\bar{\rho}_{E,\ell}$ is surjective, we expect the algorithm to terminate in $O(\log \ell)$ iterations (around ten). Otherwise, for $\epsilon = 2^{-n}$, we typically need $O(n)$ iterations (a few hundred).

For small $p$ we can quickly compute $\#E(\mathbb{F}_p)$ and determine the structure of $E(\mathbb{F}_p)$ using generic group algorithms.

This is much faster than an $\ell$-adic approach for $\ell > 2$, and allows us to treat many $\ell$ simultaneously at almost no cost.
Efficient implementation

If $\bar{\rho}_{E,\ell}$ is surjective, we expect the algorithm to terminate in $O(\log \ell)$ iterations (around ten). Otherwise, for $\epsilon = 2^{-n}$, we typically need $O(n)$ iterations (a few hundred).

For small $p$ we can quickly compute $\#E(\mathbb{F}_p)$ and determine the structure of $E(\mathbb{F}_p)$ using generic group algorithms.

This is much faster than an $\ell$-adic approach for $\ell > 2$, and allows us to treat many $\ell$ simultaneously at almost no cost.

Precomputing the $s_H$ and $\delta_H$ is non-trivial, but this only needs to be done once for each $\ell$. 
Computational results for the Stein-Watkins database

Testing 136,663,068 curves $E/\mathbb{Q}$ without CM for all $\ell < 60$ took 12 CPU-hours, using $\epsilon = 2^{-100}$, or about 307 $\mu$s per curve.

Approximately 1 in 4 curves had non-surjective $\bar{\rho}_{E,\ell}$ for some $\ell$, about 1 in 600 for some $\ell > 3$.

In the surjective cases, an average of 9.2 primes $p$ were used, versus 168.5 primes in the non-surjective case.

The most primes used for any one curve was 2061.
mod $\ell$ images of Galois for $E/Q$ without CM

<table>
<thead>
<tr>
<th>$\ell$</th>
<th>$#H$</th>
<th>$\delta_H$</th>
<th>abelian</th>
<th>all traces</th>
<th>all $n$</th>
<th>torsion/isogeny</th>
<th>SW curves</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
<td>0.500</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$</td>
<td>1673058</td>
</tr>
<tr>
<td>2</td>
<td>0.500</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>$\mathbb{Z}/2\mathbb{Z}$</td>
<td>33352376</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>0.333</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>none</td>
<td>128670</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>0.250</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>$\mathbb{Z}/3\mathbb{Z}$</td>
<td>3519</td>
</tr>
<tr>
<td>4</td>
<td>0.167</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>3-isogeny</td>
<td>74933</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>0.250</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>$\mathbb{Z}/3\mathbb{Z}$</td>
<td>354246</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>0.250</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>none</td>
<td>18642</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>0.375</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>3-isogeny</td>
<td>3165972</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>0.167</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>none</td>
<td>53202</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>0.200</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>$\mathbb{Z}/5\mathbb{Z}$</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>0.200</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>5-isogeny</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>0.100</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>5-isogeny</td>
<td>3120</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>0.050</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>5-isogeny</td>
<td>500</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>0.250</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>none</td>
<td>512</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>0.375</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>5-isogeny</td>
<td>504</td>
<td></td>
</tr>
<tr>
<td>* 20</td>
<td>0.375</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>5-isogeny</td>
<td>520</td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>0.333</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>none</td>
<td>3480</td>
<td></td>
</tr>
<tr>
<td>40</td>
<td>0.250</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>5-isogeny</td>
<td>109970</td>
<td></td>
</tr>
<tr>
<td>48</td>
<td>0.300</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>none</td>
<td>3090</td>
<td></td>
</tr>
<tr>
<td>80</td>
<td>0.417</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>5-isogeny</td>
<td>44272</td>
<td></td>
</tr>
<tr>
<td>96</td>
<td>0.217</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>none</td>
<td>15246</td>
<td></td>
</tr>
<tr>
<td>( \ell )</td>
<td>#H</td>
<td>( \delta_H )</td>
<td>abelian</td>
<td>all traces</td>
<td>all n</td>
<td>torsion/isogeny</td>
<td>SW curves</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>7</td>
<td>18</td>
<td>0.250</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>7-isogeny</td>
<td>2</td>
</tr>
<tr>
<td>36</td>
<td>0.333</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>7-isogeny</td>
<td>414</td>
<td></td>
</tr>
<tr>
<td>42</td>
<td>0.250</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>7-isogeny</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>42</td>
<td>0.417</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>( \mathbb{Z}/7\mathbb{Z} )</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td>* 42</td>
<td>0.417</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>7-isogeny</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td>72</td>
<td>0.399</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>none</td>
<td>52</td>
<td></td>
</tr>
<tr>
<td>84</td>
<td>0.667</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>7-isogeny</td>
<td>1194</td>
<td></td>
</tr>
<tr>
<td>84</td>
<td>0.444</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>7-isogeny</td>
<td>12172</td>
<td></td>
</tr>
<tr>
<td>96</td>
<td>0.357</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>none</td>
<td>112</td>
<td></td>
</tr>
<tr>
<td>126</td>
<td>0.250</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>7-isogeny</td>
<td>1042</td>
<td></td>
</tr>
<tr>
<td>252</td>
<td>0.438</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>7-isogeny</td>
<td>28922</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>110</td>
<td>0.450</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>11-isogeny</td>
<td>2</td>
</tr>
<tr>
<td>* 110</td>
<td>0.450</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>11-isogeny</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>220</td>
<td>0.640</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>11-isogeny</td>
<td>2044</td>
<td></td>
</tr>
<tr>
<td>240</td>
<td>0.409</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>none</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>288</td>
<td>0.250</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>13-isogeny</td>
<td>108</td>
</tr>
<tr>
<td>468</td>
<td>0.375</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>13-isogeny</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>* 468</td>
<td>0.375</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>13-isogeny</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>624</td>
<td>0.667</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>13-isogeny</td>
<td>184</td>
<td></td>
</tr>
<tr>
<td>624</td>
<td>0.444</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>13-isogeny</td>
<td>580</td>
<td></td>
</tr>
<tr>
<td>936</td>
<td>0.250</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>13-isogeny</td>
<td>3194</td>
<td></td>
</tr>
<tr>
<td>1872</td>
<td>0.464</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>13-isogeny</td>
<td>3352</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>1088</td>
<td>0.375</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>17-isogeny</td>
<td>368</td>
</tr>
<tr>
<td>37</td>
<td>15984</td>
<td>0.444</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>37-isogeny</td>
<td>1024</td>
</tr>
</tbody>
</table>
This is a work in progress, with much still to be done:

1. Test more curves, analyze the results.
2. Compute mod $\ell^k$ and mod $m$ Galois images.
3. Consider curves over number fields other than $\mathbb{Q}$.
4. Look at genus 2 Galois images in $\text{GSp}(4, \mathbb{Z}/\ell\mathbb{Z})$. 
Computing the image of Galois representations attached to an elliptic curve

Andrew V. Sutherland (MIT)

December 1, 2009

joint work with Nicholas Katz (Princeton)