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.

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 φ necessarily ramifies as soon as the genus of $X_0(N)$ is at least 2, and we may ask whether these 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 φ on the imaginary axis [11]. Further results and numerical examples were obtained by Delaunay [7].

In this article, we consider the following problem.

Problem 0.1. Compute the ramification index $e_\varphi(x)$ of φ at a given cusp $x \in X_0(N)(\mathbf{C})$.

Let ω_E be a Néron differential form on E. Its pull-back $\varphi^*\omega_E$ is a rational multiple of $\omega_{f_E} = 2\pi i f_E(z)dz$, where f_E is the newform of weight 2 on $\Gamma_0(N)$ associated to E. It follows that $e_\varphi(x) = 1 + \mathrm{ord}_x\, \omega_{f_E}$ depends only on f_E, and not on φ. We prove the following result.

Theorem 0.2. *Let $f \in S_2(\Gamma_0(N))$ be a newform having minimal level among all its twists by Dirichlet characters. Then the differential form $\omega_f = 2\pi i f(z)dz$ doesn't vanish at the cusps of $X_0(N)$.*

A newform having minimal level among its twists by Dirichlet characters is said to be *minimal by twist*.

Corollary 0.3. *If the newform f_E associated to E is minimal by twist, then φ is unramified at the cusps.*

2000 *Mathematics Subject Classification.* 11F03, 11F30, 11F70.

If N is squarefree, then all newforms of level N are minimal by twist, and in this particular case, Theorem 0.2 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 §2 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 §3 to reduce Theorem 0.2 to a purely local non-vanishing statement. We prove this non-vanishing in §5-6 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.

Theorem 0.2 was suggested by numerical computations, which we report in §7. Using Pari/GP [14], we estimated numerically the ramification indices at all cusps for all elliptic curves of conductor ≤ 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.

I would like to thank Christophe Delaunay for helpful suggestions regarding this work.

1. First properties of the ramification index

Let f be a newform of weight 2 on $\Gamma_0(N)$. For any $x \in X_0(N)(\mathbf{C})$, we define $e_f(x) = 1 + \mathrm{ord}_x(\omega_f)$.

Lemma 1.1. *Let Q be a divisor of N such that $(Q, \frac{N}{Q}) = 1$, and let W_Q be the corresponding Atkin-Lehner involution of $X_0(N)$. 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 1.2. *Let $\sigma \in \mathrm{Aut}(\mathbf{C})$ and let $f^\sigma \in S_2(\Gamma_0(N))$ be the newform obtained by applying σ 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 1.1 from $\sigma_*\omega_f = \omega_{f^\sigma}$. □

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

Definition 1.3. 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 1.4. *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 [13, Thm 1.3.1]. □

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

Lemma 1.5. *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 1.5, 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 0.2 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 1.6. *We have $e_f(\frac{1}{d}) = \min\{n \geq 1 : b_{d,n} \neq 0\}$.*

Proof. The matrix $M = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & \frac{1}{d} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix} \in \mathrm{SL}_2(\mathbf{R})$ satisfies $M(\infty) = \frac{1}{d}$ 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 1.7. *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 $e_f(\frac{1}{2}) = e_f(0) = 1$. □

2. 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 ϕ denote Euler's function. For any integer $m \geq 1$, let Σ_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 χ is $\tau(\chi) = \sum_{a \in (\mathbf{Z}/m\mathbf{Z})^\times} \chi(a) e^{2\pi i a/m}$, and the conductor of χ is denoted by m_χ. For any newform F of weight $k \geq 2$ on $\Gamma_1(M)$ and for any prime p, let $L_p(F, X) = 1 - a_p(F)X + a_{p,p}(F)X^2 \in \mathbf{C}[X]$ 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

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

where χ runs through the primitive Dirichlet characters of conductor m_χ 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 χ 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 χ 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

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

3. 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 purely 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 (6) 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 ϖ_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 induced map $(\mathbf{Z}/p^{m_p}\mathbf{Z})^\times \cong \mathbf{Z}_p^\times/(1 + p^{m_p}\mathbf{Z}_p) \to \mathbf{C}^\times$ is the inverse of the p-component of χ.

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 3.1. *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 π_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 ψ_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 $\pi_{f\otimes\chi,v}$ denotes the local representation of $f\otimes\chi$ at v. The quantity $\epsilon(\pi_{f\otimes\chi,v}, s, \psi_v)$ is the Godement-Jacquet local constant of $f\otimes\chi$.

For any character χ 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 3.2. *There exist a constant $C \in \mathbf{C}^\times$ and an element $a \in (\mathbf{Z}/d\mathbf{Z})^\times$, depending on f and ψ but not on χ, 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, Thm 6.16], we have $\epsilon(\pi_{f\otimes\chi,\infty}, \psi_\infty, s) = -1$, 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 χ_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 ω_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 χ, 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 $\chi : \mathbf{Q}_p^\times \to \mathbf{C}^\times$ such that $\chi(p) = 1$,

$\chi(1+p^m\mathbf{Z}_p)=1$ and $\chi(1+p^{m-1}\mathbf{Z}_p)\neq 1$ 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 $m_p=v_p(d)$.

Theorem 0.2 is thus reduced to the following purely local statement.

Theorem 3.3. *Fix a prime p such that $p^2|N$, and let $\pi=\pi_{f,p}$. Let m be an integer such that $1\leq m\leq\frac{v_p(N)}{2}$. Then for any characters $\psi,\psi':\mathbf{Q}_p\to\mathbf{C}^\times$ of respective levels 1 and m, we have*

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

4. Cuspidal inducing data

In this section we recall how the local automorphic representations $\pi_{f,p}$ with $p^2|N$ can be described in terms of cuspidal inducing data.

Let p be a prime such that $p^2|N$. Then $\pi=\pi_{f,p}$ is an irreducible cuspidal representation of $G=\mathrm{GL}_2(\mathbf{Q}_p)$ [10, Prop. 2.8]. By the classification theorem [5, 15.5,15.8], the representation π is induced by a cuspidal datum : there exist a maximal compact-mod-center subgroup K of G, and an irreducible complex representation ξ of K, such that $\pi\cong\text{c-Ind}_K^G\,\xi$, where c-Ind denotes compact induction.

Since π has trivial central character, the restriction of ξ to the center $Z=\mathbf{Q}_p^\times$ of G is trivial, and since K/Z is compact, ξ is finite-dimensional. The contragredient of ξ 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 $K_n=1+p^nM_2(\mathbf{Z}_p)$ 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 ξ is the least integer $r\geq 1$ such that $\xi(K_r)=1$. The relation between the conductors of π and ξ is as follows [4, A.3].

In the *unramified case* $v_p(N)=2n$, we may take $K=K'$ and $r(\xi)=n$, and we define $c=p^{1-n}\cdot I_2\in K$.

In the *ramified case* $v_p(N) = 2n+1$, we may take $K = K''$ and $r(\xi) = 2n$, and we define $c = \begin{pmatrix} 0 & -p^{-n} \\ p^{1-n} & 0 \end{pmatrix} \in K$.

The proof of Theorem 3.3 relies on the following explicit formula, due to Bushnell, for the Godement-Jacquet local constant of π.

Theorem 4.1. [5, 25.2 Thm] *Let $r \geq 1$ be the conductor of ξ. If $\psi : \mathbf{Q}_p \to \mathbf{C}^\times$ is a character of level one, then*

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

We now express the sum of local constants appearing in Theorem 3.3 in terms of ξ.

Proposition 4.2. *Let m be an integer such that $1 \leq m \leq \frac{v_p(N)}{2}$. For any characters $\psi, \psi' : \mathbf{Q}_p \to \mathbf{C}^\times$ of respective levels 1 and m, the sum*

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

is the unique eigenvalue of the scalar endomorphism

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

Proof. Let $r = r(\xi)$ and $\chi \in \widetilde{S}(p^m)$. Since f is minimal by twist, we have $r(\chi\xi) = r$ and Theorem 4.1 gives

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

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 χ, we get

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

Let $C(p^m)$ be the set of all Dirichlet characters modulo p^m. For $a \in (\mathbf{Z}/p^m\mathbf{Z})^\times$, the sum $\sum_{\chi \in C(p^m)} \chi(a)$ equals $p^{m-1}(p-1)$ if $a = 1$, and 0 otherwise. So for $m = 1$, (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 $m \geq 2$ then $\widetilde{S}(p^m) = C(p^m) - C(p^{m-1})$ so that (21) can be written

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

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

Since ψ' has level m, the inner sum over y vanishes. In all cases, this gives the proposition as stated. □

Remark 4.3. The formula (15), together with Proposition 4.2, provides an expression of $b_{d,n}$ purely in terms of the local components of π_f. This leads to an explicit formula for the Fourier expansion of f at an arbitrary cusp of $X_0(N)$, and may be of independent interest.

Definition 4.4. 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 3.3, it suffices, thanks to Proposition 4.2, to show that $T(\xi, \psi, \psi') \neq 0$. We prove this in the following sections, distinguishing the unramified and ramified cases.

5. The unramified case

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

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

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

$$\begin{aligned} 0 = T(\xi,\psi,\psi')\check{\xi}(y^{-1}) &= \sum_{x\in \mathrm{GL}_2(\mathbf{Z}/p^n\mathbf{Z})}\psi(\mathrm{tr}\,x)\psi'(\det x)\check{\xi}(xy^{-1})\\ &= \sum_{x\in \mathrm{GL}_2(\mathbf{Z}/p^n\mathbf{Z})}\psi(\mathrm{tr}(xy))\psi'(\det(xy))\check{\xi}(x). \end{aligned}$$

Taking $y = \begin{pmatrix}1 & t\\ 0 & 1\end{pmatrix}$ with $t \in \mathbf{Z}/p^n\mathbf{Z}$ and writing $x = \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$, we have $\mathrm{tr}(xy) = \mathrm{tr}(x) + \gamma t$. So summing over t, we get

$$\sum_{x\in B}\psi(\mathrm{tr}\,x)\psi'(\det x)\check{\xi}(x) = 0 \tag{26}$$

where B is the subgroup of upper-triangular matrices in $\mathrm{GL}_2(\mathbf{Z}/p^n\mathbf{Z})$. Multiplying similarly on the left by lower-triangular matrices, we get

$$\sum_{a,d\in(\mathbf{Z}/p^n\mathbf{Z})^\times} \psi(a+d)\psi'(ad)\xi\begin{pmatrix} a^{-1} & 0 \\ 0 & d^{-1}\end{pmatrix} = 0. \tag{27}$$

We now make use of the existence of a new vector for π. More precisely, let V be the space of ξ. By a result of Loeffler and Weinstein [10, Thm 3.6], there exists $v \in V - \{0\}$ which is fixed by all diagonal matrices of K. Evaluating (27) at $\xi\begin{pmatrix} 1 & b \\ 0 & 1\end{pmatrix} v$ with $b \in \mathbf{Z}/p^n\mathbf{Z}$, we get

$$\sum_{a,d\in(\mathbf{Z}/p^n\mathbf{Z})^\times} \psi(a+d)\psi'(ad)\xi\begin{pmatrix} 1 & a^{-1}db \\ 0 & 1\end{pmatrix} v = 0 \qquad (b \in \mathbf{Z}/p^n\mathbf{Z}). \tag{28}$$

We will need further results about ξ, for which we refer the reader to [10, Thm 3.6] and its proof. The restriction of ξ 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 n. Since Nv spans V, the components of v with respect to this decomposition are nonzero. In particular, taking the ψ-component of (28) yields

$$\sum_{a,d\in(\mathbf{Z}/p^n\mathbf{Z})^\times} \psi(a+d)\psi'(ad)\psi(a^{-1}db) = 0 \qquad (b \in \mathbf{Z}/p^n\mathbf{Z}). \tag{29}$$

We now distinguish according to the value of m.

First case : $m = n$. Taking $b = 0$ in (29), we have

$$\sum_{a,d\in(\mathbf{Z}/p^n\mathbf{Z})^\times} \psi(a+d)\psi'(ad) = 0. \tag{30}$$

Let $a_0 \in (\mathbf{Z}/p^n\mathbf{Z})^\times$ be the unique element such that $\psi'(a_0) = \bar{\psi}(1)$. Fixing $a \in (\mathbf{Z}/p^n\mathbf{Z})^\times$, we have

$$\sum_{d\in(\mathbf{Z}/p^n\mathbf{Z})^\times} \psi(a+d)\psi'(ad) = \begin{cases} p^{n-1}(p-1)\psi(a_0) & \text{if } a = a_0, \\ -p^{n-1}\psi(a) & \text{if } a \equiv a_0 \pmod{p^{n-1}} \text{ and } a \neq a_0, \\ 0 & \text{if } a \not\equiv a_0 \pmod{p^{n-1}}. \end{cases}$$

Now summing over a, we get

$$\begin{aligned} 0 &= p^{n-1}(p-1)\psi(a_0) - p^{n-1}\sum_{\substack{a\equiv a_0 \pmod{p^{n-1}} \\ a\neq a_0}} \psi(a) \\ &= p^n\psi(a_0) - p^{n-1}\sum_{a\equiv a_0 \pmod{p^{n-1}}} \psi(a). \end{aligned}$$

If $n = 1$ (resp. $n \geq 2$) then this equality reads $p\psi(a_0) + 1 = 0$ (resp. $p^n\psi(a_0) = 0$), which gives a contradiction.

Second case : $m < n$. Making the change of variables $d = ca$ in (29), we get

$$\sum_{a,c\in(\mathbf{Z}/p^n\mathbf{Z})^\times} \psi((1+c)a)\psi'(ca^2)\psi(cb) = 0. \tag{31}$$

Fix $a_0 \in (\mathbf{Z}/p^m\mathbf{Z})^\times$ and consider first the sum over all $a \in (\mathbf{Z}/p^n\mathbf{Z})^\times$ such that $a \equiv a_0 \ (p^m)$. It is zero except possibly when $1+c \equiv 0 \ (p^{n-m})$. Putting $c = -1 + kp^{n-m}$ with $k \in \mathbf{Z}/p^m\mathbf{Z}$, we get

$$\sum_{\substack{k\in\mathbf{Z}/p^m\mathbf{Z}\\ a_0\in(\mathbf{Z}/p^m\mathbf{Z})^\times\\ a\equiv a_0 \ (p^m)}} \psi(kp^{n-m}a)\psi'((-1+kp^{n-m})a^2)\psi((-1+kp^{n-m})b) = 0, \tag{32}$$

which simplifies to

$$\sum_{\substack{k\in\mathbf{Z}/p^m\mathbf{Z}\\ a_0\in(\mathbf{Z}/p^m\mathbf{Z})^\times}} \psi(kp^{n-m}(a_0+b))\psi'(-a_0^2)\psi'(kp^{n-m}a_0^2) = 0. \tag{33}$$

Let $u \in (\mathbf{Z}/p^m\mathbf{Z})^\times$ be the unique element such that $\psi'(1) = \psi(p^{n-m}u)$. The equality (33) can be rewritten

$$\sum_{a\in(\mathbf{Z}/p^m\mathbf{Z})^\times} \psi'(-a^2) \sum_{k\in\mathbf{Z}/p^m\mathbf{Z}} \psi(kp^{n-m}(a+b+p^{n-m}ua^2)) = 0. \tag{34}$$

Lemma 5.1. *The map* $h : (\mathbf{Z}/p^m\mathbf{Z})^\times \to (\mathbf{Z}/p^m\mathbf{Z})^\times$ *defined by* $h(a) = a + p^{n-m}ua^2$ *is a bijection.*

Proof. Let $a, a' \in (\mathbf{Z}/p^m\mathbf{Z})^\times$ such that $a + p^{n-m}ua^2 \equiv a' + p^{n-m}ua'^2 \ (p^m)$. In particular $a \equiv a' \ (p)$, and an easy induction gives $a \equiv a' \ (p^\ell)$ for every $1 \le \ell \le m$, so that $a = a'$. □

The inner sum over k in (34) vanishes except when $b = -h(a)$, in which case it is equal to p^m. Thus taking $b = -h(1)$, the equality (34) reads $p^m\psi'(-1) = 0$ by Lemma 5.1, a contradiction.

6. The ramified case

In this section we assume $v_p(N) = 2n+1$ with $n \ge 1$, so that $c = \begin{pmatrix} 0 & -p^{-n} \\ p^{1-n} & 0 \end{pmatrix}$. Note that $\psi(\mathrm{tr}(cx)) = \psi(p^{1-n}\,\mathrm{tr}'\,x)$ 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 n, m with $1 \le m \le n$, and we wish to prove that

$$T(\xi, \psi, \psi') := \sum_{x\in K_0/K_{2n}} \psi(\mathrm{tr}'\,x)\psi'(\det x)\check{\xi}(x) \tag{35}$$

is non-zero. Assume the contrary.

We have explicitly

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

Moreover, we have an isomorphism of groups

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

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

$$\sum_{x \in K_0/K_{2n}} \psi(\mathrm{tr}'(xy))\psi'(\det(xy))\check{\xi}(x) = 0. \tag{36}$$

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

$$\psi(\mathrm{tr}'(xy))\psi'(\det(xy)) = \psi(\mathrm{tr}'\, x)\psi'(\det x)\Phi_x(y) \qquad (y \in K_n) \tag{37}$$

is a character which depends only on the coset xK_n.

Lemma 6.1. *The characters $(\Phi_x)_{x \in K_0/K_n}$ are pairwise distinct.*

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

$$\Phi_x(y) = \psi(at + bv - cs - du)\psi'((ad - pbc)(s + v)). \tag{38}$$

Let $x' = \begin{pmatrix} a' & b' \\ pc' & d' \end{pmatrix} \in K_0$ such that $\Phi_x = \Phi_{x'}$. By (38), we already get $a, d \equiv a', d' \ (p^{\lceil \frac{n}{2} \rceil})$. Let $\lambda \in (\mathbf{Z}/p^m\mathbf{Z})^\times$ be the unique element such that $\psi'(1) = \psi(p^{n-m}\lambda)$. It remains to prove that the map

$$h_{a,d} : (\mathbf{Z}/p^{\lfloor \frac{n}{2} \rfloor}\mathbf{Z})^2 \to (\mathbf{Z}/p^{\lfloor \frac{n}{2} \rfloor}\mathbf{Z})^2 \tag{39}$$
$$(b, c) \mapsto (b + p^{n-m}\lambda(ad - pbc), -c + p^{n-m}\lambda(ad - pbc))$$

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

Fix $x_0 \in K_0$. If we multiply (36) by $\bar{\Phi}_{x_0}(y)$ and sum over $y \in K_n/K_{2n}$, we get

$$\sum_{y \in K_n/K_{2n}} \bar{\Phi}_{x_0}(y) \sum_{x \in K_0/K_{2n}} \psi(\mathrm{tr}'\, x)\psi'(\det x)\Phi_x(y)\check{\xi}(x) = 0. \tag{40}$$

According to Lemma 6.1, this simplifies to

$$\sum_{x \in x_0 K_n/K_{2n}} \psi(\mathrm{tr}'\, x)\psi'(\det x)\check{\xi}(x) = 0. \tag{41}$$

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

$$\sum_{y \in K_n/K_{2n}} \Phi_{x_0}(y)\check{\xi}(y) = 0. \tag{42}$$

Fix $a_0, d_0 \in (\mathbf{Z}/p^{\lceil \frac{n}{2} \rceil}\mathbf{Z})^\times$. We sum (42) over all matrices $x_0 \in K_0/K_n$ 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

$$\sum_{x_0} \Phi_{x_0}(y) = \sum_{b_0, c_0 \in \mathbf{Z}/p^{\lfloor \frac{n}{2} \rfloor}\mathbf{Z}} \psi(a_0 t + d_0 u)\psi(h_{a_0,d_0}(b_0, c_0) \cdot (v, s)) \tag{43}$$

where h_{a_0,d_0} is the map of (39). Since h_{a_0,d_0} is bijective, we get

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

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

$$\sum_{t,u \in p^{\lfloor \frac{n}{2} \rfloor}\mathbf{Z}/p^n\mathbf{Z}} \psi(a_0 t + d_0 u)\check{\xi}\begin{pmatrix} 1 & t \\ pu & 1 \end{pmatrix} = 0. \tag{44}$$

As in section 5, the restriction of ξ 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 n. Conjugating by the matrix $\begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix}$, the same is true for the restriction of ξ to $N' = \begin{pmatrix} 1 & 0 \\ p\mathbf{Z}_p & 1 \end{pmatrix}$. For any $t, u \in p^{\lfloor \frac{n}{2} \rfloor}\mathbf{Z}/p^n\mathbf{Z}$, 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 $\omega, \omega' : \mathbf{Z}/p^{\lceil \frac{n}{2} \rceil}\mathbf{Z} \to \mathbf{C}^\times$ such that

$$\check{\xi}\begin{pmatrix} 1 & p^{\lfloor \frac{n}{2} \rfloor}t \\ p^{\lfloor \frac{n}{2} \rfloor + 1}u & 1 \end{pmatrix} v = \omega(t)\omega'(u)v \qquad (t, u \in \mathbf{Z}/p^{\lceil \frac{n}{2} \rceil}\mathbf{Z}). \tag{45}$$

We may write the characters ω, ω' as $\omega(t) = \bar{\psi}(p^{\lfloor \frac{n}{2} \rfloor}a_0 t)$ and $\omega'(u) = \bar{\psi}(p^{\lfloor \frac{n}{2} \rfloor}d_0 u)$ for some $a_0, d_0 \in (\mathbf{Z}/p^{\lceil \frac{n}{2} \rceil}\mathbf{Z})^\times$. For this choice of a_0, d_0, the identity (44) evaluated at v gives a contradiction. This finishes the proof of Theorem 0.2.

7. Numerical investigations

We now report on the computations which led to Theorem 0.2. For all elliptic curves of conductor ≤ 2000, we computed the ramifications indices of the modular parametrizations at all cusps using Pari/GP [14]. Since we have no theoretical formula for the ramification index at a cusp in general, we just compared numerically $\log|f|$ and $\log|q|$ in the neighborhood of the given cusp. This method is of course 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 ≤ 200. We restrict to the cusps $\frac{1}{d}$ with $d^2|N$. In the last column, we indicate the minimal twist of the newform. Note that this 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".

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 ≤ 200

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 in the case N is odd. 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	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 (electronic).

[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 $\mathbf{Q}$", 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] G. Stevens – *Arithmetic on modular curves*, Progress in Mathematics, vol. 20, Birkhäuser Boston Inc., Boston, MA, 1982.
[14] The PARI Group – Bordeaux, *PARI/GP, version* `2.5.0`, 2011, available from `http://pari.math.u-bordeaux.fr/`.

E-mail address: `francois.brunault@ens-lyon.fr`

ÉNS Lyon, Unité de mathématiques pures et appliquées, 46 allée d'Italie, 69007 Lyon, France