On higher congruences between cusp forms and Eisenstein series

Bartosz Naskręcki

Abstract In this paper we present several finite families of congruences between cusp forms and Eisenstein series of higher weights at powers of prime ideals. We formulate a conjecture which describes properties of the prime ideals and their relation to the weights and we check its validity on several numerical examples.

1 Introduction

In this paper we present new numerical data concerning congruences between cusp forms and Eisenstein series.

Let p be a rational prime. For a Hecke eigenform $f \in \mathscr{S}_k(\Gamma_0(p))$, let $K = K_f = \mathbb{Q}(\{a_n(f)\}_{n\geq 0})$ be the field generated by the Fourier coefficients of the form f and let $\mathscr{O} = \mathscr{O}_f$ be its ring of integers. From the theorem of Mazur [9] we know that for $k = 2$ and for any fixed prime $p \geq 11$ if we choose any prime $\ell \neq 2,3$ dividing the numerator of the zeroth coefficient of the Eisenstein series $E_2 - pE_2^{(p)}$ of weight 2, then there exists a Hecke eigenform f in $\mathscr{S}_2(\Gamma_0(p))$ and a maximal ideal $\lambda \in \mathscr{O}$ above l such that

$$a_r(f) \equiv a_r(E_2 - pE_2^{(p)}) \bmod \lambda \tag{1}$$

for almost all primes r.

In this paper we present the algorithm which supports the following conjecture related to the Mazur's theorem.

Conjecture 1. Let $k \geq 2$ and $p \geq 3$ be a prime number. Choose $E = E_k - p^{k-1}E_k^{(p)}$, where $E_k^{(p)}(\tau) = E_k(p\tau)$. Assume there exists a newform $f \in \mathscr{S}_k(\Gamma_0(p))$, a natural number $r \geq 1$ and a maximal ideal $\lambda \in \mathscr{O}_f$, such that

Bartosz Naskręcki
Graduate School, Faculty of Mathematics and Computer Science, Adam Mickiewicz University, Poznań, Poland, e-mail: bartnas@amu.edu.pl

$$a_n(E) \equiv a_n(f) \bmod \lambda^r \tag{2}$$

for all $n \geq 0$. Let ℓ be the rational prime below λ. Then ℓ divides the numerator of $a_0(E)$. If $\ell > 2$, then

$$ord_\lambda(\ell) = 1 \quad \text{or} \quad r \leq ord_\lambda(\ell).$$

Moreover, the newform f satisfying the congruence (2) is uniquely determined. The symbol ord_λ denotes the λ-valuation. The valuation is normalized, i.e. $\mathrm{ord}_\lambda(\lambda) = 1$.

Congruences between modular forms modulo prime powers were studied in papers [3], [4], [7], [8]. In [8] the authors ask a question about the behaviour of the congruences between cusp forms and Eisenstein series which is related to the conjecture formulated above.

In Section 2 we introduce basic notation and describe Hecke algebras and Hecke eigenforms. Next, in Section 3 we describe the algorithm which computes congruences between cuspidal eigenforms and Eisenstein series. We state all necessary ingredients from algebraic number theory and theory of modular forms. All algorithms were implemented in MAGMA [2] and the source code is available on the request.

In Section 4 for the convenience of the reader we collected basic facts of the theory of p-maximal orders which is an important ingredient of our algorithm. These facts are crucial are for several improvements in the algorithm speed.

Section 5 is devoted to presentation of the numerical data which supports the conjecture. We discuss several explicit examples and the numerical data collected in tables.

2 Notation and definitions

Let p be an odd prime number and k a positive even integer. The space $\mathscr{M}_k(\Gamma_0(p))$ of holomorphic modular forms of weight k splits over $\mathbb{C}$ into a direct sum

$$\mathscr{M}_k(\Gamma_0(p)) = \mathscr{E}_k(\Gamma_0(p)) \oplus \mathscr{S}_k(\Gamma_0(p))$$

of Eisenstein part and the space of cuspidal modular forms (cf.[6]).

From dimension formulas for modular forms we have

$$\dim_{\mathbb{C}}(\mathscr{E}_k(\Gamma_0(p)) = \begin{cases} 1, & k = 2 \\ 2, & k \geq 4. \end{cases}$$

Let $\sigma_r(n) = \sum_{d|n} d^r$ and $q = e^{2\pi i\tau}$, where $\tau \in \mathscr{H}$. Explicitly, for $\mathscr{E}_2(\Gamma_0(p))$ we have the generator

$$E_2(\tau) - pE_2(p\tau) = \frac{p-1}{24} + \sum_{n=1}^{\infty} \sigma_1(n)q^n - p\sum_{n=1}^{\infty} \sigma_1(n)q^{pn}.$$

When $k \geq 4$ we define

$$E_k(\tau) = -\frac{B_k}{2k} + \sum_{n=1}^{\infty} \sigma_{k-1}(n)q^n.$$

The space $\mathscr{E}_k(\Gamma_0(p))$ is generated by $E_k(\tau)$ and $E_k(p\tau)$. The sequence of Bernoulli numbers $\{B_m\}_{m\in\mathbb{N}}$ is defined as usual by the series $\sum_{m=0}^{\infty} B_m t^m = \frac{t}{e^t-1}$.

The space of modular forms $\mathscr{M}_k(\Gamma_0(p))$ carries a natural action of a commutative $\mathbb{C}$-algebra $\mathbb{T}$ generated by the Hecke operators,cf.[6]. The algebra is generated by two types of operators. The first type is defined for the primes $l \neq p$ by the formula

$$T_l(f) = \sum_{n=0}^{\infty} a_{nl}(f)q^n + l^{k-1}\sum_{n=0}^{\infty} a_n(f)q^{nl},$$

where $f \in M_k(\Gamma_0(p))$ and $a_n(f)$ denotes the n-th Fourier coefficient of the form f at infinity. For $l = p$ there is a single operator

$$T_p(f) = \sum_{n=0}^{\infty} a_{np}(f)q^n.$$

We define the algebra $\mathbb{T}$ to be equal to

$$\mathbb{T} = \mathbb{C}[\{T_q\}_{q\in \text{ Primes}}].$$

The action of Hecke algebra $\mathbb{T}$ on the space $\mathscr{M}_k(\Gamma_0(p)) = \mathscr{E}_k(\Gamma_0(p)) \oplus \mathscr{S}_k(\Gamma_0(p))$ preserves the direct sum splitting into Eisenstein and cuspidal part. For $k = 2$ since $\dim \mathscr{E}_2(\Gamma_0(p)) = 1$, the series E_2 is the Hecke eigenform.

For $k \geq 4$ the dimension of the space $\mathscr{E} = \mathscr{E}_2(\Gamma_0(p))$ is equal to two. Let $B_1(\tau) = E_k(\tau)$ and $B_2(\tau) = E_k^{(p)}(\tau) = E_k(p\tau)$. We have a basis of $\mathscr{E}$ consisting of Hecke eigenforms

$$F_1 = B_1 - p^{k-1}B_2,$$
$$F_2 = B_1 - B_2.$$

3 Description of the algorithm

Let k be an even positive integer. We want to find congruences between Eisenstein eigenforms and cuspidal newforms in the space of modular forms $\mathscr{M}_k(\Gamma_0(p))$. For $k = 2$ we have one Eisenstein eigenform

$$E_2 - pE_2^{(p)} = \frac{p-1}{24} + \sum_{n=1}^{\infty} \sigma_1(n) q^n - p \sum_{n=1}^{\infty} \sigma_1(n) q^{pn}.$$

Let f be a newform in $\mathscr{S}_2(\Gamma_0(p))$ (cf. [6]) and let K_f denote the number field generated by its Fourier coefficients. We denote by $\mathscr{O}_f$ the ring of integers of the number field K_f. Assume there exists a prime ideal λ in $\mathscr{O}_f$ and a natural number r such that

$$a_n(E_2 - pE_2^{(p)}) \equiv a_n(f) \bmod \lambda^r,$$

for all $n \geq 0$. The congruences of this type will be of interest to us when $k = 2$. If $k \geq 4$ there could be a congruence

$$a_n(E_k - p^{k-1} E_k^{(p)}) \equiv a_n(f) \bmod \lambda^r \tag{3}$$

or

$$a_n(E_k - E_k^{(p)}) \equiv a_n(f) \bmod \lambda^r. \tag{4}$$

The modular curve $X_0(p)$ has two cusps, 0 and ∞, for a prime p. Hence for any modular form $f \in M_k(\Gamma_0(p))$ we have q-expansions at ∞ and 0. We compute Fourier expansions for f and $f \mid_k \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. The n-th coefficient of the q-expansion at 0 is denoted by a_n^0 and is the n-th coefficient of the q-expansion at ∞ of the form $f \mid_k \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. We denote by $\mu(f)$ the coefficient $a_0^0(f)$.

Lemma 1. *Let p be a prime number and $k \geq 2$. Let $f \in \mathscr{S}_k^{new}(\Gamma_0(p))$ be a newform. Let $K = K_f$ be the field of coefficients of the newform f. Let $\lambda \in \mathscr{O}_K$ be a prime ideal such that $p \notin \lambda$ and $r \geq 1$ a natural number. Choose $E \in \mathscr{E}_k(\Gamma_0(p))$ with K_f-rational q-expansion coefficients. We assume that $ord_\lambda(a_n(E)) \geq 0$ for all $n \geq 0$. Suppose we have a congruence*

$$a_n(f) \equiv a_n(E) \bmod \lambda^r \tag{5}$$

for all $n \geq 0$. Then $\mu(E) \equiv 0 \bmod \lambda^r$. Hence the form E is cuspidal modulo λ^r. Explicitely, $\mu(\alpha E_k + \beta E_k^{(p)}) = \frac{-B_k}{2k}(\alpha + \frac{\beta}{p^k})$.

Proof. Let $k = 2$. Then $E = \alpha(E_2 - pE_2^{(p)})$ for some $\alpha \in K_f$ with $ord_\lambda(\alpha) \geq 0$. From the assumptions we have $1 \equiv a_1(f) \equiv \alpha \bmod \lambda^r$. We have

$$(E_2 - pE_2^{(p)}) \mid_2 \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = E_2 - \frac{1}{p} E_2^{(1/p)}.$$

Hence $\mu(E) = \alpha(\frac{-B_2}{4})(1 - \frac{1}{p})$. The assumption $p \notin \lambda$ and $a_0(E) \equiv 0 \bmod \lambda^r$ implies that $\mu(E) \equiv 0 \bmod \lambda^r$.

Let $k > 2$ and even. Then $E = \alpha E_k + \beta E_k^{(p)}$ for $\alpha, \beta \in K_f$ such that $ord_\lambda(\alpha) \geq 0$ and $ord_\lambda(\beta) \geq 0$. We have $\alpha \equiv a_1(E) \equiv 1 \bmod \lambda^r$ from the assumptions of the lemma. By [1, Thm.3] we have that

$$a_p(f) = -\varepsilon_p p^{k/2-1}$$

for some $\varepsilon_p \in \{-1,1\}$. On the other side, $a_p(E) = (1+p^{k-1})\alpha+\beta$. Combining the facts above

$$\alpha+\beta \equiv -\varepsilon_p p^{k/2-1} - p^{k-1} \bmod \lambda^r$$

because $\alpha \equiv 1 \bmod \lambda^r$. By (5) for $n=0$ we have

$$\frac{-B_k}{2k}(\alpha+\beta) \equiv 0 \bmod \lambda^r.$$

Then

$$\frac{-B_k}{2k} p^{k/2-1}(-\varepsilon_p - p^{k/2}) \equiv 0 \bmod \lambda^r.$$

We multiply both sides by $(-\varepsilon_p + p^{k/2})$ to get

$$\frac{-B_k}{2k}(1-p^k) \equiv 0 \bmod \lambda^r.$$

We divide by p^k and multiply by β to get

$$\frac{-B_k}{2k}\beta(\frac{1}{p^k}-1) \equiv 0 \bmod \lambda^r.$$

The coefficient $\mu(E) = \frac{-B_k}{2k}(\alpha+\frac{\beta}{p^k})$ satisfies the congruence

$$\frac{-B_k}{2k}(\alpha+\frac{\beta}{p^k}) \equiv \frac{-B_k}{2k}(\alpha+\beta)+\frac{-B_k}{2k}(-\beta+\frac{\beta}{p^k}) \equiv 0+\frac{-B_k}{2k}\beta(\frac{1}{p^k}-1) \equiv 0 \bmod \lambda^r.$$

Corollary 1. *Let f be a newform in $\mathscr{S}_k^{new}(\Gamma_0(p))$ and let $K = K_f$ be the field of coefficients of f. Suppose that for a natural $r \geq 1$ we have a congruence*

$$a_n(f) \equiv a_n(\alpha E_k + \beta E_k^{(p)}) \ mod\ \lambda^r$$

for all $n \geq 0$. If $p \notin \lambda$, then

$$r \leq \min\{ord_\lambda\left(\frac{-B_k}{2k}(\alpha+\beta)\right), ord_\lambda\left(\frac{-B_k}{2k}(\alpha+\frac{\beta}{p^k})\right)\}.$$

In particular, if

$$a_n(f) \equiv a_n(E_k - p^{k-1}E_k^{(p)}) \ mod\ \lambda^r$$

for all $n \geq 0$ and $p \notin \lambda$, then

$$r \leq ord_\lambda(\frac{-B_k}{2k}(1-p)).$$

Similarly, if

$$a_n(f) \equiv a_n(E_k - E_k^{(p)}) \; mod \; \lambda^r$$

for all $n \geq 0$ *and* $p \notin \lambda$*, then*

$$r \leq ord_{\lambda}(\frac{-B_k}{2k}(1-p^k)).$$

Proof. We observe that the upper bound for r is given by the conditions $a_0(E) \equiv 0 \bmod \lambda^r$ and $\mu(E) \equiv 0 \bmod \lambda^r$. The statement holds by Lemma 1 and explicit formulas for $a_0(E)$ and $\mu(E)$. In the first special case we put $\alpha = 1$, $\beta = -p^{k-1}$. In the second we put $\alpha = 1$ and $\beta = -1$.

Remark 1. If $p \in \lambda$ then we can check that for $k > 2$ and $\beta = -p^{k-1}$ and $\alpha = 1$ we get $\alpha \equiv 0 \bmod \lambda$ which is a contradiction. In the case $k = 2$, we observe that $\frac{-B_2}{4} \equiv 0 \bmod \lambda$ and $\varepsilon_p \equiv -1 \bmod \lambda$. However, in our computations we have not found any congruence satisfying this condition.

The case $\beta = -1$ and $\alpha = 1$ for $k = 2$ implies $0 \equiv \varepsilon_p \bmod \lambda$ which is impossible. For $k > 2$ we don't get any nontrivial condition modulo λ.

Let $K = \mathbb{Q}(\theta)$ be a number field with a primitive element θ. Let $\mathscr{O}_K$ be its ring of integers and $\mathscr{O}$ be an ℓ-maximal order over $\mathbb{Z}[\theta]$ for a fixed prime ℓ. Choose $\lambda \subset \mathscr{O}_K$ to be a non-zero prime ideal above ℓ and put $\tilde{\lambda} = \lambda \cap \mathscr{O}$. By the results of Section 4 below we have that for $x \in \mathscr{O}$

$$x = u_1 \pi^r$$

for a uniformizer π in $\mathscr{O}_{\tilde{\lambda}}$ and a unit u_1. In the end of Section 4 we define a $\tilde{\lambda}$-valuation

$$ord_{\tilde{\lambda}}(x) = r.$$

This extends to the field of fractions $K = Frac(\mathscr{O})$ by the formula

$$ord_{\tilde{\lambda}}\left(\frac{x}{y}\right) = ord_{\tilde{\lambda}}(x) - ord_{\tilde{\lambda}}(y).$$

In Section 4 we prove that

$$ord_{\tilde{\lambda}}(x) \geq r \Leftrightarrow x \equiv 0 \bmod \lambda^r.$$

In the algorithm presented below we use the last equivalence of orders. It is also crucial for our algorithm that the computation of ℓ-maximal order is more efficient than computation of the whole ring of algebraic integers which involves factorization of discriminants.

3.1 Sketch of the algorithm

Input: $(p,k) \in \mathbb{Z}^2$, where p is a prime number and $k \geq 2$ is an even integer.

1. Compute Galois conjugacy classes of newforms in $\mathscr{S}_k(\Gamma_0(p))$. Call the set *New*.

2. Compute Sturm bound $B = \frac{k}{12}[SL_2(\mathbb{Z}) : \Gamma_0(p)]$.

3. Let E_k be the Eisenstein series of weight k and level p. Compute the coefficients $a_n(E) = a_n(E_k - p^{k-1}E_k^{(p)})$ for $n \leq B$, where $E_k^{(p)}(\tau) = E_k(p\tau)$.

4. Compute the set of primes $L = \{\ell \text{ prime} : \ell \mid \text{Numerator}(a_0(E))\}$.

5. For each pair $(\ell, f) \in L \times New$, compute K_f, i.e., the coefficient field of f. By f we mean here a choice of a representative in Galois conjugacy class. Find the primitive element θ such that $K_f = \mathbb{Q}(\theta)$. Let $\mathscr{O}$ be the ℓ-maximal order above $\mathbb{Z}[\theta]$. Find the set $\mathscr{S} = \{\lambda \in \text{ Spec } \mathscr{O} : \lambda \cap \mathbb{Z} = \ell\mathbb{Z}\}$.

For each $\lambda \in \mathscr{S}$ compute

$$m_\lambda = \min_{n \leq B}(ord_\lambda(a_n(f) - a_n(E))).$$

If $m_\lambda > 0$ then we have a congruence

$$a_n(f) \equiv a_n(E) \bmod (\lambda\mathscr{O}_K)^{m_\lambda}$$

for all $n \geq 0$.

In the computations above we use a straightforward generalization of the well-known theorem of Sturm [11].

Theorem 1 ([3],Prop. 1). *Let N and n be two positive integers and $k \geq 2$. Let $f_1, f_2 \in M_k(\Gamma_1(N))$ be two modular forms which have coefficients in $\mathscr{O}_K$, the maximal order of number field K. Let $m = [SL_2(\mathbb{Z}) : \Gamma_1(N)]$ and $\mathfrak{p}$ - a prime ideal in $\mathscr{O}_K$.*

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

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

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

In fact, we can replace the subgroup $\Gamma_1(N)$ with any congruence subgroup Γ which contains containing $\Gamma(N)$ for some N. The proof goes through in the same way. We use the case $\Gamma = \Gamma_0(N)$.

4 Orders in number fields

In this section we introduce the concept of a p-maximal order. The content of this section is well-known, however we present the main theorems for the convenience of the reader. We follow the exposition of the subject presented in [5], [10]. In this section let $K = \mathbb{Q}(\theta)$ denotes a fixed number field with a primitive element θ.

Definition 1. An order in a number field K is a subring $R \subset K$ which is a finitely generated $\mathbb{Z}$-module of rank $\deg(K)$.

By $\mathcal{O}_K$ we will denote the ring of algebraic integers in K or equivalently the maximal order in K.

Definition 2. Let p be a prime number and K be a number field. An order $\mathcal{O}$ in K is p-maximal if

$$p \nmid [\mathcal{O}_K : \mathcal{O}].$$

Definition 3. Let $\mathcal{O}$ be an order in a number field K and let p be a prime number. The p-radical of $\mathcal{O}$ is the set

$$I_p(\mathcal{O}) = \{x \in \mathcal{O} : \exists_{m\geq 1} \quad x^m \in p\mathcal{O}\}.$$

Lemma 2 ([5],Prop.6.1.2). *The p-radical is an ideal in $\mathcal{O}$. Moreover there is a decomposition*

$$I_p(\mathcal{O}) = \prod_i \mathfrak{p}_i$$

where the product runs over prime ideals $\mathfrak{p}_i$ in $\mathcal{O}$ lying over p. Moreover there exists a positive integer m such that $I_p(\mathcal{O})^m \subset p\mathcal{O}$.

Lemma 3 ([5],Thm.6.1.3). *Let $\mathcal{O}$ be an order in K and fix a prime p. The set*

$$\mathcal{O}' = [I_p(\mathcal{O}) : I_p(\mathcal{O})] = \{x \in K : xI_p(\mathcal{O}) \subset I_p(\mathcal{O})\}.$$

The set $\mathcal{O}'$ is an order in K and either

$$\mathcal{O} = \mathcal{O}'$$

in which case $\mathcal{O}$ is p-maximal, equivalently $p \nmid [\mathcal{O}_K : \mathcal{O}]$ or

$$\mathcal{O} \subsetneq \mathcal{O}'$$

and $[\mathcal{O}' : \mathcal{O}] = p^n$ for some positive integer n.

Moreover, if $\mathcal{O} = \mathcal{O}'$, then

$$\mathcal{O} = \{x \in \mathcal{O}_K \mid \exists_{j\geq 1} \quad p^j x \in \mathcal{O}\}.$$

Corollary 2. *Let $K = \mathbb{Q}(\theta)$ be a number field. Let $R_0 = \mathbb{Z}[\theta]$ and define the chain of rings*

$$R_i \subset R_{i+1}$$

by the condition $R_{i+1} = R_i'$. There exists an m such that the chain stabilizes

$$R_m = R_{m+1}$$

and then

$$R_m = \{x \in \mathscr{O}_K \mid \exists j \geq 1 \quad p^j x \in \mathbb{Z}[\theta]\}.$$

Proof. By Lemma 3 it follows that for m such that $R_m = R_{m+1}$ we have

$$R_m = \{x \in \mathscr{O}_K \mid \exists j \geq 1 \quad p^j x \in R_m\}.$$

Let $L = \{x \in \mathscr{O}_K \mid \exists j \geq 1 \quad p^j x \in \mathbb{Z}[\theta]\}$ and $x \in L$. Then $p^j x \in \mathbb{Z}[\theta]$ for some positive j. But $\mathbb{Z}[\theta] = R_0 \subseteq R_1 \subseteq \ldots \subseteq R_m$. Therefore $p^j x \in R_m$, hence $x \in R_m$, proving $L \subset R_m$.

Let $x \in R_m$. Then $x \in \mathscr{O}_K$. By definition $R_m = R'_{m-1} = \{x \in K \mid xI_p(R_{m-1}) \subset I_p(R_{m-1})\}$. By Lemma 2 we have that $I_p(R_{m-1}) = \prod_i \mathfrak{p}_i$, primes $\mathfrak{p}_i$ in R_{m-1} containing p. So there exists $k \geq 1$ such that $p^k \in I_p(R_{m-1})$. So $p^k x \in I_p(R_{m-1})$, hence $p^k x \in R_{m-1}$. By induction we can show that there is a postive s such that $p^s x \in \mathbb{Z}[\theta]$, since $R_0 = \mathbb{Z}[\theta]$. It implies that

$$R_n \subset L.$$

This corollary shows that for each choice of the primitive element θ we can construct a p-maximal order containing $\mathbb{Z}[\theta]$.

Theorem 2. *Let p be a prime number, K a number field and $\mathscr{O}_K$ the maximal order in K and $\mathscr{O}$ a p-maximal order. We have a factorization into powers of prime ideals*

$$p\mathscr{O} = \prod_{i=1}^{n} \mathfrak{p}_i^{e_i}$$

and

$$p\mathscr{O}_K = \prod_{i=1}^{n} \mathscr{P}_i^{e_i}$$

with $\mathscr{P}_i \cap \mathscr{O} = \mathfrak{p}_i$.

Finally, we can define a valuation on elements of p-maximal order with respect to any prime ideal over p.

Let K be a number field and p a prime number. Assume we have a p-maximal order $\mathscr{O}$ in $\mathscr{O}_K$. For a nonzero prime ideal $\mathfrak{p} \in$ Spec $\mathscr{O}$ we have a prime ideal $\mathscr{P} = \mathfrak{p}\mathscr{O}_K$ in $\mathscr{O}_K$ by theorem above. Any element $x \in \mathscr{O}$ is equal to

$$x = u_1 \pi^r = u_2 \Pi^r$$

for $u_1 \in \mathscr{O}_{\mathfrak{p}}^{\times}, u_2 \in (\mathscr{O}_K)_{\mathscr{P}}^{\times}$ and uniformizers π and Π in $(\mathscr{O})_{\mathfrak{p}}$ and $(\mathscr{O}_K)_{\mathscr{P}}$ respectively. This common exponent of uniformizers we denote by

$$ord_{\mathfrak{p}}(x) = r.$$

The definition extends further to $K = Frac(\mathscr{O})$ by

$$ord_{\mathfrak{p}}\left(\frac{x}{y}\right) = ord_{\mathfrak{p}}(x) - ord_{\mathfrak{p}}(y).$$

The following equivalence holds for any $x \in \mathscr{O} \subset \mathscr{O}_K$

$$ord_{\mathfrak{p}}(x) \geq r \Leftrightarrow x \equiv 0 \bmod \mathscr{P}^r.$$

5 Numerical data

We present numerical data supporting the conjecture. We have found 740 different congruences with varying exponent and level. The levels and ranges we have examined are summarized in Table 1

Table 1 Range of computations

k	2	4	6	8	10	12	14	16	18	20	22
prime $N \leq$	1789	397	229	193	109	113	97	71	67	67	59

In total, we found 740 congruences of the form (2) for the ranges and weights described above.

There are 67 congruences such that $r > 1$. We found 106 congruences such that λ is ramified, i.e. $ord_{\lambda}(\ell) > 1$. Only 6 among them have the property that $r > 1$.

In the conjecture we have excluded a prime $\ell = 2$ because we found two congruences for the level $p = 257$, weight $k = 2$ and prime $\ell = 2$ which provide example where the exponent r of the congruence is greater than $ord_{\lambda}(\ell)$. In Table 3 we present data concerning congruences for which $ord_{\lambda}(\ell) = 1$. In Table 4 we present cases where $r > 1$ and $ord_{\lambda}(\ell) > 1$.
We are interested in a congruence of the type

$$a_n(E) \equiv a_n(f) \bmod \lambda^r$$

for all $n \geq 0$, between the Eisenstein series $E \in \mathscr{E}_k(\Gamma_0(p))$ and the newform $f \in \mathscr{S}_k(\Gamma_0(p))$ for different weights k and prime levels p. We denote by d a degree of the number field K_f containing coefficients of the form f and λ is a prime ideal in the ring of integers of K_f, above the rational prime $l \in \mathbb{Z}$. The column labelled by *nm* contains the number of elements in the residue field associated with λ. Number e denotes the ramification of the ideal λ at ℓ and $m = ord_{\lambda}(\mu(E))$. The column labelled by i contains the number of the Galois orbit of representing newform f (with respect to the internal Magma numbering).

Let $k = 2$ and $p = 1201$. We find a newform $f \in \mathscr{S}_2(\Gamma_0(1201))$ such that $K_f = \mathbb{Q}(\sqrt{2})$ and

$$f = q - q^2 - q^4 + 2\sqrt{2}q^7 + 3q^8 - 3q^9 + (2+\sqrt{2})q^{11} + \dots.$$

We have the Eisenstein series

$$E_2 - 1201E_2^{(1201)} = 50 + \sum_{n=1}^{\infty} \sigma_1(n)q^n - 1201 \sum_{n=1}^{\infty} \sigma_1(n)q^{1201n}.$$

We check, by the algorithm, that for the prime ideal $\lambda = (\sqrt{2})$

$$a_n(f) \equiv a_n(E_2 - 1201E_2^{(1201)}) \bmod \lambda$$

for all natural $n \geq 0$. We observe that the ideal $(2) \in \mathscr{O}_f = \mathbb{Z}[\sqrt{2}]$ is totally ramified with $(2) = \lambda^2$. Moreover, $a_{11}(E_2 - 1201E_2^{(1201)}) = 12$ and $a_{11}(f) = 2+\sqrt{2}$, hence the maximal exponent r of the congruence is equal to 1. The upper bound proposed in the conjecture is equal to 2, so it is not always the case that the maximal exponent r is equal to that bound.

Let $k = 2$ and $N = 109$. In this example we choose any root $\alpha \in \overline{\mathbb{Q}}$ of the equation

$$\alpha^4 + \alpha^3 - 5\alpha^2 - 4\alpha + 3 = 0$$

and form $K = \mathbb{Q}(\alpha)$. We have the Galois conjugacy class of newforms with the q-expansion

$$f = q + \alpha q^2 + (1 + 4\alpha - \alpha^3)q^3 + (\alpha^2 - 2)q^4 - \alpha q^5 + \dots.$$

The ring of integers $\mathscr{O}_f$ of $K_f = K$ is equal to $\mathbb{Z}[\alpha]$ and

$$(3) = (3,\alpha)(3, 2 + \alpha + \alpha^2 + \alpha^3)$$

is the factorization into prime ideals in $\mathscr{O}_f$. We find, by the algorithm, that for $\lambda = (3,\alpha)$

$$a_n(f) \equiv a_n(E_2 - 109E_2^{(109)}) \bmod \lambda^2$$

for all natural $n \geq 0$. In fact, this is the maximal possible exponent, since $\mu(E_2 - 109E_2^{(109)}) = \frac{9}{2}$ and $\text{ord}_\lambda(9) = 2$. In the unramified case, the conjecture only predicts that the upper bound for the maximal exponent r is smaller or equal to the one described in Corollary 1. This example shows that we cannot have a smaller bound in general.

Let $k = 8$ and $N = 43$. We choose any root $\alpha \in \overline{\mathbb{Q}}$ of the equation

$$\begin{aligned} -281015823360 + 26122731136\alpha + 25840429824\alpha^2 - 34580064\alpha^3 \\ -584457696\alpha^4 - 13609592\alpha^5 + 5061216\alpha^6 + 169726\alpha^7 \\ -18498\alpha^8 - 717\alpha^9 + 24\alpha^{10} + \alpha^{11} = 0 \end{aligned}$$

and form $K = \mathbb{Q}(\alpha)$. The ring of integers has the discriminant divisible exactly by 7. We have the Galois conjugacy class of newforms with the q-expansion

$$f = q + \alpha q^2 + a_3 q^3 + (\alpha^2 - 128)q^4 + \dots.$$

It is congruent to a suitable Eisenstein series modulo a prime ideal above 7 which is ramified of exponent 2 and has a presentation

$$\lambda = \left(7, \frac{\beta}{3456}\right)$$

where

$$\begin{aligned}\beta = 8448 + 43840\alpha + 38112\alpha^2 + 6248\alpha^3 + 7752\alpha^4 + 5918\alpha^5 \\ +2106\alpha^6 + 203\alpha^7 + 60\alpha^8 + \alpha^9.\end{aligned}$$

We get the congruence

$$a_n(f) \equiv a_n(E_8 - 43^7 E_8^{(43)}) \bmod \lambda^2$$

for all $n \geq 0$ and the exponent is maximal, what confirms the conjecture.

It is interesting to observe that some levels are better than others, because they provide much more congruences. For example, if $p = 163$ we obtain four different congruences for weights $k = 2, 4, 6$ and 8 with ideals above 3 raised to the powers $3, 3, 2$ and 3 respectively. For weight $k = 2$ or $k = 8$ the exponent of the ideal is maximal possible (cf. 3). For $k = 2$ we find a number field of degree 7 over $\mathbb{Q}$ with a primitive element α with a minimal polynomial

$$6 + 4\alpha - 23\alpha^2 + 19\alpha^4 - 5\alpha^5 - 3\alpha^6 + \alpha^7 = 0.$$

The ring of integers is equal to $\mathbb{Z}[\alpha]$. Its discriminant is equal to $2 \cdot 82536739$ and

$$3\mathbb{Z}[\alpha] = (3, \alpha)(3, 1 + \alpha + \alpha^3 + \alpha^4 + \alpha^6).$$

We find a newform of level 163 and weight 2 with q-expansion

$$\begin{aligned}f = q + \alpha q^2 + (-2 + 5\alpha + 5\alpha^2 - 6\alpha^3 - \alpha^4 + \alpha^5)q^3 \\ +(-2 + \alpha^2)q^4 + (6 + 6\alpha - 11\alpha^2 - 6\alpha^3 + 7\alpha^4 + \alpha^5 - \alpha^6)q^5 + \dots\end{aligned}$$

It is congruent to Eisenstein series $E_2 - 163E_2^{(163)} = \frac{27}{4} + \sum_{n=1}^{\infty} \sigma_1(n)q^n - 163\sum_{n=1}^{\infty} \sigma_1(n)q^{163n}$ modulo $(3, \alpha)^3$.

Remark 2. It is not always true that if we have a congruence modulo a power of a prime ideal above ℓ and $K_f = \mathbb{Q}(\theta)$, then ℓ-maximal order above $\mathbb{Z}[\theta]$ that we get from the algorithm is equal to the ring $\mathbb{Z}[\theta]$. We summarize several examples in Table 2. The prime ℓ is unramified in K_f. By i we denote the number of the Galois orbit of the newform and by *ind* the index $[\mathscr{O} : \mathbb{Z}[\theta]]$ for the ℓ-maximal order above $\mathbb{Z}[\theta]$.

Table 2 Index of the order

p	k	ℓ	i	ind
101	6	5	2	625
751	2	5	2	625
1621	2	3	3	3
1667	2	7	2	343

Table 3 Congruences with exponent greater than one and without ramification

p	k	ℓ	r	m	i	d	nm
769	2	2	5	5	2	36	2
1459	2	3	5	5	3	71	3
257	4	2	4	4	1	28	2
641	2	2	4	4	2	33	2
1409	2	2	4	4	3	65	2
163	2	3	3	3	3	7	3
163	4	3	3	3	1	19	3
163	8	3	3	3	1	46	3
193	2	2	3	3	3	8	2
193	6	2	3	3	2	41	2
251	2	5	3	3	2	17	5
449	2	2	3	3	2	23	2
487	2	3	3	4	4	16	3
577	2	2	3	3	4	18	2
811	2	3	3	3	3	40	3
1373	2	7	3	3	3	60	7
1601	2	2	3	3	2	80	2
1783	2	3	3	3	2	82	3
97	2	2	2	2	2	4	2
97	6	2	2	2	2	21	2
97	10	2	2	2	2	37	2
101	2	5	2	2	2	7	5
101	6	5	2	2	2	24	5
101	10	5	2	2	2	41	5
109	2	3	2	2	3	4	3
109	4	3	2	2	1	12	3
109	8	3	2	2	1	30	3
109	10	3	2	2	2	42	3
151	2	5	2	2	3	6	5
151	6	5	2	2	2	35	5
163	6	3	2	2	2	35	3
193	4	2	2	2	1	23	2
197	2	7	2	2	3	10	7
197	4	7	2	2	1	22	7
251	4	5	2	2	1	24	5
379	2	3	2	2	2	18	3
379	4	3	2	2	1	44	3
433	2	3	2	2	4	16	3
491	2	7	2	2	3	29	7
601	2	5	2	2	2	29	5
673	2	2	2	2	3	24	2
677	2	13	2	2	4	35	13
727	2	11	2	2	2	36	11
751	2	5	2	3	2	38	5
757	2	3	2	2	2	33	3
883	2	7	2	2	2	39	7
929	2	2	2	2	3	47	2
1051	2	5	2	2	3	48	5
1151	2	5	2	2	3	68	5
1153	2	2	2	4	3	50	2
1201	2	5	2	2	3	51	5
1217	2	2	2	3	2	58	2
1301	2	5	2	2	3	66	5
1451	2	5	2	2	2	73	5
1453	2	11	2	2	2	63	11
1471	2	7	2	2	2	72	7
1567	2	3	2	2	4	69	3
1601	2	5	2	2	2	80	5
1621	2	3	2	3	3	70	3
1667	2	7	2	2	2	82	7
1697	2	2	2	2	2	77	2

From Table 3 we can read off many properties of the congruences satisfying $ord_{\lambda}(\ell) = 1$. For $1 < r \leq ord_{\lambda}(\mu(E))$ we found only 5 congruences that do not satisfy $r = ord_\lambda(\mu(E))$ and 56 that satisfy this condition. Observe that the exponent was not maximal only for $k = 2$. In fact, for weights $k > 2$ we found congruences with nonmaximal exponent only for primes above 2. In all cases found, the residue degree was always equal to 1. Conjecture 1 is confirmed in all cases we found.

Moreover, if we fix $r \geq 2$ and look for a newform satisfying the congruence (2) for $r = ord_\lambda(\mu(E))$ and for a fixed Eisenstein series of level p we can find several examples for varying k,e.g. for $p = 163$ or for 197.

Some obvious necessary condition is that $a_q(f) \equiv a_q(E) = q^{k-1} + 1 \bmod \lambda^r$ for prime $q \notin p\lambda$. In fact, when we look for a rational newform of weight $k = 2$, by Modularity theorem this implies that we look for an elliptic curve F without complex multiplication, defined over $\mathbb{Q}$ such that

$$|F(\mathbb{F}_q)| \equiv 0 \bmod \ell^r.$$

We have found only such examples for $r = 1$.

In Table 4 we collect data about all congruences for which $ord_\lambda(l) > 1$ and $r > 1$. For primes $p \geq 3$ we found only three such cases and they agree with the conjecture. For r less than 2 we found in total 100 congruences and they agree with the conjecture. They are presented in Table 5.

Table 4 Congruences with exponent greater than one and with ramification

p	k	ℓ	r	m	e	i	d	nm
43	8	7	2	2	2	1	11	7
43	20	7	2	2	2	1	32	7
353	4	2	2	2	2	1	40	2
919	2	3	2	4	2	3	47	3
257	2	2	5	10	2	2	14	2
257	4	2	5	8	2	1	28	2

Table 5 Congruences with exponent equal to one and with ramification

p	k	ℓ	r	m	e	i	d	nm
31	2	5	1	2	2	1	2	5
31	6	5	1	2	2	2	8	5
31	10	5	1	2	2	2	13	5
31	14	5	1	2	2	2	18	5
31	18	5	1	2	2	2	23	5
31	22	5	1	2	2	2	28	5
47	10	23	1	2	2	2	20	23
47	12	23	1	2	2	1	18	23
47	16	23	1	2	2	1	26	23
47	20	23	1	2	2	1	34	23
53	6	13	1	2	2	2	12	13
53	18	13	1	2	2	2	38	13
67	4	11	1	2	2	1	7	11
67	14	11	1	2	2	2	37	11
103	2	17	1	2	2	2	6	17
113	2	2	1	2	2	2	2	2
113	6	2	1	2	2	1	21	2
113	6	2	1	2	2	1	21	4
113	6	2	1	2	2	2	25	2
113	6	2	1	2	2	2	25	2
127	2	7	1	2	2	2	7	7
127	8	7	1	2	2	1	34	7
131	2	5	1	2	2	2	10	5
131	6	5	1	2	2	2	32	5
191	6	5	1	2	2	2	46	5
199	2	3	1	2	2	3	10	3
199	4	3	1	2	2	1	20	3
211	2	5	1	2	2	1	2	5
211	6	5	1	2	2	2	47	5
223	4	37	1	2	2	1	24	37
281	2	5	1	2	2	2	16	5
307	4	3	1	2	2	1	35	3
337	2	2	1	2	2	2	15	2
337	4	7	1	2	2	1	40	7
353	4	2	1	2	2	2	48	2
353	4	11	1	2	2	1	40	11
367	4	61	1	2	2	1	41	61
401	4	5	1	2	2	1	45	5
409	2	17	1	2	2	2	20	17
409	4	17	1	2	2	1	47	17
419	4	19	1	2	2	1	43	19
523	2	3	1	2	2	3	26	3
541	2	5	1	2	2	2	24	5
571	2	5	1	2	2	9	18	5
593	2	2	1	2	2	5	27	2
661	2	11	1	2	2	3	29	11
683	2	11	1	2	2	3	31	11
691	2	5	1	2	2	2	33	5
733	2	61	1	2	2	4	32	61
761	2	5	1	2	2	3	41	5
761	2	19	1	2	2	3	41	19
881	2	2	1	2	2	2	46	2
911	2	7	1	2	2	3	53	7
941	2	5	1	2	2	2	50	5
971	2	5	1	2	2	2	55	5
1021	2	17	1	2	2	2	47	17
1091	2	5	1	2	2	3	62	5
1201	2	2	1	2	2	1	2	2
1279	2	3	1	2	2	2	64	3
1289	2	7	1	2	2	4	61	7
1291	2	5	1	2	2	2	62	5
1381	2	5	1	2	2	2	63	5
1447	2	241	1	2	2	2	71	241
1471	2	5	1	2	2	2	72	5
1483	2	13	1	2	2	4	67	13
1511	2	5	1	2	2	2	87	5
1531	2	3	1	2	2	4	73	3
1531	2	5	1	2	2	4	73	5
1553	2	2	1	2	2	2	74	2
1693	2	3	1	2	2	3	72	3
1697	2	53	1	2	2	2	77	53
1777	2	2	1	2	2	2	79	2
1789	2	149	1	2	2	2	80	149
101	4	5	1	3	3	1	9	5
101	8	5	1	3	3	1	26	5
101	12	5	1	3	3	1	42	5
181	2	5	1	3	3	2	9	5
181	6	5	1	3	3	2	40	5
353	4	2	1	3	3	1	40	2
1321	2	11	1	3	3	4	56	11
1381	2	23	1	3	3	2	63	23
1571	2	5	1	3	3	2	82	5
1747	2	3	1	3	3	3	77	3
353	4	2	1	5	5	1	40	2
353	4	2	1	5	5	2	48	2
353	4	2	1	5	5	2	48	2
1201	2	2	1	5	5	3	51	2
577	2	2	1	6	2	4	18	2
1601	2	2	1	6	2	2	80	2
257	4	2	1	8	2	1	28	2
353	2	2	1	10	5	4	14	2
257	4	2	1	12	3	1	28	2
257	4	2	1	16	4	2	36	2
1153	2	2	1	16	4	3	50	2
257	4	2	1	20	5	1	28	2
257	4	2	1	20	5	2	36	2
257	4	2	1	20	5	2	36	2
257	2	2	1	25	5	2	14	2
1249	2	2	1	26	13	3	59	2
1217	2	2	1	39	13	2	58	2

Acknowledgments

The author would like to thank Wojciech Gajda for many helpful suggestions and corrections. He thanks Gerhard Frey for reading of an earlier version of the paper and for helpful comments and remarks. He would like to thank Gabor Wiese for his help in improving the paper and suggesting one of the lemmas.

References

1. A. O. L. Atkin and J. Lehner, *Hecke operators on $\Gamma_0(m)$*, Math. Ann. **185** (1970), 134–160.
2. W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language.*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993).
3. I. Chen, I. Kiming, and J.B. Rasmussen, *On congruences mod p^m between eigenforms and their attached Galois representations.*, J. Number Theory **130** (2010), no. 3, 608–619.
4. I. Chen, I. Kiming, and G. Wiese, *On modular galois representations modulo prime powers.*, arXiv:1105.1918v1 (2011), 1 – 18.
5. H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993.
6. F. Diamond and J. Shurman, *A first course in modular forms.*, Graduate Texts in Mathematics, vol. 228, Springer-Verlag, New York, 2005.
7. L. Dieulefait and X. Taixés i Ventosa, *Congruences between modular forms and lowering the level mod l^n*, J. Théor. Nombres Bordeaux **21** (2009), no. 1, 109 – 118.
8. X. Taixés i Ventosa and G. Wiese, *Computing congruences of modular forms and Galois representations modulo prime powers.*, Arithmetic, geometry, cryptography and coding theory 2009,Contemp. Math. **521** (2010), 145–166.
9. B. Mazur, *Modular curves and the Eisenstein ideal.*, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33 – 186.
10. M. E. Pohst, *Computational algebraic number theory.*, DMV Seminar, vol. 21, Birkhäuser Verlag, Basel, 1993.
11. J. Sturm, *On the congruence of modular forms.*, Lecture Notes in Math. (1987), no. 1240, 275–280.