# On the ramification of modular parametrizations at the cusps

François Brunault

# ON THE RAMIFICATION OF MODULAR PARAMETRIZATIONS AT THE CUSPS

FRANÇOIS BRUNAULT

Abstract. We investigate the ramification of modular parametrizations of elliptic curves over $\mathbf{Q}$ at the cusps. We prove that if the modular form associated to the elliptic curve has minimal level among its twists by Dirichlet characters, then the modular parametrization is unramified at the cusps. The proof uses Bushnell's formula for the Godement-Jacquet local constant of a cuspidal automorphic representation of GL(2). We also report on numerical computations indicating that in general, the ramification index at a cusp seems to be a divisor of 24.

Résumé. Nous étudions la ramification aux pointes des paramétrisations modulaires des courbes elliptiques sur $\mathbf{Q}$. Nous montrons que si le forme modulaire associée à la courbe elliptique est de niveau minimal parmi ses tordues par les caractères de Dirichlet, alors la paramétrisation modulaire est non ramifiée aux pointes. La preuve utilise la formule de Bushnell pour la constante locale de Godement-Jacquet d'une représentation automorphe supercuspidale de GL(2). Nous présentons également des calculs numériques indiquant qu'en général, l'indice de ramification en une pointe semble être un diviseur de 24.

## 1. Introduction

Let $E/\mathbf{Q}$ be an elliptic curve of conductor $N$. It is known [3] that $E$ admits a *modular parametrization*, in other words a non-constant morphism $\varphi : X_0(N) \to E$ defined over $\mathbf{Q}$. By the Riemann-Hurwitz formula, the morphism $\varphi$ necessarily ramifies as soon as the genus of $X_0(N)$ is at least 2, and we may ask whether its ramification points have interesting properties. In this direction, Mazur and Swinnerton-Dyer discovered a link between the analytic rank of $E$ and the number of ramification points of $\varphi$ on the imaginary axis [11]. Further results and numerical examples were obtained by Delaunay [7].

In this article, we consider the following problem.

**Problem 1.1.** Compute the ramification index $e_\varphi(x)$ of $\varphi$ at a given cusp $x \in X_0(N)$.

2010 *Mathematics Subject Classification.* 11F03, 11F30, 11F70.

*Key words and phrases.* Elliptic curve, Modular parametrization, Ramification index, Automorphic representation, Local constant.

Let $f_E$ be the newform of weight 2 on $\Gamma_0(N)$ associated to $E$. The pull-back $\varphi^*\omega_E$ of a Néron differential $\omega_E$ on $E$ under $\varphi$ is a nonzero multiple of $\omega_{f_E} = 2\pi i f_E(z)dz$. It follows that the ramification index of $\varphi$ at a given point $x \in X_0(N)$ is given by $e_\varphi(x) = 1 + \mathrm{ord}_x\, \omega_{f_E}$. We prove the following result.

**Theorem 1.2.** *Let $E/\mathbf{Q}$ be an elliptic curve such that the newform $f_E$ has minimal level among its twists by Dirichlet characters. Then $\omega_{f_E}$ doesn't vanish at the cusps of $X_0(N)$. In particular, the modular parametrization of $E$ is unramified at the cusps of $X_0(N)$.*

*Remark* 1.3. A newform having minimal level among its twists by Dirichlet characters is said to be *minimal by twist*. It is not true in general that if a newform $f$ of weight 2 on $\Gamma_0(N)$ is minimal by twist, then $\omega_f$ doesn't vanish at the cusps of $\Gamma_0(N)$. For example, there is a newform $f$ of weight 2 on $\Gamma_0(625)$ such that $f$ is minimal by twist and $\omega_f$ vanishes at the cusp $1/25$ (see Remark 6.1).

If $N$ is squarefree, then all newforms of level $N$ are minimal by twist, and in this particular case, Theorem 1.2 follows easily by considering the action of Atkin-Lehner involutions. Thus modular parametrizations of semistable elliptic curves are always unramified at the cusps.

For general $N$, determining the ramification index becomes more intricate and we proceed as follows. In §3 we apply a formula of Merel which expresses the translate of a newform $f$ as a linear combination of twists of $f$ by Dirichlet characters. This enables us in §4 to reduce Theorem 1.2 to a purely local non-vanishing statement. We prove this non-vanishing in §6-7 using Bushnell's formula for the local constant of a cuspidal automorphic representation of $\mathrm{GL}(2)$, together with results of Loeffler and Weinstein on the cuspidal inducing data underlying such representations.

The following side result may be of independent interest. Given a newform $f$ which is minimal by twist, we obtain a rather explicit expression, depending only on the local components of $f$, for the Fourier expansion of $f$ at an arbitrary cusp (see Remark 5.3).

Theorem 1.2 was suggested by numerical computations, which we report in §8. Using Pari/GP [17], we estimated numerically the ramification indices at the cusps, for all elliptic curves of conductor $\leq 2000$. This provided us with a list of 745 elliptic curves (up to isogeny) whose modular parametrization seemed to have at least one ramification point among the cusps. Using Magma [2], we then checked that none of the corresponding modular forms was minimal by twist. In our examples, the ramification index always appears to be a divisor of 24. It seems interesting to find a general formula for this number in terms of $f$.

After I finished this work, I learned of the recent article [13], which provides a nice exact formula for an averaged version of the $n$-th Fourier coefficient with respect to cusps of a given level [13, Prop 3.12]. This

can be used to give an explicit formula for the ramification index of a modular parametrization at a cusp ([13, Remark 3.15],[15]).

In the first version of this work, there was a mistake in the argument of Section 6. I would like to thank the anonymous referee for pointing out this mistake, which led me to find the example alluded to in Remark 1.3. I would also like to thank Christophe Delaunay for helpful comments and Hao Chen for confirming numerically the example of Remark 6.1. Finally, I would like to thank the anonymous referee for valuable improvement suggestions on this work.

## 2. First properties of the ramification index

In this section, we establish basic properties of the ramification index.

**Definition 2.1.** Let $f$ be a newform of weight 2 on $\Gamma_0(N)$, and let $\omega_f = 2\pi i f(z)dz$ be the 1-form associated to $f$. For any point $x \in X_0(N)(\mathbf{C})$, we define the ramification index of $f$ at $x$ by $e_f(x) = 1 + \mathrm{ord}_x(\omega_f)$.

**Lemma 2.2.** *Let $Q$ be a divisor of $N$ such that $(Q, \frac{N}{Q}) = 1$, and let $W_Q$ be the corresponding Atkin-Lehner involution on $X_0(N)$. For every $x \in X_0(N)(\mathbf{C})$, we have $e_f(W_Q(x)) = e_f(x)$.*

*Proof.* We have $\mathrm{ord}_{W_Q(x)}(\omega_f) = \mathrm{ord}_x(W_Q^*\omega_f) = \mathrm{ord}_x(\omega_f)$ since $f$ is an eigenvector of $W_Q$. □

**Lemma 2.3.** *Let $\sigma \in \mathrm{Aut}(\mathbf{C})$ and let $f^\sigma \in S_2(\Gamma_0(N))$ be the newform obtained by applying $\sigma$ to the coefficients of $f$. For every $x \in X_0(N)(\mathbf{C})$, we have $e_f(x) = e_{f^\sigma}(\sigma(x))$.*

*Proof.* This follows as in Lemma 2.2 from $\sigma_*\omega_f = \omega_{f^\sigma}$. □

Recall that the set of cusps of $X_0(N)(\mathbf{C})$ is $\Gamma_0(N)\backslash\mathbf{P}^1(\mathbf{Q})$.

**Definition 2.4.** The *level* of a cusp $x$ of $X_0(N)$ is defined to be $(b, N)$, where $\frac{a}{b} \in \mathbf{P}^1(\mathbf{Q})$ is any representative of $x$ such that $(a, b, N) = 1$.

**Lemma 2.5.** *For any divisor $d$ of $N$, the group $\mathrm{Aut}(\mathbf{C})$ acts transitively on the set of cusps of level $d$ of $X_0(N)$.*

*Proof.* This is a consequence of [16, Thm 1.3.1]. □

The action of $W_Q$ on the cusps can be described as follows.

**Lemma 2.6.** *Let $N = QQ'$ with $(Q, Q') = 1$. Let $d$ be a divisor of $N$. Write $d = d_Q d_{Q'}$ with $d_Q | Q$ and $d_{Q'} | Q'$. Then $W_Q$ maps cusps of level $d$ to cusps of level $\frac{Q}{d_Q} \cdot d_{Q'}$.*

*Proof.* Since $W_Q$ is defined over $\mathbf{Q}$, it suffices to compute the level of the cusp $W_Q(\frac{1}{d})$. Let $u, v$ be two integers such that $Qu - Q'v = 1$. Then $W_Q(\frac{1}{d}) = \begin{pmatrix} Qu & v \\ N & Q \end{pmatrix}(\frac{1}{d}) = \frac{Qu+dv}{N+dQ} = \frac{a}{b}$ with $a = \frac{Q}{d_Q}u + d_{Q'}v$ and $b = \frac{N}{d_Q} + d_{Q'}Q$.

We have $(b, Q) = \frac{Q}{d_Q}$ and $(b, Q') = d_{Q'}$ so that $(b, N) = \frac{Q}{d_Q} \cdot d_{Q'}$. Since $(a, \frac{Q}{d_Q}) = (a, d_{Q'}) = 1$, it follows that $(a, b, N) = 1$, whence the result. □

Let $d$ be a divisor of $N$. By Lemma 2.6, there exists $Q$ such that $W_Q$ maps cusps of level $d$ to cusps of level $\delta = (d, \frac{N}{d})$. Note that $\delta^2 | N$. In view of the previous lemmas, Theorem 1.2 is reduced to showing that if $f$ is minimal by twist, then $e_f(\frac{1}{d}) = 1$ for every $d$ such that $d^2 | N$.

We now make use of the following idea : studying the behaviour of $f$ at $\frac{1}{d}$ amounts to studying the behaviour of $f(z + \frac{1}{d})|W_N$ at infinity. More precisely, define $f_d(z) = f(z + \frac{1}{d})$. A direct computation shows that if $d^2 | N$ then $f_d \in S_2(\Gamma_1(N))$.

From now on, we fix an integer $d \geq 1$ such that $d^2 | N$ and we define $g_d = W_N(f_d) = \sum_{n \geq 1} b_{d,n} q^n \in S_2(\Gamma_1(N))$.

**Proposition 2.7.** *We have* $e_f(\frac{1}{d}) = \min\{n \geq 1 : b_{d,n} \neq 0\}$.

*Proof.* Let $M = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & \frac{1}{d} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix} \in \mathrm{SL}_2(\mathbf{R})$. We have $M(\infty) = \frac{1}{d}$ and $f|M = g_d$. Since $M^{-1}\Gamma_0(N)M \cap \begin{pmatrix} 1 & \mathbf{R} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \mathbf{Z} \\ 0 & 1 \end{pmatrix}$, a uniformizing parameter at $[\frac{1}{d}] \in X_0(N)(\mathbf{C})$ is given by $z \mapsto \exp(2\pi i M^{-1} z)$. It follows that $\mathrm{ord}_{\frac{1}{d}} \omega_f = \mathrm{ord}_\infty \omega_{g_d}$. □

Note that $e_f(1) = e_f(\infty) = 1$. The case $d = 2$ is also easily treated.

**Proposition 2.8.** *If* $4|N$ *then* $e_f(\frac{1}{2}) = 1$.

*Proof.* Since the Fourier expansion of $f$ involves only odd powers of $q$, we have $f(z + \frac{1}{2}) = -f(z)$, so that $e_f(\frac{1}{2}) = e_f(0) = 1$. □

In Sections 3 and 4, we reduce Theorem 1.2 to a purely local question on irreducible cuspidal representations of $\mathrm{GL}_2(\mathbf{Q}_p)$. We use a formula of Merel to express the $n$-th Fourier coefficient of $f$ at a given cusp of $X_0(N)$ as a certain sum of pseudo-eigenvalues of Atkin-Lehner involutions associated to twists of $f$. We then express these pseudo-eigenvalues as products of local epsilon factors. Another way of reducing Theorem 1.2 to a local statement would have been to express the Fourier coefficients of $f$ at a given cusp in terms of the Whittaker newform associated to $f$ as in [13, Section 3.4.2], and to use the formula for the Whittaker newform in [14, Proposition 2.30].

## 3. Merel's formula

In this section, we apply a formula of Merel [12] expressing the additive translate of a newform as a linear combination of certain twists of this newform. The related problem of computing the Fourier expansion of a newform at an arbitrary cusp has also been studied by Delaunay in his PhD thesis [6, III.2]. Although Delaunay's results apply in the

particular case considered here, we prefer to use Merel's formula since it does not assume that the newform is minimal by twist.

Let us first recall the notations of [12]. Let $\phi$ denote Euler's function. For any integer $m \geq 1$, let $\Sigma_m$ be the set of prime factors of $m$. For any Dirichlet character $\chi : (\mathbf{Z}/m\mathbf{Z})^\times \to \mathbf{C}^\times$, the Gauss sum of $\chi$ is $\tau(\chi) = \sum_{a \in (\mathbf{Z}/m\mathbf{Z})^\times} \chi(a) e^{2\pi i a/m}$, and the conductor of $\chi$ is denoted by $m_\chi$. For any newform $F$ of weight $k \geq 2$ on $\Gamma_1(M)$ and for any prime $p$, let $L_p(F, X) = 1 - a_p(F)X + a_{p,p}(F)pX^2 \in \mathbf{C}[X]$ be the inverse of the Euler factor of $F$ at $p$. If $T^+$ and $T^-$ are finite sets of prime numbers, we define

$$F^{[T^+,T^-]} = F|_k \prod_{p \in T^+} L_p(F, p^{-k/2} \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}) \prod_{p \in T^-} L_p(\bar{F}, p^{-k/2} \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}).$$

There exists a unique newform $F \otimes \chi$ of weight $k$ and level dividing $\mathrm{lcm}(M, m^2)$ such that $a_p(F \otimes \chi) = a_p(F)\chi(p)$ for any prime $p \notin \Sigma_{Mm}$.

Using [12, (5)] with $\frac{n}{N} = \frac{1}{d}$, we get

$$f_d = \sum_\chi \frac{\tau(\bar{\chi})}{\phi(d)} (f \otimes \chi)^{[\Sigma_d, \Sigma_d - \Sigma_{m_\chi}]} | \prod_{p \in \Sigma_{d/m_\chi}} P_p(\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}) \tag{1}$$

where $\chi$ runs through the primitive Dirichlet characters of conductor $m_\chi$ dividing $d$, and the polynomial $P_p(X) \in \mathbf{C}[X]$ is given by

$$P_p(X) = \begin{cases} -\bar{\chi}(p) & \text{if } a_p(f) = 0, v_p(d) = 1, v_p(m_\chi) = 0, \\ (a_p(f)X)^{v_p(d/m_\chi)} & \text{otherwise.} \end{cases}$$

Since $a_p(f) = 0$ for $p \in \Sigma_d$, the product over $p$ in (1) vanishes unless $(m_\chi, \frac{d}{m_\chi}) = 1$ and $\frac{d}{m_\chi}$ is squarefree. Let $S'(d)$ be the set of primitive Dirichlet characters $\chi$ such that $m_\chi | d$, $(m_\chi, \frac{d}{m_\chi}) = 1$ and $\frac{d}{m_\chi}$ is squarefree. Taking into account $L_p(f \otimes \chi, X) = 1$ for $p \in \Sigma_{d/m_\chi}$, we get

$$f_d = \sum_{\chi \in S'(d)} \frac{\tau(\bar{\chi})}{\phi(d)} \Big( \prod_{p \in \Sigma_{d/m_\chi}} -\bar{\chi}(p) \Big) \cdot (f \otimes \chi)^{[\Sigma_{m_\chi}, \varnothing]}. \tag{2}$$

*From now on, we assume that $f$ is minimal by twist.* Then $f \otimes \chi$ has level exactly $N$ for every character $\chi$ of conductor dividing $d$, so that $(f \otimes \chi)^{[\Sigma_{m_\chi}, \varnothing]} = f \otimes \chi$ for every $\chi \in S'(d)$.

Let $S(d)$ be the set of Dirichlet characters modulo $d$ induced by the elements of $S'(d)$. If $\chi' \in S'(d)$ induces $\chi \in S(d)$, then

$$\tau(\chi) = \tau(\chi') \cdot \prod_{p \in \Sigma_{d/m_\chi}} -\chi'(p).$$

Thus $f_d$ can finally be rewritten

$$f_d = \sum_{\chi \in S(d)} \frac{\tau(\bar{\chi})}{\phi(d)} \cdot f \otimes \chi. \tag{3}$$

We now apply $W_N$. We have $W_N(f \otimes \chi) = w(f \otimes \chi) \cdot f \otimes \bar{\chi}$, where $w(f \otimes \chi)$ is the pseudo-eigenvalue of $W_N$ at $f \otimes \chi$. It follows that

$$g_d = \sum_{\chi \in S(d)} \frac{\tau(\bar{\chi})}{\phi(d)} \cdot w(f \otimes \chi) \cdot f \otimes \bar{\chi}. \tag{4}$$

In particular, we get

$$b_{d,n} = \frac{a_n(f)}{\phi(d)} \sum_{\chi \in S(d)} \tau(\bar{\chi}) \cdot \bar{\chi}(n) \cdot w(f \otimes \chi) \qquad (n \geq 1). \tag{5}$$

Note that $b_{d,n} = 0$ whenever $(n, d) > 1$, and that the inner sum in (5) depends only on $n \mod d$. If $n = 1$, then (5) simplifies to

$$b_{d,1} = \frac{1}{\phi(d)} \sum_{\chi \in S(d)} \tau(\bar{\chi}) \cdot w(f \otimes \chi). \tag{6}$$

## 4. Reduction to a local computation

In this section, we show that $b_{d,n}$ is a product of local terms depending only on the local automorphic representations associated to $f$, thereby reducing the non-vanishing of $b_{d,n}$ to a local question.

The basic observation is that if $d = p_1^{m_1} \dots p_k^{m_k}$ is the prime factorization of $d$, then we have a natural bijection $S(d) \cong S(p_1^{m_1}) \times \cdots \times S(p_k^{m_k})$. Moreover $S(p)$ (resp. $S(p^m)$ with $m \geq 2$) is the set of Dirichlet characters modulo $p$ (resp. of conductor $p^m$). We will show that the summand in (5) decomposes accordingly as a product of local terms. We shift to the adelic language, which is more convenient for our purposes.

Let $\mathbf{A_Q}$ be the ring of adèles of $\mathbf{Q}$. We view Dirichlet characters as characters of $\mathbf{A_Q^\times}/\mathbf{Q}^\times$ as follows. We attach to $\chi \in S(d)$ the unique (continuous) character $\chi_{\mathbf{A}} : \mathbf{A_Q^\times}/\mathbf{Q}^\times \to \mathbf{C}^\times$ such that for any $p \notin \Sigma_d$, we have $\chi_{\mathbf{A}}(\varpi_p) = \chi(p)$, where $\varpi_p$ denotes a uniformizer of $\mathbf{Q}_p^\times \subset \mathbf{A_Q^\times}$. For any $p \in \Sigma_d$, we denote by $\chi_p : \mathbf{Q}_p^\times \to \mathbf{C}^\times$ the $p$-component of $\chi_{\mathbf{A}}$. Letting $m_p = v_p(d)$, we have $\chi_p(1 + p^{m_p}\mathbf{Z}_p) = 1$. A word of caution is in order here: with the above convention, the map $\mathbf{Z}_p^\times/(1 + p^{m_p}\mathbf{Z}_p) \to \mathbf{C}^\times$ induced by $\chi_p$ is the inverse of the $p$-component of $\chi$.

The level of a non-trivial additive character $\psi : \mathbf{Q}_p \to \mathbf{C}^\times$ is the unique integer $\ell \in \mathbf{Z}$ such that $\ker(\psi) = p^\ell \mathbf{Z}_p$. For any character $\psi : \mathbf{Q}_p \to \mathbf{C}^\times$ of level $m_p = v_p(d)$, we define the local Gauss sum of $\chi \in S(d)$ at $p$ by

$$\tau(\chi_p, \psi) = \sum_{x \in \mathbf{Z}_p^\times/(1+p^{m_p}\mathbf{Z}_p)} \chi_p(x)\psi(x). \tag{7}$$

**Lemma 4.1.** *For any $n \in (\mathbf{Z}/d\mathbf{Z})^\times$, there exist characters $\psi'_p : \mathbf{Q}_p \to \mathbf{C}^\times$ of respective levels $m_p = v_p(d)$ such that*

$$\tau(\bar{\chi}) \cdot \bar{\chi}(n) = \prod_{p \in \Sigma_d} \tau(\chi_p, \psi'_p) \qquad (\chi \in S(d)). \tag{8}$$

*Proof.* Multiplying $\tau(\bar{\chi})$ by $\bar{\chi}(n)$ only amounts to change the additive character in the definition of the Gauss sum of $\bar{\chi}$. The lemma now follows from the Chinese remainder theorem. □

Let $\pi_f$ be the automorphic representation of $\mathrm{GL}_2(\mathbf{A_Q})$ associated to $f$ [10, §2.1]. For any $\chi \in S(d)$, we have a canonical isomorphism $\pi_{f\otimes\chi} \cong \chi\pi_f$, where the latter representation is $g \mapsto \chi_{\mathbf{A}}(\det g)\pi_f(g)$. The $L$-function of $\pi_{f\otimes\chi}$ satisfies a functional equation [9, Thm 11.1]

$$L(\pi_{f\otimes\chi}, s) = \epsilon(\pi_{f\otimes\chi}, s)L(\pi_{f\otimes\bar{\chi}}, 1-s), \tag{9}$$

Fix an additive character $\psi = \prod_v \psi_v : \mathbf{A_Q}/\mathbf{Q} \to \mathbf{C}^\times$ such that $\psi_p$ has level one for every $p \in \Sigma_d$. By [9, §11], we have

$$\epsilon(\pi_{f\otimes\chi}, s) = \prod_v \epsilon(\pi_{f\otimes\chi,v}, s, \psi_v) \tag{10}$$

where $v$ runs through the places of $\mathbf{Q}$, and $\pi_{f\otimes\chi,v} \cong \chi_v\pi_{f,v}$ denotes the local component of $f\otimes\chi$ at $v$. The quantity $\epsilon(\pi_{f\otimes\chi,v}, s, \psi_v)$ is the Godement-Jacquet local constant of $\pi_{f\otimes\chi}$.

For any character $\chi$ of $\mathbf{Q}_p^\times$, we let $\widetilde{\chi}$ be the unique character of $\mathbf{Q}_p^\times$ such that $\widetilde{\chi}(p) = 1$ and $\widetilde{\chi}|_{\mathbf{Z}_p^\times} = \chi|_{\mathbf{Z}_p^\times}$. The following proposition shows that $w(f\otimes\chi)$ can be written as a product of local constants.

**Proposition 4.2.** *There exist a constant $C \in \mathbf{C}^\times$ and an element $a \in (\mathbf{Z}/d\mathbf{Z})^\times$, depending on $f$ and $\psi$ but not on $\chi$, such that*

$$w(f\otimes\chi) = C\cdot\chi(a)\prod_{p\in\Sigma_d}\epsilon(\widetilde{\chi}_p\pi_{f,p}, \frac{1}{2}, \psi_p) \qquad (\chi \in S(d)). \tag{11}$$

*Proof.* Let $L(f\otimes\chi, s)$ be the usual $L$-function of $f\otimes\chi$. It relates to the automorphic $L$-function by $L(\pi_{f\otimes\chi}, s-\frac{1}{2}) = (2\pi)^{-s}\Gamma(s)L(f\otimes\chi, s)$. Comparing (9) with the usual functional equation yields

$$w(f\otimes\chi) = -N^{s-\frac{1}{2}}\epsilon(\pi_{f\otimes\chi}, s). \tag{12}$$

By [8, Prop 5.21, Thm 6.16], we have $\epsilon(\pi_{f\otimes\chi,\infty}, s, \psi_\infty) = -1$, so we get

$$w(f\otimes\chi) = \prod_{p\in\Sigma_N}\epsilon(\pi_{f\otimes\chi,p}, \frac{1}{2}, \psi_p) = \prod_{p\in\Sigma_N}\epsilon(\chi_p\pi_{f,p}, \frac{1}{2}, \psi_p). \tag{13}$$

It follows from the definition of the epsilon factor [5, §24.2] that there exists an integer $b_p \in \mathbf{Z}$ not depending on $\chi_p$ such that for every unramified character $\omega_p : \mathbf{Q}_p^\times \to \mathbf{C}^\times$, we have

$$\epsilon(\omega_p\chi_p\pi_{f,p}, s, \psi_p) = \omega_p(p^{b_p})\epsilon(\chi_p\pi_{f,p}, s, \psi_p). \tag{14}$$

Choosing $\omega_p$ such that $\omega_p\chi_p = \widetilde{\chi}_p$, and noting that

$$\prod_{p\in\Sigma_N}\bar{\omega}_p(p^{b_p}) = \prod_{p\in\Sigma_N}\chi_p(p^{b_p})$$

may be written $\chi(a)$ with $a \in (\mathbf{Z}/d\mathbf{Z})^\times$ not depending on $\chi$, we get the result by taking $C = \prod_{p\in\Sigma_N-\Sigma_d}\epsilon(\pi_{f,p}, \frac{1}{2}, \psi_p)$. □

The map $\chi \mapsto (\widetilde{\chi}_p)_{p\in\Sigma_d}$ provides a bijection $S(d) \cong \prod_{p\in\Sigma_d} \widetilde{S}(p^{m_p})$, where $\widetilde{S}(p^m)$ is the set of characters $\omega : \mathbf{Q}_p^\times \to \mathbf{C}^\times$ such that $\omega(p) = 1$, $\omega(1+p^m\mathbf{Z}_p) = 1$, and $\omega(1+p^{m-1}\mathbf{Z}_p) \neq 1$ if $m \geq 2$. Putting together the formulas (5), (8) and (11), we get

$$b_{d,n} = \frac{C}{\phi(d)} \cdot a_n(f) \prod_{p\in\Sigma_d} \sum_{\chi_p \in \widetilde{S}(p^{m_p})} \tau(\chi_p, \psi_p') \cdot \epsilon(\chi_p \pi_{f,p}, \frac{1}{2}, \psi_p) \tag{15}$$

for some characters $\psi_p' : \mathbf{Q}_p \to \mathbf{C}^\times$ of respective levels $m_p = v_p(d)$.

Let $E$ be an elliptic curve over $\mathbf{Q}$ of conductor $N$. Assume that the newform $f_E$ associated to $E$ is minimal by twist. For any prime $p$ such that $p^2|N$, the local component $\pi_{f_E,p}$ is an irreducible cuspidal representation of $\mathrm{GL}_2(\mathbf{Q}_p)$ by [10, Prop. 2.8]. Theorem 1.2 is thus reduced to the following purely local statement.

**Theorem 4.3.** *Let $\pi$ be an irreducible cuspidal representation of $\mathrm{GL}_2(\mathbf{Q}_p)$ with trivial central character and of conductor $p^n$ with $n \geq 2$. Assume that $\pi$ is twist minimal, and that $\pi$ can be realized over $\mathbf{Q}$. Let $m$ be an integer such that $1 \leq m \leq n/2$. Then for any characters $\psi, \psi' : \mathbf{Q}_p \to \mathbf{C}^\times$ of respective levels 1 and $m$, we have*

$$\sum_{\chi \in \widetilde{S}(p^m)} \tau(\chi, \psi') \epsilon(\chi\pi, \frac{1}{2}, \psi) \neq 0. \tag{16}$$

*Remark* 4.4. There are examples of newforms $f$ of weight 2 on $\Gamma_0(N)$ such that the local component $\pi_{f,p}$ is cuspidal and twist minimal, but the sum (16) vanishes (see Remark 6.1). Therefore the assumption that $\pi$ can be realized over $\mathbf{Q}$ is necessary.

## 5. Cuspidal inducing data

In this section we recall how cuspidal representations of $\mathrm{GL}_2(\mathbf{Q}_p)$ can be described in terms of cuspidal inducing data, and we recast Theorem 4.3 in terms of this data using a formula of Bushnell for the local constant.

Let $\pi$ be an irreducible cuspidal representation of $G = \mathrm{GL}_2(\mathbf{Q}_p)$ with trivial central character and of conductor $p^n$ with $n \geq 2$. By the classification theorem [5, 15.5,15.8], the representation $\pi$ is induced by a cuspidal datum : there exist a maximal compact-mod-center subgroup $K$ of $G$, and an irreducible complex representation $\xi$ of $K$, such that $\pi \cong \text{c-Ind}_K^G \xi$, where c-Ind denotes compact induction.

Since $\pi$ has trivial central character, the restriction of $\xi$ to the center $Z = \mathbf{Q}_p^\times$ of $G$ is trivial, and since $K/Z$ is compact, $\xi$ is finite-dimensional. The contragredient of $\xi$ is defined by $\check{\xi}(k) = \xi(k^{-1})^*$. Finally, note that $\chi\pi \cong \text{c-Ind}_K^G(\chi\xi)$ for any character $\chi : \mathbf{Q}_p^\times \to \mathbf{C}^\times$.

There are two maximal compact-mod-center subgroups of $G$ up to conjugacy, namely $K' = p^{\mathbf{Z}} \cdot \mathrm{GL}_2(\mathbf{Z}_p)$ and $K'' = \begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix}^{\mathbf{Z}} \cdot \begin{pmatrix} \mathbf{Z}_p^\times & \mathbf{Z}_p \\ p\mathbf{Z}_p & \mathbf{Z}_p^\times \end{pmatrix}$.

They are equipped with a canonical decreasing sequence of compact normal subgroups $(K_n)_{n\geq 0}$, which are defined as follows.

If $K = K'$ then $K_0 = \mathrm{GL}_2(\mathbf{Z}_p)$ and $K_n = 1 + p^n M_2(\mathbf{Z}_p)$ for any $n \geq 1$. Note that $K_0/K_n \cong \mathrm{GL}_2(\mathbf{Z}/p^n\mathbf{Z})$.

If $K = K''$ then $K_0 = \begin{pmatrix} \mathbf{Z}_p^\times & \mathbf{Z}_p \\ p\mathbf{Z}_p & \mathbf{Z}_p^\times \end{pmatrix}$ and $K_n = 1 + \mathfrak{P}^n$ for any $n \geq 1$, where $\mathfrak{P} = \begin{pmatrix} p\mathbf{Z}_p & \mathbf{Z}_p \\ p\mathbf{Z}_p & p\mathbf{Z}_p \end{pmatrix}$.

The *conductor* $r(\xi)$ of $\xi$ is the least integer $r \geq 1$ such that $\xi(K_r) = 1$. The relation between the conductors of $\pi$ and $\xi$ is as follows [4, A.3].

If $n = 2m$ is even, we are in the *unramified case*: we have $K = K'$ and $r(\xi) = m$, and we define $c = p^{1-m} \cdot I_2 \in K$.

If $n = 2m + 1$ is odd, we are in the *ramified case*: we have $K = K''$ and $r(\xi) = 2m$, and we define $c = \begin{pmatrix} 0 & -p^{-m} \\ p^{1-m} & 0 \end{pmatrix} \in K$.

The proof of Theorem 4.3 relies on the following explicit formula, due to Bushnell, for the Godement-Jacquet local constant of $\pi$.

**Theorem 5.1.** [5, 25.2 Thm] *Let $r$ be the conductor of $\xi$, and let $m = \lfloor \frac{n}{2} \rfloor$. If $\psi : \mathbf{Q}_p \to \mathbf{C}^\times$ is a character of level one, then*

$$\sum_{x \in K_0/K_r} \psi(\mathrm{tr}(cx))\check{\xi}(cx) = p^{2m}\epsilon(\pi, \frac{1}{2}, \psi) \cdot \mathrm{id}\,. \tag{17}$$

We now express the sum of local constants appearing in Theorem 4.3 in terms of $\xi$.

**Proposition 5.2.** *Let $r$ be the conductor of $\xi$, and let $m = \lfloor \frac{n}{2} \rfloor$. Let $k$ be an integer such that $1 \leq k \leq m$. For any characters $\psi, \psi' : \mathbf{Q}_p \to \mathbf{C}^\times$ of respective levels $1$ and $k$, the sum*

$$\sum_{\chi \in \widetilde{S}(p^k)} \tau(\chi, \psi')\epsilon(\chi\pi, \frac{1}{2}, \psi) \tag{18}$$

*is the unique eigenvalue of the scalar endomorphism*

$$\frac{p-1}{p^{2m-k+1}} \sum_{x \in K_0/K_r} \psi(\mathrm{tr}(cx))\psi'(\det x)\check{\xi}(cx). \tag{19}$$

*Proof.* Let $\chi \in \widetilde{S}(p^k)$. Since $\pi$ is minimal by twist, we have $r(\chi\xi) = r$ and Theorem 5.1 gives

$$\sum_{x \in K_0/K_r} \psi(\mathrm{tr}(cx))\bar{\chi}(\det(cx))\check{\xi}(cx) = p^{2m}\epsilon(\chi\pi, \frac{1}{2}, \psi) \cdot \mathrm{id}\,. \tag{20}$$

Because $\det(c)$ is a power of $p$, we have $\bar{\chi}(\det(c)) = 1$. Multiplying the left hand side of (20) by $\tau(\chi, \psi')$ and summing over $\chi$, we get

$$\sum_{\chi \in \widetilde{S}(p^k)} \sum_{y \in (\mathbf{Z}/p^k\mathbf{Z})^\times} \chi(y)\psi'(y) \sum_{x \in K_0/K_r} \psi(\mathrm{tr}(cx))\bar{\chi}(\det x)\check{\xi}(cx)$$

$$= \sum_{x \in K_0/K_r} \psi(\mathrm{tr}(cx))\check{\xi}(cx) \sum_{y \in (\mathbf{Z}/p^k\mathbf{Z})^\times} \psi'(y) \sum_{\chi \in S(p^k)} \chi(y)\bar{\chi}(\det x). \tag{21}$$

Let $C(p^k)$ be the set of all Dirichlet characters modulo $p^k$. For $a \in (\mathbf{Z}/p^k\mathbf{Z})^\times$, the sum $\sum_{\chi \in C(p^k)} \chi(a)$ equals $p^{k-1}(p-1)$ if $a = 1$, and 0 otherwise. So for $k = 1$, (21) simplifies to

$$(p-1) \sum_{x \in K_0/K_r} \psi(\mathrm{tr}(cx))\psi'(\det x)\check{\xi}(cx). \tag{22}$$

If $k \geq 2$ then $\widetilde{S}(p^k) = C(p^k) - C(p^{k-1})$ so that (21) can be written

$$p^{k-1}(p-1) \sum_{x \in K_0/K_r} \psi(\mathrm{tr}(cx))\psi'(\det x)\check{\xi}(cx)$$

$$- p^{k-2}(p-1) \sum_{x \in K_0/K_r} \psi(\mathrm{tr}(cx)) \left( \sum_{\substack{y \in (\mathbf{Z}/p^k\mathbf{Z})^\times \\ y \equiv \det x \pmod{p^{k-1}}}} \psi'(y) \right) \check{\xi}(cx). \tag{23}$$

Since $\psi'$ has level $k$, the inner sum over $y$ vanishes. In all cases, this gives the proposition as stated. □

*Remark* 5.3. The formula (15), together with Proposition 5.2, leads to an explicit formula for the Fourier expansion of $f$ at an arbitrary cusp of $X_0(N)$ purely in terms of the local components of $f$, and may be of independent interest.

**Definition 5.4.** For any characters $\psi, \psi' : \mathbf{Q}_p \to \mathbf{C}^\times$ of respective levels 1 and $m$, we define $T(\xi, \psi, \psi')$ to be the endomorphism

$$T(\xi, \psi, \psi') = \sum_{x \in K_0/K_{r(\xi)}} \psi(\mathrm{tr}(cx))\psi'(\det x)\check{\xi}(x). \tag{24}$$

In order to establish Theorem 4.3, it suffices, thanks to Proposition 5.2, to show that $T(\xi, \psi, \psi') \neq 0$. We prove this in the following sections, distinguishing the unramified and ramified cases.

## 6. The unramified case

In this section we assume $n = 2m$ with $m \geq 1$, so that $c = p^{1-m} \cdot I_2$. Note that $\psi(\mathrm{tr}(cx)) = \psi(p^{1-m} \mathrm{tr}\, x)$ and $a \mapsto \psi(p^{1-m}a)$ is a character of level $m$. So we fix characters $\psi, \psi' : \mathbf{Q}_p \to \mathbf{C}^\times$ of respective levels $m, m'$ with $1 \leq m' \leq m$, and we wish to prove that

$$T(\xi, \psi, \psi') := \sum_{x \in \mathrm{GL}_2(\mathbf{Z}/p^m\mathbf{Z})} \psi(\mathrm{tr}\, x)\psi'(\det x)\check{\xi}(x) \tag{25}$$

is non-zero. Assuming the contrary, for every $y \in \mathrm{GL}_2(\mathbf{Z}/p^m\mathbf{Z})$ we have

$$0 = \check{\xi}(y^{-1})T(\xi,\psi,\psi') = \sum_{x\in \mathrm{GL}_2(\mathbf{Z}/p^m\mathbf{Z})} \psi(\operatorname{tr} x)\psi'(\det x)\check{\xi}(y^{-1}x)$$
$$= \sum_{x\in \mathrm{GL}_2(\mathbf{Z}/p^m\mathbf{Z})} \psi(\operatorname{tr}(yx))\psi'(\det(yx))\check{\xi}(x).$$

Taking $y = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$ with $t \in \mathbf{Z}/p^m\mathbf{Z}$ and writing $x = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, we have $\operatorname{tr}(yx) = \operatorname{tr}(x) + \gamma t$. We get

$$\sum_{x\in \mathrm{GL}_2(\mathbf{Z}/p^m\mathbf{Z})} \psi(\gamma t)\psi(\operatorname{tr} x)\psi'(\det x)\check{\xi}(x) = 0. \tag{26}$$

For any $c_0 \in \mathbf{Z}/p^m\mathbf{Z}$, let $B(c_0) \subset \mathrm{GL}_2(\mathbf{Z}/p^m\mathbf{Z})$ be the set of matrices of the form $x = \begin{pmatrix} * & * \\ c_0 & * \end{pmatrix}$. Since (26) is true for every $t \in \mathbf{Z}/p^m\mathbf{Z}$, we get

$$\sum_{x\in B(c_0)} \psi(\operatorname{tr} x)\psi'(\det x)\check{\xi}(x) = 0 \qquad (c_0 \in \mathbf{Z}/p^m\mathbf{Z}). \tag{27}$$

Fix $c_0 \in (\mathbf{Z}/p^m\mathbf{Z})^\times$. Then every matrix $x \in B(c_0)$ may be written uniquely in the form $x = \begin{pmatrix} 0 & 1 \\ c_0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}\begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix}$ with $a, b \in \mathbf{Z}/p^m\mathbf{Z}$ and $d \in (\mathbf{Z}/p^m\mathbf{Z})^\times$. We have $\operatorname{tr} x = a + bc_0$ and $\det x = -dc_0$, so that

$$\sum_{\substack{a,b\in \mathbf{Z}/p^m\mathbf{Z} \\ d\in(\mathbf{Z}/p^m\mathbf{Z})^\times}} \psi(a+bc_0)\psi'(-dc_0)\check{\xi}\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}\check{\xi}\begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} = 0 \qquad (c_0 \in (\mathbf{Z}/p^m\mathbf{Z})^\times). \tag{28}$$

We now make use of further properties of the representation $\xi$, for which we refer to [10]. Let $V$ be the space of $\check{\xi}$. By [10, Thm 3.5], the restriction of $\check{\xi}$ to $N = \begin{pmatrix} 1 & \mathbf{Z}_p \\ 0 & 1 \end{pmatrix}$ is isomorphic to the direct sum of the additive characters of $\mathbf{Z}_p$ of level $m$, each character appearing with multiplicity 1. We denote by $V = \bigoplus_\chi V(\chi)$ this direct sum decomposition. Moreover, by the proof of [10, Thm 3.6], the representation $\pi$ admits a new vector: there exists $v \in V - \{0\}$ which is fixed by all diagonal matrices of $K$. Since $Nv$ spans $V$, the components $v_\chi$ of $v$ with respect to the above decomposition are nonzero. Note that the diagonal matrix $\delta = \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}$ sends $V(\chi)$ to $V(\chi_d)$, where $\chi_d$ denotes the character $t \mapsto \chi(dt)$. Since $\delta$ fixes $v$, we get $\delta(v_\chi) = v_{\chi_d}$. It follows that

$$\check{\xi}\begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} v_\chi = \check{\xi}\begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}\check{\xi}\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} v_\chi = \chi(b) v_{\chi_d}. \tag{29}$$

Let $p'_\psi = \sum_{a\in\mathbf{Z}/p^m\mathbf{Z}} \psi(a)\check{\xi}\begin{pmatrix}1 & 0\\ a & 1\end{pmatrix}$. Since the matrix $\begin{pmatrix}1 & 0\\ a & 1\end{pmatrix}$ is conjugate to $\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}$ and $\psi$ has level $m$, we see that $p'_\psi$ is a projector of rank 1. Evaluating (28) at $v_\chi$, we get

$$p'_\psi \sum_{\substack{b\in\mathbf{Z}/p^m\mathbf{Z}\\ d\in(\mathbf{Z}/p^m\mathbf{Z})^\times}} \psi(bc_0)\psi'(-dc_0)\chi(b)v_{\chi_d} = 0 \qquad (c_0 \in (\mathbf{Z}/p^n\mathbf{Z})^\times). \tag{30}$$

The sum over $b$ is zero unless $\chi(t) = \psi(-c_0 t)$, in which case (30) simplifies to

$$p'_\psi \sum_{d\in(\mathbf{Z}/p^m\mathbf{Z})^\times} \psi'(-dc_0)v_{\psi_{-c_0 d}} = 0 \qquad (c_0 \in (\mathbf{Z}/p^m\mathbf{Z})^\times). \tag{31}$$

Let $\lambda \in \mathbf{Z}/p^m\mathbf{Z}$ be such that $\psi' = \psi_\lambda$ (we have $\lambda \neq 0$ since $m' \geq 1$). Then (31) implies

$$p'_\psi \sum_\chi \chi(\lambda)v_\chi = 0 \tag{32}$$

where the sum runs over all primitive characters of $\mathbf{Z}/p^m\mathbf{Z}$. This can be rewritten as

$$p'_\psi \check{\xi}\begin{pmatrix}1 & \lambda\\ 0 & 1\end{pmatrix} v = 0. \tag{33}$$

We now make use of the assumption that the representation $\xi$ can be realized over $\mathbf{Q}$. The subspace of $V$ fixed by all diagonal matrices is one-dimensional and is clearly rational. The new vector $v$ can thus be chosen to be rational. By taking Galois conjugates, if (33) holds for one particular value of $\psi$, then it holds for all $\psi$ of level $m$. But the projectors $p'_\psi$ add up to the identity of $V$, so that we get $v = 0$, a contradiction.

*Remark* 6.1. If we don't assume that $\xi$ can be realized over $\mathbf{Q}$, then it may happen that $T(\xi, \psi, \psi') = 0$ even if $\xi$ is twist minimal. We found examples of this phenomenon already in the case $p = 5$ and $m = 2$. There is a cuspidal representation $\xi$ of $\mathrm{GL}_2(\mathbf{Z}/25\mathbf{Z})$ of dimension 20 with coefficients in $\mathbf{Q}(\sqrt{5})$ such that $T(\xi, \psi, \psi_\lambda) = 0$ if $\lambda \equiv \pm 1 \pmod 5$. There is a newform $f$ of weight 2 on $\Gamma_0(625)$ with coefficients in $\mathbf{Q}(\sqrt{5})$ whose Fourier expansion begins with

$$f = q + \left(\frac{-1-\sqrt{5}}{2}\right)q^2 + \left(\frac{-3-\sqrt{5}}{2}\right)q^3 + \left(\frac{-1+\sqrt{5}}{2}\right)q^4 \ldots$$

such that $\pi_{f,5}$ is induced from $\xi$. The newform $f$ is twist minimal, and the formula (15) together with Proposition 5.2 implies that $\omega_f$ vanishes at the cusps $\lambda/25$ with $\lambda \equiv \pm 1 \pmod 5$. Hao Chen has checked numerically that it is indeed the case.

## 7. The ramified case

In this section we assume $n = 2m+1$ with $m \geq 1$, so that $c = \begin{pmatrix} 0 & -p^{-m} \\ p^{1-m} & 0 \end{pmatrix}$. Note that $\psi(\mathrm{tr}(cx)) = \psi(p^{1-m}\,\mathrm{tr}'\,x)$ where the function $\mathrm{tr}' : K_0 \to \mathbf{Z}_p$ is defined by $\mathrm{tr}'\begin{pmatrix} \alpha & \beta \\ p\gamma & \delta \end{pmatrix} = \beta - \gamma$. So we fix characters $\psi, \psi' : \mathbf{Q}_p \to \mathbf{C}^\times$ of respective levels $m, m'$ with $1 \leq m' \leq m$, and we wish to prove that

$$T(\xi, \psi, \psi') := \sum_{x \in K_0/K_{2m}} \psi(\mathrm{tr}'\,x)\psi'(\det x)\check{\xi}(x) \tag{34}$$

is non-zero. Assume the contrary.

We have explicitly

$$K_\ell = \begin{pmatrix} 1 + p^{\lceil \frac{\ell}{2} \rceil}\mathbf{Z}_p & p^{\lfloor \frac{\ell}{2} \rfloor}\mathbf{Z}_p \\ p^{\lfloor \frac{\ell}{2} \rfloor + 1}\mathbf{Z}_p & 1 + p^{\lceil \frac{\ell}{2} \rceil}\mathbf{Z}_p \end{pmatrix} \qquad (\ell \geq 1).$$

Moreover, we have an isomorphism of groups

$$\begin{aligned} K_m/K_{2m} &\xrightarrow{\cong} (\mathbf{Z}/p^{\lfloor \frac{m}{2} \rfloor}\mathbf{Z})^2 \oplus (\mathbf{Z}/p^{\lceil \frac{m}{2} \rceil}\mathbf{Z})^2 \\ \begin{pmatrix} 1 + p^{\lceil \frac{m}{2} \rceil}\alpha & p^{\lfloor \frac{m}{2} \rfloor}\beta \\ p^{\lfloor \frac{m}{2} \rfloor + 1}\gamma & 1 + p^{\lceil \frac{m}{2} \rceil}\delta \end{pmatrix} &\mapsto (\alpha, \delta, \beta, \gamma). \end{aligned}$$

Let $y \in K_m$. Multiplying $T(\xi, \psi, \psi')$ on the right by $\check{\xi}(y^{-1})$, we get

$$\sum_{x \in K_0/K_{2m}} \psi(\mathrm{tr}'(xy))\psi'(\det(xy))\check{\xi}(x) = 0. \tag{35}$$

If we fix $x \in K_0$, then the map $\Phi_x : K_m/K_{2m} \to \mathbf{C}^\times$ defined by

$$\psi(\mathrm{tr}'(xy))\psi'(\det(xy)) = \psi(\mathrm{tr}'\,x)\psi'(\det x)\Phi_x(y) \qquad (y \in K_m) \tag{36}$$

is a character which depends only on the coset $xK_m$.

**Lemma 7.1.** *The characters $(\Phi_x)_{x \in K_0/K_m}$ are pairwise distinct.*

*Proof.* If $x = \begin{pmatrix} a & b \\ pc & d \end{pmatrix} \in K_0$ and $y = \begin{pmatrix} 1+s & t \\ pu & 1+v \end{pmatrix} \in K_m$, an explicit computation gives

$$\Phi_x(y) = \psi(at + bv - cs - du)\psi'((ad - pbc)(s + v)). \tag{37}$$

Let $x' = \begin{pmatrix} a' & b' \\ pc' & d' \end{pmatrix} \in K_0$ such that $\Phi_x = \Phi_{x'}$. By (37), we already get $a, d \equiv a', d' \ (p^{\lceil \frac{m}{2} \rceil})$. Let $\lambda \in (\mathbf{Z}/p^{m'}\mathbf{Z})^\times$ be the unique element such that $\psi'(1) = \psi(p^{m-m'}\lambda)$. It remains to prove that the map

$$\begin{aligned} h_{a,d} : (\mathbf{Z}/p^{\lfloor \frac{m}{2} \rfloor}\mathbf{Z})^2 &\to (\mathbf{Z}/p^{\lfloor \frac{m}{2} \rfloor}\mathbf{Z})^2 \\ (b, c) &\mapsto (b + p^{m-m'}\lambda(ad - pbc), -c + p^{m-m'}\lambda(ad - pbc)) \end{aligned} \tag{38}$$

is injective. Assume $h_{a,d}(b,c) = h_{a,d}(b',c')$. Then $b - p^{m-m'+1}\lambda bc \equiv b' - p^{m-m'+1}\lambda b'c'$ $(p^{\lfloor \frac{m}{2} \rfloor})$ and $c + p^{m-m'+1}\lambda bc \equiv c' + p^{m-m'+1}\lambda b'c'$ $(p^{\lfloor \frac{m}{2} \rfloor})$. In particular $b, c \equiv b', c'$ $(p)$ and an easy induction gives $b, c \equiv b', c'$ $(p^{\lfloor \frac{m}{2} \rfloor})$. □

Fix $x_0 \in K_0$. If we multiply (35) by $\bar{\Phi}_{x_0}(y)$ and sum over $y \in K_m/K_{2m}$, we get

$$\sum_{y \in K_m/K_{2m}} \bar{\Phi}_{x_0}(y) \sum_{x \in K_0/K_{2m}} \psi(\mathrm{tr}'\, x)\psi'(\det x)\Phi_x(y)\check{\xi}(x) = 0. \tag{39}$$

According to Lemma 7.1, this simplifies to

$$\sum_{x \in x_0 K_m/K_{2m}} \psi(\mathrm{tr}'\, x)\psi'(\det x)\check{\xi}(x) = 0. \tag{40}$$

In other words, for every $x_0 \in K_0$ we have

$$\sum_{y \in K_m/K_{2m}} \Phi_{x_0}(y)\check{\xi}(y) = 0. \tag{41}$$

Fix $a_0, d_0 \in (\mathbf{Z}/p^{\lceil \frac{m}{2} \rceil}\mathbf{Z})^\times$. We sum (41) over all matrices $x_0 \in K_0/K_m$ of the form $x_0 = \begin{pmatrix} a_0 & * \\ * & d_0 \end{pmatrix}$. Letting $y = \begin{pmatrix} 1+s & t \\ pu & 1+v \end{pmatrix}$, we compute

$$\sum_{x_0} \Phi_{x_0}(y) = \sum_{b_0, c_0 \in \mathbf{Z}/p^{\lfloor \frac{m}{2} \rfloor}\mathbf{Z}} \psi(a_0 t + d_0 u)\psi(h_{a_0,d_0}(b_0,c_0)\cdot(v,s)) \tag{42}$$

where $h_{a_0,d_0}$ is the map of (38). Since $h_{a_0,d_0}$ is bijective, we get

$$\begin{aligned} \sum_{x_0} \Phi_{x_0}(y) &= \psi(a_0 t + d_0 u) \sum_{b_0, c_0 \in \mathbf{Z}/p^{\lfloor \frac{m}{2} \rfloor}\mathbf{Z}} \psi(b_0 v + c_0 s) \\ &= \begin{cases} p^{2\lfloor \frac{m}{2} \rfloor}\psi(a_0 t + d_0 u) & \text{if } s \equiv v \equiv 0 \quad (p^m) \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

So for any $a_0, d_0 \in (\mathbf{Z}/p^{\lceil \frac{m}{2} \rceil}\mathbf{Z})^\times$, we get

$$\sum_{t,u \in p^{\lfloor \frac{m}{2} \rfloor}\mathbf{Z}/p^m\mathbf{Z}} \psi(a_0 t + d_0 u)\check{\xi}\begin{pmatrix} 1 & t \\ pu & 1 \end{pmatrix} = 0. \tag{43}$$

As in section 6, the restriction of $\xi$ to $N = \begin{pmatrix} 1 & \mathbf{Z}_p \\ 0 & 1 \end{pmatrix}$ is isomorphic to the direct sum of the characters of $\mathbf{Z}_p$ of level $m$. Conjugating by the matrix $\begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix}$, the same is true for the restriction of $\xi$ to $N' = \begin{pmatrix} 1 & 0 \\ p\mathbf{Z}_p & 1 \end{pmatrix}$. For any $t, u \in p^{\lfloor \frac{m}{2} \rfloor}\mathbf{Z}/p^m\mathbf{Z}$, the matrices $\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ pu & 1 \end{pmatrix}$ commute. By simultaneous diagonalization, there exists a nonzero vector $v$ in the space of $\check{\xi}$ and primitive characters $\omega, \omega' : \mathbf{Z}/p^{\lceil \frac{m}{2} \rceil}\mathbf{Z} \to \mathbf{C}^\times$ such that

$$\check{\xi}\begin{pmatrix} 1 & p^{\lfloor \frac{m}{2} \rfloor}t \\ p^{\lfloor \frac{m}{2} \rfloor+1}u & 1 \end{pmatrix} v = \omega(t)\omega'(u)v \qquad (t, u \in \mathbf{Z}/p^{\lceil \frac{m}{2} \rceil}\mathbf{Z}). \tag{44}$$

We may write the characters $\omega, \omega'$ as $\omega(t) = \bar{\psi}(p^{\lfloor \frac{m}{2} \rfloor} a_0 t)$ and $\omega'(u) = \bar{\psi}(p^{\lfloor \frac{m}{2} \rfloor} d_0 u)$ for some $a_0, d_0 \in (\mathbf{Z}/p^{\lceil \frac{m}{2} \rceil}\mathbf{Z})^\times$. For this choice of $a_0, d_0$, the identity (43) evaluated at $v$ gives a contradiction. This finishes the proof of Theorem 1.2.

## 8. Numerical investigations

We now report on the computations which led to Theorem 1.2. For all elliptic curves of conductor $\leq 2000$, we computed all the ramification indices at the cusps of the modular parametrizations using Pari/GP [17]. Since we have no theoretical formula for the ramification index in general, we just compared numerically $\log|f_E|$ and $\log|q|$ in the neighborhood of the given cusp. This method is not rigorous, but it gives good results in practice. We ended up with a list of 745 isogeny classes of elliptic curves for which the modular parametrization seemed to ramify at some cusp. We then observed and checked, with the help of Magma [2], that for each curve in this list, the associated newform was not minimal by twist.

In Table 1 below, we give all instances of ramified cusps for elliptic curves of conductor $\leq 200$ (we restrict to the cusps $[\frac{1}{d}]$ with $d^2|N$). In the last column, we indicate a minimal twist for the newform (it need not be unique, for example $96a$ has quadratic twist $96b$). Furthermore, a minimal twist need not have trivial character. For example, the minimal twist of $162b$ and $162c$ is a newform of level 18 and non-trivial character, which we just denote by "18".

Note also that being minimal by twist is far from being a necessary condition in order for the modular parametrization to be unramified at the cusps. For example, the isogeny class $45a$, which is a twist of $15a$, has a modular parametrization which is unramified at the cusps.

In all cases we computed, the following properties seem to hold :

(1) If $e_\varphi(\frac{1}{d})$ is even then $v_2(d) \in \{2,3,4\}$ and $v_2(N) = 2v_2(d)$;
(2) If $e_\varphi(\frac{1}{d})$ is divisible by 8 then $v_2(d) = 4$ and $v_2(N) = 8$;
(3) If $e_\varphi(\frac{1}{d})$ is divisible by 3 then $v_3(d) = 2$ and $v_3(N) = 4$.

These observations are consistent with the following theorem of Atkin and Li [1, Thm 4.4.i)] : if $f \in S_2(\Gamma_0(N))$ is a newform and $v_p(N)$ is odd, then $f$ is $p$-minimal, in the sense that it has minimal level among its twists by characters of $p$-power conductor.

Looking at elliptic curves whose conductor is highly divisible by 2 or 3, we also found examples of higher ramification indices. These are given in Table 2 below. In this table, we also give examples of ramified cusps for elliptic curves of odd conductor. In all examples we computed, the ramification index seems to be a divisor of 24. This may be related to the fact that the exponent of the conductor of an elliptic curve at 2 (resp. 3) is bounded by 8 (resp. 5). It would be interesting to prove this divisibility in general.

| Isogeny class | $d$ | $e_\varphi(\frac{1}{d})$ | Minimal twist |
|---|---|---|---|
| $48a$ | 4 | 2 | $24a$ |
| $64a$ | 8 | 2 | $32a$ |
| $80a$ | 4 | 2 | $40a$ |
| $80b$ | 4 | 4 | $20a$ |
| $112a$ | 4 | 2 | $56b$ |
| $112b$ | 4 | 2 | $56a$ |
| $112c$ | 4 | 4 | $14a$ |
| $144a$ | $\begin{cases} 4 \\ 12 \end{cases}$ | $\begin{matrix} 4 \\ 4 \end{matrix}$ | $36a$ |
| $144b$ | $\begin{cases} 4 \\ 12 \end{cases}$ | $\begin{matrix} 2 \\ 2 \end{matrix}$ | $24a$ |
| $162b$ | 9 | 3 | 18 |
| $162c$ | 9 | 3 | 18 |
| $176a$ | 4 | 2 | $88a$ |
| $176b$ | 4 | 4 | $11a$ |
| $176c$ | 4 | 4 | $44a$ |
| $192a$ | 8 | 2 | $96a$ |
| $192b$ | 8 | 2 | $96a$ |
| $192c$ | 8 | 4 | $24a$ |
| $192d$ | 8 | 4 | $24a$ |

TABLE 1. Ramified cusps for conductors $\leq 200$

| Isogeny class | $N$ | $d$ | $e_\varphi(\frac{1}{d})$ |
|---|---|---|---|
| $405c$ | $3^4 \cdot 5$ | 9 | 3 |
| $768b$ | $2^8 \cdot 3$ | 16 | 8 |
| $891b$ | $3^4 \cdot 11$ | 9 | 3 |
| $1296c$ | $2^4 \cdot 3^4$ | 36 | 6 |
| $1296e$ | $2^4 \cdot 3^4$ | 36 | 12 |
| $20736c$ | $2^8 \cdot 3^4$ | 144 | 24 |

TABLE 2. Higher ramification indices

## REFERENCES


[1] A. O. L. ATKIN & W. C. W. LI – "Twists of newforms and pseudo-eigenvalues of $W$-operators", *Invent. Math.* **48** (1978), no. 3, p. 221–243.

[2] W. BOSMA, J. CANNON & C. PLAYOUST – "The Magma algebra system. I. The user language", *J. Symbolic Comput.* **24** (1997), no. 3-4, p. 235–265, Computational algebra and number theory (London, 1993).

[3] C. BREUIL, B. CONRAD, F. DIAMOND & R. TAYLOR – "On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises", *J. Amer. Math. Soc.* **14** (2001), no. 4, p. 843–939.

[4] C. BREUIL & A. MÉZARD – "Multiplicités modulaires et représentations de $\mathrm{GL}_2(\mathbf{Z}_p)$ et de $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ en $l = p$", *Duke Math. J.* **115** (2002), no. 2, p. 205–310, With an appendix by Guy Henniart.

[5] C. J. Bushnell & G. Henniart – *The local Langlands conjecture for* GL(2), Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 335, Springer-Verlag, Berlin, 2006.
[6] C. Delaunay – "Formes modulaires et invariants de courbes elliptiques définies sur **Q**", Thèse de doctorat, Université Bordeaux 1, décembre 2002.
[7] C. Delaunay – "Critical and ramification points of the modular parametrization of an elliptic curve", *J. Théor. Nombres Bordeaux* **17** (2005), no. 1, p. 109–124.
[8] S. S. Gelbart – *Automorphic forms on adèle groups*, Princeton University Press, Princeton, N.J., 1975, Annals of Mathematics Studies, No. 83.
[9] H. Jacquet & R. P. Langlands – *Automorphic forms on* GL(2), Lecture Notes in Mathematics, Vol. 114, Springer-Verlag, Berlin, 1970.
[10] D. Loeffler & J. Weinstein – "On the computation of local components of a newform", *Mathematics of Computation* **81** (2012), p. 1179–1200.
[11] B. Mazur & P. Swinnerton-Dyer – "Arithmetic of Weil curves", *Invent. Math.* **25** (1974), p. 1–61.
[12] L. Merel – "Symboles de Manin et valeurs de fonctions $L$", in *Algebra, arithmetic, and geometry: in honor of Yu. I. Manin. Vol. II*, Progr. Math., vol. 270, Birkhäuser Boston Inc., Boston, MA, 2009, p. 283–309.
[13] P. D. Nelson, A. Pitale & A. Saha – "Bounds for Rankin-Selberg integrals and quantum unique ergodicity for powerful levels", *J. Amer. Math. Soc.* **27** (2014), no. 1, p. 147–191.
[14] A. Saha – "Large values of newforms on GL(2) with highly ramified central character", To appear in International Mathematics Research Notices, Preprint at `http://www.maths.bris.ac.uk/~as12313/research/sup-norm-whittaker.pdf`.
[15] ———, "Ramification at the cusps", Unpublished note, July 2012.
[16] G. Stevens – *Arithmetic on modular curves*, Progress in Mathematics, vol. 20, Birkhäuser Boston Inc., Boston, MA, 1982.
[17] The PARI Group – Bordeaux, *PARI/GP, version* `2.5.0`, 2011, available from `http://pari.math.u-bordeaux.fr/`.

François Brunault, ÉNS Lyon, Unité de mathématiques pures et appliquées, 46 allée d'Italie, 69007 Lyon, France
*E-mail address*: `francois.brunault@ens-lyon.fr`
*URL*: `http://perso.ens-lyon.fr/francois.brunault/`