Samuele Anni (IWR - Universität Heidelberg)
joint with Vandita Patel (University of Warwick)

(work in progress)

FoCM 2017,
UB, 12\textsuperscript{th} July 2017
The theory of **congruences** between modular forms is a central topic in number theory.

Congruences display relations between **geometry** and **arithmetic**.
1 Congruences

2 Congruence graphs

3 Checking congruences

4 Conjectures and congruence graphs

5 Data collected
Let $n$ be a positive integer, the congruence subgroup $\Gamma_0(n)$ is a subgroup of $\text{SL}_2(\mathbb{Z})$ given by

$$\Gamma_0(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) : n \mid c \right\}.$$ 

Given a pair of integers $n$ (level) and $k$ (weight), a **modular form** $f$ for $\Gamma_0(n)$ is an holomorphic function on the complex upper half-plane $\mathbb{H}$ satisfying

$$f(\gamma z) = f\left(\frac{az + b}{cz + d}\right) = (cz + d)^k f(z) \quad \forall \gamma \in \Gamma_0(n), z \in \mathbb{H}$$

and a growth condition for the coefficients of its power series expansion

$$f(z) = \sum_{0}^{\infty} a_n q^n, \quad \text{where} \quad q = e^{2\pi i z}.$$
There are families of operators acting on the space of modular forms. In particular, the \textbf{Hecke operators} $T_p$ for every prime $p$. These operators describe the interplay between different group actions on the complex upper half-plane.

We will consider only cuspidal \textbf{newforms}: cuspidal modular forms ($a_0 = 0$), normalized ($a_1 = 1$), which are eigenforms for the Hecke operators and arise from level $n$.

We will denote by $S(n, k)_\mathbb{C}$ the space of cuspforms and by $S(n, k)_{\mathbb{C}}^{\text{new}}$ the subspace of newforms.
Let $f$ and $g$ be two newforms.

$$f = \sum a_m q^m \quad g = \sum b_m q^m.$$ 

Then $\mathbb{Q}_f = \mathbb{Q}(\{a_m\})$ is a number field, the **Hecke eigenvalue field** of $f$. 

**Definition**

We say that $f$ and $g$ are **congruent** mod $p$, if there exists an ideal $\mathfrak{p}$ dividing $p$ in the compositum of the Hecke eigenvalue fields of $f$ and $g$ such that

$$a_m \equiv b_m \mod \mathfrak{p} \quad \text{for all } m.$$
**Example: $S(77, 2)^{\text{new}}_\mathbb{C}$**

\[f_0(q) = q - 3q^3 - 2q^4 - q^5 - q^7 + 6q^9 - q^{11} + 6q^{12} - 4q^{13} + 3q^{15} + \ldots\]

\[f_1(q) = q + q^3 - 2q^4 + 3q^5 + q^7 - 2q^9 - q^{11} - 2q^{12} - 4q^{13} + 3q^{15} + \ldots\]

\[f_2(q) = q + q^2 + 2q^3 - q^4 - 2q^5 + 2q^6 - q^7 - 3q^8 + q^9 - 2q^{10} + q^{11} + \ldots\]

\[f_{3,4}(q) = q + \alpha q^2 + (-\alpha + 1) q^3 + 3q^4 - 2q^5 + (\alpha - 5) q^6 + q^7 + \alpha q^8 + \ldots\]

where $\alpha$ satisfies $x^2 - 5 = 0$.

The Hecke eigenvalue fields are $\mathbb{Q}$ for $f_0, f_1, f_2$ and $\mathbb{Q}(\sqrt{5})$ for $f_3$ and $f_4$. The following congruences hold:

\[f_0 \equiv f_1 \mod 2, \quad f_1 \equiv f_{3,4} \mod p_5, \quad f_2 \equiv f_{3,4} \mod p_2,\]

where $p_2, p_5$ are primes in $\mathbb{Q}(\sqrt{5})$.

This is the **complete** list of possible congruences!
1 Congruences

2 Congruence graphs

3 Checking congruences

4 Conjectures and congruence graphs

5 Data collected
**Congruence Graphs**

- **Vertices**: each vertex in the graph corresponds to a Galois orbit of newforms of level and weight in a given set.

- **Edges**: an edge between two vertices is drawn if there exists a prime $p$ such that a congruence mod $p$ holds between two forms in the Galois orbits considered.

Let $S$ be the set of **divisors of a positive integer** and let $W$ be a **finite set of weights**, we will denote by $G_{S,W}$ the associated graph.
$\mathcal{G}_{[1,7,11,77],[2]}$
Congruences, graphs and modular forms

$G_{[1,2,3,5,6,10,15,30],[2,4]}$
Congruences, graphs and modular forms

Congruence graphs

$G_{[1,19],[2,4]}$
Congruence graphs

$G_{[1,19],[2,4,6]}$
Congruences, graphs and modular forms

Congruence graphs

$G_{1,2,4,8,16,32,64,128},[4]$
1. Congruences

2. Congruence graphs

3. Checking congruences

4. Conjectures and congruence graphs

5. Data collected
How do we check congruence?

**Sturm Theorem**

Let $n \geq 1$ be an integer. Let $f(q) = \sum a_m q^m$ be a modular form of level $n$ and weight $k$, with coefficients in the ring of integers of a number field, and let $\lambda$ be a maximal ideal herein. Suppose that the reduction of the $q$-expansion of $f$ modulo $\lambda$ satisfies

$$a_m \equiv 0 \pmod{\lambda} \text{ for all } m \leq \frac{k}{12}[\text{SL}_2(\mathbb{Z}) : \Gamma_0(n)].$$

Then $a_m \equiv 0 \pmod{\lambda}$ for all $m$.

Suppose $n \geq 5$. Sturm Theorem then follows from the fact that the line bundle of modular forms of weight $k$ on $X(n)_{\mathbb{C}}$ has degree:

$$\deg(\omega^\otimes k) = \frac{k}{24} \cdot [\text{SL}_2(\mathbb{Z}) : \Gamma_0(n)].$$

Considering automorphisms, we obtain the Sturm bound.
**Theorem (Kohnen+ε)**

Let $k_1, k_2 \geq 2$ and $n$ be positive integers. Let $f_1, f_2$ be modular forms of level $n$ and weight $k_1, k_2$ respectively. Let $\ell$ be a prime number. Assume that the $q$-expansions of $f_1$ and $f_2$ have coefficients in the ring of integers of a number field, and let $\lambda$ be a maximal ideal herein such that $(\ell) \subset \lambda$.

If $a_m(f_1) \equiv a_m(f_2) \mod \lambda$ for every $m$ such that

$$m \leq \frac{\max\{k_1, k_2\}}{12} \cdot \begin{cases} [\text{SL}_2(\mathbb{Z}) : \Gamma_0(n) \cap \Gamma_1(\ell)] & \text{if } \ell > 2, \\ [\text{SL}_2(\mathbb{Z}) : \Gamma_0(n) \cap \Gamma_1(4)] & \text{if } \ell = 2 \end{cases}$$

then $a_m(f_1) \equiv a_m(f_2) \mod \lambda$ for every $m$.

$$n \in \mathbb{Z}_{>0} \quad \Gamma_1(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) : n \mid a-1, n \mid c \right\}.$$
The previous results can be combined and enhanced in order to give bounds to check congruences between newforms (also for general levels).

Anyway, these kind of result rely on **number fields arithmetic**: if the form do not have the same Hecke eigenvalue field, one needs to work in their compositum, and this is generally computationally expensive.

### Idea

Resultants and computations in positive characteristic.
In our approach we compute the **resultant** of the minimal polynomials of the coefficients, indexed by prime numbers, of the $q$-expansions up to the Sturm bound (we work only with newforms).

Taking the GCDs of several of these resultants, we write a finite set of “potential” congruence primes.

For each prime in this set, we check the existence of congruences working in positive characteristic, i.e. only looking at the generators of the Hecke algebra over finite fields.
Example: $S(59, 4)^{\text{new}}_C$

Let us only look at the $(-1)$-eigenspace for the Atkin-Lehner operator.

$$f(q) = q + \alpha_0 q^2 - q^3 + (-4\alpha_0 - 7) q^4 + (-2\alpha_0 - 1) q^5 + \ldots$$

$$g(q) = q + \alpha_1 q^2 + (-3\alpha_1 + 1) q^3 + (\alpha_1 - 4) q^4 + (3\alpha_1 - 17) q^5 + \ldots$$

where $\alpha_0$ satisfies $x^2 + 4x - 1 = 0$ and $\alpha_1$ satisfies $x^2 - x - 4 = 0$, so

$\mathbb{Q}_f = \mathbb{Q}(\sqrt{5})$, $\mathbb{Q}_g = \mathbb{Q}(\sqrt{17})$

$$\text{Res}(\text{mpoly}(a_2(f)), \text{mpoly}(a_2(g))) = \text{Res}(x^2+4x-1, x^2-x-4) = -2^2 \cdot 19$$

$$\text{Res}(\text{mpoly}(a_3(f)), \text{mpoly}(a_3(g))) = -2 \cdot 19$$

$$\text{Res}(\text{mpoly}(a_5(f)), \text{mpoly}(a_5(g))) = -2^2 \cdot 19 \cdot 1021$$

so the primes of possible congruences are only primes above 2 and 19.
Example: $S(59, 4)^{new}$

Let us reduce $f$ and $g$ modulo 2. Since 2 is inert in $\mathbb{Q}_f$ and split in $\mathbb{Q}_g$, we obtain the mod 2 modular forms $f_1$, $g_1$ and $g_2$ by reduction. These forms have coefficients in $\mathbb{F}_2$ and

\[
a_{2n+1}(f_1) = a_{2n+1}(g_1),
\]

\[
a_{2n}(f_1) = a_{2n}(g_2).
\]

There is no congruence mod 2. Anyway there is a congruence mod 19.

**Question**

Does this happen only modulo 2?
1. Congruences

2. Congruence graphs

3. Checking congruences

4. Conjectures and congruence graphs
   - Hecke algebra: connectedness
   - Rayuela conjecture and chain of congruences

5. Data collected
Motivations

- Connectedness of Hecke algebras;
- Factorization of characteristic polynomials of Hecke operators modulo primes;
- Building databases of mod $\ell$ modular Galois representation;
- Study of generalizations of Maeda’s conjecture;
- Central values of $L$-functions;
- Study of chain of congruences techniques developed by Dieulefait;
- Serre’s conjecture modulo $pq$;
- Prove cases of base change in the Langlands program;
- Study of $GL_2$-type abelian varieties in positive characteristic.
Motivations

- Connectedness of Hecke algebras;
- Factorization of characteristic polynomials of Hecke operators modulo primes;
- Building databases of mod ℓ modular Galois representation;
- Study of generalizations of Maeda’s conjecture;
- Central values of $L$-functions;
- Study of chain of congruences techniques developed by Dieulefait;
- Serre’s conjecture modulo $pq$;
- Prove cases of base change in the Langlands program;
- Study of GL$_2$-type abelian varieties in positive characteristic.
**Hecke Algebra: Connectedness**

**Definition**

*The Hecke algebra* $\mathbb{T}(n, k)$ is the $\mathbb{Z}$-subalgebra of $\text{End}_\mathbb{C}(S(n, k)_\mathbb{C})$ generated by Hecke operators $T_p$ for every prime $p$.

**Question (Ash, Mazur)**

Is $\text{Spec } \mathbb{T}(n, k)$ connected?

$k=2$ yes! This was proved by Mazur for prime levels.

Main idea: work with the Jacobian of the modular curve $X_0(p)$. If the spectrum is disconnected the Jacobian will decompose as a nontrivial direct product of principally polarized abelian varieties.

The congruence graphs are related to the dual graphs of the spectrum of the Hecke algebra.
primes up to 293 and weight 2
Open problem when $k > 2$.

**Quote from a talk of William Stein (December 1999)**

“Well, the reason why the question is particularly intriguing is that we don’t seem to have any hope of a proof that mimics the proof for weight 2. The higher weight motives just don’t (yet...) have the precise algebro-geometric structure that come from principally polarized abelian varieties. So one would need an utterly different kind of proof, (if the connectedness property is true... which, after your calculations\textsuperscript{a} looks possible).” Mazur, email, yesterday.

\textsuperscript{a}for $k \leq 8$ and $p \leq 53$

Verified for primes up to 997 and weight 4, primes up to 293 and weight up to 8, primes up to 97 weight up to 12.
primes up to 293 and weight 4
primes up to 293 and weight 6
primes up to 97 and weight 10
Congruences, graphs and modular forms
Conjectures and congruence graphs

primes up to 97 and weight 12
Warning: here there are also forms of level 1!
**Conjecture I**

**Theorem**

$\text{Spec } \mathbb{T}(p, k)$ is connected for

- $p$ prime $\leq 997$ with $k = 4$,
- $p$ prime $\leq 293$ with $k = 6, 8$,
- $p$ prime $\leq 97$ with $k = 10, 12$.

This implies that $G_{[p],[k]}$ is a connected graphs for $p$ and $k$ as above.

**Theorem**

$G_{[p],[4]}$ is a complete graph for $p$ prime $\leq 997$.

**Conjecture**

$G_{[p],[4]}$ is a complete graph for all primes $p$. 
The graph $G_{S,W}$ may not be connected. The computations suggest the following conjecture:

**Conjecture**

Given $S$ and $W$, there exists a finite set $W'$, with $W \subseteq W'$, such that the graph $G_{S,W'}$ is connected.

This conjecture is a theorem if we assume Maeda’s conjecture for level 1 modular forms.

This conjecture is equivalent to the connectedness of the Hecke algebra acting on the disjoint sum of newform spaces in the given set of levels and weights.
$G_{[1,7,11,77],[2]}$
$G_{[1,2,43,86],[2]}$
$G_{[1, 2, 43, 86], [2, 4]}$
Another observation obtained through extensive computations is the existence of forms which are congruent modulo different primes to each of the newforms in the set considered.

These forms or at least the connectedness of the graphs may lead to new results in the chain of congruences techniques developed by Dieulefait and towards the Rayuela conjecture.
\[ G_{[1,2,43,86],[2,4]} \]
SUBGRAPH OF $G_{[1,2,43,86],[2,4]}$
$G_{[1,19],[2,4]}$
Congruences, graphs and modular forms

Conjectures and congruence graphs

$G_{[1,19],[2,4,6]}$
Subgraph of $G_{[1,19],[2,4,6]}$
Conjecture (Rayuela Conjecture (Dieulefait, Pacetti))

Let $F$ be a totally real number field, $\ell_0$, $\ell_\infty$ prime numbers and

$$\rho_i : \text{Gal}(\overline{F}/F) \to \text{GL}_2(\overline{\mathbb{F}}_{\ell_i}), \quad i = 0, \infty,$$

two absolutely irreducible odd Galois representations. Then there exists a family of odd, absolutely irreducible, 2-dimensional strictly compatible systems of Galois representations $\{\rho_i, \lambda\}_{i=1}^n$ such that:

- $\rho_0 \equiv \rho_{1,\lambda_0} \pmod{\lambda_0}$, with $\lambda_0 | \ell_0$.
- $\rho_\infty \equiv \rho_{n,\lambda_\infty} \pmod{\lambda_\infty}$, with $\lambda_\infty | \ell_\infty$.
- for $i = 1, \ldots, n - 1$ there exist $\lambda_i$ prime such that $\rho_{i,\lambda_i} \equiv \rho_{i+1,\lambda_i} \pmod{\lambda_i}$,
- all the congruences involved are MLT (all the congruences involved are of big, odd and absolutely irreducible representations).
1. **Congruences**

2. **Congruence graphs**

3. **Checking congruences**

4. **Conjectures and congruence graphs**

5. **Data collected**
All the computations have been done on a server at the University of Warwick:

<table>
<thead>
<tr>
<th>server</th>
<th>year</th>
<th>speed</th>
<th>total cores</th>
<th>RAM</th>
<th>disks</th>
</tr>
</thead>
<tbody>
<tr>
<td>hecke</td>
<td>2012</td>
<td>2600(MHz)</td>
<td>64</td>
<td>512(gb)</td>
<td>19 (tb)</td>
</tr>
</tbody>
</table>

Levels of type $pq$ for $p$ and $q$ primes up to 300 (less when the weight is higher $\sim 150$) and weights up to 12.
Data analysis

- Level up to 360, weights in $[2, 4]$
- Level up to 360, weights in $[2, 4, 6]$
- Level up to 120, weights in $[2, 4, 6, 8, 10]$
- Level up to 120, weights in $[2, 4, 6, 8, 10, 12]$
Data collected

Data analysis: vertices
Data analysis: edges
Data analysis: number of connected components

level up to 360, weights in \([2, 4]\)  

level up to 360, weights in \([2, 4, 6]\)
Data collected

- Level up to 120, weights in [2, 4, 6, 8, 10]
- Level up to 120, weights in [2, 4, 6, 8, 10, 12]
Questions:

- Is it possible to predict the number of edges?
- What is the smallest weight for which a given graph becomes connected?
- Extensions to number fields: Hilbert modular forms and Bianchi forms and extensions to Siegel modular forms.
- Relax the requirements: ask for isomorphic mod $\ell$ Galois representations or projective mod $\ell$ Galois representations.
Congruences, graphs and modular forms

Samuele Anni (IWR - Universität Heidelberg)
joint with Vandita Patel (University of Warwick)

FoCM 2017,
UB, 12\textsuperscript{th} July 2017

Thanks!