Higher Congruences Between Modular Forms

Catherine Hsu · University of Oregon · cathyh@uoregon.edu

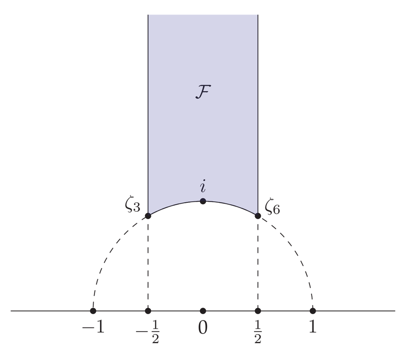
Motivating Goal

Use a certain p-adic value to bound the depths of Eisenstein congruences for squarefree level N

What is a modular form?

$SL(2,\mathbb{Z})$ acts on the complex upper half-plane $\mathfrak{h}$ via Möbius transformations: for

$$z \in \mathfrak{h}, \quad \gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL(2,\mathbb{Z}), \quad \gamma z := \frac{az+b}{cz+d}.$$



Fundamental domain: $SL(2,\mathbb{Z}) \circlearrowright \mathfrak{h}$

Given a positive integer N, the **congruence subgroup** $\Gamma_0(N) \subseteq SL(2,\mathbb{Z})$ is the subgroup of matrices γ with $c \equiv 0 \pmod N$.

For a non-negative integer k and congruence subgroup $\Gamma_0(N)$, a **modular form of weight k and level N** is a function $f : \mathfrak{h} \to \mathbb{C}$ satisfying

(i) f is holomorphic on $\mathfrak{h}$;
(ii) $f(\gamma z) = (cz+d)^k f(z)$ for all $\gamma \in \Gamma_0(N)$;
(iii) a certain growth condition as $\mathrm{Im}(z) \to \infty$.

The modularity property (ii) implies each modular form has a **Fourier expansion** given by

$$f = \sum_{n=-\infty}^{\infty} a_n q^n, \quad q = e^{2\pi i}.$$

The growth condition (iii) on f means $a_n = 0$ for all $n < 0$. If f is a **cusp form**, then $a_0 = 0$.

What are p-adic numbers?

Because congruences between integers play a central role in number theory, we use a metric in which a number is "small" if it is divisible by a high power of p. The ***p*-adic metric** is

$$|u \cdot p^s|_p = p^{-s},$$

where $\gcd(u,p) = 1$. The ***p*-adic numbers** $\mathbb{Q}_p$ are the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$, and each ***p*-adic integer** $a \in \mathbb{Z}_p$ can be expressed as

$$a = a_0 + a_1 p + \cdots + a_n p^n + \cdots,$$

where $a_i \in \mathbb{Z}$. A finite extension $K/\mathbb{Q}_p$ is called a ***p*-adic field**, and the integral closure of $\mathbb{Z}_p$ in K is a local ring $\mathcal{O}$ with uniformizer ϖ.

What is a congruence between modular forms?

For a prime p, two modular forms

$$f_1 = \sum_{n=0}^{\infty} a_n q^n, \quad f_2 = \sum_{n=0}^{\infty} b_n q^n$$

are **congruent modulo** $\mathfrak{p}$ if for each $n \in \mathbb{Z}_{\geq 0}$,

$$a_n \equiv b_n \pmod{\mathfrak{p}}, \qquad (*)$$

where $\mathfrak{p} \subseteq \overline{\mathbb{Q}}$ is a prime ideal lying over p. The **depth of congruence** is related to the highest power of $\mathfrak{p}$ for which $(*)$ holds for all $n \in \mathbb{Z}_{\geq 0}$.

In this project, we examine **Eisenstein congruences** between certain cusp forms called **newforms** and the weight 2 Eisenstein series

$$E_{2,N} = (-1)^{t+1}\frac{\varphi(N)}{24} + \sum_{n=1}^{\infty} \sigma^*(n) q^n,$$

where $t = \Omega(N)$ and $\sigma^*(n)$ is the sum of all non-zero divisors d of n such that $\gcd(d,N) = 1$.

Higher Congruences: A Computational Approach

- Explicit computations in MAGMA [2] are the most direct approach to computing congruences.
- We require a modified **Sturm bound** to determine a finite number of Fourier coefficients that must be checked for a congruence. We use the following algorithm which was adapted from [3]:

Input: A positive squarefree integer N and a prime p. For each divisor M of N:

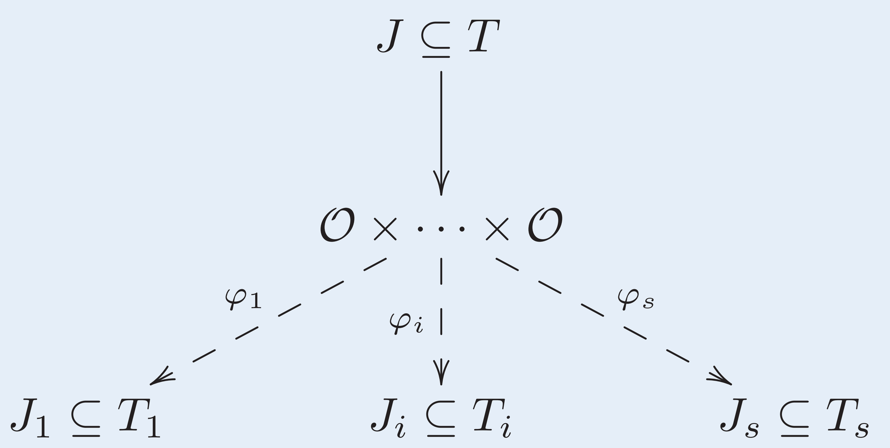
1. Compute Galois conjugacy classes of newforms in $S_2(\Gamma_0(M))$. Call the set *New(M)*.
2. Compute the modified Sturm bound $B = \frac{1}{6} \cdot [SL_2(\mathbb{Z}) : \Gamma_0(N')] = \frac{1}{6} \cdot N \cdot \prod_{p|N}(p+1)$.
3. Compute the coefficients $a_\ell(E_{2,N})$ for primes $\ell \leq B$ with $\ell \nmid N$.
4. For each $f \in$ *New(M)*, compute K_f, the coefficient field of f.
5. Compute the set $\mathcal{S} = \{\lambda \in \mathrm{Spec}(\mathcal{O}_{K_f}) : \lambda \cap \mathbb{Z} = p\mathbb{Z}\}$.
6. For each $\lambda \in \mathcal{S}$, compute $r_\lambda = \min_{\ell \leq B,\ \ell \nmid N} (\mathrm{ord}_\lambda(a_\ell(f) - a_\ell(E_{2,N})))$.

Output: $r_\lambda \in \mathbb{Z}_{\geq 0}$. If $r_\lambda > 0$, then an Eisenstein congruence of "depth" r_λ has been found!

Higher Congruences: An Algebraic Approach

General Commutative Algebra

- $K/\mathbb{Q}_p$: p-adic field with valuation ring $\mathcal{O}$
- T: local complete $\mathcal{O}$-subalgebra of rank s
- $J \subset T$: ideal of finite index

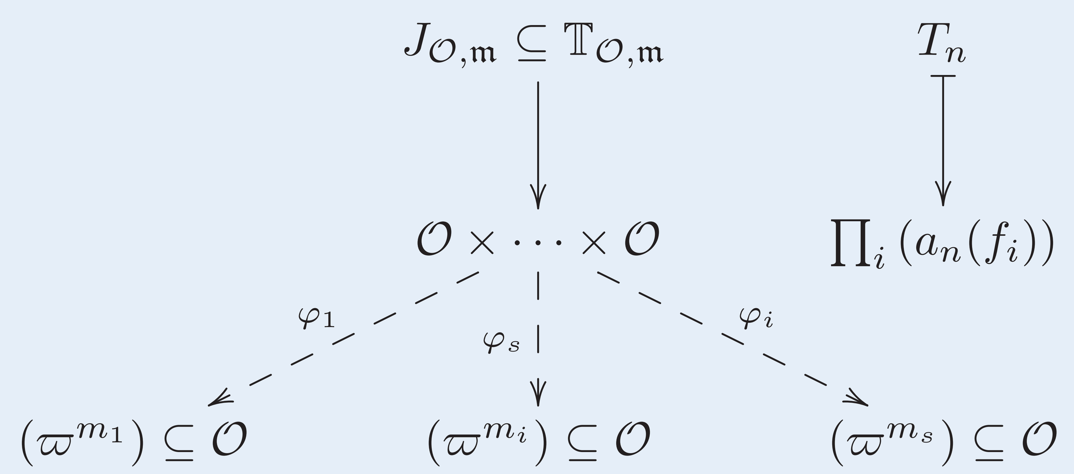


Berger, Klosin, and Kramer [1] prove

$$\#\prod_i (T_i/J_i) \geq \#T/J$$

Applied to Modular Forms

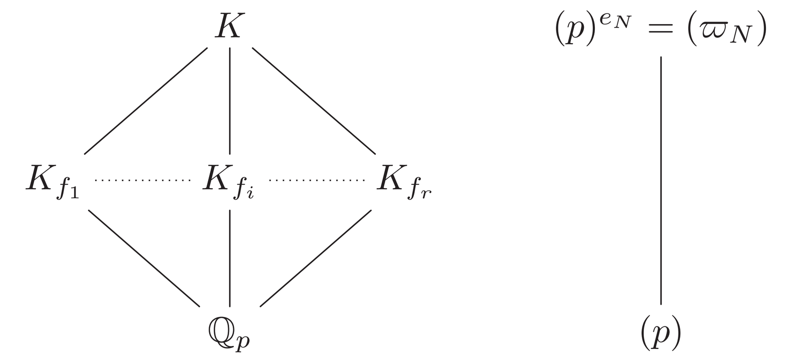
- s: $\#\{f \in New(M) : M \mid N \text{ and } r_\lambda > 0\}$
- $\mathbb{T}_{\mathcal{O},\mathfrak{m}}$: local complete **Hecke algebra**
- $J_{\mathcal{O},\mathfrak{m}}$: localized **Eisenstein ideal** in $\mathbb{T}_{\mathcal{O},\mathfrak{m}}$



$$\#\prod_i (\mathcal{O}/\varpi^{m_i}\mathcal{O}) \geq \#\mathbb{T}_{\mathcal{O},\mathfrak{m}}/J_{\mathcal{O},\mathfrak{m}}$$

Main Result

Let $N > 6$ be a squarefree integer. Let $f_1, \ldots, f_r$ be all weight 2 newforms of level N_{f_i} dividing N.



For each $i = 1, \ldots, r$, let m_i be the highest power of ϖ_N such that the Fourier coefficients of f_i and $E_{2,N}$ satisfy $(*)$ for n coprime to N. Then

$$\frac{1}{e_N}\sum_{i=1}^{s} m_i \geq \mathrm{val}_p(\mathcal{N}),$$

where $\mathcal{N}$ is the numerator of $\frac{\varphi(N)}{24}$.

Example: $N = 203$ and $p = 7$

level	depth	ramindex	resfield	conjclass
29	1	1	7	1

$$\tfrac{1}{1}(1) = 1 = \mathrm{val}_7(7)$$

Example: $N = 399$ and $p = 3$

level	depth	ramindex	resfield	conjclass
19	1	1	3	1
133	2	1	3	3
399	2	1	3	7

$$\tfrac{1}{1}(1+2+2) = 5 > 2 = \mathrm{val}_3(9)$$

Future Research

- Give sufficient conditions for $J_{\mathcal{O},\mathfrak{m}} \subset \mathbb{T}_{\mathcal{O},\mathfrak{m}}$ to be non-principal (in preparation)
- Generalize main result to modular forms of varying weight and character
- Apply method to Hilbert modular forms

References

[1] Tobias Berger, Krzysztof Klosin, and Kenneth Kramer. On higher congruences between automorphic forms. *arXiv preprint arXiv:1302.2381*, 2013.

[2] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system I: The user language. *Journal of Symbolic Computation*, 24(3):235–265, 1997.

[3] Bartosz Naskręcki. On higher congruences between cusp forms and Eisenstein series. In *Computations with Modular Forms*, pages 257–277. Springer, 2014.