ssdnm
środowiskowe
studia doktoranckie
z nauk matematycznych

Bartosz Naskręcki

Uniwersytet A. Mickiewicza w Poznaniu

On higher congruences between cusp forms and Eisenstein series

Praca semestralna nr 2

(semestr letni 2011/12)

Opiekun pracy: Wojciech Gajda

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

On higher congruences between cusp forms and Eisenstein series

Bartosz Naskręcki

Abstract The paper contains a numerical study of congruences modulo prime powers between newforms and Eisenstein series at prime levels and with equal weights. We study the upper bound on the exponent of the congruence and formulate several observations based on the results of our computations.

1 Introduction

Let p be a rational prime. For a newform $f \in \mathscr{S}_k(\Gamma_0(p))$, let $K_f = \mathbb{Q}(\{a_n(f)\}_{n\geq 0})$ be the field generated by the Fourier coefficients of the form f and let $\mathscr{O}_f$ be its ring of integers. Let E_k denote the Eisenstein series of weight k given by the q-expansion $-\frac{B_k}{2k} + \sum_{n=1}^{\infty}\left(\sum_{d|n} d^{k-1}\right)q^n$, where B_k is the k-th Bernoulli number. We define the series $E_k^{(p)}$ by $E_k^{(p)}(\tau) = E_k(p\tau)$. From the theorem of Mazur [11, Proposition 5.12, Proposition 9.6] 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 newform f in $\mathscr{S}_2(\Gamma_0(p))$ and a maximal ideal $\lambda \in \mathscr{O}_f$ above ℓ such that

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

for almost all primes r.

We study a generalization of the congruence (1). Choose $E = E_k - p^{k-1}E_k^{(p)}$. 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

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

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

for all $n \geq 0$. Let ℓ be the rational prime below λ and assume that $p \notin \lambda$. Then ℓ divides the numerator of $a_0(E)$. More precisely,

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

where ord_λ is the standard normalized λ-adic valuation on K_f and v_ℓ is the ℓ-adic valuation on $\mathbb{Q}$. This is proved in Corollary 1 and Lemma 1. In the proof, we use the explicit description of $a_p(f)$ for a newform $f \in \mathscr{S}_k(\Gamma_0(p))$, cf. [1, Theorem 3]. In general, the maximal exponent r of the congruence (2) can be equal to

$$m := e \cdot v_\ell(\frac{-B_k}{2k}(1-p)),$$

where $e = ord_\lambda(\ell)$. From now on r always denotes the maximal exponent of the congruence.

Proposition 1. *There exists a prime p, a positive even integer k and a newform $f \in \mathscr{S}_k(\Gamma_0(p))$ such that the congruence (2) holds for all $n \geq 0$ and for some $r = m > 1$.*

Proof. We present an explicit example in Section 5.2.

Proposition 2. *There exists a prime p, a positive even integer k and a newform $f \in \mathscr{S}_k(\Gamma_0(p))$ such that the congruence (2) holds for all $n \geq 0$ with $m > r$.*

Proof. We present an explicit example in Section 5.3 (for $e = 1$ and $r > 1$), in Section 5.4 (for $e > 1$ and $r = 1$) and in Section 5.5 (for $e > 1$ and $r = e > 1$), respectively.

Observation 1 *Let $k \leq 22$ be an even positive integer and p be a prime, which is bounded with respect to k as indicated in the table below.*

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

Let $\ell > 2$ be a prime such that $v_\ell(a_0(E_k - p^{k-1}E_k^{(p)})) > 0$. Let $f \in \mathscr{S}_k(\Gamma_0(p))$ be a newform and $\lambda \in \mathscr{O}_f$ be a prime ideal above ℓ which is ramified, i.e. $ord_\lambda(\ell) = e > 1$. If

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

for all $n \geq 0$, then $r \leq e$ for every computed case (we found all possible examples in the range described in Table 2, Section 5 and some further examples in the range described in Table 1, Section 5). We present nontrivial examples of such congruences in Table 5, Section 5, marking them with boldface.

For $\ell = 2$ and $e > 1$ the upper bound $r \leq e$ does not hold.

Proposition 3. *Let $\ell = 2$. There exists a prime level p and a newform $f \in S_2(\Gamma_0(p))$ such that*

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

for all $n \geq 0$ *and a prime ideal* $\lambda \in \mathscr{O}_f$ *above* 2*, such that* $1 < ord_\lambda(2) < r$.

Proof. Put $p = 257$. There is a newform f in $\mathscr{S}_2(\Gamma_0(257))$, which satisfies the congruence (2) with $r = 5$ and $ord_\lambda(2) = 2$ for a suitable $\lambda \in \mathscr{O}_f$, cf. Table 5, Section 5.

The case of congruences between rational newforms and Eisenstein series in weight $k = 2$ is easy to handle as the next result indicates.

Proposition 4. *Let* $f \in S_2(\Gamma_0(p))$ *be a newform with rational coefficients (associated to an elliptic curve over* $\mathbb{Q}$*). Let* ℓ *be a prime such that* $v_\ell(a_0(E_2 - pE_2^{(p)})) > 0$ *and*

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

for all $n \geq 0$ *and some* $r > 0$*. Then one of the following holds*

1. $\ell = 3$, $r = 1$ *and* $p = 19$ *or* $p = 37$,
2. $\ell = 5$, $r = 1$ *and* $p = 11$,
3. $\ell = 2$, $r = 1$ *and* $p = 17$,
4. $\ell = 2$, $r = 1$ *and* $p = u^2 + 64$ *for some integer* u.

Proof. The proof is given in Section 5.8.

The number of different newforms congruent to the same Eisenstein series may vary.

Proposition 5. *There exists a prime* $p > 2$ *and two newforms* $f_1, f_2 \in \mathscr{S}_2(\Gamma_0(p))$ *(which are not Galois conjugated), such that*

$$a_n(f_1) \equiv a_n(E_2 - pE_2^{(p)}) \bmod \lambda_1^{r_1},$$

$$a_n(f_2) \equiv a_n(E_2 - pE_2^{(p)}) \bmod \lambda_2^{r_2},$$

for all $n \geq 0$*, prime ideals* $\lambda_1 \in \mathscr{O}_{f_1}, \lambda_2 \in \mathscr{O}_{f_2}$ *of equal residue field characteristic and some* $r_1, r_2 > 0$.

Proof. Consider a prime level $p = 353$. The space $\mathscr{S}_2(\Gamma_0(353))$ has dimension 29 and it has 4 different Galois conjugacy classes of newforms. With respect to the internal MAGMA numbering, the first, the second and the fourth Galois conjugacy class contains a newform congruent to the Eisenstein series $E_2 - pE_2^{(p)}$ modulo a prime above $\ell = 2$. For $\ell = 3$, we can take $p = 487$ and find newforms congruent to the Eisenstein series in Galois conjugacy classes with numbers 2 and 4, cf. Section 5.3 and Table 4, Section 5.

Remark 1. Mazur suggests that there may be infinitely many such examples for $\ell = 2$, cf. [11, II.19].

The majority of our examples satisfy the property that the residue field $\mathscr{O}_f/\lambda$ is a field with ℓ elements. However, this is not always the case, cf. Section 5.7. Also the ring of integers $\mathscr{O}_f$ is not always equal to $\mathbb{Z}[\theta]$, where θ is an algebraic integer such that $K_f = \mathbb{Q}(\theta)$. It can happen also that $[\mathscr{O}_f : \mathbb{Z}[\theta]]$ is divisible by ℓ, i.e. $\mathbb{Z}[\theta]$ is not ℓ-maximal in $\mathscr{O}_f$, cf. Section 5.6.

Our motivation to study the congruences (2) comes from the question posed in [8, Paragraph 4.4]. The authors study congruences between a newform $f \in \mathscr{S}_2(\Gamma_0(p))$ and an Eisenstein series $E \in \mathscr{E}_2(\Gamma_0(p))$

$$a_n(f) \equiv a_n(E) \ mod \ \lambda^r,$$

which hold for almost all prime indices n. Our approach is more restrictive, since in the congruences we take into account all indices $n \geq 0$.

Proposition 6. *The answer to [8, Question 4.1] is negative.*

Proof. The examples that contradict [8, Question 4.1] are described in Section 5.5 (ramified case) and in Section 5.7 (unramified case). In the first case, where $k = 2$ and $p = 919$ we obtain only one (up to Galois conjugacy) newform which is congruent to the Eisenstein series modulo 3 (in the sense of [8, Definition 2.2]), while the numerator of $\frac{p-1}{12}$ is divisible by 9. In the second case ($k = 2, p = 401$), we find a newform congruent to the Eisenstein series modulo 5 (in the sense of [8, Definition 2.2]), while the numerator of $\frac{p-1}{12}$ is divisible by 25 and there is no other newform congruent modulo 5 which is not Galois conjugate to the one which we found.

It would be desirable to extend our computations to take into account the situation when the cusp form and the Eisenstein series have different weights. Such a computational and theoretical study was done for two cusp forms in [4]. Unfortunately, we cannot apply directly the results of the paper [4] to our situation.

The proposed upper bound for r recorded in Observation 1 might be linked to the behavior of the inertia group at p of the residually reducible Galois representation attached to the newform f. Such a condition is given in [7, Theorem 2], where the authors deal with congruences between two cusp forms.

Contents of the paper: In Section 2 we introduce basic notation and describe Hecke algebras and eigenforms. Next, in Section 3 we describe the upper bound for the exponent of congruences between cuspidal eigenforms and Eisenstein series.

In Section 4.1 for the convenience of the reader we collect basic facts of the theory of ℓ-maximal orders which is an important ingredient of our algorithm. These facts are crucial for several improvements of the algorithm speed.

Section 4.2 contains a pseudo code description of the main algorithm which was implemented in MAGMA [2]. The source code is available on request or online, cf. [13].

Section 5 is devoted to presentation of the numerical data and proofs of propositions stated above. We discuss several explicit examples and the numerical data collected in the tables.

2 Notation and definitions

Let p be a prime number and k a positive even integer. The space $\mathscr{M}_k(\Gamma_0(p))$ of holomorphic modular forms of weight k and level $\Gamma_0(p)$ 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 the Eisenstein part and the space of cuspidal modular forms (cf.[6, Paragraph 5.11]). 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 τ lies on the complex upper half-plane $\mathscr{H}$. We define

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

The sequence of Bernoulli numbers $\{B_m\}_{m\in\mathbb{N}}$ is defined as usual by the series $\sum_{m=0}^{\infty} B_m t^m = \frac{t}{e^t - 1}$. Explicitly, in $\mathscr{E}_2(\Gamma_0(p))$ we have a generator

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

The space $\mathscr{E}_k(\Gamma_0(p))$ is generated by $E_k(\tau)$ and $E_k(p\tau)$ when $k \geq 4$.

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, Proposition 5.2.1]. The algebra is generated by two types of operators. The first type is defined for the primes $\ell \neq p$ by the formula

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

where $f \in \mathscr{M}_k(\Gamma_0(p))$ and $a_n(f)$ denotes the n-th Fourier coefficient of the form f at infinity. For $\ell = p$ there is a single operator

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

We denote by $\mathbb{T}$ the algebra $\mathbb{C}[\{T_r\}]$ generated by the Hecke operators T_r, where r runs through all rational 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 parts. For $k = 2$ since $\dim \mathscr{E}_2(\Gamma_0(p)) = 1$, the series $E_2 - pE_2^{(p)}$ is the unique normalized eigenform.

For $k \geq 4$ the dimension of the space $\mathscr{E}_k(\Gamma_0(p))$ is equal to two. We have a basis of the space consisting of normalized eigenforms

$$E_k - p^{k-1}E_k^{(p)}, \quad E_k - E_k^{(p)}.$$

3 Bounds on congruences

Let k be an even positive integer and p be a rational prime. We want to find congruences between Eisenstein series $E_k - p^{k-1}E_k^{(p)}$ and cuspidal newforms in the space $\mathscr{M}_k(\Gamma_0(p))$. Let f be a newform in $\mathscr{S}_k(\Gamma_0(p))$. Assume there exists a prime ideal λ in $\mathscr{O}_f$ and a natural number r such that

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

The bound on r depends on the q-expansion of the Eisenstein series at cuspidal points of the modular curve $X_0(p)$. The modular curve $X_0(p)$ has two cusps, 0 and ∞. Hence for any modular form $f \in \mathscr{M}_k(\Gamma_0(p))$ we have q-expansions at ∞ and 0. We compute expansions for f and $f \mid_k \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. We denote by $\mu(f)$ the zeroth coefficient of the q-expansion of the form f at 0. Equivalently, this is the zeroth coefficient of the q-expansion of the form $f \mid_k \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ at ∞.

Lemma 1. *Let p be a prime number, $k \geq 2$ be an even integer and $f \in \mathscr{S}_k(\Gamma_0(p))$ be a newform. Let λ be a prime ideal in $\mathscr{O}_f$ such that $p \notin \lambda$ and let $r \geq 1$ be a natural number. Let E denote the Eisenstein series $E_k - p^{k-1}E_k^{(p)}$. Suppose we have a congruence*

$$a_n(f) \equiv a_n(E) \bmod \lambda^r \tag{4}$$

for all $n \geq 0$. Then $\mu(E) \equiv 0 \bmod \lambda^r$. Hence the form E is cuspidal modulo λ^r.

Proof. For any even integer $k \geq 2$ the formula

$$(E_k - p^{k-1}E_2^{(p)}) \mid_k \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = E_k - \frac{1}{p}E_k^{(1/p)}$$

holds. It follows that $\mu(E)$ equals $-\frac{B_k}{2k}\left(1 - \frac{1}{p}\right)$. By [1, Theorem 3] we have that

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

for some $\varepsilon_p \in \{-1,1\}$. On the other side, $a_p(E) = 1$, hence $-\varepsilon_p p^{k/2-1} \equiv 1 \ mod\ \lambda^r$ by (4). Thence, we obtain the congruence

$$1 - p^{k-2} \equiv 0 \ mod\ \lambda^r. \tag{5}$$

Observe that $\mu(E) = -\frac{B_k}{2k}(1-p^{k-2}) + \left(-\frac{B_k}{2k}(1-p^{k-1})\right)\left(-\frac{1}{p}\right)$. Since f is a cusp-form, the assumption (4) implies that $a_0(E) \equiv 0 \ mod\ \lambda^r$, hence $-\frac{B_k}{2k}(1-p^{k-1}) \equiv 0 \ mod\ \lambda^r$. The last congruence and the congruence (5) imply that $\mu(E) \equiv 0 \ mod\ \lambda^r$.

Corollary 1. *Let p and ℓ be two distinct rational primes. Suppose that we have two integers $k \geq 2$, $r \geq 1$ and k is even. Let f be a newform in $\mathscr{S}_k(\Gamma_0(p))$. Suppose that for $E = E_k - p^{k-1}E_k^{(p)}$ we have congruences*

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

for all $n \geq 0$ and some prime ideal λ in $\mathscr{O}_f$ dividing ℓ. There is an upper bound

$$r \leq ord_\lambda(\ell) \cdot v_\ell\left(-\frac{B_k}{2k}(1-p)\right),$$

where v_ℓ denotes the ℓ-adic valuation on $\mathbb{Q}$.

Proof. By Lemma 1 we have $\mu(E) \equiv 0 \ mod\ \lambda^r$, hence $-\frac{B_k}{2k}\left(1-\frac{1}{p}\right) \equiv 0 \ mod\ \lambda^r$. Since p is invertible modulo λ, then

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

The exponent r satisfies the inequality $r \leq min(\mathrm{ord}_\lambda(a_0(E)), \mathrm{ord}_\lambda(\mu(E)))$. But we have for $k \geq 2$

$$\mathrm{ord}_\lambda\left(-\frac{B_k}{2k}(1-p^{k-1})\right) \geq \mathrm{ord}_\lambda\left(-\frac{B_k}{2k}(1-p)\right),$$

hence

$$r \leq \mathrm{ord}_\lambda(\ell) \cdot v_\ell\left(-\frac{B_k}{2k}(1-p)\right).$$

Remark 2. Let $p \in \lambda$ or equivalently $p = \ell$. For $k > 2$ the congruence (5) (which holds either when $p = \ell$ or when $p \neq \ell$) implies that $1 - \ell^{k-2} \in \lambda^r$, hence $1 - \ell^{k-2} \in \lambda$, hence $1 \in \lambda$, which leads to a contradiction. If $k = 2$, we observe that $a_0(E_2 - pE_2^{(p)}) \equiv 0 \ mod\ \lambda^r$. Hence $\mathrm{ord}_\lambda(-\frac{1}{24}(1-p)) \geq r \geq 1$, so $1 - p \in \lambda$ and $1 \in \lambda$, since $\ell = p$, which is impossible.

In the computations below we use a straightforward generalization of the well-known theorem of Sturm [18], suitable for our purposes. A similar theorem in more general form is proved in [4, Proposition 1].

Theorem 2. *Let p be a rational prime and $k \geq 2$ be an even integer. Let $f \in \mathscr{S}_k(\Gamma_0(p))$ be a normalized eigenform. Let ℓ be a rational prime dividing the numerator of $-\frac{B_k}{2k}(1-p^{k-1})$. Suppose we have a positive integer r and a nonzero prime ideal λ in $\mathscr{O}_f$, containing ℓ, such that for all $n \leq \frac{k(p+1)}{12}$ there is a congruence*

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

Then the congruence holds for all $n \geq 0$.

Proof. Let us denote by B the number $\frac{k(p+1)}{12}$ and by E the form $E_k - p^{k-1}E_k^{(p)}$. Let m denote the denominator of $-\frac{B_k}{2k}(1-p^{k-1})$. Observe that $\ell \nmid m$. Fourier coefficients of the form mE are rational integers. Coefficients of the form f lie in $\mathscr{O}_f$. If $r = 1$, then we know that for $n \leq B$

$$a_n(mf) \equiv a_n(mE) \ mod \ \lambda,$$

hence by the theorem of Sturm (cf. [17, Theorem 9.18]) we get the congruence for all $n \geq 0$. But $m \notin \lambda$, hence

$$a_n(f) \equiv a_n(E) \ mod \ \lambda$$

for all $n \geq 0$. If $r > 1$, then we proceed by induction. Assume first that the statement is true for $r-1$. Suppose that $a_n(f) \equiv a_n(E) \ mod \ \lambda^r$ for $n \leq B$. In particular, we get $a_n(f) \equiv a_n(E) \ mod \ \lambda^{r-1}$ for all $n \geq 0$ by the induction hypothesis. Choose any algebraic integer $\pi \in \lambda \setminus \lambda^2$. Then the function $\frac{1}{\pi^{r-1}}(f-E)$ is a modular form in $\mathscr{M}_k(\Gamma_0(p))$ with Fourier coefficients lying in the localization $(\mathscr{O}_f)_\lambda$ of the ring $\mathscr{O}_f$ at the prime ideal λ. By a theorem of Shimura (cf. [16, Theorem 3.52]) the space $\mathscr{S}_k(\Gamma_0(p))$ has a basis consisting of forms with with Fourier coefficients in $\mathbb{Z}$. The same is true for $\mathscr{M}_k(\Gamma_0(p))$. Hence, there exists an algebraic integer $\alpha \in \mathscr{O}_f \setminus \lambda$ such that $\frac{\alpha}{\pi^{r-1}}(f-E)$ has the Fourier expansion in $\mathscr{O}_f$. Moreover, for all $n \leq B$ the congruence

$$a_n\left(\frac{\alpha}{\pi^{r-1}}(f-E)\right) \equiv 0 \ mod \ \lambda$$

holds. By the Sturm theorem, it is true for all $n \geq 0$. This implies

$$a_n(\alpha(f-E)) \equiv 0 \ mod \ \lambda^r$$

for all $n \geq 0$. Since $\alpha \notin \lambda$, the induction step holds true and the theorem is proved.

4 Sketch of the algorithm

4.1 Orders in number fields

Fix a rational prime ℓ. We briefly recall the concept of an ℓ-maximal order. We fix an algebraic integer θ and the number field $K = \mathbb{Q}(\theta)$. By $\mathscr{O}_K$ we denote the ring of algebraic integers in K.

An order $\mathscr{O}$ in K is *ℓ-maximal* if $\ell \nmid [\mathscr{O}_K : \mathscr{O}]$. It is always possible to construct an ℓ-maximal order $\mathscr{O}$ containing the equation order $\mathbb{Z}[\theta]$, cf. [5, Theorem 6.1.3].

Every prime ideal $\mathfrak{L}$ in $\mathscr{O}$ lying over the prime ℓ is invertible in $\mathscr{O}$, which follows from [5, Proposition 4.8.15], [5, Theorem 6.1.3] and [5, Proposition 6.1.2].

By [10, Theorem 11.4] the localization $\mathscr{O}_{\mathfrak{L}}$ of the ring $\mathscr{O}$ at the prime ideal $\mathfrak{L}$ is a discrete valuation ring which is equal to $(\mathscr{O}_K)_{\mathfrak{L}\mathscr{O}_K}$ by [14, Proposition 12.10] (from which it also follows that $\mathfrak{L}\mathscr{O}_K$ is a unique prime ideal in $\mathscr{O}_K$ above $\mathfrak{L}$).

We define a valuation on elements of an ℓ-maximal order with respect to any prime ideal over ℓ. For a nonzero prime ideal $\mathfrak{L} \in$ Spec $\mathscr{O}$ over ℓ, let $\mathscr{L} = \mathfrak{L}\mathscr{O}_K$ be the corresponding prime ideal in $\mathscr{O}_K$. Any element $x \in \mathscr{O}$ can be written as $x = u_1\pi^r = u_2\Pi^r$, for $u_1 \in \mathscr{O}_{\mathfrak{L}}^{\times}, u_2 \in (\mathscr{O}_K)_{\mathscr{L}}^{\times}$ and uniformizers π and Π in $(\mathscr{O})_{\mathfrak{L}}$ and $(\mathscr{O}_K)_{\mathscr{L}}$, respectively.
The common exponent of uniformizers will be denoted by $ord_{\mathfrak{L}}(x) := r$. The definition extends to the fraction field $K = Frac(\mathscr{O})$ as $ord_{\mathfrak{L}}\left(\frac{x}{y}\right) = ord_{\mathfrak{L}}(x) - ord_{\mathfrak{L}}(y)$.
The following equivalence holds for any $x \in \mathscr{O} \subset \mathscr{O}_K$

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

In the algorithm presented in Section 4.2 we use the last equivalence of orders. It is also crucial for the algorithm that the computation of an ℓ-maximal order is more efficient than computation of the whole ring of algebraic integers, which involves factorization of discriminants. By the result of Chistov (cf. [3, Theorem 1.3]), computation of the ring of algebraic numbers in the number field K is polynomially equivalent to finding the largest square-free divisor of the field discriminant. The latter problem has not found to date a satisfactory solution, better than just factorizing the whole integer. On the other hand, computation of an ℓ-maximal order is straightforward and quick (cf. [5, Chapter 6]). Computation of prime ideals above ℓ in an ℓ-maximal order is equally fast, cf. [5, Chapter 6.2]. In our computations we often exploit this feature of ℓ-maximal orders.

4.2 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 the Sturm bound $B = \frac{k}{12}[SL_2(\mathbb{Z}) : \Gamma_0(p)] = \frac{k}{12} \cdot (p+1)$.

3. Compute the coefficients $a_n(E_k - p^{k-1}E_k^{(p)})$ for $n \leq B$.

4. Compute the set of primes $L = \{\ell \text{ prime} : \ell \mid \text{Numerator}(-\frac{B_k}{2k}(1-p))\}$.

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.

6. Find an algebraic integer θ such that $K_f = \mathbb{Q}(\theta)$.

7. Compute an ℓ-maximal order $\mathscr{O}$ above $\mathbb{Z}[\theta]$.

8. Compute the set $\mathscr{S} = \{\lambda \in \text{ Spec } \mathscr{O} : \lambda \cap \mathbb{Z} = \ell\mathbb{Z}\}$.

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

$$r_\lambda = \min_{n \leq B}(ord_\lambda(a_n(f) - a_n(E_k - p^{k-1}E_k^{(p)}))).$$

Output: If $r_\lambda > 0$ then we have a congruence

$$a_n(f) \equiv a_n(E_k - p^{k-1}E_k^{(p)}) \bmod (\lambda \mathscr{O}_f)^{r_\lambda}$$

for all $n \geq 0$.

5 Numerical data

In this section we discuss numerical results which were gathered by a repeated use of the algorithm in Section 4.2. The levels and ranges we have examined are summarized in Table 1. In total, we found 765 congruences of the form (2) for the ranges

Table 1 Range of computations

k	2	4	6	8	10	12	14	16	18	20	22
$p \leq$	3001	919	251	193	109	113	97	73	71	71	59

and weights described above. There are 73 congruences such that $r > 1$. We found 115 congruences such that λ is ramified, i.e. $ord_\lambda(\ell) > 1$. Only 7 among them have the property that $r > 1$. For large levels, when the degree of the coefficient field K_f of a newform f was bigger than 150 or the prime ideal λ contained 2, we have skipped the computations. However, we did a complete search in the range described in Table 2.

Table 2 Levels and weights which were completely investigated

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

5.1 Description of the tables

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 $E = E_k - p^{k-1}E_k^{(p)} \in \mathscr{E}_k(\Gamma_0(p))$ and the newform $f \in \mathscr{S}_k(\Gamma_0(p))$ for different weights k and prime levels p.

Our numerical results are summarized in Table 4, Table 5 and Table 6 presented below. Complete data set is available online, cf.[13]. Each table contains 8 columns. The letters p, k and ℓ were already explained. Denote by d the degree of the number

Table 3 Sample data entry

p	k	ℓ	r	m	i	d
769	2	2	5	5	2	36

field K_f generated by the coefficients of the form f and λ is a prime ideal in the ring of integers of K_f, above the rational prime $\ell \in \mathbb{Z}$. The letter e denotes the ramification index of the ideal λ at ℓ and $m = ord_\lambda(\mu(E))$. The column labeled by i contains the number of the Galois orbit of representing newform f (with respect to the internal MAGMA numbering).

In Table 4 we present data concerning congruences for which $ord_\lambda(\ell) = 1$. In Table 5 we present cases where $ord_\lambda(\ell) > 1$ and $ord_\lambda(\mu(E)) > ord_\lambda(\ell)$. From Table 4 one 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 Table 5 we collect data about all congruences for which $ord_\lambda(\ell) > 1$ and $ord_\lambda(\mu(E)) > ord_\lambda(\ell)$. For primes $\ell \geq 3$ we found only 5. The cases when $ord_\lambda(\mu(E))$ equals $ord_\lambda(\ell)$ are presented in Table 6.

Remark 3. The main difficulty in enlarging the number of congruences in Table 5 lies in the fact that $\dim \mathscr{S}_k(\Gamma_0(p)) = O(k \cdot p)$ as $k \to \infty$ and $p \to \infty$. In a typical situation, when $f \in \mathscr{S}_k(\Gamma_0(p))$ is a newform, the degree $[K_f : \mathbb{Q}]$ is roughly of the size $\frac{1}{2}\dim \mathscr{S}_k(\Gamma_0(p))$. To check the congruence, we perform Step 9 of the algorithm in Section 4.2. We have to compute $\frac{k}{12}(p+1)$ coefficients of the newform f and this is usually the slowest part of the algorithm. For example, when $k = 2$ and

Table 4 Congruences with exponent greater than one and without ramification

p	k	ℓ	r	m	i	d
769	2	2	5	5	2	36
1459	2	3	5	5	3	71
257	4	2	4	4	1	28
641	2	2	4	4	2	33
1409	2	2	4	4	3	65
163	2	3	3	3	3	7
163	4	3	3	3	1	19
163	8	3	3	3	1	46
193	2	2	3	3	3	8
193	6	2	3	3	2	41
251	2	5	3	3	2	17
449	2	2	3	3	2	23
487	2	3	3	4	4	16
577	2	2	3	3	4	18
811	2	3	3	3	3	40
1373	2	7	3	3	3	60
1601	2	2	3	3	2	80
1783	2	3	3	3	2	82
97	2	2	2	2	2	4
97	6	2	2	2	2	21
97	10	2	2	2	2	37

p	k	ℓ	r	m	i	d
101	2	5	2	2	2	7
101	6	5	2	2	2	24
101	10	5	2	2	2	41
109	2	3	2	2	3	4
109	4	3	2	2	1	12
109	8	3	2	2	1	30
109	10	3	2	2	2	42
151	2	5	2	2	3	6
151	6	5	2	2	2	35
163	6	3	2	2	2	35
193	4	2	2	2	1	23
197	2	7	2	2	3	10
197	4	7	2	2	1	22
251	4	5	2	2	1	24
379	2	3	2	2	2	18
379	4	3	2	2	1	44
433	2	3	2	2	4	16
491	2	7	2	2	3	29
601	2	5	2	2	2	29
673	2	2	2	2	3	24
677	2	13	2	2	4	35

p	k	ℓ	r	m	i	d
727	2	11	2	2	2	36
751	2	5	2	3	2	38
757	2	3	2	2	2	33
883	2	7	2	2	2	39
929	2	2	2	2	3	47
1051	2	5	2	2	3	48
1151	2	5	2	2	3	68
1153	2	2	2	4	3	50
1201	2	5	2	2	3	51
1217	2	2	2	3	2	58
1301	2	5	2	2	3	66
1451	2	5	2	2	2	73
1453	2	11	2	2	2	63
1471	2	7	2	2	2	72
1567	2	3	2	2	4	69
1601	2	5	2	2	2	80
1621	2	3	2	3	3	70
1667	2	7	2	2	2	82
1697	2	2	2	2	2	77

Table 5 Congruences with $m > e$ and with ramification

p	k	ℓ	r	m	e	i	d
3001	**2**	**5**	**1**	**6**	**2**	**1**	**2**
3001	**2**	**5**	**1**	**9**	**3**	**3**	**132**
251	**6**	**5**	**1**	**6**	**2**	**2**	**59**
919	**2**	**3**	**2**	**4**	**2**	**3**	**47**
919	**4**	**3**	**2**	**4**	**2**	**1**	**105**
257	2	2	1	25	5	2	14
257	2	2	5	10	2	2	14
353	2	2	1	10	5	4	14

p	k	ℓ	r	m	e	i	d
577	2	2	1	6	2	4	18
1153	2	2	1	16	4	3	50
1249	2	2	1	26	13	3	59
1601	2	2	1	6	2	2	80
1217	2	2	1	39	13	2	58
1889	2	2	1	4	2	3	96
2113	2	2	1	15	5	2	91
2273	2	2	1	10	5	3	105

p	k	ℓ	r	m	e	i	d
257	4	2	1	12	3	1	28
257	4	2	1	16	4	2	36
257	4	2	1	20	5	1	28
257	4	2	1	20	5	2	36
257	4	2	1	20	5	2	36
257	4	2	1	8	2	1	28
257	4	2	5	8	2	1	28

$p > 3000$, this means that we work with the field K_f of degree at least 150 over $\mathbb{Q}$. In the range described in Table 2 we found all possible congruences such that $ord_\lambda(\ell) > 1$. For levels and weights described in Table 1, we have decided to look only for congruences such that $[K_f : \mathbb{Q}] < 150$. This condition guarantees that Step 9 of the algorithm can be executed in less than 48 hours of computational time on the computer with Intel i5, 2.53 GHz processor and 4GB RAM.

5.2 The case $r = m > 1$ and $e = 1$

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

Table 6 Congruences with $m = e$ and with ramification

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

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

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

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

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 $\mathrm{ord}_\lambda(9) = 2$. In the unramified case, the upper bound for the maximal exponent r is smaller or equal to the one described in Corollary 1. This example shows that the equality can occur.

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 weights $k = 2,4$ or 8 the exponent of the ideal is maximal possible (cf. Table 4). 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

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

It is congruent to the 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 $(3,\alpha)^3$.

5.3 The case $m > r > 1$ and $e = 1$

Let $k = 2$ and $p = 487$. The space of cusp forms $\mathscr{S}_2(\Gamma_0(487))$ contains five Galois conjugacy classes of newforms. We take f such that

$$f = q+\alpha q+\cdots,$$

where α is an algebraic integer such that

$$\begin{aligned} &\alpha^{16}-7\alpha^{15}-5\alpha^{14}+131\alpha^{13}-132\alpha^{12}-977\alpha^{11}+1666\alpha^{10} \\ &+3671\alpha^9-8191\alpha^8-7212\alpha^7+20571\alpha^6+6937\alpha^5 \\ &-27100\alpha^4-2748\alpha^3+17207\alpha^2+360\alpha-3825=0. \end{aligned}$$

The field K_f is equal to $\mathbb{Q}(\alpha)$ and the ideal $3\mathscr{O}_K$ is a product of four distinct prime ideals

$$3\mathscr{O}_K = \lambda_1\lambda_2\lambda_3\lambda_4.$$

Let $\lambda_1 = (3, \frac{1}{105}\beta)$, where

$$\beta = 2\alpha^{15} + 106\alpha^{14} + 50\alpha^{13} + 112\alpha^{12} + 156\alpha^{11} + 161\alpha^{10} + 392\alpha^9 + 307\alpha^8 + 148\alpha^7 + 126\alpha^6 + 192\alpha^5 + 194\alpha^4 + 280\alpha^3 + 279\alpha^2 + 124\alpha + 705.$$

We check that f is congruent to $E_2 - 487E_2^{(487)}$ modulo λ_1^3 and $m = \mu(E_2 - 487E_2^{(487)}) = 4$ (cf. Corollary 1). Moreover, there is no congruence modulo λ_1^4, hence the maximal exponent $r = 3$ is smaller than the theoretical upper bound m in Corollary 1.

5.4 The case $r < e < m$ and $e > 1$

Let $k = 2$ and $p = 3001$. The space of cusp forms $\mathscr{S}_2(\Gamma_0(3001))$ has dimension 249 and it is a direct sum of three subspaces S_1, S_2 and S_3 of dimensions 2, 115 and 132, respectively. The space S_1 is generated by two Galois conjugate newforms

$$f_1 = q + \alpha_1 q^2 + (\alpha_1 + 1)q^3 + (\alpha_1 - 1)q^4 + 2\alpha_1 q^5 + (2\alpha_1 + 1)q^6 + \cdots,$$

$$f_2 = q + \alpha_2 q^2 + (\alpha_2 + 1)q^3 + (\alpha_2 - 1)q^4 + 2\alpha_2 q^5 + (2\alpha_2 + 1)q^6 + \cdots,$$

where α_1 and α_2 are roots of the polynomial $x^2 - x - 1$. Since the forms are Galois conjugate, we will consider only one of them. Assume $\alpha_1 = \frac{1+\sqrt{5}}{2}$. The ring of integers of $K_{f_1} = \mathbb{Q}(\sqrt{5})$ is $\mathscr{O}_{f_1} = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ and

$$5\mathscr{O}_{f_1} = \lambda^2,$$

for the prime ideal λ which equals $(5, 2 + \frac{1+\sqrt{5}}{2})$. We check that $a_0(E_2 - 3001E_2^{(3001)}) = 125$ and $\mu(E_2 - 3001E_2^{(3001)}) = 125$, and $ord_\lambda(125) = 6$. Corollary 1 shows that the upper bound for the exponent r of the congruence is 6. We checked by MAGMA that for $n \leq \frac{3001+1}{12}$ the congruence

$$a_n(f_1) \equiv a_n(E_2 - 3001E_2^{(3001)}) \bmod \lambda$$

holds. Hence, by Theorem 2 the congruence holds for all $n \geq 0$. But we also find that $a_2(f_1) - a_2(E_2 - 3001E_2^{(3001)}) = \frac{1+\sqrt{5}}{2} - 3 \notin \lambda^2$, which proves that the maximal exponent r, for which the congruence holds is equal to 1.

5.5 The case $r = e < m$ and $e > 1$

Let $k = 2$ and $p = 919$. The space $S_2(\Gamma_0(919))$ contains 3 Galois conjugacy classes of newforms, with coefficient fields of degrees 2, 27 and 47, respectively. We take

a representative f of the class with the coefficient field of degree 47 over $\mathbb{Q}$. The form f equals $q+\alpha q+\ldots$, where the algebraic integer α is a root of a monic integral polynomial of degree 47. The discriminant of the field K_f is approximately equal to $0.5995\cdot 10^{304}$. We were not able to compute the factorization of the discriminant. Instead, we work with a 3-maximal order $\mathscr{O}$ above $\mathbb{Z}[\alpha]$, where $K_f=\mathbb{Q}(\alpha)$. There are 6 different prime ideals above $3\mathscr{O}$ and $3\mathscr{O}=\lambda_1^2\cdot\prod_{i=2}^{6}\lambda_i$. We check that f is congruent to $E_2-919E_2^{(919)}$ modulo λ_1^2, while the maximal exponent $m=ord_{\lambda_1}(\mu(E_2-919E_2^{(919)}))$ equals 4. The discussion in Section 4.1 implies that there is a congruence between f and $E_2-919E_2^{(919)}$ modulo $(\lambda_1 O_f)^2$ and $ord_{\lambda_1 O_f}(\mu(E_2-919E_2^{(919)}))=4$, hence we find that $r=e<m$ and $e>1$.

5.6 Equation order is not always ℓ-maximal

It is not always true that if we have a congruence modulo a power of a prime ideal above ℓ and $K_f=\mathbb{Q}(\theta)$, where θ is an algebraic integer, then an ℓ-maximal order above $\mathbb{Z}[\theta]$ that we get from the algorithm implemented in MAGMA, is equal to the ring $\mathbb{Z}[\theta]$. We summarize several examples in Table 7. 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 7 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

5.7 Large residue field

Let $k=2$ and $p=401$. The space $\mathscr{S}_2(\Gamma_0(401))$ is a direct sum $S_1\oplus S_2$ of two new subspaces. The space S_1 is of dimension 12 over $\mathbb{C}$ and it is generated by a newform and its Galois conjugates, none of which is congruent to the Eisenstein series $E_2-401E_2^{(401)}$ modulo any power of a prime ideal. The space S_2 is generated by a newform $f=q+\alpha q^2+\cdots$, such that α is an algebraic integer satisfying

$$\begin{aligned}&-44+1058\alpha-4111\alpha^2-24699\alpha^3+12831\alpha^4+93934\alpha^5-14353\alpha^6\\&-152221\alpha^7+8292\alpha^8+132085\alpha^9-2749\alpha^{10}-67876\alpha^{11}+519\alpha^{12}\\&+21617\alpha^{13}-51\alpha^{14}-4305\alpha^{15}+2\alpha^{16}+521\alpha^{17}-35\alpha^{19}+\alpha^{21}=0.\end{aligned}$$

The field K_f is generated by $\theta = \alpha$. The ideal $5\mathscr{O}_f$ is a product of four distinct prime ideals, i.e. every prime ideal above 5 is unramified in $\mathscr{O}_f$. The prime ideal $\lambda = (5, \frac{1}{8}\beta)$ with

$$\begin{aligned}\beta = {} & 32 + 48\alpha + 82\alpha^2 + 75\alpha^3 + 66\alpha^4 + 70\alpha^5 + 39\alpha^6 + 62\alpha^7 + 50\alpha^8 + 37\alpha^9 \\ & + 22\alpha^{10} + 56\alpha^{11} + 17\alpha^{12} + 2\alpha^{13} + 16\alpha^{14} + 26\alpha^{15} + 3\alpha^{16} + 7\alpha^{17} + \alpha^{18} + \alpha^{19}\end{aligned}$$

gives the quotient map $\pi : \mathscr{O}_f \to \mathscr{O}_f/\lambda \cong \mathbb{F}_{25}$. The image $\pi(\mathbb{Z}[\{a_n(f)\}_{n\in\mathbb{N}}\}])$ is a subfield $\mathbb{F}_5$ in $\mathscr{O}_f/\lambda$. Observe that $a_0(E_2 - 401E_2^{(401)}) = \frac{50}{3}$ and $v_5(\mu(E_2 - 401E_2^{(401)})) = 2$. One could expect that

$$a_n(f) \equiv a_n(E_2 - 401E_2^{(401)}) \bmod \lambda^r$$

holds for all $n \geq 0$ and $r \leq 2$. However, the coefficient $a_2(f) - a_2(E_2 - 401E_2^{(401)})$ is not congruent to 0 modulo λ^2. The differences $a_n(f) - a_n(E_2 - 401E_2^{(401)})$ are congruent to 0 modulo λ for n less or equal to the Sturm bound, hence, the congruence modulo λ holds for all $n \geq 0$. The order $\mathscr{O} = \mathbb{Z}[\{a_n(f)\}_{n\in\mathbb{N}}]$ equals also $\mathbb{Z}[\{a_2(f), a_3(f), a_5(f)\}]$ and can be obtained by performing the *pMaximalOrder* algorithm in MAGMA, starting with $\mathbb{Z}[\theta]$. Let $\mathscr{O}^{(2)}$ denote a 2-maximal order obtained from $\mathbb{Z}[\theta]$. Then, let $\mathscr{O}^{(2,3697)}$ be an 3697-maximal order above $\mathscr{O}^{(2)}$ obtained by the MAGMA algorithm. Finally, let $\mathscr{O}^{(2,3697,34759357)}$ denote a 34759357-maximal order above $\mathscr{O}^{(2,3697)}$. The order $\mathscr{O}^{(2,3697,34759357)}$ equals $\mathscr{O}$ and $[\mathscr{O}_f : \mathscr{O}] = 5$. The maximal order $\mathscr{O}_f$ is the 5-maximal order above $\mathscr{O}$. Note also that we have proper inclusions

$$\mathbb{Z}[\theta] \subsetneq \mathscr{O}^{(2)} \subsetneq \mathscr{O}^{(2,3697)} \subsetneq \mathscr{O}^{(2,3697,34759357)}.$$

In the algorithm in Section 4.2 we use only a 5-maximal order above $\mathbb{Z}[\theta]$. This is sufficient when we check the congruence modulo a prime above 5 in $\mathscr{O}_f$. In order to compute $\mathscr{O}_f$, we should run *pMaximalOrder* algorithm with primes $2, 5, 3697$ and 34759357, respectively. Observe that in this particular case, the computation of 3697 and 34759357-maximal orders is completely unnecessary, because we check congruences modulo primes above 2 and 5 and $a_0(E_2 - 401E_2^{(401)}) = \frac{50}{3}$. This shows that in Step 7 of the algorithm in Section 4.2 we gain some significant amount of time by skipping the superfluous computation of $\mathscr{O}_f$.

5.8 Congruences over $\mathbb{Q}$

Let f in $S_2(\Gamma_0(p))$ be a rational newform for which the congruence (2) holds for all $n \geq 0$. In particular, $a_q(f) \equiv a_q(E) = q^{k-1} + 1 \bmod \lambda^r$ for all primes $q \neq p$. Finding a rational newform f as above amounts to a search for an elliptic curve F (attached to f by the modularity theorem) defined over $\mathbb{Q}$, of prime conductor p, such that

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

where $\tilde{F}_q$ denotes the reduction of F at the prime q. It follows from [9, Theorem 2], that there exists an elliptic curve F' over $\mathbb{Q}$ which is $\mathbb{Q}$-isogenous to F and the group of $\mathbb{Q}$-rational points on F' contains a point of order ℓ^r. The conductor of F' is p. For an elliptic curve defined over $\mathbb{Q}$ the smallest possible conductor is 11. Hence F' has good reduction at 2. The group of $\mathbb{Q}$-rational points of F' contains the torsion subgroup, which we denote by T. The reduction at 2 maps T into $\tilde{F}'_2(\mathbb{F}_2)$. The kernel of this homomorphism has order a power of 2. By Hasse theorem for elliptic curves the inequality $|\tilde{F}'_2(\mathbb{F}_2)| \leq 5$ holds. Hence, the order $|T|$ equals 2^m, $2^m \cdot 3$ or $2^m \cdot 5$, for some $m \geq 0$. Suppose that $|T| > 2$.

If $|T| = 2^m$, then [12, Theorem 2] and [12, Theorem 3] imply that $T \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ or $T \cong \mathbb{Z}/4\mathbb{Z}$ and in both cases $p = 17$. The only $\mathbb{Q}$-isogeny class of elliptic curves of conductor 17 is attached to the newform $f = q - q^2 - q^4 + \cdots$ in $\mathscr{S}_2(\Gamma_0(17))$. For any prime $q \neq p$ the coefficient $a_q(f) = 1 + q - |\tilde{F}'_q(\mathbb{F}_q)|$ is congruent to $1 + q$ modulo 4. We check directly that $a_p(f) = 1$. The congruence $a_n(f) \equiv a_n(E_2 - 17E_2^{(17)}) \bmod 4$ holds for all $n \geq 1$. However, $a_0(E_2 - 17E_2^{(17)}) = \frac{2}{3}$, so for all $n \geq 0$ we have only a congruence modulo 2.

If $|T| = 2^m \cdot 3$, then [12, Theorem 1] implies that $T \cong \mathbb{Z}/3\mathbb{Z}$ and $p = 19$ or $p = 37$. There is exactly one $\mathbb{Q}$-isogeny class of elliptic curves of conductor 19. It provides the newform $f = q - 2q^3 - 2q^4 + \cdots$ in $\mathscr{S}_2(\Gamma_0(19))$ congruent to $E_2 - 19E_2^{(19)}$ modulo 3 at all coefficients. If the conductor p equals 37, then there are two $\mathbb{Q}$-isogeny classes of elliptic curves. Only the class associated with the newform $f = q + q^3 - 2q^4 + \cdots$ in $\mathscr{S}_2(\Gamma_0(37))$ provides the congruence $a_n(f) \equiv a_n(E_2 - 37E_2^{(37)}) \bmod 3$ for all $n \geq 0$. The other newform f' satisfies $a_p(f') = -1$, so the congruence cannot hold.

If $|T| = 2^m \cdot 5$, then by [12, Theorem 4] we get $T \cong \mathbb{Z}/5\mathbb{Z}$ and $p = 11$. The unique newform $f \in \mathscr{S}_2(\Gamma_0(11))$ satisfies $a_p(f) = 1$. Moreover, $a_0(E_2 - 11E_2^{(11)}) = \frac{5}{12}$, hence the congruence $a_n(f) \equiv a_n(E_2 - 11E_2^{(11)}) \bmod 5$ holds for all $n \geq 0$.

We are left with only one case, when $|T|$ equals 2. If the elliptic curve F' of prime conductor $p > 17$ satisfies $|T| = 2$, then $p = u^2 + 64$ for some rational number u. This is proved in [15, Theorem 2]. The primes $p = 113, 353, 593$ and 1153 are of the form $u^2 + 64$ for $u \in \mathbb{Z}$ and on these levels we find newforms $f \in \mathscr{S}_2(\Gamma_0(p))$ congruent congruent to $E_2 - pE_2^{(p)}$ modulo 2. However, in general it is not known whether the sequence $\{u^2 + 64\}_{u \in \mathbb{N}}$ contains an infinite number of primes.

Acknowledgments

The author would like to thank Wojciech Gajda for many helpful suggestions and corrections. He thanks Gerhard Frey for reading 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. Finally, the author wishes to express his thanks to an anonymous referee for the careful reading of the paper and a detailed list of comments which improved the exposition and removed several inaccuracies. The author was supported by the National Science Centre research grant 2012/05/N/ST1/02871.

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. J. A. Buchmann and H. W. Lenstra, Jr., *Approximating rings of integers in number fields*, J. Théor. Nombres Bordeaux **6** (1994), no. 2, 221–260.
4. 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.
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. Nicholas M. Katz, *Galois properties of torsion points on abelian varieties*, Invent. Math. **62** (1981), no. 3, 481–502.
10. Hideyuki Matsumura, *Commutative ring theory*, second ed., Cambridge Studies in Advanced Mathematics, vol. 8, Cambridge University Press, Cambridge, 1989, Translated from the Japanese by M. Reid.
11. B. Mazur, *Modular curves and the Eisenstein ideal.*, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33 – 186.
12. Isao Miyawaki, *Elliptic curves of prime power conductor with* $\mathbf{Q}$*-rational points of finite order*, Osaka J. Math. **10** (1973), 309–323. MR 0327776 (48 #6118)
13. B. Naskręcki, *Algorithm*, http://bnaskrecki.faculty.wmi.amu.edu.pl/doku.php/magma.
14. Jürgen Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999, Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.
15. Bennett Setzer, *Elliptic curves of prime conductor*, J. London Math. Soc. (2) **10** (1975), 367–378.
16. Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo, 1971, Kanô Memorial Lectures, No. 1.
17. William Stein, *Modular forms, a computational approach*, Graduate Studies in Mathematics, vol. 79, American Mathematical Society, Providence, RI, 2007, With an appendix by Paul E. Gunnells.
18. J. Sturm, *On the congruence of modular forms.*, Lecture Notes in Math. (1987), no. 1240, 275–280.