Computing with modular forms (mod $p$)

Alex Ghitza

The University of Melbourne
(joint work with Craig Citro, University of Washington)

Monash University
Tuesday 12 May 2009
# Outline

1. **Introduction**
   - Primes and squares
   - Galois representations
   - Modular forms
   - The bridge

2. **A computational problem**
   - Two upper bounds
   - The algorithm
Conjecture (Euler 1744)

Let $p \neq 7$ be an odd prime. Then

$$p = \begin{cases} 
    x^2 + 14y^2 \\
    2x^2 + 7y^2
\end{cases} \iff p \equiv 1, 9, 15, 23, 25, 39 \pmod{56}.$$ 

Let’s back up a bit:

Theorem (Fermat 1640)

If $p$ is an odd prime, then

$$p = x^2 + y^2 \iff p \equiv 1 \pmod{4}.$$
Conjecture (Euler 1744)

Let $p \neq 7$ be an odd prime. Then

$$p = \begin{cases} 
  x^2 + 14y^2 \\
  2x^2 + 7y^2 
\end{cases} \iff p \equiv 1, 9, 15, 23, 25, 39 \pmod{56}.$$

Let’s back up a bit:

Theorem (Fermat 1640)

If $p$ is an odd prime, then

$$p = x^2 + y^2 \iff p \equiv 1 \pmod{4}.$$
One way we might approach Euler’s conjecture is to factor:

\[ p = x^2 + 14y^2 = (x - \sqrt{14}y)(x + \sqrt{14}y) \]

In other words, we want to do arithmetic in \( K = \mathbb{Q}(\sqrt{-14}) \). This study is related to the Galois group \( \text{Gal}(K/\mathbb{Q}) \). (In fact, to get the full picture one needs to work with \( L = K(\sqrt{2\sqrt{2} - 1}) \) and its Galois group.)

Problem: study arithmetic of number fields \( K/\mathbb{Q} \); study structure of Galois groups \( \text{Gal}(K/\mathbb{Q}) \).
We package all Galois groups of number fields together into the absolute Galois group of $\mathbb{Q}$:

$$G_{\mathbb{Q}} := \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = \lim_{\leftarrow} \text{Gal}(K/\mathbb{Q})$$

This is a big topological group. For each prime $\ell$, there is a distinguished element $\text{Frob}_\ell$, and their collection is dense in $G_{\mathbb{Q}}$. 
We study the Galois group $G_{\mathbb{Q}}$ by studying its continuous linear representations

$$\rho : G_{\mathbb{Q}} \longrightarrow \text{GL}(V)$$

We will focus on the case where $V$ is a two-dimensional vector space over $\overline{\mathbb{F}}_p$ for a fixed prime $p$, and refer to such $\rho$ as a Galois representation (mod $p$).
Modular forms: The analytic definition

A modular form of weight $k \in \mathbb{Z}$ is a holomorphic function

$$f: \mathcal{H} \longrightarrow \mathbb{C} \quad \mathcal{H} := \{ \tau \in \mathbb{C} \mid \Im(\tau) > 0 \}$$

satisfying a certain growth condition as $\tau \to i\infty$, as well as the modularity property

$$f \left( \frac{a\tau + b}{c\tau + d} \right) = (c\tau + d)^k f(\tau) \quad \tau \in \mathcal{H}, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}).$$

In particular,

$$f(\tau + 1) = f \left( \frac{1\tau + 1}{0\tau + 1} \right) = (0\tau + 1)^k f(\tau) = f(\tau).$$
A modular form of weight $k \in \mathbb{Z}$ is a holomorphic function

$$f : \mathcal{H} \longrightarrow \mathbb{C} \quad \mathcal{H} := \{ \tau \in \mathbb{C} | \Im(\tau) > 0 \}$$

satisfying a certain growth condition as $\tau \rightarrow i\infty$, as well as the modularity property

$$f \left( \frac{a\tau + b}{c\tau + d} \right) = (c\tau + d)^{k}f(\tau) \quad \tau \in \mathcal{H}, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}).$$

In particular,

$$f(\tau + 1) = f \left( \frac{1\tau + 1}{0\tau + 1} \right) = (0\tau + 1)^{k}f(\tau) = f(\tau).$$
Changing the coefficient ring

So $f$ is periodic with period 1 and has a Fourier expansion

$$f(\tau) = \sum_{n \geq 0} a_n e^{2\pi i n \tau} \in \mathbb{C}[[q]], \quad q = e^{2\pi i \tau}.$$ 

We let $M_k(\mathbb{Z}(p))$ denote the space of modular forms whose Fourier coefficients are $p$-integral, i.e. rational numbers with denominators not divisible by $p$.

We define the space of modular forms (mod $p$) to consist of all reductions modulo $p$ of forms in $M_k(\mathbb{Z}(p))$:

$$M_k(\mathbb{F}_p) := \left\{ \tilde{f} = \sum \tilde{a}_n q^n \in \mathbb{F}_p[[q]] \mid \sum a_n q^n \in M_k(\mathbb{Z}(p)) \right\}.$$
This modular form was known to Ramanujan:

\[ \Delta = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = q - 24q^2 + 252q^3 - 1472q^4 + \ldots \in M_{12}(\mathbb{Z}) \]

We can reduce it, for instance, modulo 5:

\[ \Delta_5 = q + q^2 + 2q^3 + 3q^4 + \ldots \in M_{12}(\mathbb{F}_5). \]
Hecke operators

For each prime $\ell \neq p$, there is a Hecke operator $T_\ell$ on $M_k(\mathbb{F}_p)$, given by

$$T_\ell \left( \sum a_n q^n \right) := \sum a_n \ell q^n + \ell^{k-1} \sum a_n q^{n\ell}$$

An eigenform is an $f \in M_k(\mathbb{F}_p)$ which is a simultaneous eigenvector for all the $T_\ell$'s, for instance:

$$\Delta_5 = q + q^2 + 2q^3 + 3q^4 + 2q^6 + \ldots$$

$$T_3 \Delta_5 = 2q + 2q^2 + 4q^3 + q^4 + 4q^6 + \ldots = 2\Delta_5$$

$$T_{97} \Delta_5 = q + q^2 + 2q^3 + 3q^4 + 2q^6 + \ldots = \Delta_5.$$
Theorem (Deligne, ...)  

Given a Hecke eigenform \( f \in M_k(\overline{\mathbb{F}}_p) \) with eigenvalues \( a_\ell \), there exists a Galois representation 

\[
\rho_f : G_\mathbb{Q} \longrightarrow GL_2(\overline{\mathbb{F}}_p)
\]

which is unramified outside \( p \) and such that for any \( \ell \neq p \):

\[
\text{charpoly } \rho_f(\text{Frob}_\ell) = X^2 - a_\ell X + \ell^{k-1}.
\]

Theorem (Khare-Wintenberger)  

If \( \rho \) is an odd semisimple Galois representation unramified outside \( p \), there exists a Hecke eigenform \( f \in M_k(\overline{\mathbb{F}}_p) \) such that \( \rho \cong \rho_f \), where the weight \( k \) can be chosen according to a precise recipe of Serre.
Theorem (Deligne, ...)

Given a Hecke eigenform \( f \in M_k(\overline{\mathbb{F}}_p) \) with eigenvalues \( a_\ell \), there exists a Galois representation

\[
\rho_f : G_\mathbb{Q} \longrightarrow \text{GL}_2(\overline{\mathbb{F}}_p)
\]

which is unramified outside \( p \) and such that for any \( \ell \neq p \):

\[
\text{charpoly } \rho_f(\text{Frob}_\ell) = X^2 - a_\ell X + \ell^{k-1}.
\]

Theorem (Khare-Wintenberger)

If \( \rho \) is an odd semisimple Galois representation unramified outside \( p \), there exists a Hecke eigenform \( f \in M_k(\overline{\mathbb{F}}_p) \) such that \( \rho \cong \rho_f \), where the weight \( k \) can be chosen according to a precise recipe of Serre.
It is an open problem to determine the number of odd semisimple Galois representations unramified outside $p$. Using the result of Khare-Wintenberger, one can give an upper bound, as well as a guess for the asymptotics: $p^3/48$.

Our objective: enumerate the set of such Galois representations, by enumerating the systems of Hecke eigenvalues occurring in the spaces $M_k(\overline{\mathbb{F}}_p)$.

Note that an eigenform $f$ gives rise to a system of eigenvalues

$$\Phi_f := (a_\ell)_{\ell \neq p}.$$
For all integers $k$:
- compute (a basis for) the space of modular forms $M_k$
- decompose $M_k$ under the action of the Hecke operators $T_\ell$
- make a list $E_k$ of eigensystems

Take the union of all $E_k$. 
How many $k$’s do we need to work with?

**Theorem (Serre-Tate)**

*Every Hecke eigensystem (mod $p$) occurs in weight at most $p^2 - 1$.***

How many $a_\ell$’s do we need to check?

**Theorem (Citro-G)**

*Let $\Phi_1$ and $\Phi_2$ be two Hecke eigensystems (mod $p$) occurring in level one and weights $k_1$ and $k_2$, such that $k_1 \equiv k_2 \pmod{p - 1}$ and

$$\Phi_1(T_\ell) = \Phi_2(T_\ell) \quad \text{for all } \ell \leq \frac{2p + 1}{12}, \ell \neq p.$$*

*Then $\Phi_1 = \Phi_2$.***
How many $k$’s do we need to work with?

**Theorem (Serre-Tate)**

*Every Hecke eigensystem (mod $p$) occurs in weight at most $p^2 - 1$.***

How many $a_\ell$’s do we need to check?

**Theorem (Citro-G)**

*Let $\Phi_1$ and $\Phi_2$ be two Hecke eigensystems (mod $p$) occurring in level one and weights $k_1$ and $k_2$, such that $k_1 \equiv k_2 \pmod{p - 1}$ and

$$\Phi_1(T_\ell) = \Phi_2(T_\ell) \quad \text{for all } \ell \leq \frac{2p + 1}{12}, \ell \neq p.$$*

Then $\Phi_1 = \Phi_2$.**
Main ingredients: Hasse invariant, Sturm bound, theta operator.

- the Hasse invariant $A \in M_{p-1}$ satisfies $T_\ell(Af) = T_\ell(f)$ for all $\ell \neq p$
- Sturm 1987: two cusp forms $f_1, f_2$ of the same weight $k$ and level 1 are equal if their first $k/12$ Fourier coefficients agree
- $\vartheta: M_k \rightarrow S_{k+p+1}$ satisfies $T_\ell \circ \vartheta = \ell \vartheta \circ T_\ell$ for all $\ell$
For $2 \leq k \leq p^2$:

- compute (a basis for) the space of cusp forms $S_k$
- decompose $S_k$ under the action of the Hecke operators $T_\ell$ (requires at most $\ell = k/12$)
- make a list $\mathcal{E}_k$ of eigensystems, keeping track of the first $(2p + 1)/12$ eigenvalues

Take the union of all $\mathcal{E}_k$. 

Alex Ghitza
Computing with modular forms (mod $p$)
There are at least two general approaches to computing the spaces of cusp forms $S_k$ and the Hecke action on them:

- modular symbols (over $\mathbb{Z}$ or directly over $\mathbb{F}_p$)
- isogeny graphs of supersingular elliptic curves

In our experience, the second method is significantly slower than the first. It turns out that there is an even better choice: the Victor Miller basis for $S_k$. This is a reduced echelon form basis, using the fact that the algebra of forms of level one is generated by the Eisenstein series $E_4$ and $E_6$. 
Some results

We implemented our algorithm in Sage.

<table>
<thead>
<tr>
<th>$p$</th>
<th>bound</th>
<th>number</th>
<th>$[p^3/48]$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>7</td>
<td>12</td>
<td>9</td>
<td>7</td>
</tr>
<tr>
<td>11</td>
<td>50</td>
<td>35</td>
<td>27</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>193</td>
<td>297984</td>
<td>150144</td>
<td>149772</td>
</tr>
<tr>
<td>197</td>
<td>316932</td>
<td>160132</td>
<td>159278</td>
</tr>
<tr>
<td>199</td>
<td>326700</td>
<td>164637</td>
<td>164179</td>
</tr>
<tr>
<td>211</td>
<td>389550</td>
<td>196560</td>
<td>195706</td>
</tr>
</tbody>
</table>
Future plans

- gather data up to $p = 2003$ (might require parallelising)
- extend to levels $N > 1$ (find explicit generators for the algebra of modular forms, construct Victor-Miller-like basis)
- extend to other types of automorphic forms (requires infrastructure)