Math. Res. Lett. **21** (2014), *no.* 1, 71–82

ON HIGHER CONGRUENCES BETWEEN AUTOMORPHIC FORMS

Tobias Berger, Krzysztof Klosin and Kenneth Kramer

Abstract. We prove a commutative algebra result which has consequences for congruences between automorphic forms modulo prime powers. If C denotes the congruence module for a fixed automorphic Hecke eigenform π_0, we prove an exact relation between the p-adic valuation of the order of C and the sum of the exponents of p-power congruences between the Hecke eigenvalues of π_0 and other automorphic forms. We apply this result to several situations including the congruences described by Mazur's Eisenstein ideal.

1. Introduction

Let p be a prime. Let $f_1, \dots, f_r$ be all weight 2 normalized cuspidal simultaneous eigenforms of level $\Gamma_0(N)$ with N prime. A famous result of Mazur's ([13] Proposition 5.12(iii)) states that at least one of these forms is congruent modulo p to the Eisenstein series $E_2^* = 1 - N + 24\sum_{n=1}^{\infty} \sigma^*(n)q^n$ for

$$\sigma^*(n) = \sum_{0<d|n,(d,N)=1} d,$$

if p divides the numerator $\mathcal{N}$ of $\frac{N-1}{12}$. One may ask for the precise relation between $\mathrm{val}_p(\mathcal{N})$ and the "depth" of congruence of the newforms $f_1, \dots, f_r$ to E_2^*. One of our results (Proposition 3.1) provides an answer to this question. More precisely, if ϖ_N is a uniformizer in the valuation ring of a finite extension of $\mathbf{Q}_p$ (of ramification index e_N) which contains all of the eigenvalues of the f_i's and m_i is defined as the largest integer such that $E_2^* \equiv f_i \bmod \varpi_N^{m_i}$, then

$$\frac{1}{e_N}\sum_{i=1}^{r} m_i = \mathrm{val}_p(\mathcal{N}). \tag{1.1}$$

In general, the Hecke eigenvalue congruences between a fixed automorphic eigenform π_0 on a reductive algebraic group G and other eigenforms (call the set of them Π) on G are controlled by the order of the so-called *congruence module*. This module can be defined as the quotient of the Hecke algebra $\mathbf{T}$ acting on the forms in Π by the image J in $\mathbf{T}$ of the annihilator of π_0 in the Hecke algebra $\mathbf{T}_0$ acting on the forms in $\Pi \cup \{\pi_0\}$ (for details on this setup see Section 4). In the more classical situation, where π_0 is an Eisenstein series, J is often called the *Eisenstein ideal*. However, our considerations apply in a much more general framework, e.g., when J corresponds to a primitive cusp form or to a cuspidal associated to parabolics (CAP) automorphic representation (see Section 5).

Received by the editors February 10, 2013.
2000 *Mathematics Subject Classification.* 11F33.
Key words and phrases. congruences, automorphic forms.

In this general setup, one may ask again how many of the automorphic forms in Π have Hecke eigenvalues congruent to those of π_0 and what the "depth" of these congruences is. We prove that whenever the ideal J is principal (as in the Mazur example above) then an equality analogous to (1.1) can be achieved with $\#\mathbf{T}/J$ replacing $\mathcal{N}$. However, if the ideal J is not principal, we show that instead of equality the analogue S of the quantity on the left of (1.1) (the total "depth" of the congruences) is bounded strictly from below by $\mathrm{val}_p(\#\mathbf{T}/J)$ (cf. Proposition 4.3). Let us note here that in general principality of J is not known or even expected to hold. In many cases, it is conjectured or known that the order $\#\mathbf{T}/J$ is related to a special value of an appropriate L-function. In this case, our results provide an L-value bound on S.

Our paper is organized as follows. In Section 2, we prove a commutative algebra result which will be the basis for all of our applications to congruences among automorphic forms. In fact, it can be seen as a more general result regarding the distribution of congruences among various subsets of automorphic forms (not just single automorphic forms) — for an application in this context to a modularity problem see [2]. In Section 3, we apply this result to Mazur's congruences and derive (1.1). In Section 4, we set up a framework to deal with the general types of congruences among automorphic forms and prove a lower bound on the total depth of congruences in terms of the order of a congruence module. Finally, in Section 5 we provide more examples.

On completion of this paper, we learned from Fred Diamond that a similar argument was already used by him and Wiles to prove an analogue of the inequality in our Proposition 4.3 in the case of congruences between cusp forms of different levels (cf. Theorem 4C in [7] and Lemma 1.4.3 in [18]).

2. Commutative algebra

Let p be a prime. Let $\mathcal{O}$ be the valuation ring of a finite extension E of $\mathbf{Q}_p$. Fix a choice of a uniformizer ϖ of $\mathcal{O}$ and write $\mathbf{F} = \mathcal{O}/\varpi\mathcal{O}$ for the residue field.

Let $s \in \mathbf{Z}_+$ and let $\{n_1, n_2, \dots, n_s\}$ be a set of s positive integers. Set $n = \sum_{i=1}^s n_i$. Let $A_i = \mathcal{O}^{n_i}$ with $i \in \{1, 2, \dots, s\}$. Set $A = \prod_{i=1}^s A_i = \mathcal{O}^n$. Let $\varphi_i : A \twoheadrightarrow A_i$ be the canonical projection. Let $T \subset A$ be a local complete $\mathcal{O}$-subalgebra which is of full rank as an $\mathcal{O}$-submodule and let $J \subset T$ be an ideal of finite index. Set $T_i = \varphi_i(T)$ and $J_i = \varphi_i(J)$. Note that each T_i is also a local complete $\mathcal{O}$-subalgebra and the projections $\varphi_i|_T$ are local homomorphisms. Then J_i is also an ideal of finite index in T_i.

Theorem 2.1. *If $\#\mathbf{F}^\times \geq s-1$ and each J_i is principal, then $\#\prod_{i=1}^s T_i/J_i \geq \#T/J$.*

Remark 2.2. Note that the inequality in Theorem 2.1 may be strict. Consider, for example, $T = \{(a,b) \in \mathcal{O} \times \mathcal{O} \mid a \equiv b \pmod{\varpi}\} \subset \mathcal{O} \times \mathcal{O} = A$ with $A_i = \mathcal{O}$ $(i = 1, 2)$. Let $J = \{(\varpi a, \varpi b) \in \mathcal{O} \times \mathcal{O} \mid a, b \in \mathcal{O}\}$ be the maximal ideal of T. Then $T/J \cong T_1/J_1 \cong T_2/J_2 \cong \mathcal{O}/\varpi$. Let us also note that the conclusion of Theorem 2.1 is false if J is only assumed to be an $\mathcal{O}$-submodule of T, but not an ideal. Indeed, let T be as above and $J = \{(a,b) \in \mathcal{O} \times \mathcal{O} \mid a \equiv b \pmod{\varpi^2}\}$. Then $T/J \cong \mathcal{O}/\varpi$, but $T_1/J_1 \cong T_2/J_2 \cong 0$.

As explained in Remark 2.2, the inequality in Theorem 2.1 may be strict; however, this is not the case when J itself is principal. For principal J one not only obtains equality but also the assumption on the residue field is unnecessary. Let us state this as a separate proposition.

Proposition 2.3. *If J is principal, then $\# \prod_{i=1}^{s} T_i/J_i = \#T/J$.*

We prepare the proofs of Theorem 2.1 and Proposition 2.3 by two lemmas and the proposition will follow from these alone, while the proof of the Theorem requires Proposition 2.6 whose proof is more difficult.

If M is any finitely presented $\mathcal{O}$-module, we will write $\mathrm{Fit}_{\mathcal{O}}(M)$ for its Fitting ideal (see e.g., the Appendix of [14] for a treatment of Fitting ideals).

Lemma 2.4. *Let M be an $\mathcal{O}$-module of finite cardinality. Then $\#M = \#\mathcal{O}/\mathrm{Fit}_{\mathcal{O}}(M)$.*

Proof. This is easy. □

Lemma 2.5. *Suppose there exists $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_s) \in J$ such that α_i generates J_i as an ideal of T_i for each $1 \leq i \leq s$. Then $\#T/J \leq \#T/\alpha T = \# \prod_{i=1}^{s} T_i/\alpha_i T_i$.*

Proof. The first inequality is clear. Let $B \in M_n(\mathcal{O})$ be such that $T = B\mathcal{O}^n$. Write $\alpha_i = (\beta_1^i, \beta_2^i, \dots, \beta_{n_i}^i) \in A_i$. Let

$$\mathrm{diag}(\alpha) = \mathrm{diag}(\beta_1^1, \beta_2^1, \dots, \beta_{n_1}^1, \beta_1^2, \beta_2^2, \dots, \beta_{n_2}^2, \dots, \beta_1^s, \beta_2^s, \dots, \beta_{n_s}^s) \in \mathcal{O}^n.$$

Note that $\alpha T = \mathrm{diag}(\alpha) T = \mathrm{diag}(\alpha) B\mathcal{O}^n$. Thus, we have $\mathrm{Fit}_{\mathcal{O}}(\mathcal{O}^n/T) = (\det B)\mathcal{O}$ and $\mathrm{Fit}_{\mathcal{O}}(\mathcal{O}^n/\alpha T) = \det(\mathrm{diag}(\alpha)B)\mathcal{O}$. It follows that

$$\#T/\alpha T = \#\mathcal{O}/\det \mathrm{diag}(\alpha) = \#\mathcal{O}/\left(\prod_{i=1}^{s}\prod_{j=1}^{n_i} \beta_j^i\right).$$

Now let us compute $\#T_1/\alpha_1 T_1$. For a matrix $M \in M_n(\mathcal{O})$ write M_1 for the first n_1 rows of M. Note that $T_1 = B_1\mathcal{O}^n$ and $\alpha_1 T_1 = \mathrm{diag}(\alpha)_1 T_1 = \mathrm{diag}(\alpha)_1 B\mathcal{O}^n$. We have

$$\mathrm{Fit}_{\mathcal{O}}(\mathcal{O}^{n_1}/T_1) = \mathrm{Fit}_{\mathcal{O}}(\mathcal{O}^{n_1}/B_1\mathcal{O}^n) \text{ and } \mathrm{Fit}_{\mathcal{O}}(\mathcal{O}^{n_1}/J_1) = \mathrm{Fit}_{\mathcal{O}}(\mathcal{O}^{n_1}/\,\mathrm{diag}(\alpha)_1 B\mathcal{O}^n).$$

Note that every entry in any row (say jth row) of $\mathrm{diag}(\alpha)_1 B$ equals the corresponding entry in the jth row of B_1 times β_j^1. Thus the determinant of every $n_1 \times n_1$ minor of $\mathrm{diag}(\alpha)_1 B$ equals the determinant of the corresponding minor of B_1 times $\prod_{j=1}^{n_1} \beta_j^1$. Hence by the definition of the Fitting ideals we get

$$\mathrm{Fit}_{\mathcal{O}}(\mathcal{O}^{n_1}/J_1) = \left(\prod_{j=1}^{n_1} \beta_j^1\right) \mathrm{Fit}_{\mathcal{O}}(\mathcal{O}^{n_1}/T_1).$$

Thus we conclude that $\#T_1/\alpha_1 T_1 = \#\mathcal{O}/\prod_{j=1}^{n_1} \beta_j^1$. Analogous argument works for all $1 < i \leq s$. □

Proof of Proposition 2.3. Take α in Lemma 2.5 to be a generator of J. □

For the remainder of the section assume that each J_i is principal. Let α_i be any generator of J_i. Note that α_1 is not a zero divisor in T_1 since it is of the form $(a_1, \dots, a_{n_1})$ with $a_i \in \mathcal{O}$. If α_1 were to be a zero-divisor, one of the a_i must be zero, but then J_1 is not of finite index. Also α_i is not a zero-divisor in T_i for $i > 1$.

Proposition 2.6. *Assume that* $\#\mathbf{F}^\times \geq s-1$. *There exists* $\alpha_i \in J_i$ *such that* $(\alpha_1, \dots, \alpha_s) \in J$ *and each* α_i *generates* J_i.

Before we prove Proposition 2.6, let us show how it implies Theorem 2.1 as well as provides a converse to Proposition 2.3 under the assumption that $\#\mathbf{F} \geq s-1$.

Proof of Theorem 2.1. Let $\alpha := (\alpha_1, \dots, \alpha_s) \in J$ be as in Proposition 2.6. Then α satisfies the assumptions of Lemma 2.5 and we conclude that $\#T/J \leq \# \prod_{i=1}^s T_i/J_i$ as claimed. □

Corollary 2.7. *Assume that* $\#\mathbf{F}^\times \geq s-1$. *Then the ideal* J *is principal if and only if* $\# \prod_{i=1}^s T_i/J_i = \#T/J$.

Proof. The fact that principality of J implies equality of the orders follows directly from Proposition 2.3. Conversely, if J is not principal, then for any α as in Lemma 2.5 (which exists by Proposition 2.6) one has $\#T/J < \#T/\alpha T$, hence it follows from Lemma 2.5 that equality cannot hold. □

Proof of Proposition 2.6. We proceed by induction on s. The case $s=1$ is clear. Assume that the statement is true for $s = n \geq 1$. Let $s = n+1$. Let T' (resp. J') be the image of T (resp. J) under the projection $A \twoheadrightarrow \prod_{i=1}^n T_i$. Then by the inductive hypothesis we know there exists $(\alpha_1, \dots, \alpha_n) \in J'$ such that each α_i generates J_i. Since J' is exactly the image of J we know that there exists $x \in J_{n+1}$ such that $(\alpha_1, \dots, \alpha_n, x) \in J$. By symmetry the inductive hypothesis also gives an element $(x', \beta_2, \dots, \beta_{n+1}) \in J$ such that each β_i generates J_i.

There exists $z_{n+1} \in T_{n+1}$ such that $x = z_{n+1}\beta_{n+1}$. Lift z_{n+1} to $(z_1, \dots, z_{n+1}) \in T$ and consider the difference:

$$(\alpha_1, \alpha_2, \dots, x) - (z_1, z_2, \dots, z_{n+1})(x', \beta_2, \dots, \beta_{n+1})$$
$$= (\alpha_1 - z_1 x', \alpha_2 - z_2\beta_2, \dots, \alpha_n - z_n\beta_n, 0).$$

There exists $u_1 \in T_1$ and (if $n > 1$) $u_i, u_i' \in T_i$ $(i = 2, 3, \dots, n)$ such that

$$\alpha_1 - z_1 x' = u_1\alpha_1 \quad \text{and} \quad \alpha_i - z_i\beta_i = u_i\alpha_i = u_i'\beta_i, \;\; i = 2, 3, \dots, n.$$

This gives us

$$z_1 x' = (1-u_1)\alpha_1 \quad \text{and} \quad z_i\beta_i = (1-u_i)\alpha_i \quad \text{and} \quad \alpha_i = (u_i' + z_i)\beta_i, \;\; i = 2, 3, \dots, n.$$

First let us assume that $n > 1$ and consider the last set of equations first. It implies that $u_i' + z_i \in T_i^\times$ $(i = 2, 3, \dots, n)$. This means either u_i' or z_i is a unit. If for any $i = 2, 3, \dots, n$ one has $z_i \in T_i^\times$, then $(z_1, z_2, \dots, z_{n+1}) \in T^\times$, because a non-unit cannot map to a unit under a local homomorphism. But then we get that $z_{n+1} \in T_{n+1}^\times$ and hence, x generates J_{n+1}, so $(\alpha_1, \alpha_2, \dots, \alpha_n, x) \in J$ has the property that all the coordinates generate the corresponding J_i and this concludes the inductive step in this case.

If $z_i \notin T_i^\times$ for any $i = 2, 3, \dots, n$, then $u_i' \in T_i^\times$ for all $i = 2, 3, \dots, n$. Then $\alpha_i - z_i\beta_i$ generates J_i for all $i = 2, 3 \dots, n$.

Now, let us come back to the general case $n \geq 1$. First assume that $u_1 \in \mathfrak{m}_{T_1}$. Since T_1 is local and complete, this implies that $1 - u_1 \in T_1^\times$ (cf. [8], Proposition 7.10). Moreover, $x' \in J_1$, so there exists $z \in T_1$ such that $x' = z\alpha_1$. So, we have

$$z_1 z\alpha_1 = z_1 x' = (1-u_1)\alpha_1.$$

Since α_1 is a generator of J_1, we know it is a non-zero divisor, so we can cancel it and get

$$z_1 z = 1 - u_1 \in T_1^\times.$$

Thus both $z_1 \in T_1^\times$ and $z \in T_1^\times$. This implies that $J_1 = \alpha_1 T_1 = x' T_1$ (i.e., x' also generates J_1). Therefore $(x', \beta_2, \dots, \beta_{n+1}) \in J$ has the property that each coordinate generates the respective ideal (this concludes the inductive step in this case). Now assume that $u_1 \in T_1^\times$. Then $\alpha_1 - z_1 x'$ also generates J_1.

This shows that either we have an element that satisfies the hypothesis of Proposition 2.6 or we have one consisting of generators of the ideals J_i for $i \leq n$ on the first n coordinates and zero on the last one. By symmetry, we have proved the following lemma.

Lemma 2.8. *Either there exists* $(\alpha_1, \dots, \alpha_{n+1}) \in J$ *such that* $\alpha_i T_i = J_i$ *for all* i *or there exist elements*

$$a_1 := (0, \alpha_2^1, \dots, \alpha_{n+1}^1), a_2 := (\alpha_1^2, 0, \dots, \alpha_{n+1}^2), \dots, a_{n+1} := (\alpha_1^{n+1}, \alpha_2^{n+1}, \dots, 0) \in J$$

such that $\alpha_i^j T_i = J_i$ *for all* $i \neq j$.

Assume that there is no element $(\alpha_1, \dots, \alpha_{n+1}) \in J$ such that $\alpha_i T_i = J_i$ for all i. Then by Lemma 2.8, we get the elements described in the second part of the lemma. If $n = 1$, then $a_1 + a_2 \in J$ and each of its coordinates generates the corresponding J_i. This completes the inductive step in this case.

Now assume that $n > 1$. For every $2 \leq i \leq n$ consider the set $\Sigma_i = \{\alpha_i^1 + u\alpha_i^{n+1}\}$, where $u \in \mathcal{O}^\times$ runs over the set of representatives S of $\mathbf{F}^\times$. We claim that there exist at least $\#\mathbf{F}^\times - 1$ elements of Σ_i such that each of them generates J_i. Indeed, suppose that there exist $a, b \in S$ such that $\alpha_i^1 + a\alpha_i^{n+1} = \nu_1$ and $\alpha_i^1 + b\alpha_i^{n+1} = \nu_2$ and both ν_1 and ν_2 do not generate J_i. Then since $\nu_1 - \nu_2$ also does not generate J_i, we get that $(a - b)\alpha_i^{n+1}$ does not generate J_i. However since α_i^{n+1} generates J_i, we must have that $\varpi \mid (a - b)$, hence $a = b$.

We conclude that there are at least $\#\mathbf{F}^\times - (n-1)$ elements $u \in S$ such that the element $a_1 + u a_{n+1} \in J$ and each of its $n+1$ coordinates generates the corresponding J_i. This contradicts the assumption that no such element exists and concludes the inductive step in this last case. □

3. Eisenstein congruences among elliptic modular forms

We note the following application to Eisenstein congruences for elliptic modular forms: let $f_1, \dots, f_r$ be all weight 2 normalized simultaneous cuspidal eigenforms for $\Gamma_0(N)$ for N prime. Mazur proved in [13] Proposition 5.12(iii) that if p divides the numerator of $\frac{N-1}{12}$ then at least one of these forms is congruent modulo p to the Eisenstein series $E_2^* = 1 - N + 24\sum_{n+1}^{\infty} \sigma^*(n) q^n$ for

$$\sigma^*(n) = \sum_{0<d|n,(d,N)=1} d.$$

Note that $T_N E_2^* = E_2^*$ for the Hecke operator T_N.

From now on for the rest of the paper fix an embedding $\overline{\mathbf{Q}}_p \hookrightarrow \mathbf{C}$. For $1 \leq i \leq r$ write K_{f_i} for the (finite) extension of $\mathbf{Q}_p$ generated by the Hecke eigenvalues of f_i. Let $\mathcal{O}_N$ be the ring of integers in the compositum of all the coefficient fields K_{f_i} and write ϖ_N for a choice of uniformizer, e_N for the ramification index of $\mathcal{O}_N$ over $\mathbf{Z}_p$ and d_N for the degree of its residue field over $\mathbf{F}_p$. We have the following result regarding the exponents of the Eisenstein congruences modulo powers of ϖ_N:

Proposition 3.1. *For $i = 1, \dots, r$ let $\varpi_N^{m_i}$ be the highest power of ϖ_N such that the Hecke eigenvalues of f_i are congruent to those of E_2^* modulo $\varpi_N^{m_i}$ for Hecke operators T_ℓ for all primes $\ell \nmid N$. Then $\frac{1}{e_N}(m_1 + \cdots + m_r)$ is equal to the p-valuation of the numerator of $\frac{N-1}{12}$.*

Proof. Denote by $S_2(N)$ the $\mathbf{C}$-space of cusp forms of weight 2 and level $\Gamma_0(N)$. For any subring $R \subset \mathbf{C}$ write $\mathbf{T}_R$ for the R-subalgebra of $\mathrm{End}_{\mathbf{C}}(S_2(N))$ generated by the Hecke operators T_ℓ for all primes $\ell \nmid N$. Let J_R be the Eisenstein ideal, i.e., the ideal of $\mathbf{T}_R$ generated by $T_\ell - (1+\ell)$ for $\ell \nmid N$. For a prime ideal $\mathfrak{n}$ of $\mathbf{T}_R$ write $\mathbf{T}_{R,\mathfrak{n}}$ for the localization of $\mathbf{T}_R$ at $\mathfrak{n}$ and set $J_{R,\mathfrak{n}} := J_R \mathbf{T}_{R,\mathfrak{n}}$.

Note that it follows from the definition of J_R that the R-algebra structure map $R \to \mathbf{T}_R/J_R$ is surjective. Hence, if R is a local ring with maximal ideal $\mathfrak{m}_R$, then the ideal $J_R + \mathfrak{m}_R \mathbf{T}_R$ is the unique maximal ideal of $\mathbf{T}_R$ containing J_R. To ease notation in the proof write $\mathcal{O}$ for $\mathcal{O}_N$ and ϖ for ϖ_N. Let $\mathfrak{m}$ be the unique maximal ideal of $\mathbf{T}_{\mathcal{O}}$ containing $J_{\mathcal{O}}$. Renumber f_i's if necessary so that $m_i > 0$ for $0 < i \leq s \leq r$ and $m_i = 0$ for $s < i \leq r$. Note that one has $\mathbf{T}_{\mathcal{O}}/J_{\mathcal{O}} \cong \mathbf{T}_{\mathcal{O},\mathfrak{m}}/J_{\mathcal{O},\mathfrak{m}}$.

By Theorem II.18.10 in [13], the ideal J is principal, hence we apply Proposition 2.3 with $T = \mathbf{T}_{\mathcal{O},\mathfrak{m}}$ and let $T_i = \mathcal{O}$ (i.e., we take $n_1 = n_2 = \cdots = n_s = 1$ with n_i's as in Section 2) and $\varphi_i : T \to T_i$ the map sending a Hecke operator to its eigenvalue corresponding to f_i. Set $\mathfrak{m}_{\mathbf{Z}_p} = \mathfrak{m} \cap \mathbf{Z}_p$. One has $\mathbf{T}_{\mathcal{O},\mathfrak{m}_{\mathcal{O}}} = \mathbf{T}_{\mathbf{Z}_p,\mathfrak{m}_{\mathbf{Z}_p}} \otimes_{\mathbf{Z}_p} \mathcal{O}$ ([6], Lemma 3.27 and Proposition 4.7) and $J_{\mathcal{O},\mathfrak{m}} = J_{\mathbf{Z}_p,\mathfrak{m}_{\mathbf{Z}_p}} \otimes_{\mathbf{Z}_p} \mathcal{O}$, hence,

$$\mathbf{T}_{\mathcal{O},\mathfrak{m}}/J_{\mathcal{O},\mathfrak{m}} \cong \frac{\mathbf{T}_{\mathbf{Z}_p,\mathfrak{m}_{\mathbf{Z}_p}} \otimes_{\mathbf{Z}_p} \mathcal{O}}{J_{\mathbf{Z}_p,\mathfrak{m}_{\mathbf{Z}_p}} \otimes_{\mathbf{Z}_p} \mathcal{O}} \cong (\mathbf{T}_{\mathbf{Z}_p,\mathfrak{m}_{\mathbf{Z}_p}}/J_{\mathbf{Z}_p,\mathfrak{m}_{\mathbf{Z}_p}}) \otimes_{\mathbf{Z}_p} \mathcal{O}.$$

We have

$$\mathrm{val}_p(\# T_i/J_i) = \mathrm{val}_p\left(\# \mathcal{O}/\varpi^{m_i}\mathcal{O}\right) = m_i d_N = m_i \frac{[\mathcal{O} : \mathbf{Z}_p]}{e_N}.$$

On the other hand,

$$\mathrm{val}_p(\# T/J) = \mathrm{val}_p\left(\# \frac{\mathbf{T}_{\mathbf{Z}_p,\mathfrak{m}_{\mathbf{Z}_p}}}{J_{\mathbf{Z}_p,\mathfrak{m}_{\mathbf{Z}_p}}} \otimes_{\mathbf{Z}_p} \mathcal{O}\right) = [\mathcal{O} : \mathbf{Z}_p]\, \mathrm{val}_p\left(\# \frac{\mathbf{T}_{\mathbf{Z}_p,\mathfrak{m}_{\mathbf{Z}_p}}}{J_{\mathbf{Z}_p,\mathfrak{m}_{\mathbf{Z}_p}}}\right).$$

By [13] Proposition II.9.7 we know that $\mathrm{val}_p\left(\# \frac{\mathbf{T}_{\mathbf{Z}_p,\mathfrak{m}_{\mathbf{Z}_p}}}{J_{\mathbf{Z}_p,\mathfrak{m}_{\mathbf{Z}_p}}}\right)$ equals the p-adic valuation of the numerator of $\frac{N-1}{12}$. [Indeed, note that while Mazur's Hecke algebra includes the operator T_N and ours does not, it makes no difference since $T_N = 1$ in $\mathbf{T}_{\mathbf{Z}_p,\mathfrak{m}_{\mathbf{Z}_p}}$. This was observed by Calegari and Emerton — see Proposition 3.19 of [5] — and in fact follows from Proposition II.17.10 of [13].] This implies that the p-valuation of the order of T/J is given by the p-valuation of the numerator of $\frac{N-1}{12}$ times $[\mathcal{O} : \mathbf{Z}_p]$. By Proposition 2.3 we have $\mathrm{val}_p(\#T/J) = \sum_{i=1}^{s} \mathrm{val}_p(T_i/J_i)$, hence the Proposition follows. □

Remark 3.2.

(1) A very similar statement to that of the proposition was posed as Question 4.1 in [17]. One of the consequences of Proposition 3.1 is an affirmative answer to that question.
(2) Recently, such higher Eisenstein congruences were also investigated numerically by Naskręcki [15] (but demanding congruence of all the Hecke eigenvalues). He proves an upper bound for the exponent of the congruence for particular cuspforms and conjectures a stronger one in the case that the coefficient field is ramified. We note that as opposed to Naskręcki our set $f_1, \dots, f_r$ includes all cuspidal eigenforms and not just representatives of distinct Galois conjugacy classes.

Example 3.3. A particular example that illustrates the statement of Proposition 3.1 can be taken from Section 19 of [13]: Let $p = 2$ and $N = 113$. Mazur states that in this case $\mathrm{val}_p\left(\#\frac{\mathbf{T}_{\mathbf{Z}_p,\mathfrak{m}_{\mathbf{Z}_p}}}{J_{\mathbf{Z}_p,\mathfrak{m}_{\mathbf{Z}_p}}}\right)$=2 and $\mathrm{rank}_{\mathbf{Z}_p}(\mathbf{T}_{\mathbf{Z}_p,\mathfrak{m}_{\mathbf{Z}_p}}) = 3$.

One checks that there is one cuspform defined over $\mathbf{Z}_p$ congruent to the Eisenstein series modulo p and that over a ramified quadratic extension of $\mathbf{Z}_p$ there are two additional Galois conjugate cuspforms congruent to the Eisenstein series modulo a uniformizer of that extension. Using the notation of Proposition 3.1 we therefore have $e_{113} = 2, m_1 = 2, m_2 = m_3 = 1$, and indeed $\frac{1}{2}(2+1+1) = 2 = \mathrm{val}_p \frac{113-1}{12}$.

Example 3.4. Other examples can be taken from [15]. In particular, in Table 6 of [loc.cit.] Naskręcki considers the following example: let $p = 5$ and $N = 31$. In this case, there are two Galois conjugate cuspforms over a ramified extension of degree 2, and $m_1 = m_2 = 1$, so that $\frac{1}{2}(1+1) = 1 = \mathrm{val}_p \frac{31-1}{12}$. In Section 5.7, he also considers an example with $p = 5$ and $N = 401$. In this case, there is only one Galois conjugacy class of newforms (containing two forms f_1, f_2) congruent to the Eisenstein series whose Fourier coefficients generate an order in the ring of integers of $K_{f_1}K_{f_2}$. In this case $e_{401} = 1$, and $m_1 = m_2 = 1$. So one has $1 + 1 = 2 = \mathrm{val}_p \frac{401-1}{12}$.

4. Congruences - the general case

The results of Section 2 can be applied in the context of congruences among automorphic forms on a general reductive group whenever there is a p-integral structure on the Hecke algebra. It is also worth noting that in many situations one does not know or even does not expect the ideal J to be principal. In this section, we introduce a general framework of working with such congruences and prove an analogue of Proposition 3.1 (Proposition 4.3) which uses Theorem 2.1 instead of Proposition 2.3.

Let p be a prime as before. Let E be a finite extension of $\mathbf{Q}_p$. Write $\mathcal{O}$ for its valuation ring and ϖ for a choice of a uniformizer. Let e be the ramification index of $\mathcal{O}$ over $\mathbf{Z}_p$ and set $d := [\mathcal{O}/\varpi\mathcal{O} : \mathbf{F}_p]$. Let $\mathcal{S}_0$ be a (finite-dimensional) $\mathbf{C}$-space whose elements are modular forms (or more generally automorphic forms for a reductive algebraic group). We assume that there is some naturally defined $\mathcal{O}$-lattice $\mathcal{S}_{0,\mathcal{O}}$ inside $\mathcal{S}_0$. Such a lattice may consist, for example, of forms with Fourier coefficients in $\mathcal{O}$ or of images of cohomology classes with coefficients in $\mathcal{O}$ under an Eichler–Shimura-type isomorphism.

Let $\mathbf{T}_0 \subset \mathrm{End}_{\mathcal{O}} \mathcal{S}_{0,\mathcal{O}}$ be a commutative $\mathcal{O}$-subalgebra of endomorphisms which can be simultaneously diagonalized over E. Write Π_0 for the set of systems of eigenvalues of $\mathbf{T}_0$, that is for the set of $\mathcal{O}$-algebra homomorphisms $\lambda : \mathbf{T}_0 \twoheadrightarrow \mathcal{O}$. Then we can identify $\mathbf{T}_0$ with an $\mathcal{O}$-subalgebra of $\mathcal{O}^{\#\Pi_0}$ of finite index in a natural way.

Let λ_0 be a fixed element of Π_0. Set $\Pi := \Pi_0 \setminus \{\lambda_0\}$. Let $\mathbf{T}$ be the image of $\mathbf{T}_0$ under the projection $\varphi_0 : \prod_{\lambda\in\Pi_0} \mathcal{O} \twoheadrightarrow \prod_{\lambda\in\Pi} \mathcal{O}$. If necessary we extend E further so that $\#(\mathcal{O}/\varpi\mathcal{O})^\times \geq \#\Pi - 1$. Let $\pi_0 \in \mathcal{S}_{0,\mathcal{O}}$ be an eigenform corresponding to λ_0, i.e., such that $T\pi_0 = \lambda_0(T)\pi_0$ for every $T \in \mathbf{T}_0$. Let $J \subset \mathbf{T}$ be the ideal $\varphi_0(\mathrm{Ann}_{\mathbf{T}_0} \pi_0)$.

Remark 4.1. Note that the quotient $\mathbf{T}/J$ is finite. Indeed, for every $\lambda \neq \lambda_0$ there is $T_\lambda \in J$ such that $\lambda(T_\lambda) \neq 0$. Since $\lambda(\mathbf{T}) \cong \mathcal{O}$, we conclude that $\#\lambda(\mathbf{T})/\lambda(J) < \infty$. Note that it follows from the definition of J that the structure map $\iota : \mathcal{O} \to \mathbf{T}/J$ is surjective. Hence if $\mathbf{T}/J$ is infinite, ι must be an isomorphism. However, the (finitely many) maps $\lambda \in \Pi$ account for all $\mathcal{O}$-algebra maps from $\mathbf{T}$ to $\mathcal{O}$. Hence there must exist $\lambda \neq \lambda_0$ such that λ factors through $\mathbf{T}/J$ which implies that $\lambda(J) = 0$. This contradicts finiteness of $\lambda(\mathbf{T})/\lambda(J)$.

Remark 4.2. The quotient $\mathbf{T}/J$ measures p-adic congruences between Hecke eigenvalues of an eigenform corresponding to λ_0 and automorphic eigenforms corresponding to $\lambda \in \Pi$. It can be interpreted in terms of the congruence module $C(\mathbf{T}_0)$ as defined in [9], Section 1. Indeed, the Hecke algebra $\mathbf{T}_0$ decomposes over E as $\mathbf{T}_0 \otimes_{\mathcal{O}} E = X \oplus Y$ with $X = \lambda_0(\mathbf{T}_0) \otimes_{\mathcal{O}} E = E$ and $Y = \varphi_0(\mathbf{T}_0) \otimes_{\mathcal{O}} E = \mathbf{T} \otimes_{\mathcal{O}} E$. If we denote the corresponding projections as π_X and π_Y and set $\mathbf{T}^X := \pi_X(\mathbf{T}_0) = \mathcal{O}$, $\mathbf{T}^Y = \pi_Y(\mathbf{T}_0) = \mathbf{T}$, $\mathbf{T}_X := \mathbf{T}_0 \cap X$ and $\mathbf{T}_Y = \mathbf{T}_0 \cap Y = J$ then the congruence module $C(\mathbf{T}_0)$ is defined as $\frac{\mathbf{T}^X \oplus \mathbf{T}^Y}{\mathbf{T}}$. By Lemma 1 in [loc.cit.] we further know that $\mathbf{T}/J = \mathbf{T}^Y/\mathbf{T}_Y$ is isomorphic to $C(\mathbf{T}_0)$.

Proposition 4.3. *For every $\lambda \in \Pi$ write m_λ for the largest integer such that $\lambda_0(T) \equiv \lambda(T)$ mod ϖ^{m_λ} for all $T \in \mathbf{T}_0$. Then*

$$\frac{1}{e} \cdot \sum_{\lambda\in\Pi} m_\lambda \geq \mathrm{val}_p(\#\mathbf{T}/J). \tag{4.1}$$

The inequality (4.1) becomes an equality if and only if J is principal.

Proof. By our assumption on E the residue field condition in Theorem 2.1 is satisfied. Recall that the structure map $\mathcal{O} \to \mathbf{T}/J$ is surjective. Hence as in the proof of Proposition 3.1 it follows that there exists a unique maximal ideal $\mathfrak{m} \subset \mathbf{T}$ containing J. Write $\mathbf{T}_\mathfrak{m}$ for the localization of $\mathbf{T}$ at $\mathfrak{m}$. Number the elements of Π as $\lambda_1, \lambda_2, \dots, \lambda_r$. By renumbering the λ_is, we may assume that for $i = 1, 2, \dots, s \leq r$ the map $\lambda_i : \mathbf{T} \twoheadrightarrow \mathcal{O}$ factors through $\mathbf{T}_\mathfrak{m}$. Then $m_{\lambda_i} = 0$ for $s < i \leq r$. Now the Proposition follows from Theorem 2.1 (or Corollary 2.7 if J is principal) upon taking $T = \mathbf{T}_{\mathfrak{m}}$, $T_i = \mathcal{O}$, $i = 1, 2, \ldots, s$ (i.e, by taking $n_1 = n_2 = \cdots = n_s = 1$ in Section 2), $\varphi_i = \lambda_i : T \twoheadrightarrow T_i$. □

5. Further examples of applications to congruences between automorphic forms

In this section, we will present a few examples where our general result can be applied. We will use notation introduced in Section 4.

Example 5.1 (More general Eisenstein congruences)**.** Let p be an odd prime and χ a Dirichlet character of order prime to p. Let the conductor of χ be Np^r with $(N,p) = 1$ (so $r = 0$ or 1). For each integer $k \geq 2$ such that $\chi(-1) = (-1)^k$ let $S_k(Np, \chi)$ be the space of cuspforms of weight k, level Np and character χ. Let $\mathcal{S}_0$ be the complex vector space of modular forms $S_k(Np, \chi) \oplus \mathbf{C}\mathrm{E}_\chi$, where $E_\chi \in M_k(Np, \chi)$ is one of the Eisenstein series with Hecke eigenvalues $1 + \chi(\ell)\ell^{k-1}$ for $\ell \nmid Np$.

Let $\mathbf{T}_0$ be the $\mathcal{O}$-subalgebra of endomorphisms of $S_k(Np, \chi) \oplus \mathbf{C}\mathrm{E}_\chi$ generated by the classical Hecke operators T_ℓ for $\ell \nmid Np$. Write λ_0 for the Hecke eigenvalue character corresponding to E_χ. Then J is given by the Eisenstein ideal generated by $T_\ell - 1 - \chi(\ell)\ell^{k-1}$ for $\ell \nmid Np$ in the cuspidal Hecke algebra $\mathbf{T}$.

One expects that the order of the congruence module $\mathbf{T}/J$ is bounded from below by the order of the quotient $\mathcal{O}/L(\chi, 1-k)$, where $L(\chi, s)$ is the usual Dirichlet L-series attached to χ (case $k = 2$ is proven in Proposition 5.1 of [16], certain cases are implicit in e.g. [14, 19], general case is treated in an unpublished work of Skinner). Assuming this bound we can apply Proposition 4.3 to conclude that

$$\frac{1}{e} \cdot \sum_{\lambda \in \Pi} m_\lambda \geq \mathrm{val}_p(\#\mathcal{O}/L(\chi, 1-k)).$$

Remark 5.2. A similar result on higher Eisenstein congruences can also be proven for modular forms over imaginary quadratic fields. In this case, one also does not generally have principality of J, so Proposition 2.3 cannot be used and one only gets the inequality from Theorem 2.1. For details we refer the reader to the upcoming work of the first two authors [2].

Example 5.3 (Congruence primes for primitive forms)**.** Let $k \geq 2, N \geq 1$ be integers and write $\mathcal{S}$ for the $\mathbf{C}$-space of elliptic modular forms of weight 2 and level N. Let $p \geq 5$ be a prime. Let $f \in \mathcal{S}$ be a *primitive* form, i.e., an eigenform for the Hecke operators and a newform. Let $f_1, \ldots, f_{r'}$ be eigenforms spanning the subspace of $\mathcal{S}$ orthogonal to f under the Petersson inner product. Let $f_1, \ldots, f_r$ be a maximal subset of the above (after possibly renumbering the f_i's) with the property that no pair of the f_i's shares the same eigenvalues for all Hecke operators away from primes $\ell \mid N$. As in Section 3 we write ϖ_N for a uniformizer of the ring of integers of the compositum of all the coefficient fields, and e_N for the ramification index of $\mathcal{O}_N$ over $\mathbf{Z}_p$. Let $\varpi_N^{m_i}$ be the highest power of ϖ_N such that the Hecke eigenvalues of f are congruent to f_i modulo $\varpi_N^{m_i}$ for Hecke operators T_ℓ for all primes $\ell \nmid N$. Let $\mathbf{T}_0$ (resp. $\mathbf{T}_0^N$) be the $\mathcal{O}$-subalgebra acting on the space $\mathcal{S}_0 = \bigoplus_{i=1}^r \mathbf{C}f_i \oplus \mathbf{C}f$ generated by the Hecke operators T_ℓ for $\ell \nmid N$ (resp. for all ℓ).

Assume now that f is ordinary at p and that the p-adic Galois representation associated to f is residually absolutely irreducible when restricted to the absolute Galois group of $\mathbf{Q}(\sqrt{(-1)^{(p-1)/2}p})$. Under some mild technical assumptions Hida (see e.g., Theorem 5.20 and (Cg2) in [10]) proved that the p-valuation of the order of the congruence module $C(\mathbf{T}_0^N)$ (as defined in Remark 4.2) equals the p-valuation of $\#\mathcal{O}/L^{\rm alg}(1, \mathrm{Ad}(f))$, where $L^{\rm alg}(1, \mathrm{Ad}(f))$ denotes the algebraic part of the value at $s = 1$ of the adjoint L-function attached to f (for details see [10]).

By Proposition 4.3 we can conclude that

$$\frac{1}{e_N} \cdot \sum_{i=1}^{r} m_i \geq \mathrm{val}_p(\#C(\mathbf{T}_0)).$$

If including the operators T_ℓ for primes $\ell \mid N$ does not affect the depth of the congruences, i.e., if $\#C(\mathbf{T}_0) = \#C(\mathbf{T}_0^N)$, we also get

$$\frac{1}{e_N} \cdot \sum_{i=1}^{r} m_i \geq \mathrm{val}_p(\#(\mathcal{O}/L^{\rm alg}(1, \mathrm{Ad}(f)))).$$

Example 5.4 (Congruences to Saito–Kurokawa lifts)**.** Let k be an even positive integer and let $p > k$ as before be a fixed prime. Let $f \in S_{2k-2}(\mathrm{SL}_2(\mathbf{Z}))$ be a newform and write F_f for the Saito–Kurokawa lift of f. Write $\mathcal{S}$ for the $\mathbf{C}$-space of Siegel cusp forms of weight k and full level. Then $F_f \in \mathcal{S}$. Write $\mathcal{S}^{\rm SK} \subset \mathcal{S}$ for the subspace spanned by Saito–Kurokawa lifts. Let $\mathcal{S}_0 = \mathcal{S}_{\rm SK} \oplus \mathbf{C}F_f$, where $\mathcal{S}_{\rm SK}$ is the orthogonal complement of $\mathcal{S}^{\rm SK}$ with respect to the standard Petersson inner product on $\mathcal{S}$. Set $\Sigma = \{p\}$. Let $\mathbf{T}_0$ be the standard Siegel Hecke algebra generated over $\mathcal{O}$ by the Hecke operators (away from p) acting on $\mathcal{S}_0$. Let λ_0 be the Hecke eigencharacter corresponding to F_f. Then $\mathbf{T}$ can be identified with the quotient of $\mathbf{T}_0$ acting on $\mathcal{S}_{\rm SK}$ and $\mathbf{T}/J$ measures congruences between the Hecke eigenvalues corresponding to F_f and those corresponding to Siegel eigenforms which are not Saito–Kurokawa lifts (cf. [3, 4] for details).

From now on assume that f is ordinary at p and that the p-adic Galois representation attached to f is residually absolutely irreducible. It has been shown by Brown ([4], Corollary 5.6) that under some mild assumptions the order of the finite quotient $\mathbf{T}/J$ is bounded from below by the order of the quotient $\mathcal{O}/L^{\rm alg}(k, f)$, where $L^{\rm alg}(k, f)$ denotes the algebraic part of the special value at k of the standard L-function of f (for details see [loc.cit.]). Hence we can apply Proposition 4.3 to conclude that

$$\frac{1}{e} \cdot \sum_{\lambda \in \Pi} m_\lambda \geq \mathrm{val}_p(\#\mathcal{O}/L^{\rm alg}(k, f)). \tag{5.1}$$

Since strong multiplicity one holds for forms in $\mathcal{S}$, the elements of Π are in one-to-one correspondence with eigenforms (up to scalar multiples) in $\mathcal{S}_{\rm SK}$. So, (5.1) tells us that the "depths" m of the (mod ϖ^m) congruences to F_f of the eigenforms in $\mathcal{S}_{\rm SK}$ add up to no less than the ϖ-adic valuation of the standard L-value of f at k.

Remark 5.5. There are several other situations where similar conclusions can be drawn (e.g., in the context of congruences among automorphic forms on the unitary group $U(2,2)$ and the CAP ideal [11, 12] or the Yoshida congruences on Sp_4 [1]). Since the reasoning is verbatim to the examples listed above we leave their formulation to the interested reader.

Acknowledgments

The second and the third author were partially supported by a PSC-CUNY Award, jointly funded by The Professional Staff Congress and The City University of New York. We would like to express special thanks to Gabor Wiese for his comments on the paper and for help with verifying some numerical examples. We would also like to thank Jim Brown for an email correspondence regarding multiplicity one for Saito–Kurokawa lifts.

References

[1] M. Agarwal and K. Klosin, *Yoshida lifts and the Bloch–Kato conjecture for the convolution L-function*, J. Number Theory **133**(8) (2013), 2496–2537.

[2] T. Berger and K. Klosin, *On lifting and modularity of reducible residual Galois representations over imaginary quadratic fields*, preprint (2013). `http://arxiv.org/abs/1103.5100`

[3] J. Brown, *Saito-Kurokawa lifts and applications to the Bloch–Kato conjecture*, Compos. Math. **143**(2) (2007), 290–322.

[4] ———, *On the cuspidality of pullbacks of Siegel Eisenstein series and applications*, Int. Math. Res. Not. IMRN **7** (2011), 1706–1756.

[5] F. Calegari and M. Emerton, *On the ramification of Hecke algebras at Eisenstein primes*, Invent. Math. **160**(1) (2005), 97–144.

[6] H. Darmon, F. Diamond, and R. Taylor, *Fermat's last theorem*, in Elliptic curves, modular forms & Fermat's last theorem (Hong Kong, 1993), 2–140, International Press, Cambridge, MA, 1997.

[7] F. Diamond, *On congruence modules associated to Λ-adic forms*, Compos. Math. **71**(1) (1989), 49–83.

[8] D. Eisenbud, Commutative algebra with a view toward algebraic geometry, Vol. 150 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, 1995.

[9] E. Ghate, *An introduction to congruences between modular forms*, in Currents trends in number theory (Allahabad, 2000), 39–58, Hindustan Book Agency, New Delhi, 2002.

[10] H. Hida, Modular forms and Galois cohomology, Vol. 69 of *Cambridge Studies in Advanced Mathematics*, Cambridge University Press, Cambridge, 2000.

[11] K. Klosin, *Congruences among automorphic forms on* $\mathrm{U}(2,2)$ *and the Bloch–Kato conjecture*, Annales de l'institut Fourier **59**(1) (2009), 81–166.

[12] ———, *Maass spaces on U(2,2) and the Bloch–Kato conjecture for the symmetric square motive of a modular form*, to appear in Journal of the Mathematical Society of Japan . `arXiv:math.NT/0606531`.

[13] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186 (1978).

[14] B. Mazur and A. Wiles, *Class fields of abelian extensions of* $\mathbf{Q}$, Invent. Math. **76**(2) (1984), 179–330.

[15] B. Naskręcki, *On higher congruences between cusp form and Eisenstein series*, in Computations with Modular Forms, Contributions in Mathematical and Computational Sciences, Vol. 6, Springer (2014). `http://arxiv.org/abs/1206.1881`.

[16] C. M. Skinner and A. J. Wiles, *Ordinary representations and modular forms*, Proc. Natl Acad. Sci. USA. **94**(20) (1997), 10520–10527.

[17] X. Taixés i Ventosa and G. Wiese, *Computing congruences of modular forms and Galois representations modulo prime powers*, in Arithmetic, geometry, cryptography and coding theory

2009, Vol. 521 of Contemporary Mathematics, 145–166, Amer. Math. Soc., Providence, RI, 2010. http://arxiv.org/pdf/0909.2724v2.pdf.

[18] A. Wiles, *On ordinary λ-adic representations associated to modular forms*, Invent. Math. **94**(3) (1988), 529–573.

[19] ———, *The Iwasawa conjecture for totally real fields*, Ann. Math. (2) **131**(3) (1990), 493–540.

School of Mathematics and Statistics, University of Sheffield, Hounsfield Road, Hicks Building, Sheffield S3 7RH, UK

E-mail address: tberger@cantab.net

Department of Mathematics, Queens College, City University of New York, 65-30 Kissena Blvd, Queens, NY 11367, USA

E-mail address: kklosin@qc.cuny.edu

Department of Mathematics, Queens College, City University of New York, 65-30 Kissena Blvd, Queens, NY 11367, USA

E-mail address: kenneth.kramer@qc.cuny.edu