ssdnm
środowiskowe
studia doktoranckie
z nauk matematycznych

Bartosz Naskręcki

Uniwersytet A. Mickiewicza w Poznaniu

Congruences for modular forms modulo powers of prime ideals

Praca semestralna nr 1

(semestr letni 2010/11)

Opiekun pracy: Wojciech Gajda

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

CONGRUENCES FOR MODULAR FORMS MODULO POWERS OF PRIME IDEALS

BARTOSZ NASKRĘCKI

Abstract. We investigate several classes of congruences between modular forms modulo prime powers. We apply two different algorithms to obtain new examples of such congruences and we also generalize some results concerning congruences between Eisenstein series and cuspidal eigenforms. A sample of numerical data is presented.

Introduction

The aim of this paper is to present new examples of families of congruences between modular forms modulo prime powers. In Section 1 we introduce definitions and notations. In particular, in Section 1.3 we describe Hecke algebra acting on the spaces of modular forms and show how to use its structure to extract congruences between eigenforms. Main references for this part are [3], [4] and [7].

In Section 2, we first discuss a standard result of Sturm (cf. [10]) about congruences of modular forms modulo prime ideals. Secondly, we sketch the algorithm from [11] and a generalization of theorem of Sturm (cf. [2]). This is used in computations done in Section 3.1.

Next we apply both techniques to study several new examples of congruences. First we use algorithm of [11] to detect possible congruences. Then we lay out a new algorithm (due to the author) based on the generalized Sturm's theorem, cf. [2], which is used to confirm the congruences between coefficients of modular forms. We would like to point out the difference between the two approaches. Algorithms based on [11] tend to be quick but they rely on the assumption that the congruences of coefficients modulo prime powers (and with different Galois embeddings) agree. The algorithm finds a congruence between two cuspforms up to the Galois conjugacy of modular forms representing the class. Our algorithm is based on the generalized Sturm's theorem. It shows that in each case computed by the first algorithm we actually get a congruence of modular forms modulo powers of explicit prime ideals.

Finally, in Section 3.1 we present a new numerical data concerning congruences between cusp forms of weight 4 and a family of congruences between cusp forms and Eisenstein series which is a natural generalization of Theorem 3.2. The data were obtained in computer algebra systems Magma (cf. [1]) and SAGE (cf. [9]). In the Appendix we collect the code descriptions of algorithms used in Section 3.1.

1. Definitions

Let $\mathcal{H}$ be the complex upper half-plane

$$\mathcal{H} = \{\tau \in \mathbb{C} : \Im\tau > 0\}.$$

This paper was prepared as a semester paper under the guidance of prof. Wojciech Gajda in the framework of joint Ph.D. programme ŚSDNM.

For any matrix

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2,2}(\mathbb{Q})$$

with $\det \gamma > 0$ we define a map

$$\gamma : \mathcal{H} \to \mathcal{H}$$

which is a linear fractional transformation given by

$$\gamma(\tau) = \frac{a\tau + b}{c\tau + d}.$$

In fact, the imaginary part has the following form

$$\Im(\gamma(\tau)) = \frac{\det \gamma \cdot \Im\tau}{|c\tau + d|^2},$$

hence the map γ is well-defined.
The map γ provides a natural action of the group $GL_2^+(\mathbb{Q})$ of 2 by 2 matrices with positive determinant and rational entries on the upper half-plane. We specialize the action to certain subgroups of $GL_2^+(\mathbb{Q})$.

Definition 1.1 (Congruence subgroups)**.** Fix an integer $N \geqslant 1$. Let $\Gamma(N) \subset GL_2^+(\mathbb{Q})$ be the subgroup

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod N \right\}.$$

A subgroup $\Gamma \subset SL_2(\mathbb{Z})$ is called a congruence subgroup if $\Gamma(N) \subset \Gamma$ for some integer $N \geqslant 1$. In particular, Γ is called a congruence subgroup of level N.

We define two families of congruence subgroups of particular interest to us:

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : c \equiv 0 \pmod N \right\},$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : c \equiv 0 \pmod N, a, c \equiv 1 \pmod N \right\}.$$

There are inclusions

$$\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset SL_2(\mathbb{Z}).$$

Proposition 1.1 ([7], Ch. 1.6)**.** *Let $\Gamma \subset SL_2(\mathbb{Z})$ be a congruence subgroup. The index*

$$[SL_2(\mathbb{Z}) : \Gamma]$$

is finite. Moreover:

$$[SL_2(\mathbb{Z}) : \Gamma(N)] = N^3 \prod_{p|N} \left(1 - \frac{1}{p^2}\right) \tag{1}$$

$$[\Gamma_0(N) : \Gamma_1(N)] = N \prod_{p|N} \left(1 - \frac{1}{p}\right), \tag{2}$$

$$[\Gamma_1(N) : \Gamma(N)] = N. \tag{3}$$

We will define the space of modular forms of certain level and weight. For further reference cf. [4] Ch. 1.1.

Definition 1.2 (Weak modular forms)**.** Fix a non-negative integer k and a positive integer N. Let Γ be a congruence subgroup of level N. A function $f : \mathcal{H} \to \mathbb{C}$ is a weak modular form of weight k with respect to Γ if

(i) f is holomorphic on $\mathcal{H}$,

(ii) for every $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ the function f satisfies:

$$f(\begin{pmatrix} a & b \\ c & d \end{pmatrix}(\tau))(c\tau + d)^{-k} = f(\tau)$$

for every $\tau \in \mathcal{H}$.

Since any congruence subgroup Γ contains $\Gamma(N)$ for some N there exists a matrix $T_h = \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$ with minimal positive $h \in \mathbb{N}$ such that $T_h \in \Gamma(N)$. If we consider any weak modular form of weight k with respect to Γ we obtain from condition (ii)

$$f(\tau + h) = f(\tau)$$

for any $\tau \in \mathcal{H}$. Hence f is h-periodic and there exists a holomorphic function

$$g : B(0,1) \setminus \{0\} \to \mathbb{C}$$

on punctured unit disk with the property $g(e^{2\pi i\tau/h}) = f(\tau)$. If g extends to 0 we say that f is holomorphic at infinity and f has Fourier expansion

$$f(\tau) = \sum_{n=0}^{\infty} a_n q_h^n$$

where $q_h = e^{2\pi i\tau/h}$. In the sequel we use notation $q = q_1$. Moreover we want to define holomorphy condition at rational points $\mathbb{Q} \subset \mathbb{C}$ in analogy to holomorphy at ∞. We can extend the action of group $GL_2^+(\mathbb{Q})$ to the projective line $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$ as follows

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \frac{ax + by}{cx + dy} =: \begin{pmatrix} a & b \\ c & d \end{pmatrix}([x : y]).$$

Since we have $\frac{x}{y} = [\frac{x}{y} : 1] = [x, y]$ in projective coordinates and the point at infinity $\infty = [1, 0]$, we can also act on that point

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}([1 : 0]) = [a : c].$$

Provided that $c \neq 0$ we have $\begin{pmatrix} a & b \\ c & d \end{pmatrix}(\infty) = \frac{a}{c}$. Now holomorphy at $s \in \mathbb{Q}$ is defined as follows. A weakly modular function f of weight k and with respect to Γ is holomorphic at $s \in \mathbb{Q}$ if and only if the following condition holds true. The weakly modular function $f(\tau)(c\tau + d)^{-k}$ of weight k and with respect to the congruence subgroup $\alpha\Gamma\alpha^{-1}$ is holomorphic at infinity provided that

$$\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$$

and

$$\alpha(\infty) = s.$$

The points on $\mathbb{P}^1(\mathbb{Q})$ are called cusp(idal) points.

Definition 1.3 (Modular forms)**.** Fix a non-negative integer k and a positive integer N. Let Γ be a congruence subgroup of level N. A function $f : \mathcal{H} \to \mathbb{C}$ is a modular form of weight k with respect to Γ if

(i) f is a weak modular form of weight k with respect to Γ,
(ii) f is holomorphic at all cusps.

If $a_0 = 0$ in the Fourier expansion at ∞ of $f(\tau)(c\tau + d)^{-k}$, for all

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}),$$

then f is a **cusp form**.

The vector space of modular forms of weight k and with respect to Γ is denoted $\mathcal{M}_k(\Gamma)$, similarly the space of cusp forms is denoted $\mathcal{S}_k(\Gamma)$.

We can easily multiply two modular forms of weight k and l with respect to the same group. The product is a modular form of weight $k + l$. This shows that the direct sum

$$\mathcal{M}(\Gamma) = \bigoplus_k \mathcal{M}_k(\Gamma)$$

is a graded ring with a graded ideal

$$\mathcal{S}(\Gamma) = \bigoplus_k \mathcal{S}_k(\Gamma).$$

We work with Fourier expansions of modular forms at ∞ to avoid ambiguous Fourier expansions at different cusps. It is noteworthy that condition (ii) can be expressed equivalently as a certain growth condition of Fourier coefficients

Proposition 1.2 ([4], Prop. 1.2.4)**.** *Let Γ be a congruence subgroup of level N and $q_N(\tau) = e^{2\pi i\tau/N}$ for $\tau \in \mathcal{H}$. Let f be a weak modular form of weight k and with respect to Γ. Then $f(\tau) = \sum_{n=0}^{\infty} a_n q_N^n$ and the coefficients for $n > 0$ satisfy the condition*

$$|a_n| \leqslant Cn^r$$

for some positive C and r independent of n, then the weak modular form f is modular, i.e. $f \in \mathcal{M}_k(\Gamma)$.

Example 1.1 ([4])**.** Let $k > 2$ be an even integer. We define

$$G_k(\tau) = \sum_{c^2+d^2 \neq 0} \frac{1}{(c\tau + d)^k}$$

where the sum is over $c, d \in \mathbb{Z}$ and $\tau \in \mathcal{H}$. It is a holomorphic function which is bounded as $\Im\tau \to \infty$. Moreover it is a weak modular form of weight k with respect to the full modular group $SL_2(\mathbb{Z})$. There is just one cusp with respect to $SL_2(\mathbb{Z})$, hence G_k is a modular form of weight k. The modular form G_k has Fourier expansion

$$G_k(\tau) = 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$$

where $\sigma_m(n) = \sum_{d|n} d^m$. The form G_k is called the Eisenstein series of weight k. Combining G_4 and G_6 we can obtain another important modular form of weight 12:

$$\widetilde{\Delta}(\tau) = (60G_4(\tau))^3 - 27(140G_6(\tau))^2.$$

It can be shown that

$$\widetilde{\Delta}(\tau) = (2\pi)^{12} q \prod_{n=1}^{\infty} (1 - q^n)^{24} = (2\pi)^{12} \sum_{n=1}^{\infty} \tau(n) q^n.$$

The coefficients $\tau(n)$ define a mutliplicative function, proved by L. Mordell in 1917. We will show further that this function satisfies some remarkable congruences pointed out by Ramanujan

$$\tau(n) \equiv \sigma_{11}(n) \pmod{691}.$$

We summarize few important facts about modular forms.

Theorem 1.1 ([4], Ch. 3). (i) *For every $k < 0$ the space $M_k(\Gamma) = \{0\}$, for any congruence subgroup Γ.*
(ii) *For every $k \geqslant 0$ the space $M_k(\Gamma)$ has finite dimension over $\mathbb{C}$, for any congruence subgroup Γ.*
(iii) *The ring $\mathcal{M}(SL_2(\mathbb{Z}))$ is isomorphic as a $\mathbb{C}$-algebra to $\mathbb{C}[G_4, G_6]$. The subring $\mathcal{S}(SL_2(\mathbb{Z})) = \Delta\mathcal{M}(SL_2(\mathbb{Z}))$ is a principal ideal of $\mathcal{M}(SL_2(\mathbb{Z}))$.*

1.1. **Hecke operators.** We describe briefly the action of algebra of Hecke operators on the vector space $M_k(\Gamma_1(N))$. For a recent account of the theory we refer the reader to [4], Ch. 5. For a fuller treatment, cf. [7], Ch. 3. Let $f = \sum_{n=0}^{\infty} a_n q^n$ be a Fourier expansion of a modular form of weight k for the group $\Gamma_1(N)$. We define the Hecke operator at the prime p by the formula

$$T_p(f) = \sum_{n=0}^{\infty} (a_{np} + 1_N(p) p^{k-1} a_{n/p}(\langle p \rangle f)) q^n$$

where $a_{n/p}$ is equal to 0 if $p \nmid n$ and (for $(d, N) = 1$)

$$\langle d \rangle f(\tau) = (c\tau + \delta)^{-k} f(\frac{a\tau + b}{c\tau + \delta})$$

for any matrix in $\Gamma_0(N)$ with entries a, b, c, δ and $d \equiv \delta \pmod{N}$. If $(d, N) > 1$ we put $\langle d \rangle = 0$). The function 1_N is the trivial Dirichlet character modulo N. It is straightforward to see that the operator T_p is linear, however the formula doesn't show why it is an endomorphism. For n composite we define T_n as a composition of operators T_{p^i} for appropriate primes p appearing in the factorization of n. The operators T_p and T_q do commute for distinct prime numbers p and q. The operators commute also with $\langle d \rangle$. Furthermore we have the relation

$$T_{p^r} = T_p T_{p^{r-1}} - p^{k-1} \langle p \rangle T_{p^{r-2}}.$$

Definition 1.4. We say that a nonzero modular form f in $M_k(\Gamma_1(N))$ is an **eigenform** if f is an eigenvector with respect to Hecke operators T_n and diamond operators $\langle n \rangle$ for all $n \geqslant 0$. We say that an eigenform is **normalized** if $a_1(f) = 1$.

1.2. **Hecke algebra.** Hecke operators defined in the previous section form an algebra which encapsulates the properties of eigenforms for different weights and levels, cf. [3]. Assume that Γ contains $\Gamma_1(N)$ for some positive integer N. Let

$$\mathbb{T}_{\mathbb{C}}(M_k(\Gamma))$$

be the $\mathbb{C}$-algebra generated by the Hecke operators T_n and $\langle d \rangle$. In fact, we can ommit diamond operators since they can be generated by operators T_n. The algebra $\mathbb{T}_{\mathbb{C}}$ is a subalgebra in the algebra of endomorphisms $End_{\mathbb{C}}(M_k(\Gamma))$.

Theorem 1.2. *Hecke algebra $T_{\mathbb{C}}$ is finitely generated as a $\mathbb{C}$-module. There exists a perfect pairing*

$$(\cdot, \cdot) : \mathbb{T}_{\mathbb{C}} \times M_k(\Gamma) \to \mathbb{C}$$

defined by $(T, f) = a_1(T(f))$.

Proof. We will first prove the perfectness of the pairing. Since the space of modular forms $M_k(\Gamma)$ is finite-dimensional, the first statement of the theorem follows. Since $\mathbb{C}$ is a field, we need only to show that the pairing is non-degenerate, i.e. left and right kernels are trivial.

Let $T \in \mathbb{T}$ be fixed and $(T, f) = a_1(T(f)) = 0$ for all $f \in M_k(\Gamma)$. We can take $f = T_n(g)$ where $g \in M_k(\Gamma)$. Since $TT_n = T_n T$, we get $a_1(T_n(T(f))) = 0$, but $a_1(T_n(h)) = a_n(h)$, so we have $a_n(T(f)) = 0$ for any $n \geqslant 1$ and any form f. Since $k \geqslant 1$ there are no non-zero modular forms which are constant, hence $T(f) = 0$ for any modular form f, so the operator T is zero.

Let $f \in M_k(\Gamma)$ be fixed and $(T, f) = 0$ for any $T \in \mathbb{T}_{\mathbb{C}}$. In particular, $(T_n, f) = 0$ for any $n \geqslant 1$, so $a_n(f) = 0$, so $f = c \in \mathbb{C}$, but again $k \geqslant 1$, hence there are no non-zero constant modular forms and $f = 0$. □

The space of modular forms is a direct sum $M_k(\Gamma) = S_k(\Gamma) \oplus E_k(\Gamma)$ and the Hecke operators act separetly on each factor. We define then suitable $\mathbb{C}$-algebras

$$\mathbb{T}_{\mathbb{C}}^S = \mathbb{T}_{\mathbb{C}}(S_k(\Gamma))$$
$$\mathbb{T}_{\mathbb{C}}^E = \mathbb{T}_{\mathbb{C}}(E_k(\Gamma))$$

We will establish now a similar result for Hecke algebras over any unital commutative ring R. Again we will assume that $k \geqslant 1$ and $\Gamma(N) \subset \Gamma$ for some positive integer N.

Let $\mathbb{T}_{\mathbb{Z}}(M_k(\Gamma))$ be the $\mathbb{Z}$-submodule obtained by restriction of scalars induced from $\mathbb{T}_{\mathbb{C}}$. In the same way we define $\mathbb{T}_{\mathbb{Z}}^S(S_k(\Gamma))$ and $\mathbb{T}_{\mathbb{Z}}^E(E_k(\Gamma))$. We define also

$$\mathbb{T}_R = \mathbb{T}_{\mathbb{Z}} \otimes_{\mathbb{Z}} R$$
$$\mathbb{T}_R^S = \mathbb{T}_{\mathbb{Z}} \otimes_{\mathbb{Z}} R$$
$$\mathbb{T}_R^E = \mathbb{T}_{\mathbb{Z}} \otimes_{\mathbb{Z}} R$$

for any $\mathbb{Z}$-algebra R. Similarly, we define a space of modular forms with coefficients in $\mathbb{Z}$

$$M_k(\Gamma, \mathbb{Z}) = M_k(\Gamma) \cap \mathbb{Z}[[q]]$$
$$S_k(\Gamma, \mathbb{Z}) = S_k(\Gamma) \cap \mathbb{Z}[[q]]$$
$$E_k(\Gamma, \mathbb{Z}) = E_k(\Gamma) \cap \mathbb{Z}[[q]]$$

where we assume that the expansion is taken at infinity, i.e. $q = e^{2\pi i \tau}$ for $\Im(\tau) > 0$. By spaces of modular forms with coefficients in $\mathbb{Z}$-algebra R we understand

$$M_k(\Gamma, R) = M_k(\Gamma, \mathbb{Z}) \otimes_{\mathbb{Z}} R$$
$$S_k(\Gamma, R) = S_k(\Gamma, \mathbb{Z}) \otimes_{\mathbb{Z}} R$$
$$E_k(\Gamma, R) = E_k(\Gamma, \mathbb{Z}) \otimes_{\mathbb{Z}} R.$$

There is a direct sum decomposition

$$M_k(\Gamma, R) = S_k(\Gamma, R) \oplus E_k(\Gamma, R).$$

Theorem 1.3. *Let R be a $\mathbb{Z}$-algebra. An R-algebra $\mathbb{T}_R$ is a finitely generated R-module, $M_k(\Gamma, R)$ is a finitely generated R-module and there exists a non-degenerate R-pairing*

$$(\cdot, \cdot) : \mathbb{T}_R \times M_k(\Gamma, R) \to R$$

given by $(T \otimes r, f \otimes s) = a_1(T(f)) \otimes (rs)$, $f \in M_k(\Gamma, \mathbb{Z})$, $T \in \mathbb{T}_{\mathbb{Z}}$. We get also similar pairings for Eisenstein submodule and cusp forms submodule

$$(\cdot, \cdot) : \mathbb{T}_R^E \times E_k(\Gamma, R) \to R,$$
$$(\cdot, \cdot) : \mathbb{T}_R^S \times S_k(\Gamma, R) \to R.$$

The pairings are both non-degenerate. The pairing of cusp forms with its Hecke algebra is perfect, hence we get an isomorphism

$$S_k(\Gamma, R) \cong Hom_R(\mathbb{T}_R^S, R).$$

Proof. Our proof starts with the observation that $\mathbb{T}_{\mathbb{Z}}$ is a finitely generated $\mathbb{Z}$-module since we can view it as a subring of endomorphisms of $H_1(X_1(N), \mathbb{Z})$. Here $X_1(N)$ is the compact Riemann surface $\Gamma_1(N) \backslash (\mathcal{H} \cup \mathbb{P}^1(\mathbb{Q}))$. The homology group is a finitely generated free $\mathbb{Z}$-module, hence the same is true for its endomorphism ring. This implies that the $\mathbb{Z}$-modules $\mathbb{T}_{\mathbb{Z}}^E$ and $\mathbb{T}_{\mathbb{Z}}^S$ are finitely generated. Non-degeneracy

in the case $R = \mathbb{Z}$ is proved in the same way as in the previous theorem. Hence we get two injective homomorphisms

$$M_k(\Gamma, \mathbb{Z}) \hookrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_{\mathbb{Z}}, \mathbb{Z}),$$
$$\mathbb{T}_{\mathbb{Z}} \hookrightarrow \mathrm{Hom}_{\mathbb{Z}}(M_k(\Gamma, \mathbb{Z}), \mathbb{Z}).$$

Since $\mathbb{T}_{\mathbb{Z}}$ is finitely generated and free, it implies that $M_k(\Gamma, \mathbb{Z})$ is finite free over $\mathbb{Z}$ and it follows that $\mathrm{rank}_{\mathbb{Z}}\mathbb{T}_{\mathbb{Z}} = \mathrm{rank}_{\mathbb{Z}}M_k(\Gamma, \mathbb{Z})$. It implies that the quotient $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_{\mathbb{Z}}, \mathbb{Z})/M_k(\Gamma, \mathbb{Z})$ is a finite abelian group. In case of Hecke algebra of cusp forms we will show that this quotient is trivial

$$S_k(\Gamma, \mathbb{Z}) \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}^S_{\mathbb{Z}}, \mathbb{Z}).$$

Suppose its order is greater than 1. Then there exists a map $\phi \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}^S_{\mathbb{Z}}, \mathbb{Z})$ and $k > 1$ such that

$$k\phi \in S_k(\Gamma, \mathbb{Z}).$$

Take f such that it represents $k\phi$, namely $k\phi(T_n) = a_n(f)$. If $f \in S_k(\Gamma, \mathbb{Z})$, then it shows that there exists a cusp form $g \in S_k(\Gamma, \mathbb{Z})$ such that $f = kg$, hence $\phi(T_n) = a_n(g)$ for any natural n. This implies that $\phi \in M_k(\Gamma, \mathbb{Z})$ since the operators T_n generate the module. Consequently, $k = 1$ a contradiction and the result follows.

We observe that $\mathrm{Hom}_{\mathbb{Z}}(M_k(\Gamma, \mathbb{Z}), \mathbb{Z})$ is a finitely generated free $\mathbb{Z}$ module, hence it is flat. By [5], Ch.1.2 Prop.2.6 it follows that, for any $\mathbb{Z}$-module R the sequence

$$0 \to \mathbb{T}_{\mathbb{Z}} \otimes_{\mathbb{Z}} R \to \mathrm{Hom}_{\mathbb{Z}}(M_k(\Gamma, \mathbb{Z}), \mathbb{Z}) \otimes_{\mathbb{Z}} R$$

is exact, because the pairing with $\mathbb{T}_{\mathbb{Z}}$ is non-degenerate. Similar property holds for the space of cusp forms and the space of Eisenstein series. By duality we get that the sequence

$$0 \to M_k(\Gamma, \mathbb{Z}) \otimes_{\mathbb{Z}} R \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_{\mathbb{Z}}, \mathbb{Z}) \otimes_{\mathbb{Z}} R$$

is exact. In the same way we prove that the sequences for $\mathbb{T}^E$ and $\mathbb{T}^S$ are exact. In order to generalize to modules over any commutative unital ring, we use the following standard fact. Let A be a right R-module, B a (R, S)-module and C a right S-module. Then there is a natural isomorphism

$$\mathrm{Hom}_S(A \otimes_R B, C) \cong \mathrm{Hom}_R(A, \mathrm{Hom}_S(B, C)). \tag{4}$$

Let R be any $\mathbb{Z}$-algebra. From (4) it follows that

$$\mathrm{Hom}_R(\mathbb{T}_R, R) \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_{\mathbb{Z}}, \mathrm{Hom}_R(R, R)) \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_{\mathbb{Z}}, R)$$

and since $\mathbb{T}_{\mathbb{Z}}$ is free of rank r we have isomorphisms

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_{\mathbb{Z}}, \mathbb{Z}) \otimes_{\mathbb{Z}} R \cong \mathbb{Z}^r \otimes_{\mathbb{Z}} R \cong R^r \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_{\mathbb{Z}}, R)$$

which dependend on the choice of a basis. By the same method we obtain

$$\mathrm{Hom}_{\mathbb{Z}}(M_k(\Gamma, \mathbb{Z}), \mathbb{Z}) \otimes_{\mathbb{Z}} R \cong \mathrm{Hom}_R(M_k(\Gamma, R), R).$$

The non-degeneracy of the pairing $\mathbb{T}_R \times M_k(\Gamma, R) \to R$ follows, and in the consequence for $\mathbb{T}^E_R$ and $\mathbb{T}^S_R$.

We have shown that the injective map $S_k(\Gamma, \mathbb{Z}) \hookrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}^S_{\mathbb{Z}}, \mathbb{Z})$ is in fact an isomorphism. It follows that

$$S_k(\Gamma, R) \cong \mathrm{Hom}_R(\mathbb{T}^S_R, R).$$

□

Remark 1.1. In general the injective map $\psi : M_k(\Gamma, \mathbb{Z}) \hookrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_{\mathbb{Z}}, \mathbb{Z})$ is not an isomorphism. We show that the cokernel of the map ψ is of order 24 for $\Gamma = \Gamma_0(2)$ and $k = 2$. We know that $M_2(\Gamma_0(2), \mathbb{C})$ is one-dimensional vector space and it is spanned by the modular form

$$F_2 = 1 + 24(\sum_{n=1}^{\infty} \sigma_1(n)q^n - 2\sum_{n=1}^{\infty} \sigma_1(n)q^{2n})$$

where $\sigma_1(n) = \sum_{d|n} d$. Hence we have $M_2(\Gamma_0(2), \mathbb{Z}) = \mathrm{span}_{\mathbb{Z}}(F_2)$. The Hecke operators act as follows

$$T_p F_2 = \begin{cases} F_2 & \text{if } p = 2, \\ (1+p)F_2 & \text{if } p \neq 2. \end{cases}$$

By a simple inductive argument the formula $T_{p^r} = T_p T_{p^{r-1}} - p\langle p \rangle T_{p^{r-2}}$, for a prime p, implies that

$$T_{p^r} = \begin{cases} 1 & \text{if } p = 2, \\ \sigma_1(p^r) & \text{if } p \neq 2. \end{cases}$$

This gives a general formula for the Hecke operator

$$T_n = \prod_{p^r || n, p \text{ odd prime}} \sigma_1(p^r).$$

On the other hand, for n odd, greater than 1, the n-th Fourier coefficient $a_n(F_2)$ of F_2 is equal to $24\sigma_1(n)$ and for $2|n$

$$a_n(F_2) = 24(\sigma_1(n) - 2\sigma_1(n/2)) = 24 \prod_{p^r || n, p \text{ odd prime}} \sigma_1(p^r)$$

which we get from the multiplicativity of σ_1. Finally, the image of $M_2(\Gamma_0(2), \mathbb{Z})$ by the map ψ is generated by the homomorphism of $\mathbb{Z}$-modules

$$T_n \mapsto a_n(F_2).$$

The module $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_{\mathbb{Z}}, \mathbb{Z})$ equals $\mathbb{Z}$ and is generated by the identity map ι

$$\iota(T_n) = \prod_{p^r || n, p \text{ odd prime}} \sigma_1(p^r).$$

Hence $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_{\mathbb{Z}}, \mathbb{Z})/\psi(M_2(\Gamma_0(2), \mathbb{Z})) = \mathbb{Z}/24\mathbb{Z}$.

1.3. **The eigencurve.** It is important to analyze the structure of the scheme $\mathrm{Spec}\ \mathbb{T}^S_{\mathbb{Z}} \to \mathrm{Spec}\ \mathbb{Z}$. By studying its fibers we can obtain all possible congruences between Hecke eigenforms modulo a prime.

Let K be a field and $\overline{K}$ its algebraic closure. We denote by G the absolute Galois group $Gal(\overline{K}/K)$. By the adjoint property of functors $\mathrm{Hom}_S(B, \cdot)$ and $(\cdots) \otimes_R B$ for (R, S)-module B (see (4)) we have the isomorphisms

$$S_k(\Gamma, \overline{K}) \cong \mathrm{Hom}_{\overline{K}}(\mathbb{T}^S_{\overline{K}}, \overline{K}) \cong \mathrm{Hom}_K(\mathbb{T}^S_K, \overline{K})$$

Let $\sigma \in Gal(\overline{K}/K)$ be the Galois automorphism. It acts on the homomorphism $\phi \in \mathrm{Hom}_K(\mathbb{T}^S_K, \overline{K})$ by the composition $\phi \mapsto \sigma \circ \phi$ and by the above homomorphisms we get an action on $S_k(\Gamma, \overline{K})$.

By the q-expansion principle (cf. [3], Thm. 12.3.2), we can identify the space $S_k(\Gamma, \mathbb{Z}) \otimes_{\mathbb{Z}} \overline{K}$ with the space of modular forms with coefficients in $\overline{K}$ if $\mathrm{char}\ K = 0$ or $k > 1$ and N is invertivle in K. For example, if $K = \mathbb{Q}$ we have the needed identification.

Moreover, we can attach to each prime ideal $\mathfrak{p} \in \mathrm{Spec}\ \mathbb{T}^S_K$ a unique K-algebra homomorphism $\phi_{\mathfrak{p}} : \mathbb{T}^S_K \to \overline{K}$ where $ker(\phi_{\mathfrak{p}}) = \mathfrak{p}$. The image of $\phi_{\mathfrak{p}}$ is an integral

domain over the field K and it is finitely generated since $\mathbb{T}_K^S$ is finitely generated. Thus it is a field and $\mathfrak{p}$ is a maximal ideal. So we have proven

$$\text{Spec } \mathbb{T}_K^S = \text{Spm}\mathbb{T}_K^S.$$

Since K-algebra homomorphisms correspond to eigenforms by the *Hom* identification and the action of the Galois group commutes with Hecke operators, each prime ideal $\mathfrak{p} \in \text{Spec } \mathbb{T}_K^S$ corresponds to a unique Galois orbit of normalized eigenforms. We denote by $\text{Eigen}(G)$ the set of Galois orbits of normalized eigenforms. Altogether this defines a function of sets

$$\text{Spec } \mathbb{T}_K \to \text{Eigen}(G)$$

$$\mathfrak{p} \mapsto (T_n \mapsto \phi_{\mathfrak{p}}(T_n)).$$

This map is a bijection by Theorem 1.3. In the case $K = \mathbb{Q}$ by the q-expansion principle the series $\sum_{n=1}^{\infty} \phi_{\mathfrak{p}}(T_n)q^n$ is a genuine normalized eigenform. If the representing eigenform is f, then the associated prime ideal is denoted by $\mathfrak{p}_f$.

Theorem 1.4 ([10], Thm. 9.23)**.** *Let Γ be a congruence subgroup containing $\Gamma_1(N)$ and put $r = \frac{k[SL_2(\mathbb{Z}):\Gamma]}{12} - \frac{[SL_2(\mathbb{Z}):\Gamma]-1}{N}$. Then the Hecke algebra $\mathbb{T}_{\mathbb{Z}}^S$ is generated as a $\mathbb{Z}$-module by Hecke operators T_n for $n \leqslant r$.*

As an algebra $T_{\mathbb{Z}}^S$ is generated by T_1 and T_p for primes $p \leqslant r$ where r denotes the integer from Theorem 1.4. In general, the algebra $\mathbb{T}_{\mathbb{Z}}^S$ is not generated by a single element of $\mathbb{T}_{\mathbb{Z}}^S$. We will illustrate this fact with the following example.

Proposition 1.3. *The Hecke algebra $\mathbb{T}_{\mathbb{Z}}^S$ over $\mathbb{Z}$ acting on $S = S_2(\Gamma_0(40), \mathbb{Z})$ is equal to*

$$\mathbb{Z}[T_2, T_3]$$

as a $\mathbb{Z}$-algebra. However, there is no element $T \in \mathbb{T}_{\mathbb{Z}}^S$ such that

$$\mathbb{T}_{\mathbb{Z}}^S = \mathbb{Z}[T].$$

Proof. Let $S = S_2(\Gamma_0(40), \mathbb{Z})$, $\text{rank}_{\mathbb{Z}} S = 3$. By Theorem 1.4 and Proposition 1.1 we have that the Hecke algebra $\mathbb{T}_{\mathbb{Z}}^S$ is generated as a $\mathbb{Z}$-module by Hecke operators $T_1, T_2, \cdots, T_{10}$ (the bound is $r = \frac{409}{40}$).
We choose a basis of S as follows

$$\begin{aligned} f_1 &= q + q^5 + O(q^6), \\ f_2 &= q^2 + O(q^6), \\ f_3 &= q^3 + q^5 + O(q^6). \end{aligned}$$

With respect to this basis we can represent the operators T_2 and T_3 by the following matrices

$$T_2 = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & -2 \\ 0 & 0 & 0 \end{bmatrix}$$

and

$$T_3 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & -2 & 0 \\ 1 & 0 & -2 \end{bmatrix}.$$

We can check directly that $T_2^2 = 0$ and $T_3(T_3+2) = 0$ and $T_2T_3 = -2T_2$. Moreover,

$$\begin{aligned} T_1 &= id_S, \\ T_4 &= 0 \cdot T_1, \\ T_5 &= T_1 + T_3, \\ T_6 &= -2T_2, \\ T_7 &= -4T_1 - 3T_3, \\ T_8 &= 0 \cdot T_1, \\ T_9 &= -3T_1 - 2T_3, \\ T_{10} &= -T_2, \end{aligned}$$

hence

$$\mathbb{T}_{\mathbb{Z}}^S = \mathbb{Z}[T_2, T_3]$$

as a $\mathbb{Z}$-algebra.

In order to show the second statement suppose that there exists an element $T \in \mathbb{T}_{\mathbb{Z}}^S$ such that $\mathbb{T}_{\mathbb{Z}}^S = \mathbb{Z}[T]$ as an algebra. Since T_2 and T_3 generate $\mathbb{T}_{\mathbb{Z}}^S$ as a $\mathbb{Z}$-module, $T = a + bT_2 + cT_3$, for some $a, b, c \in \mathbb{Z}$. Therefore

$$T = \begin{bmatrix} a & 0 & 0 \\ b & a-2c & -2b \\ c & 0 & a-2c \end{bmatrix}.$$

We know that $3 = \operatorname{rank}_{\mathbb{Z}} S = \operatorname{rank}_{\mathbb{Z}} \mathbb{T}_{\mathbb{Z}}^S$ and the characteristic polynomial of T is of degree 3, therefore $1, T, T^2$ must be linearly independent over $\mathbb{Z}$. But then there exist $u, v, w \in \mathbb{Z}$ such that

$$u + vT + wT^2 = T_2.$$

and we can assume $b \neq 0$ and $c \neq 0$ (otherwise the minimal polynomial of T would have degree less than 3). It follows that

$$\begin{aligned} u &= \frac{a^2 + 2ac}{2bc} \\ v &= \frac{a-c}{bc} \\ w &= \frac{-1}{2bc} \end{aligned}$$

and $w \notin \mathbb{Z}$, a contradiction. □

1.4. **Congruences mod ℓ.** The main reference for this part is [3].

Let $S = S_k(\Gamma, \mathbb{Z})$ be the cuspidal module. The Hecke algebra $\mathbb{T} = \mathbb{T}_{\mathbb{Z}}^S$ tensored with $\mathbb{Q}$ is a finitely generated $\mathbb{Q}$-algebra of finite dimension. It is an Artinian ring and it splits canonically into a product

$$\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Q} = \prod_{\mathfrak{p}} \mathbb{T}_{\mathfrak{p}}$$

of its localizations at primes $\mathfrak{p}$ such that $\mathfrak{p} \cap \mathbb{Z} = 0$. The ideals correspond to $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugacy classes of eigenforms in $S_k(\Gamma, \overline{\mathbb{Q}})$.
In the same way we obtain the decomposition

$$\mathbb{T}_{\mathbb{Z}_l} = \prod_{\mathfrak{m}} (\mathbb{T}_{\mathbb{Z}_l})_{\mathfrak{m}}$$

where $\mathfrak{m}$ runs over maximal ideals of $\mathbb{T}$ containing a prime l. They correspond to $\operatorname{Gal}(\overline{\mathbb{F}_l}/\mathbb{F}_l)$-conjugacy classes of eigenforms in $S_k(\Gamma, \overline{\mathbb{F}_l})$.

We identify each factor $(\mathbb{T}_{\mathbb{Z}_l})_{\mathfrak{m}}$ with the $\mathfrak{m}$-adic completion $\hat{\mathbb{T}}_{\mathfrak{m}}$ of the ring $\mathbb{T}$, since l belongs to $\mathfrak{m}$. It is a finite flat $\mathbb{Z}_l$-algebra and the following isomorphism holds

$$\hat{\mathbb{T}}_{\mathfrak{m}} \otimes_{\mathbb{Z}_l} \mathbb{Q}_l \cong \prod_{\mathfrak{p} \subset \mathfrak{m}} \mathbb{T}_{\mathfrak{p}} \otimes_{\mathbb{Q}} \mathbb{Q}_l$$

where $\mathfrak{p}$ runs over minimal prime ideals $\mathfrak{p}$ contained in $\mathfrak{m}$.

Definition 1.5. Let f_1 and f_2 be two eigenforms lying in different $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugacy classes. Let $\mathfrak{p}_{f_1}$ and $\mathfrak{p}_{f_2}$ be the corresponding minimal prime ideals of $\mathbb{T}$ attached to Galois conjugacy classes of forms f_1 and f_2. We say that f_1 is **congruent** to f_2 **modulo** a prime above l if and only if there exists a maximal ideal $\mathfrak{m}$ in $\mathbb{T}$ containing l such that

$$\mathfrak{p}_{f_1} \subset \mathfrak{m} \text{ and } \mathfrak{p}_{f_2} \subset \mathfrak{m}.$$

Remark 1.2. By the q-expansion principle two modular forms $f, g \in S_k(\Gamma, \mathcal{O})$, where $\mathcal{O}$ is the ring of algebraic integers of a number field, are congruent modulo l, if and only if,

$$a_n(f) \equiv a_n(g) \pmod{\lambda}$$

for any prime λ in $\mathcal{O}$ dividing l.

Example 1.2. Let $S = S_2(\Gamma_0(169), \mathbb{Z})$, $\mathbb{T} = \mathbb{T}^S_{\mathbb{Z}}$. We compute in SAGE that $\operatorname{rank}_{\mathbb{Z}} \mathbb{T} = 8$ and the characteristic polynomial of the operator $T_2 \in \mathbb{T}$ is its minimal polynomial, so the elements $T_1, T_2, T_2^2, \ldots, T_2^7$ are linearly independent over $\mathbb{Z}$. By Theorem 1.3 the rank of $\mathbb{T}$ as the $\mathbb{Z}$-module is 8 and it is easy to express all Hecke operators (up to the Sturm bound) as $\mathbb{Z}$-linear combinations of the powers of T_2. Hence

$$\mathbb{T} = \mathbb{Z}[T_2] \cong \mathbb{Z}[x]/(f_1 f_2 f_3),$$

where

$$\begin{aligned} f_1 &= x^2 - 3, \\ f_2 &= x^3 - 2x^2 - x + 1 \\ f_3 &= x^3 + 2x^2 - x - 1, \end{aligned}$$

are irreducible, pairwise coprime polynomials over $\mathbb{Z}$. The product $f_1 \cdot f_2 \cdot f_3$ is the characteristic polynomial of T_2 in S.

The epimorphism $\mathbb{Z}[x] \twoheadrightarrow \mathbb{Z}[x]/(f_1 f_2 f_3)$ defines a bijection between prime ideals of $\mathbb{Z}[x]/(f_1 f_2 f_3)$ and prime ideals of $\mathbb{Z}[x]$ containing $h = (f_1 f_2 f_3)$. Let $\mathfrak{p}$ be non-zero prime ideal in $\mathbb{Z}[x]$ such that $\mathfrak{p} \cap \mathbb{Z} = (0)$. Then there exists an irreducible (over $\mathbb{Z}$) polynomial $f \in \mathbb{Z}[x]$ such that $\mathfrak{p} = (f)$. If $\mathfrak{p} \cap \mathbb{Z} = (p)$ and p is a prime number in $\mathbb{Z}$, there we have the equality $\mathfrak{p} = (p, g)$ where g is irreducible modulo p. This gives a complete description of prime ideals in $\mathbb{Z}[x]$.

If $\mathcal{P} \subset \mathbb{Z}[x]/(h)$ is a prime ideal, there exists a prime ideal $\mathfrak{p}$ in $\mathbb{Z}[x]$ such that

$$\mathfrak{p}Z[x]/(h) = \mathcal{P}$$

and $(h) \subset \mathfrak{p}$. Two prime ideals $(\bar{f}_i)$, $(\bar{f}_j)$ $(i \neq j)$ are contained in the same maximal ideal $\mathfrak{m}$, where l belongs to $\mathfrak{m}$ if and only if the reductions modulo l have a non-trivial factor. This is equivalent to the fact that the resultant of polynomials f_i and f_j is divisible by l.

We compute suitable resultants

$$\begin{aligned} \mathrm{Res}(f_1, f_2) &= 13 \\ \mathrm{Res}(f_1, f_3) &= 13 \\ \mathrm{Res}(f_2, f_3) &= -8. \end{aligned}$$

Each polynomial f_i corresponds to a $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugacy class of eigenforms and hence to a localization of $\mathbb{T}$ at a suitable minimal prime $\mathfrak{p}_i = (f_i(T_2))$. Thus, each such prime defines an irreducible component of the scheme

$$\text{Spec } \mathbb{T} \to \text{Spec } \mathbb{Z}.$$

Moreover, the components intersect at maximal primes above 13 and 2 or more precisely

$$\begin{aligned}
(f_1) &\subset (13, x+4),\\
(f_2) &\subset (13, x+4),\\
(f_1) &\subset (13, x+9),\\
(f_3) &\subset (13, x+9),\\
(f_2) &\subset (2, x^3+x+1),\\
(f_3) &\subset (2, x^3+x+1).
\end{aligned}$$

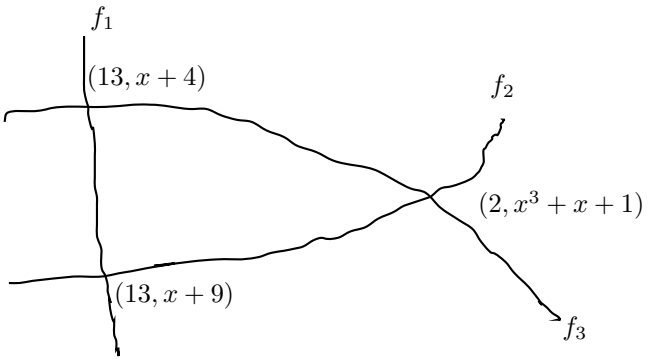

FIGURE 1. Sketch of Spec $\mathbb{T}$, the lines correspond to irreducible components defined by f_i.

2. Congruences between modular forms

We consider reductions of coefficients of modular forms modulo prime ideals in rings of integers of the coefficient fields.

2.1. **Sturm theorem and applications.** In this section we consider modular forms with respect to a fixed congruent subgroup Γ of level N. Let f be a modular form and let $\sum a_n q_N^n$ be its Fourier expansion. Suppose the coefficients of f lie in $\mathcal{O}_K$, which is the ring of algebraic integers of a number field K containing coefficients a_n. For any non-zero prime ideal $\mathfrak{p}$ we define

$$\text{ord}_{\mathfrak{p}}(f) = min\{n \in \mathbb{N} \cup 0 : a_n \notin \mathfrak{p}\}$$

and we call the number **order** of f at $\mathfrak{p}$. If for every n the condition $a_n \in \mathfrak{p}$ holds, then we put $\text{ord}_{\mathfrak{p}}(f) = +\infty$.
Observe that $\text{ord}_{\mathfrak{p}}(fg) = \text{ord}_{\mathfrak{p}}(f) + \text{ord}_{\mathfrak{p}}(g)$.

Let R be a subring of $\mathbb{C}$. We denote by $M_k(\Gamma, R)$ the R-module of modular forms which have the q-expansion with coefficients in R.

Theorem 2.1 ([10])**.** *Let K be a number field, let Γ be a congruence subgroup of level N and $m = [SL_2(\mathbb{Z}) : \Gamma]$. If f belongs to $M_k(\Gamma, \mathcal{O}_K)$ and*

$$ord_{\mathfrak{p}}(f) > \frac{km}{12},$$

then $f \equiv 0 \pmod{\mathfrak{p}}$. *Moreover, if* $f \in S_k(\Gamma, \mathcal{O}_K)$ *and*

$$ord_{\mathfrak{p}}(f) > \frac{km}{12} - \frac{m-1}{N}$$

then $f \equiv 0 \pmod{\mathfrak{p}}$.

Example 2.1. The space $M_{12}(\mathrm{SL}_2(\mathbb{Z}))$ is of dimension two. Its cuspidal part is one dimensional and it is spanned by

$$\Delta = q\prod_{n=1}^{\infty}(1-q^n)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n.$$

The Eisenstein subspace is generated by

$$E = \frac{12!\cdot 2730}{(2\pi)^{12}}G_{12} = 691 + 65520\sum_{n=1}^{\infty}\sigma_{11}(n)q^n.$$

The coefficients of both forms lie in $\mathbb{Z}$. We choose the prime ideal $\mathfrak{p} = (691)$. The Sturm bound $\frac{km}{12} = 1$ and we have

$$E - 65520\Delta = 691 + (\sigma_{11}(2)\cdot 65520 + 1572480)q^2 + O(q^3).$$

Since $\sigma_{11}(2)\cdot 65520 + 1572480 = 196560\cdot 691$, we obtain

$$\mathrm{ord}_{(691)}(E - 65520\Delta) > 1$$

which implies by Theorem 2.1 that

$$E - 65520\Delta \equiv 0 \pmod{\mathfrak{p}}.$$

Hence we get

$$\tau(n) \equiv \sigma_{11}(n) \pmod{691}.$$

Corollary 2.1. *Let* $\mathfrak{p}$ *be a prime ideal in* $\mathcal{O}_K$ *for a number field* K *and* Γ *be a congruent subgroup of level* N. *If* f *and* g *lie in* $M_k(\Gamma, \mathcal{O}_K)$ *and*

$$a_n(f) \equiv a_n(g) \pmod{\mathfrak{p}}$$

for $n \leqslant \frac{k[SL_2(\mathbb{Z}):\Gamma]}{12}$, *then*

$$f \equiv g \pmod{\mathfrak{p}}.$$

If $f - g \in S_k(\Gamma, \mathcal{O}_K)$ *and the congruence* $a_n(f) \equiv a_n(g) \pmod{\mathfrak{p}}$ *holds for* $n \leqslant \frac{k[SL_2(\mathbb{Z}):\Gamma]}{12} - \frac{[SL_2(\mathbb{Z}):\Gamma]-1}{N}$, *then*

$$f \equiv g \pmod{\mathfrak{p}}.$$

2.2. **Congruences mod ℓ^n.** In this section we present the algorithm for finding congruences with respect to powers of prime ideals in number fields for the coefficients of normalized eigenforms.

The algorithm closely follows the approach to the problem described in [11]. Explicit congruences in certain cases can be checked via the generalization of Sturm's theorem as indicated in [2].

From now on we fix a rational prime l, algebraic closures $\overline{\mathbb{Q}}$ and $\overline{\mathbb{Q}_l}$ and an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}_l}$. We denote by $\overline{\mathbb{Z}_l}$ the ring of roots of monic polynomials with coefficients in $\mathbb{Z}_l$. We choose a valuation v_l on $\overline{\mathbb{Q}_l}$ such that $v_l(l) = 1$.

Definition 2.1. Let $n \in \mathbb{N}$ be a natural number and $\alpha, \beta \in \overline{\mathbb{Z}_l}$ be two algebraic integers. We say that α is **congruent** to β modulo l^n if and only if $v_l(\alpha-\beta) > n-1$. We denote this fact by

$$\alpha \equiv \beta \pmod{l^n}.$$

The definition doesn't depend on a choice of the extension $K/\mathbb{Q}_l$. In the case of unramified extensions it really means that if π_K is a uniformizer in $\mathcal{O}_K$, then $\alpha - \beta \in (\pi_K^n)$. If $n = 1$, it means that the elements α and β are equal in $\overline{\mathbb{F}_l}$.

It is convienient to reinterpret the above definiton.

Definition 2.2. Let $K/\mathbb{Q}_l$ be a finite field extension, L/K be a finite extension and let $e_{L/K}$ denote the ramification index of L/K. For $n \in \mathbb{N}$, let

$$\gamma_{L/K}(n) = (n-1)e_{L/K} + 1.$$

Proposition 2.1 ([11], Def. 2.2)**.** *The function $\gamma_{L/K}$ satisfies the following properties*

(i) $\gamma_{L/K}(1) = 1$
(ii) *If L/K is unramified, then $\gamma_{L/K}(n) = n$.*
(iii) *For extensions M/L and L/K we have $\gamma_{M/K}(n) = \gamma_{M/L}(\gamma_{L/K}(n))$.*
(iv) *For extensions L/K, the integer $\gamma_{L/K}(n)$ is the minimal one such that the embedding $\mathcal{O}_K \hookrightarrow \mathcal{O}_L$ induces an injection $\mathcal{O}_K/(\pi_K^n) \hookrightarrow \mathcal{O}_L/(\pi_L^{\gamma_{L/K}(n)})$.*
(v) *For $\alpha, \beta \in K$ and $K/\mathbb{Q}_l$ finite, we have*

$$v_K(\alpha - \beta) \geqslant \gamma_{K/\mathbb{Q}_l}(n) \Leftrightarrow v_l(\alpha - \beta) > n - 1 \Leftrightarrow \alpha \equiv \beta \ (mod\ l^n).$$

By Proposition 2.1 we are allowed to define the "algebraic closure" of $\mathbb{Z}/l^n\mathbb{Z}$

$$\overline{\mathbb{Z}/l^n\mathbb{Z}} := \varinjlim_{K} [\mathcal{O}_K/(\pi_K^{\gamma_{K/\mathbb{Q}_l}(n)})]$$

where K runs through all finite extensions of $\mathbb{Q}_l$ with respect to the family of compatible maps from Proposition 2.1 (iv).

The natural projection $\mathcal{O}_K \twoheadrightarrow \mathcal{O}_K/(\pi_K^{\gamma_{K/\mathbb{Q}_l}(n)})$ induces an epimorphism

$$\pi_n : \overline{\mathbb{Z}_l} \twoheadrightarrow \overline{\mathbb{Z}/l^n\mathbb{Z}}.$$

Hence we can reformulate the congruence condition as

$$\pi_n(\alpha) = \pi_n(\beta).$$

It is always possible to choose π_n in a compatible way. Let then $\pi_{n,m} : \overline{\mathbb{Z}/l^n\mathbb{Z}} \twoheadrightarrow \overline{\mathbb{Z}/l^m\mathbb{Z}}$ be a natural projection for $m < n$. We have the obvious equality

$$\pi_{n,m} \circ \pi_n = \pi_m.$$

To find congruences between algebraic integers we consider minimal polynomials defining them.

In the sequel we also denote by π_n its restriction to $\overline{\mathbb{Z}}$. Let $P, Q \in \mathbb{Z}[x]$ be two coprime monic polynomials and let $n \in \mathbb{N}$.
We want to check the following conditions hold

There exist $\alpha, \beta \in \overline{\mathbb{Z}}$ such that

(i) $P(\alpha) = Q(\beta) = 0$,
(ii) $\pi_n(\alpha) = \pi_n(\beta)$, or equivalently $\alpha \equiv \beta \pmod{l^n}$.

In order to check this conditions we define a map

$$\mathbb{Z}[X]_{<n} \oplus \mathbb{Z}[X]_{<m} \longrightarrow \mathbb{Z}[x]_{<m+n}$$
$$(f, g) \mapsto fP + gQ$$

where $\mathbb{Z}[X]_{<k}$ denotes the polynomials of degree less then k. We call it the Sylvester map. The map is injective and the least degree polynomials in the image are constants.

Definition 2.3. For coprime monic polynomials P and Q in $\mathbb{Z}[x]$ we define a number $c(P,Q)$ which is the least positive integer in the image of the Sylvester map.

In general $c(P,Q)$ is a proper divisor of the resultant of the polynomials P and Q. Furthermore it can be computed from the matrix associated to the Sylvester map. Let $M = M(P,Q)$ be such a matrix (computed with respect to the standard basis in $\mathbb{Z}[x]$). The number $c(P,Q)$ equals $a_{m+n,m+n}$ where $\tilde{M} = (a_{i,j})_{1\leqslant i,j\leqslant m+n}$ is the upper triangular row echelon form of M.

Proposition 2.2 ([11], Prop. 2.7)**.** *Let $P, Q \in \mathbb{Z}[x]$ be coprime polynomials and $l^n || c(P,Q)$ be the exact power of l dividing $c(P,Q)$. Then there are no $\alpha, \beta \in \overline{\mathbb{Z}}$ such that*

(i) $P(\alpha) = Q(\beta) = 0$,
(ii) $\pi_m(\alpha) = \pi_m(\beta)$ *for any* $m > n$.

Proof. There exists polynomials $f, g \in \mathbb{Z}[x]$ such that $c(P,Q) = fP + gQ$. Let $\alpha, \beta \in \overline{\mathbb{Z}}$ be zeros of P and Q, respectively and such that $\pi_m(\alpha) = \pi_m(\beta)$. It follows that

$$\begin{aligned}\pi_m(c(P,Q)) &= \pi_m(f(\alpha)P(\alpha) + g(\alpha)Q(\alpha)) = \pi_m(f(\alpha))\pi_m(Q(\alpha)) \\ &= \pi_m(f(\beta))\pi_m(Q(\beta)) = 0\end{aligned}$$

and in consequence l^m divides $c(P,Q)$, hence $m \leqslant n$. □

The Proposition 2.2 establishes an upper bound for the exponent of l in congruences between modular forms. Further refinement of the method (see [11], Cor. 2.12) gives a lower bound for such congruences. However the bounds are not always the same.

Let $\mathbb{T} = \mathbb{T}_{\mathbb{Z}}^S$ be the $\mathbb{Z}$-algebra of Hecke endomorphisms of the space $S = S_k(\Gamma_0(N))$. We define a modular form of weight k and level N over $\mathbb{Z}/l^n\mathbb{Z}$ to be a $\mathbb{Z}$-module homomorphism

$$f : \mathbb{T} \to \overline{\mathbb{Z}/l^n\mathbb{Z}}.$$

Definition 2.4. We say that modular forms $f : \mathbb{T} \to \overline{\mathbb{Z}_l}$ and $g : \mathbb{T} \to \overline{\mathbb{Z}_l}$ are **congruent modulo** l^n if $\pi_n \circ f = \pi_n \circ g$. This is the same as saying that $a_m(f) \equiv a_m(g) \pmod{l^n}$ in the sense of valuation v_l.

Definition 2.5. We say that eigenforms f and g are **almost congruent** modulo l^n if for all but finitely many prime numbers p

$$a_p(f) \equiv a_p(g) \pmod{l^n}.$$

Let $f, g \in S_k(\Gamma_0(N))$ be two normalized eigenforms and let l be a prime number. We describe the algorithm from [11] which produces two numbers (L^-, L^+) such that if $l^n | L^-$ then f is almost congruent to g modulo l^n and if $l^m \nmid L^+$ then f is **not** almost congruent to g modulo l^m. The algorithm disregards the congruences of coefficients a_p for $p|N$ up to the Sturm bound, but if N is a prime there is no such p. Since we work with $\overline{\mathbb{Z}/l^n\mathbb{Z}}$-forms we need to assume the following hypothesis

Hypothesis ([11])
Let f_1 and f_2 be normalized eigenforms and $n \in \mathbb{N}$. Suppose that for all primes p there are embeddings $\sigma_{i,p} : K \to \overline{\mathbb{Q}}$ $(i = 1, 2)$ where K is a number field containing coefficients of both forms and

$$\sigma_{1,p}(a_p(f_1)) \equiv \sigma_{2,p}(a_p(f_2)) \pmod{l^n}.$$

Then there are embeddings σ_1 and σ_2 such that

$$\sigma_1(f_1) \equiv \sigma_2(f_2) \pmod{l^n}.$$

This is a rather restrictive condition, however in most cases such embeddings do exist.

3. Algorithms

In this section we discuss several results established via computations in SAGE and Magma. We obtain a finite family of generalized congruences between certain cuspidal eigenforms and Eisenstein series modulo powers of prime ideals in number fields.
Let $f_1, f_2 \in S_k(\Gamma_0(N))$ be normalized eigenforms which are not $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugated.

Let p be a prime number. For the Galois conjugacy class $[f_i]$ of f_i we compute the action of the Hecke operator T_p and compute the characteristic polynomial $P_{f_i,p}$. For each such pair we compute the congruence number

$$c_p = c(P_{f_{1,p}}, P_{f_{2,p}}). \tag{5}$$

In fact, polynomials $P_{f_{1,p}}$ and $P_{f_{2,p}}$ are coprime because the Hecke algebra respects the Galois conjugacy classes which are simple $\mathbb{T}$-modules.

We calculate

$$L^+ = gcd_{p \leqslant B}(c_p) \tag{6}$$

where B is the Sturm bound (see Theorem 2.1) for $p \nmid N$. The function gcd is computed in slightly modified way - for two congruence numbers c_{p_1} and c_{p_2} we compute

$$c = gcd(c_{p_1} \cdot p_1^{v_{p_1}(c_{p_2})}, c_{p_2} \cdot p_2^{v_{p_2}(c_{p_1})}) \tag{7}$$

to disregard the coefficient a_p while reducing modulo powers of p. Inductively for any new c_p and c given we compute $c' = gcd(c_p \cdot p^{v_p(c)}, c)$.

Second step of the algorithm is to compute L^-. For each $l|L^+$ we compute a local factor $L_l^- = min_{p \leqslant B} l^{d_p}$. The numbers d_p determine the maximal power of l modulo which polynomials $P_{f,p}$ and $P_{g,p}$ have a root in common. Finally, we take

$$L^- = \prod_{l|L^+} L_l^-. \tag{8}$$

In general, we will have $L^- \neq L^+$. However in some cases we can obtain the equality. In that case we know that modulo $l^n || L^- = L^+$ we have a congruence of almost all coefficients a_p of both forms.
In Section 4.1 we present the code for the algorithm above with all technical details and further description.

We can obtain a more precise result applying the generalization of Sturm's theorem. This is used in refined computations with rational eigenforms in Section 3.1. Moreover, on its base, we build an algorithm to refine Theorem 3.2 and show some interesting class of congruences modulo powers of prime ideals (see Section 3.2).

Theorem 3.1 ([2], Prop. 1)**.** *Let N and n be two positive integers and $k \geqslant 2$. Let $f_1, f_2 \in M_k(\Gamma_1(N))$ be modular forms which have coefficients in $\mathcal{O}_K$, the ring of algebraic integers of a number field K. Let $m = [SL_2(\mathbb{Z}) : \Gamma_1(N)]$ and $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$.*

If $a_n(f_1) \equiv a_n(f_2)$ $(mod\ \mathfrak{p}^n)$ for all $0 \leqslant n \leqslant \frac{km}{12}$ then

$$f_1 \equiv f_2\ (mod\ \mathfrak{p}^n).$$

Proof. The theorem is proved by induction on n. Instead of working with $\mathcal{O}_K$ we switch to work with the localization $(\mathcal{O}_K)_{\mathfrak{p}}$. It is essential to use the property of 'bounded denominators' for modular forms with respect to a congruent subgroup. □

3.1. **Examples.** We present the data computed according to the algorithms in last section. In Section 4 the reader can find the code of all algorithms. Table 2 and Table 3 presented below describe the following data.

For each tuple (N, i, j, L^-, L^+) there is a congruence of coefficients a_p, for almost all primes p, between Galois conjugacy classes of eigenforms f_i and f_j in $S_4(\Gamma)$ (internal numeration in SAGE 4.6.1) in the sense of Definition 2.1

$$a_p(f_i) \equiv a_p(f_j) \pmod{l^k}$$

where $l^k \mid L^-$ and l is a prime number, and $p \nmid N$. There is no such congruence for $l^m \nmid L^+$ (see 3).

N	i	j	L^-	L^+	N	i	j	L^-	L^+	N	i	j	L^-	L^+
13	0	1	26	52	33	0	1	2	2	45	0	3	9	18
14	0	1	2	10	33	0	2	6	12	45	0	4	10	20
15	0	1	2	2	33	0	3	22	176	45	1	2	2	4
17	0	1	34	68	33	1	2	22	88	45	1	3	7	14
19	0	1	38	38	33	1	3	6	12	45	1	4	2	2
21	0	1	7	14	33	2	3	2	64	45	2	3	5	10
21	0	2	6	384	34	0	1	34	34	45	2	4	6	6
21	1	2	2	8	34	0	2	2	12	45	3	4	1	2
22	0	1	11	11	34	1	2	2	4	46	0	1	2	2
22	0	2	4	8	35	0	1	7	7	46	0	2	46	92
22	1	2	1	1	35	0	2	10	20	46	0	3	4	4
23	0	1	46	368	35	1	2	2	4	46	1	2	4	4
25	0	1	2	2	37	0	1	74	592	46	1	3	46	92
25	0	2	5	5	38	0	1	19	19	46	2	3	2	4
25	1	2	3	3	38	0	2	4	24	47	0	1	94	752
26	0	1	2	2	38	1	2	2	2	48	0	1	32	32
26	0	2	1	1	39	0	1	13	52	48	0	2	6	24
26	1	2	5	5	39	0	2	6	48	48	1	2	2	8
27	0	1	6	6	39	1	2	2	16	49	0	1	2	2
27	0	2	3	9	40	0	1	10	10	49	0	2	7	7
27	1	2	3	9	40	0	2	16	16	49	0	3	7	7
28	0	1	14	14	40	1	2	2	2	49	0	4	14	196
29	0	1	58	116	41	0	1	82	164	49	1	2	3	3
30	0	1	2	12	42	0	1	2	8	49	1	3	1	1
31	0	1	124	496	43	0	1	86	172	49	1	4	14	28
32	0	1	8	8	44	0	1	22	22	49	2	3	14	14
32	0	2	16	16	45	0	1	2	2	49	2	4	7	49
32	1	2	8	8	45	0	2	2	2	49	3	4	7	49

FIGURE 2. Data set: $12 \leqslant N \leqslant 49$, $k = 4$

The case $N = 48$ from Table 2 with $L^- = L^+$ corresponds to two eigenforms with rational coefficients

$$f_1 = q - 3q^3 - 18q^5 - 8q^7 + 9q^9 - 36q^{11} - 10q^{13} + 54q^{15} + 18q^{17} + 100q^{19} + O(q^{20}),$$

$$f_2 = q - 3q^3 + 14q^5 + 24q^7 + 9q^9 + 28q^{11} - 74q^{13} - 42q^{15} + 82q^{17} - 92q^{19} + O(q^{20}).$$

We can check directly that all coefficients are congruent modulo 2^5. The Sturm bound (as defined in Theorem 3.1) is equal to 32, so we need to compare 32 coefficients modulo 2^5. By direct computation we obtain that the statement holds. Hence

$$f_1 \equiv f_2 \pmod{2^5}.$$

N	i	j	L^-	L^+	N	i	j	L^-	L^+
50	0	1	5	5	54	0	3	4	24
50	0	2	15	15	54	1	2	2	6
50	0	3	1	1	54	1	3	1	3
50	0	4	2	2	54	2	3	9	9
50	1	2	10	10	55	0	1	2	2
50	1	3	4	4	55	0	2	22	22
50	1	4	1	1	55	0	3	10	10
50	2	3	2	2	55	1	2	10	20
50	2	4	1	1	55	1	3	22	176
50	3	4	5	5	55	2	3	2	16
51	0	1	6	36	56	0	1	8	8
51	0	2	2	2	56	0	2	14	56
51	0	3	17	17	56	1	2	2	8
51	0	4	2	2	57	0	1	2	8
51	1	2	2	2	57	0	2	2	2
51	1	3	1	1	57	0	3	38	76
51	1	4	34	34	57	1	2	38	304
51	2	3	17	17	57	1	3	2	8
51	2	4	6	24	57	2	3	6	96
51	3	4	2	4	58	0	1	2	2
52	0	1	26	26	58	0	2	58	58
53	0	1	7	14	58	0	3	2	2
53	0	2	106	424	58	1	2	2	2
53	1	2	106	848	58	1	3	58	58
54	0	1	9	9	58	2	3	4	8
54	0	2	1	3	59	0	1	38	76

FIGURE 3. Data set: $50 \leqslant N \leqslant 59$, $k = 4$

We present a more extensive data set in Table 4. Description and code of the algorithm can be found in Section 4.1. The computations were done in SAGE 4.6.1. Number N ($2 \leqslant N \leqslant 119$) is the level, the weight $k = 4$ and i, j are internal numbers (in SAGE 4.6.1) for the normalized eigenforms Galois conjugacy classes (the data presented below only includes eigenforms with integral coefficients, so each class corresponds to a single eigenform). The number l^m indicates the maximal power of a prime l for which we have $f_i \equiv f_j \pmod{l^m}$. In the case $l = 2$ we present congruences with $m \geqslant 4$ and in the case $l = 3$ we pick only those with $m \geqslant 2$.

3.2. **Congruences with Eisenstein series.** In paper [6] Mazur described a class of congruences between cusp forms and Eistenstein series of weight 2 and level $N = p$, a prime. The Eisenstein subspace is in that case always generated by a single eigenform

$$E_p = \frac{p-1}{24} + \sum_{n=1}^{\infty} \sigma_1(n) q^n - p \sum_{n=1}^{\infty} \sigma_1(n) q^{pn}. \tag{9}$$

Theorem 3.2 ([6])**.** *Let p be a prime number $p \geqslant 11$. Let l be a prime ($l \neq 2, 3$) dividing the numerator of $\frac{p-1}{12}$. There exists a normalized cuspidal eigenform in $S_2(\Gamma_0(p))$ with coefficients in $\mathcal{O}_K$,which is the ring of algebraic integers of the number field K. The cuspidal eigenform is congruent to Eisenstein series E_p modulo a prime $\lambda \mid l$ at almost all coefficients a_q with q a prime.*

N	i	j	l^m	N	i	j	l^m
32	0	2	2^4	80	1	2	2^5
40	0	2	2^4	90	0	1	3^2
45	0	3	3^2	96	0	1	2^4
48	0	1	2^5	96	3	4	2^4
51	0	1	3^2	96	0	3	3^2
54	0	1	3^2	108	0	1	3^2
54	2	3	3^2	108	0	2	3^2
64	0	4	2^4	108	0	3	3^2
72	0	3	2^5	108	1	2	3^3
72	1	2	2^4	108	1	3	3^2
72	0	2	3^2	108	2	3	3^2
78	0	1	3^2	112	1	6	2^4
80	0	4	2^4	112	3	5	2^5

FIGURE 4. Data set: $2 \leqslant N \leqslant 119$, $k = 4$

We apply Theorem 3.1 to show that for several cases the congruence holds for powers of prime ideals. Below $p < 500$ there are only four primes $p = 101, 151, 197, 251$ and 491 such that the numerator of $\frac{p-1}{12}$ is divisible by a power of prime different than 2 and 3. For every such p we obtain the maximal possible congruence. Each one happens with prime l which is totally split in the coefficient field of the suitable eigenform. Algorithm was performed in MAGMA V2.17 and the code is presented in Section 4.2.

The numbers i and j denote the number of Galois orbits and the position on the orbit in the internal MAGMA enumeration. The number field K is defined by a single root of irreducible polynomial defined above. We also indicate the factorization of the primes (p) in $\mathcal{O}_K$. All primes p are totally split, hence the ramification degree $e = 1$. The number $\mid \mathcal{O}_K/\lambda \mid$ denotes the order of the residue class field with respect to λ. Finally

$$f_\lambda \equiv E_p \pmod{\lambda^{ke}}$$

is the congruence between the cuspidal eigenform f_λ and the Eisenstein series E_p modulo λ^{ke}. We omit the explicit presentation of several coefficients of cusp forms involved in the congruence due to its excessive length.

N	$l^k \mid\mid \mathrm{num}(\frac{N-1}{12})$	i	j	K	$(p) = \prod \lambda_i$	e	$\mid \mathcal{O}_K/\lambda \mid$	$f_\lambda \equiv E_p \pmod{\lambda^{ke}}$
101	5^2	2	1	$\mathbb{Q}(\alpha_{101})$	$(5) = \lambda\lambda_2$	1	5	$f_\lambda \equiv E_5 \pmod{\lambda^2}$
151	5^2	3	1	$\mathbb{Q}(\alpha_{151})$	$(5) = \lambda\lambda_2\lambda_3$	1	5	$f_\lambda \equiv E_5 \pmod{\lambda^2}$
197	7^2	3	1	$\mathbb{Q}(\alpha_{197})$	$(7) = \lambda\lambda_2\lambda_3\lambda_4$	1	7	$f_\lambda \equiv E_7 \pmod{\lambda^2}$
251	5^3	2	1	$\mathbb{Q}(\alpha_{251})$	$(5) = \lambda\lambda_2\lambda_3\lambda_4$	1	5	$f_\lambda \equiv E_5 \pmod{\lambda^3}$
497	7^2	3	1	$\mathbb{Q}(\alpha_{497})$	$(7) = \lambda \prod_{n=2}^{6} \lambda_i$	1	7	$f_\lambda \equiv E_7 \pmod{\lambda^2}$

$$f_{101}(x) = x^7 - 13x^5 + 2x^4 + 47x^3 - 16x^2 - 43x + 14$$
$$f_{101}(\alpha_{101}) = 0$$
$$f_{151}(x) = x^6 - x^5 - 7x^4 + 3x^3 + 13x^2 + 3x - 1$$
$$f_{151}(\alpha_{151}) = 0$$
$$f_{197}(x) = x^{10} - 15x^8 + x^7 + 78x^6 - 7x^5 - 165x^4 + 15x^3 + 123x^2 - 9x - 26$$
$$f_{197}(\alpha_{151}) = 0$$
$$\begin{aligned} f_{251}(x) = {} & x^{17} - 2x^{16} - 28x^{15} + 54x^{14} + 317x^{13} - 582x^{12} - 1867x^{11} + 3178x^{10} \\ & + 6186x^9 - 9216x^8 - 11921x^7 + 13680x^6 + 13752x^5 - 9400x^4 - 8800x^3 \\ & + 1920x^2 + 2240x + 256 \end{aligned}$$
$$f_{251}(\alpha_{251}) = 0$$
$$\begin{aligned} f_{491}(x) = {} & x^{29} - 49x^{27} + x^{26} + 1068x^{25} - 39x^{24} - 13655x^{23} + 658x^{22} + 113723x^{21} \\ & - 6306x^{20} - 647801x^{19} + 37953x^{18} + 2578721x^{17} - 150115x^{16} - 7201417x^{15} \\ & + 398246x^{14} + 13959112x^{13} - 711934x^{12} - 18310154x^{11} + 839798x^{10} + 15574775x^9 \\ & - 585854x^8 - 8065060x^7 + 132680x^6 + 2339280x^5 + 83968x^4 - 350400x^3 - 36608x^2 \\ & + 20992x + 3584 \end{aligned}$$
$$f_{491}(\alpha_{491}) = 0$$

4. Codes for the algorithms

In this section we present the algorithms used to produce the results in the preceding section.

4.1. **SAGE code.** First algorithm computes the pair of numbers (L^-, L^+) (code in SAGE 4.6.1).

Function `EigenRange(k,N)` returns the simple factors, Galois conjugacy classes of normalized eigenforms of weight k and level N with respect to group $\Gamma_0(N)$. We use modular symbols, since from computational perspective it is much more effective than working with modular forms (cf. [8], Ch. 3, Ch. 8).

Function `Sturm(k,N)` returns the Sturm bound of Theorem 3.1.

Function `c(f1,f2,p)` returns the congruent number with respect to Hecke operator T_p of two conjugacy classes of eigenforms f_1 and f_2 (see (5)).

Function `conglist(f1,f2)` returns all the congruence numbers up to Sturm bound.

Function `modgcdinit(l1,l2)` returns a modified greatest common divisor according to (7). Similarly, function `modgcd(l1,c)` does the same (the difference is that first function computes with two elements at first position in both lists `l1` and `l2` and the second function computes with `c` and a single list `l1`).

Function `Lplus(f1,f2)` returns the number L^+ for two different conjugacy classes `f1` and `f2` (see (6)).

Function `Lminus(f1,f2)` return the number L^- for two different conjugacy classes `f1` and `f2` (see (8)). Other function `rs(P,Q)`, `congnumber(f,g)`, `Newtoncong(P,Q,l)`, `primitivefactorscongnumber(P,Q,l)` and `localcongnumber(P,Q,l)` are used to compute the local factors L_l^- for each prime $l \nmid N$ up to the Sturm bound. Further description of the algorithm can be found, without a code, in [11].

```
 R.<x>=ZZ[];
def EigenRange(k,N):
    M=ModularSymbols(Gamma0(N),k,sign=1).cuspidal_submodule();
    return M.new_submodule().simple_factors()
def Sturm(k,N):
    b=Gamma0(N).index();bound=k*b/12-(b-1)/N;
    return bound
def c(f1,f2,p):
    t1=R(f1.hecke_operator(p).charpoly());t2=R(f2.hecke_operator(p).charpoly());
    H=t1.sylvester_matrix(t2).hermite_form();
    r=len(H.rows());c=len(H.columns());
    return H[r-1,c-1];
def conglist(f1,f2):
    N1=f1.level();N2=f2.level();k=f1.weight();clist=[];
    if (k==f2.weight()):
        s=max(Sturm(k,N1),Sturm(k,N2));
        for i in range(1,int(s)+1):
            if(((i in Primes())==True)&(mod(N1*N2,i)!=0)):
                if(c(f1,f2,i)!=0):
                    clist.append([c(f1,f2,i),i]);
    return clist
def modgcdinit(l1,l2):
    c1=l1[0];p1=l1[1];c2=l2[0];p2=l2[1];
    return gcd(c1*p1^(c2.valuation(p1)),c2*p2^(c1.valuation(p2)))
def modgcd(l1,c):
    c1=l1[0];p1=l1[1];
    return gcd(c1*p1^(c.valuation(p1)),c)
def Lplus(f1,f2):
    l=conglist(f1,f2);n=len(l);
    if(len(l)==1):
        return l[0][0];
    else:
        ctmp=modgcdinit(l[0],l[1]);
        for i in range(2,n):
            ctmp=modgcd(l[i],ctmp);
        return ctmp;
def rs(P,Q):
    g=P.variables()[0];S=P.sylvester_matrix(Q);
    H,E=S.hermite_form(transformation=True);
    dP=P.degree();dQ=Q.degree();coeff=E.rows()[dP+dQ-1];
    r=0;s=0;
    for i in range(dP+dQ-1,dQ-1,-1):
        s+=coeff[i]*g^(dP+dQ-1-i);
    for i in range(dQ-1,-1,-1):
        r+=coeff[i]*g^(dQ-1-i);
    return [r,s];
def congnumber(f,g):
    S=f.sylvester_matrix(g);H=S.hermite_form();
    return H[len(H.rows())-1,len(H.columns())-1];
def Newtoncong(P,Q,l):
    T.<X,Y>=PolynomialRing(ZZ,2);S=P.parent();f1=S.hom([X],T);f2=S.hom([X+Y],T);
    Pim=f1(P);Qim=f2(Q);r=Pim.resultant(Qim,X);
    g=S.gens()[0];f3=T.hom([0,g],S);r=f3(r);
    slope=r.newton_slopes(l);slope.sort();
    return ceil(slope[len(slope)-1]);
def primitivefactorscongnumber(P,Q,l):
    if (gcd(P,Q)!=1):
```

```
        return "not coprime";
    r,s=rs(P,Q);c=cong_number(P,Q);n=c.valuation(l);
    if(n==0):
        return n;
    if(n==1):
        return n;
    S.<y>=GF(l)[];Pbar=S(P);Qbar=S(Q);
    c1=cong_number(P,P.derivative());c2=cong_number(Q,Q.derivative());
    if((c1.valuation(l)==0) & (c2.valuation(l)==0)):
        return n;
    rbar=S(r);sbar=S(s);
    if((c2.valuation(l)==0) & (gcd(sbar,Qbar)==1)):
        return n;
    if((c1.valuation(l)==0) & (gcd(rbar,Pbar)==1)):
        return n;
    if(gcd(sbar,Qbar)==1):
        return ceil(n/Q.degree());
    if(gcd(rbar,Pbar)==1):
        return ceil(n/P.degree());
    return Newton_cong(P,Q,l);
def localcong_number(P,Q,l):
    A=P.factor();B=Q.factor();n=0;
    for i in range(0,len(A)):
        for j in range(0,len(B)):
            n=max(n,primitive_factors_cong_number(A[i][0],B[j][0],l));
    return n;
def Lminus(f1,f2):
    Lp=Lplus(f1,f2);fact=Lp.prime_factors();N1=f1.level();N2=f2.level();
    k=f1.weight();Lmin=1;S.<x>=ZZ[];
    if (k==f2.weight()):
        s=max(Sturm(k,N1),Sturm(k,N2));
        for i in range(0,len(fact)):
            l=fact[i];val=Lp.valuation(l);
            for j in range(1,s):
                if ((j in Primes()) & (j<=s)):
                    P=S(f1.hecke_operator(j).charpoly());
                    Q=S(f2.hecke_operator(j).charpoly());
                    val=min(val,local_cong_number(P,Q,l));
            Lmin*=l^(val);
    return Lmin;
```

The second set of functions, defined below, is used to produce congruences between eigenforms with rational coefficients. We use the function `Lminus` and `Lplus` to obtain the maximal and minimal bounds for the powers of prime with respect to which we compute congruences of coefficients.

Function `RationalNewforms(N,k)` returns the eigenforms at level N and weight k in $S_k(\Gamma_0(N), \mathbb{Z})$.

Function `congrationalpot(N,k)` returns the bounds `Lminus` and `Lplus` of congruences between rational eigenforms.

Function `congrational(N,k,p,r)` checks if there exists a congruence of two rational cuspidal eigenforms modulo p^{r+1}.

Function `directcheck(N,k,f,g,p,r)` operates on coefficients of eigenforms (rather then minimal polynomials of Hecke operators, as we proceded in the case of functions `Lminus` and `Lplus`) and checks directly the congruence between coefficients.

The upshot is that we check the congruence of all coefficients up to the Sturm bound computed in Theorem 3.1.

Function `congruenceeigenforms(N,k,p,r)` checks if the predicted congruence holds.

```
def RationalNewforms(N,k):
    M=ModularSymbols(Gamma0(N),k,sign=1).cuspidal_submodule().new_submodule();
    N=M.simple_factors();
    R=[];
    for i in range(0,len(N)):
        if (N[i].dimension()==1):
            R.append(N[i]);
    return R;

def congrationalpot(N,k):
    li=RationalNewforms(N,k);
    c=[];
    if (len(li)>1):
        for i in range(0, len(li)):
            for j in range(i+1,len(li)):
                c.append([li[i],li[j],[Lminus(li[i],li[j]),Lplus(li[i],li[j])],[i,j]]);
    return c;

def congrational(N,k,p,r):
    c=cong_rational_pot(N,k);
    s=[];
    for i in c:
        if (i[2][1].valuation(p)>r):
            s.append(i);
    return s;

def directcheck(N,k,f,g,p,r):
    bound=Gamma0(N).index()*k/12;
    fq=f.q_eigenform(bound+2);
    gq=g.q_eigenform(bound+2);
    for i in range(0,bound+2):
        if( mod(fq[i]-gq[i],p^r)!=0):
            return false;
    return true;

def congruenceeigenforms(N,k,p,r):
    c=cong_rational(N,k,p,r);
    s=[];
    for i in c:
        if (direct_check(N,k,i[0],i[1],p,r)==true):
            s.append(i);
    return s;
```

4.2. **MAGMA code.** In this section we present the code in MAGMA V2.17 which we used to produce the congruences between cusp forms and Eisenstein series in Section 3.2.

Function `Mazur(N)` returns the numerators of the number $\frac{N-1}{12}$.

Function `getfactors(n)` produces the factorization of number n given.

Function `getMazurfactors(N)` returns the factors of the numerator of number $\frac{N-1}{12}$ and rips off the powers of 2 and 3 in factorization.

Function `CongruenceMazur(N)` takes N as an argument (the level of the space of cuspidal modular forms of weight $k = 2$) and returns the list of eigenforms at this level and weight which are congruent to the Eisenstein series (9) modulo a power of prime ideal dividing each rational prime occuring in the factorization `getMazurfactors(N)`.

```
function Mazur(N)
l:=Numerator((N-1)/12);
return l;
end function;

function getfactors(n)
s:=Factorization(n);r:=[ [f[1],f[2]]: f in s];
return r;
end function;

function getMazurfactors(N)
m:=Mazur(N);
t:=m/(2^Valuation(m,2));t:=t/(3^Valuation(t,3));
m:=Numerator(t);s:=Factorization(m);
m2:=&*[ f[1]^( f[2] gt 1 select f[2] else 0) : f in s];
s:=getfactors(m2);
return s;
end function;

function CongruenceMazur(N)
 factors:=getMazurfactors(N);
 S:=Newforms(CuspForms(Gamma0(N),2));
 E:=Basis(EisensteinSubspace(ModularForms(Gamma0(N),2)))[1];
 E_a1:=Coefficient(E,1);
 B:=Ceiling(2*Index(Gamma0(N))/12);
 Collection:=[];
 for pfactors in factors do
  p:=pfactors[1];
  k:=pfactors[2];
 for ind1 in [1..#S] do
 for ind2 in [1..#(S[ind1])] do
  f:=S[ind1][ind2];
  K:=CoefficientField(f);
  O:=MaximalOrder(K);
  I:=ideal<O|p>;
  factI:=Factorization(I);
  for ind3 in [1..#factI] do
   ptuple:=factI[ind3];
   J:=ptuple[1]^(k*ptuple[2]);
   R,m:=quo<O|J>;
   cong:=true;
   for i in [0..B] do
    if (not( m(E_a1*Coefficient(f,i)-Coefficient(E,i)) eq m(0))) then
 cong:=false;
 break;
end if;
   end for;
   if (cong eq true) then
    Include(~Collection,[N,p,k,ind1,ind2,ind3]);
   end if;
   end for;
```

```
 end for;
 end for;
 end for;
 return Collection;
end function;
```

References

[1] W. Bosma, J. Cannon, and C. Playous. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24:235 – 265, 1997.

[2] I. Chen, I. Kiming, and J. Rasmussen. On congruences mod $\mathfrak{p}^m$ between eigenforms and their attached Galois representations. arXiv:0809.3622v1, 2008.

[3] F. Diamond and J. Im. Modular forms and modular curves. In *Seminar on Fermat's Last Theorem (Toronto, ON, 1993–1994)*, pages 39 – 133. CMS Conf. Proc. and Amer. Math. Soc., 1995.

[4] F. Diamond and J. Shurman. *A first course in modular forms.*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.

[5] Q. Liu. *Algebraic geometry and arithmetic curves.*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002.

[6] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33 – 186, 1978.

[7] G. Shimura. *Introduction to the arithmetic theory of automorphic functions.* Number 1 in Kanô Memorial Lectures. Princeton University Press, Princeton, Publications of the Mathematical Society of Japan, no. 11. edition, 1971.

[8] W. Stein. *Modular forms, a computational approach. With an appendix by Paul E. Gunnells.*, volume 79 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2007.

[9] W. Stein et al. Sage Mathematics Software (Version 4.6.1). The Sage Development Team, 2011. http://www.sagemath.org.

[10] J. Sturm. On the congruence of modular forms. In *Number theory*, volume 1240 of *Lecture Notes in Math.*, pages 275 – 280. Springer, Berlin, 1987.

[11] X. Taixes i Ventosa and G. Wiese. Computing Congruences of Modular Forms and Galois Representations Modulo Prime Powers. arXiv:0909.2724v2, 2009.

Faculty of Mathematics and Computer Science, Adam Mickiewicz University, ul. Umultowska 87, 61-614 Poznań, Poland

E-mail address: bartnas@amu.edu.pl