EXPLICIT REDUCTION MODULO p OF CERTAIN 2-DIMENSIONAL CRYSTALLINE REPRESENTATIONS, II

KEVIN BUZZARD AND TOBY GEE

Abstract. We complete the calculations begun in [BG09], using the p-adic local Langlands correspondence for $\mathrm{GL}_2(\mathbb{Q}_p)$ to give a complete description of the reduction modulo p of the 2-dimensional crystalline representations of $G_{\mathbb{Q}_p}$ of slope less than 1, when $p > 2$.

1. Introduction

This paper is a sequel to [BG09], and we refer the reader to the introduction to that paper for a detailed discussion of (and the motivation for) the problem solved in this paper. Another good reference is §5.2 of [Ber11]. Let p be a prime, choose an algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$, let $\overline{\mathbb{Z}}_p$ be the integers in $\overline{\mathbb{Q}}_p$ and let $\overline{\mathbb{F}}_p$ be the residue field of $\overline{\mathbb{Z}}_p$. We let v be the p-adic valuation on $\overline{\mathbb{Q}}_p^\times$, normalised so that $v(p) = 1$. We set $v(0) = +\infty$. We decree that the cyclotomic character has Hodge–Tate weight $+1$. We recall that given a positive integer $k \geq 2$ and an element $a \in \overline{\mathbb{Q}}_p$ with $v(a) > 0$ there is a uniquely determined two-dimensional crystalline representation $V_{k,a}$ of $\mathrm{Gal}\,(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ with Hodge–Tate weights 0 and $k-1$, determinant the cyclotomic character to the power of $k-1$, and with the characteristic polynomial of crystalline Frobenius on the contravariant Dieudonne module being $X^2 - aX + p^{k-1}$ (see for example §3.1 of [Bre03] for a detailed construction of this representation). Let $\overline{V}_{k,a}$ denote the semisimplification of the reduction of $V_{k,a}$ modulo the maximal ideal of $\overline{\mathbb{Z}}_p$. Let ω denote the mod p cyclotomic character, and if $p+1 \nmid n$ let $\mathrm{ind}(\omega_2^n)$ denote the unique irreducible 2-dimensional representation of $G_{\mathbb{Q}_p}$ with determinant ω^n and with restriction to inertia equal to $\omega_2^n \oplus \omega_2^{pn}$, with ω_2 the "niveau 2" character of inertia (see for example §1.1 of [Ber11]).

Our main result is the following, which is an immediate consequence of Theorem 1.6 of [BG09] (the case $k \not\equiv 3 \bmod p-1$), Theorem 3.2.1 of [Ber10] (the cases $k = 3$ and $k = p+2$), and Corollary 4.7 below. Recall $k \geq 2$; let $[k-2]$ denote denote the integer in the set $\{0, 1, \ldots, p-2\}$ congruent to $k-2 \bmod p-1$, and set $t = [k-2]+1$, so $1 \leq t \leq p-1$.

Theorem A. *Assume that $p > 2$ and that $0 < v(a) < 1$. Then $\overline{V}_{k,a} \cong \mathrm{ind}(\omega_2^t)$ is irreducible, unless $k > 3$, $k \equiv 3 \pmod{p-1}$, and $v(k-3)+1+v(a) \leq v(a^2-(k-2)p)$, in which case $\omega^{-1} \otimes \overline{V}_{k,a}$ is unramified, and the trace of a geometric Frobenius Frob_p on $\omega^{-1} \otimes \overline{V}_{k,a}$ is $\overline{\tau}$, where $\tau = \frac{(k-2)p-a^2}{ap(k-3)}$.*

Note that when $k \equiv 3 \pmod{p-1}$ and $v(k-3)+1+v(a) \leq v(a^2-(k-2)p)$, the τ in the theorem is in $\overline{\mathbb{Z}}_p$, and its reduction is also the trace of an arithmetic Frobenius, because $\omega^{-1} \otimes \overline{V}_{k,a}$ has trivial determinant in this case.

2000 *Mathematics Subject Classification.* 11F33.

For a fixed k one can look at the behaviour of the representation $V_{k,a}$ as a varies through the annulus $0 < |a| < 1$, and we can give a more prosaic description of what our theorem says: it says that often $V_{k,a} = \mathrm{ind}(\omega_2)$ is constant on this annulus, the only exception being when $k > 3$, $k \equiv 3 \bmod p-1$ and $k \not\equiv 2 \bmod p$, in which case the representation is $\mathrm{ind}(\omega_2)$ everywhere other than two small closed discs with centre $\pm\sqrt{(k-2)p}$ and radius $p^{-1-v(k-3)}$. Note that both these small discs are contained in the annulus $v(a) = 1/2$, and that as $k > 3$ tends to 3 p-adically the radius of the discs tends to zero. Note also that the limit of $\pm\sqrt{(k-2)p}$ as $k > 3$ tends to 3 p-adically is $\pm\sqrt{p}$, however $a = \pm\sqrt{p}$ is not in any of the discs; furthermore the intersection of all these discs as k varies is empty, and in particular our result does not contradict the local constancy results of [Ber12], contrary to one's initial reaction.

This theorem was proved in the case $k \not\equiv 3 \pmod{p-1}$ in [BG09] using the p-adic local Langlands correspondence for $\mathrm{GL}_2(\mathbb{Q}_p)$. In the present paper we build on the results and methods of [BG09] to handle the case $k \equiv 3 \pmod{p-1}$; as one might expect from the statement of the theorem, the necessary calculations are more complicated in this case, because we have to control what is going on modulo an arbitrarily large power of p in the auxiliary calculations.

We would like to thank Christophe Breuil for sharing with us the details of his unpublished calculations for $k = 2p+1$, which were the starting point for this article. We would also like to thank Mathieu Vienney for pointing out a howler of a typo in the statement of the main theorem in an earlier version of this paper, and John Enns for pointing out another typo later in the paper. We would also like to thank the anonymous referee for a careful reading, and several helpful corrections and improvements.

1.1. **Notation.** Throughout the paper, p denotes an odd prime, and r and n are integers. If $\lambda \in \mathbb{F}_p$, we write $[\lambda] \in \mathbb{Z}_p$ for its Teichmueller lift.

2. Combinatorial Lemmas

In this section we prove some elementary lemmas about congruences of binomial coefficients, that we will make repeated use of in the rest of the paper.

Lemma 2.1. *Assume that $p > 2$ and that $r \in \mathbb{Z}_{\geq 2}$, and write $t = v(r-1) \geq 0$. Then*

(1) *for all integers $n \geq 2$ we have $v\left(\binom{r}{n}\right) + n \geq t+2$, and*
(2) *for all integers $n \geq 1$, $v\left(\binom{r-1}{n}\right) + n \geq t+1$.*

Proof. (1) The left hand side is $v(r(r-1)(r-2)\cdots(r-(n-1))) - v(n!) + n$ which is at least $v(r-1) - v(n!) + n = t + n - v(n!)$. If $n = 2$ then the result holds as $p > 2$. If $n \geq 3$ then we need to check $n - v(n!) \geq 2$ but this is clear because $v(n!) \leq n/(p-1)$ and hence $n - v(n!) \geq n(p-2)/(p-1) \geq 3(p-2)/(p-1)$, and it is enough to prove that $\lceil 3(p-2)/(p-1) \rceil \geq 2$, which is true (by an explicit check for $p = 3$ and true even without the $\lceil\cdot\rceil$ for $p \geq 5$).

(2) The left hand side is $v((r-1)(r-2)\cdots(r-n)) - v(n!) + n \geq v(r-1) - v(n!) + n = t + n - v(n!)$. Again, $v(n!) \leq n/(p-1)$, and hence the left hand side is at least $t + n(p-2)/(p-1)$. Now the result is true for $n = 1$ so it suffices to prove that $\lceil 2(p-2)/(p-1) \rceil \geq 1$, which follows as $p > 2$.

∎

Lemma 2.2. *Assume that $p > 2$ and that $r > 1$, and write $t = v(r-1) \geq 0$. Assume that $r \equiv 1 \pmod{p-1}$. Then $r \geq t+3$.*

Proof. $r - 1 \geq (p-1)p^t \geq 2 \cdot 3^t \geq t+2$ by easy induction. □

Lemma 2.3. *Assume that $p > 2$ and $r > 1$, and that $r \equiv 1 \pmod{p-1}$. Write $t = v(r-1) \geq 0$. If $\mu \in \mathbb{F}_p$, then $(-[\mu]x + py)^r - x^{r-1}(-[\mu]x + py)$ is congruent modulo $p^{t+2}\overline{\mathbb{Z}}_p[x,y]$ to*

$$-px^{r-1}y$$

if $\mu = 0$, and to

$$(r-1)px^{r-1}y$$

if $\mu \neq 0$.

Proof. If $\mu = 0$ then we just need to check that $r \geq t+2$, which follows from Lemma 2.2.

If however $\mu \neq 0$ then we expand via the binomial theorem and use part Lemma 2.1(1) (and the fact that $(p-1)|(r-1)$, so $[\mu]^{r-1} = 1$) to get that modulo p^{t+2} we have

$$\begin{aligned}
&(-[\mu]x + py)^r - x^{r-1}(-[\mu]x + py) \\
&\equiv -[\mu]x^r + rpx^{r-1}y + [\mu]x^r - x^{r-1}py \\
&\equiv (r-1)px^{r-1}y,
\end{aligned}$$

as required. □

Lemma 2.4. *If $p > 2$ and $r > 1$ with $r \equiv 1 \pmod{p-1}$, and if $t = v(r-1)$, then*

(1) $\sum_{\mu \in \mathbb{F}_p} (1 + [\mu])^r \equiv rp \pmod{p^{t+2}}$, *and*
(2) $\sum_{\mu \in \mathbb{F}_p} (1 + [\mu])^{r-1} \equiv p - 1 \pmod{p^{t+1}}$.

Proof. (1) We rewrite $(1+[\mu])^r$ as $([1+\mu] + (1+[\mu]-[1+\mu]))^r$ and expand using the binomial theorem. Since $(1+[\mu]-[1+\mu])$ is divisible by p, by Lemma 2.1(1) we only need to look at the first two terms in the binomial expansion to compute it modulo p^{t+2}, and we see that the sum is congruent modulo p^{t+2} to

$$\sum_{\mu \in \mathbb{F}_p} \left([1+\mu]^r + r[1+\mu]^{r-1}(1+[\mu]-[1+\mu])\right).$$

Since $r \equiv 1 \pmod{p-1}$, we have $\sum_{\mu \in \mathbb{F}_p} [1+\mu]^r = \sum_{\mu \in \mathbb{F}_p} [\mu] = 0$, and since $[1+\mu]^{r-1} = 1$ unless $\mu = -1$, and if $\mu = -1$ then $1 + [\mu] - [1+\mu] = 0$, the sum is congruent modulo p^{t+2} to

$$\begin{aligned}
\sum_{\mu} r[1+\mu]^{r-1}(1+[\mu]-[1+\mu]) &= r \sum_{\mu \neq -1} (1+[\mu]-[1+\mu]) \\
&= r \sum_{\mu} (1+[\mu]-[1+\mu]) \\
&= r \sum_{\mu} 1 = rp
\end{aligned}$$

and we are done.

(2) We do the same trick using Lemma 2.1(2), which implies that we only have to look at the first term of the binomial expansion. Modulo p^{t+1} we have

$$\begin{aligned}\sum_\mu (1+[\mu])^{r-1} &= \sum_\mu ([1+\mu] + (1+[\mu]-[1+\mu]))^{r-1} \\ &\equiv \sum_\mu [1+\mu]^{r-1} \\ &= p-1,\end{aligned}$$

as required. □

Corollary 2.5. *If $p>2$ and $r>1$ with $r\equiv 1 \pmod{p-1}$, and if $t=v(r-1)$, then for all $\lambda\in\mathbb{F}_p$ we have*

(1) $\sum_{\mu\in\mathbb{F}_p}([\mu]-[\lambda])^r \equiv -[\lambda]rp \pmod{p^{t+2}}$, *and*
(2) $\sum_{\mu\in\mathbb{F}_p}([\mu]-[\lambda])^{r-1} \equiv p-1 \pmod{p^{t+1}}$.

Proof. If $\lambda=0$ then both statements are obvious. If $\lambda\neq 0$ then we simply take out a factor of $(-[\lambda])^r$ (resp. $(-[\lambda])^{r-1}$) and observe that as $[\mu]$ runs over the Teichmueller lifts, so does $-[\mu]/[\lambda]$. This reduces both claims to the case $\lambda=-1$, which is Lemma 2.4. □

Corollary 2.6. *If $p>2$ and $r>1$ with $r\equiv 1 \pmod{p-1}$, and if $t=v(r-1)$, then for all $\lambda\in\mathbb{F}_p$ we have*

$$\sum_{\mu\in\mathbb{F}_p}([\mu]x-[\lambda]x+py)^r \equiv -[\lambda]rpx^r + rp(p-1)x^{r-1}y \pmod{p^{t+2}\overline{\mathbb{Z}}_p[x,y]}.$$

Proof. Again by Lemma 2.1(1), in order to compute modulo p^{t+2} we only need to expand out the first two terms of $(([\mu]x-[\lambda]x)+py)^r$, giving that the sum is congruent to

$$\sum_{\mu\in\mathbb{F}_p}\left(([\mu]x-[\lambda]x)^r + rp([\mu]x-[\lambda]x)^{r-1}y\right).$$

The result then follows from Corollary 2.5. □

3. p-adic local Langlands: definitions and lemmas

In this section we recall some of the basic definitions and properties of the p-adic local Langlands correspondence. For more details the reader could consult section 2 of [BG09] or any of the references therein.

Say $r\in\mathbb{Z}_{\geq 0}$. Let K be the group $\mathrm{GL}_2(\mathbb{Z}_p)$, and for R a $\mathbb{Z}_p$-algebra let $\mathrm{Symm}^r(R^2)$ denote the space $\oplus_{i=0}^r Rx^{r-i}y^i$ of homogeneous polynomials in two variables x and y, with the action of K given by

$$\begin{pmatrix} a & b \\ c & d\end{pmatrix} x^{r-i}y^i = (ax+cy)^{r-i}(bx+dy)^i,$$

so $(\kappa v)(x,y)=v((x,y)\kappa)$. Set $G=\mathrm{GL}_2(\mathbb{Q}_p)$, and let Z be its centre. If V is an R-module with an action of K, then extend the action of K to the group KZ by letting $\left(\begin{smallmatrix} p & 0 \\ 0 & p\end{smallmatrix}\right)$ act trivially, and let $I(V)$ denote the representation $\mathrm{ind}_{KZ}^G(V)$ (compact induction). Explicitly, $I(V)$ is the space of functions $f:G\to V$ which have compact support modulo Z and which satisfy $f(\kappa g)=\kappa(f(g))$ for all $\kappa\in KZ$. This space has a natural action of G, defined by $(gf)(\gamma):=f(\gamma g)$. Note that §2.2 of [BL94] explains that to give an R-linear G-endomorphism of $I(V)$ is to give a certain compactly-supported function $\phi : G \to \mathrm{End}_R(V)$ such that $\phi(\kappa g \kappa') = \kappa \circ g \circ \kappa'$ for $g \in G$, $\kappa \in KZ$, $\kappa' \in KZ$ (by Frobenius reciprocity).

If $V = \mathrm{Symm}^r(R^2)$ for some integer $r \geq 0$ and $\mathbb{Z}_p$-algebra R, then there is a certain endomorphism T of $I(V)$ which corresponds to the function $G \to \mathrm{End}_R(V)$ which is supported on $KZ\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)KZ$ and sends $\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$ to the endomorphism of $\mathrm{Symm}^r(R^2)$ sending $F(x,y)$ to $F(px,y)$. Slightly more generally, if V is the representation $\det^s \otimes \mathrm{Symm}^r(R^2)$ of K then we can extend V to a representation of KZ, note that $I(V) = (\omega \circ \det^s) \otimes I(\mathrm{Symm}^r(R^2))$ and we define T on $I(V)$ via its action on $I(\mathrm{Symm}^r(R^2))$. Here $\omega : \mathbb{Q}_p^\times \to \mathbb{Z}_p^\times$ is the identity on $\mathbb{Z}_p^\times$ and sends p to 1.

We now establish some notation, following [Bre03]. Recall that for V a $\mathbb{Z}_p[K]$-module, the space $I(V)$ was defined previously to be a certain space of functions $G \to V$. We let $[g,v]$ denote the (unique) element of $I(V)$ which is supported on KZg^{-1}, and which satisfies $[g,v](g^{-1}) = v$. One can check that $[g,v]$ corresponds to $g \otimes v$ if we identify $I(V)$ with $R[G] \otimes_{R[KZ]} V$. Note that $g[h,v] = [gh,v]$ for $g,h \in G$, that $[g\kappa, v] = [g, \kappa v]$ for $\kappa \in KZ$, and that the $[g,v]$ span $I(V)$ as an abelian group, as g and v vary.

Now let $V = \mathrm{Symm}^r(R^2)$ for some $\mathbb{Z}_p$-algebra R. An easy consequence of the definition of T (cf. section 2 of [Bre03]) is that

$$T[g,v] = \sum_{\lambda \in \mathbb{F}_p} \left[g\left(\begin{smallmatrix} p & [\lambda] \\ 0 & 1 \end{smallmatrix}\right), v(x, -[\lambda]x + py)\right] + \left[g\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right), v(px,y)\right]. \tag{☎}$$

Again we assume that $r \geq p$ and $r \equiv 1 \bmod p-1$. By Lemma 3.2 of [AS86], there is a $\mathrm{GL}_2(\mathbb{F}_p)$-equivariant surjection $\Psi : \mathrm{Symm}^r \overline{\mathbb{F}}_p^2 \to \det \otimes \mathrm{Symm}^{p-2} \overline{\mathbb{F}}_p^2$, such that (using X, Y for variables in Symm^{p-2})

$$\Psi(f) = \sum_{s,t \in \mathbb{F}_p} f(s,t)(tX - sY)^{p-2}.$$

We now move on to the p-adic part of the story. Say $k \in \mathbb{Z}_{\geq 2}$ and $a \in \overline{\mathbb{Z}}_p$ with $v(a) > 0$.

Definition 3.1. Let $\Pi_{k,a} := \mathrm{ind}_{KZ}^G \mathrm{Symm}^{k-2}(\overline{\mathbb{Q}}_p^2)/(T-a)$ (compact induction, as before), and let $\Theta_{k,a}$ be the image of $\mathrm{ind}_{KZ}^G \mathrm{Symm}^{k-2}(\overline{\mathbb{Z}}_p^2)$ in $\Pi_{k,a}$.

If $a \neq \pm p^{k/2}(1+p^{-1})$ then we claim that $\Pi_{k,a}$ is irreducible and $\Theta_{k,a}$ is a lattice in it. Indeed, irreducibility of $\Pi_{k,a}$ is proved in Proposition 3.2.1(i) of [Bre03], the existence of a G-stable lattice is proved in Corollaire 5.3.4 of [BB10], and now the fact that $\Theta_{k,a}$ is a lattice follows from the fact that it is finitely-generated as a $\overline{\mathbb{Z}}_p[G]$-module (hence contained in a lattice) and visibly spans $\Pi_{k,a}$. Because of Theorem 3.2.1 of [Ber10] (which deals with $k = 3$ and $k = p+2$), and Theorem 1.6 of [BG09] and the comments following it (which deal with $k \not\equiv 3 \bmod p-1$), we are only really concerned in this paper in the case $k \geq 2p+1$, $k \equiv 3 \bmod p-1$ and $0 < v(a) < 1$, which implies $a \neq \pm(1+p^{-1})p^{k/2}$ anyway. So let us assume $k \geq 2p+1$ and $k \equiv 3 \bmod p-1$. To simplify notation set $r = k-2$, so $r \equiv 1 \bmod p-1$. Now by Corollary 5.1 of [BG09], the natural surjection $I(\mathrm{Symm}^r \overline{\mathbb{F}}_p^2) \to \overline{\Theta}_{k,a}$ factors through the map $I(\mathrm{Symm}^r \overline{\mathbb{F}}_p^2) \to I(\det \otimes \mathrm{Symm}^{p-2} \overline{\mathbb{F}}_p^2)$ induced by Ψ. The key input we need from the p-adic local Langlands correspondence is the following lemma.

Lemma 3.2. *Assume $k \geq 2p+1$, $k \equiv 3$ mod $p-1$, and $0 < v(a) < 1$.*

(1) *If* $\overline{\Theta}_{k,a}$ *is a quotient of* $I(\det\otimes\mathrm{Symm}^{p-2}\overline{\mathbb{F}}_p^2)/T$*, then* $\overline{V}_{k,a}\cong\mathrm{ind}(\omega_2^2)$ *is irreducible.*
(2) *If* $\overline{\Theta}_{k,a}$ *is a quotient of* $I(\det\otimes\mathrm{Symm}^{p-2}\overline{\mathbb{F}}_p^2)/(T^2-cT+1)$ *for some* $c\in\overline{\mathbb{F}}_p$*, then* $\overline{V}_{k,a}$ *is reducible, and* $\omega^{-1}\otimes\overline{V}_{k,a}$ *is an unramified reducible representation, and the trace of (both arithmetic and geometric)* Frob_p *is* c*.*

Proof. This may be proved in exactly the same way as Proposition 3.3 of [BG09]. Note that both arithmetic and geometric Frobenius have the same trace in case (2), because $\omega^{-1}\otimes\overline{V}_{k,a}$ has trivial determinant (as $k\equiv 3 \bmod p-1$). □

4. Computations with Hecke operators

We again assume throughout this section that $p>2$ is an odd prime and $r>p$ is an integer such that $r\equiv 1 \pmod{p-1}$. We start with a couple of results about the map $\Psi:\mathrm{Symm}^r(\overline{\mathbb{F}}_p^2)\to\det\otimes\mathrm{Symm}^{p-2}(\overline{\mathbb{F}}_p^2)$ defined in the previous section.

Lemma 4.1. (1) $\Psi(y^r)=0$.
(2) $\Psi(x^r)=0$.
(3) $\Psi(x^{r-1}y)=X^{p-2}$.

Proof. $\Psi(y^r)=\sum_{s,t\in\mathbb{F}_p}t^r(tX-sY)^{p-2}=\sum_{s,t\in\mathbb{F}_p}t(tX-sY)^{p-2}$. Expanding out using the binomial theorem and using the fact that $\sum_s s^n=0$ for $n=0,1,2,\dots,p-2$, this sum is zero. Since Ψ is $\mathrm{GL}_2(\mathbb{F}_p)$-equivariant, $\Psi(x^r)$ is also zero.

Since $r\equiv 1 \pmod{p-1}$, we have

$$\begin{aligned}\Psi(x^{r-1}y) &= \sum_{s,t\in\mathbb{F}_p} s^{p-1}t(tX-sY)^{p-2}\\ &= \sum_{s\neq 0,t\in\mathbb{F}_p} t(tX-sY)^{p-2}\end{aligned}$$

and $\sum_{s\neq 0}s^n$ is not zero if $n=0$ (although it is for $1\le n\le p-2$ as before) so expanding out we get $-\sum_{t\in\mathbb{F}_p}t(tX)^{p-2}$ which is $-\sum_{t\neq 0}X^{p-2}=X^{p-2}$. □

Lemma 4.2. *In* $I(\mathrm{Symm}^{p-2}(\overline{\mathbb{F}}_p^2))$ *we have*
(1) $T[1,X^{p-2}]=\sum_{\mu\in\mathbb{F}_p}[\left(\begin{smallmatrix}p&[\mu]\\0&1\end{smallmatrix}\right),X^{p-2}]$, *and*
(2) $T^2[1,X^{p-2}]=\sum_{\lambda,\mu\in\mathbb{F}_p}[\left(\begin{smallmatrix}p^2&p[\mu]+[\lambda]\\0&1\end{smallmatrix}\right),X^{p-2}]$.

Proof. This is immediate from (☎). □

Lemma 4.3. *Assume that* $p>2$ *and that* $r>p$ *with* $r\equiv 1 \pmod{p-1}$*. Set* $t=v(r-1)$ *and suppose* $a\in\overline{\mathbb{Q}}_p$ *with* $v(a)>0$*. Then*

$$\begin{aligned}(T-a)[g,y^r-x^{r-1}y] \equiv{}& [g\left(\begin{smallmatrix}p&0\\0&1\end{smallmatrix}\right),-px^{r-1}y]\\ &+\sum_{\lambda\neq 0}[g\left(\begin{smallmatrix}p&\lambda\\0&1\end{smallmatrix}\right),(r-1)px^{r-1}y]+[g\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right),y^r]-[g,a(y^r-x^{r-1}y)]\end{aligned}$$

modulo $p^{t+2}I(\mathrm{Symm}^r(\overline{\mathbb{Z}}_p^2))$*.*

Proof. This is immediate from (☎) and Lemma 2.3. □

We have $t = v(r-1)$; say $a \in \overline{\mathbb{Q}}_p$ satisfies $0 < v(a) < 1$, and set $t_0 = \min\{t + 1 + v(a), v(a^2 - rp)\}$.

Lemma 4.4. *Assume that $p > 2$ and that $r > p$ with $r \equiv 1 \pmod{p-1}$. If $\varphi_g = \sum_{j=0}^{N} [g\left(\begin{smallmatrix} p^j & 0 \\ 0 & 1 \end{smallmatrix}\right), a^j(y^r - x^{r-1}y)]$ where $N > t_0/v(a)$, then in $I(\mathrm{Symm}^r(\overline{\mathbb{Z}}_p^2))$ we have*

$$(T-a)\varphi_g \equiv \sum_{\lambda \in \mathbb{F}_p} [g\left(\begin{smallmatrix} p & [\lambda] \\ 0 & 1 \end{smallmatrix}\right), (r-1)px^{r-1}y] + [g\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right), y^r] + [g, ax^{r-1}y] \pmod{p^{t_0}}.$$

Proof. Throughout the proof we will write $\sum_{j \geq 0}$ rather than keeping track of the upper index of our sums, as the implied terms will all be zero modulo p^{t_0}. Since $t + 2 > t + 1 + v(a) \geq t_0$, we can apply Lemma 4.3. Noting that if $j \geq 1$, $v(a^j(r-1)p) \geq t + 1 + v(a) \geq t_0$, we see that modulo p^{t_0}, $(T-a)\varphi_g$ is just

$$\begin{aligned}
&[g\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right), -px^{r-1}y] + \sum_{\lambda \neq 0} [g\left(\begin{smallmatrix} p & [\lambda] \\ 0 & 1 \end{smallmatrix}\right), (r-1)px^{r-1}y] + [g\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right), y^r] - [g, a(y^r - x^{r-1}y)] \\
&+ \sum_{j \geq 1} [g\left(\begin{smallmatrix} p^{j+1} & 0 \\ 0 & 1 \end{smallmatrix}\right), -pa^j x^{r-1}y] \\
&+ \sum_{j \geq 1} [g\left(\begin{smallmatrix} p^{j-1} & 0 \\ 0 & 1 \end{smallmatrix}\right), a^j y^r] \\
&+ \sum_{j \geq 1} [g\left(\begin{smallmatrix} p^{j} & 0 \\ 0 & 1 \end{smallmatrix}\right), -a^{j+1} y^r + a^{j+1}x^{r-1}y]
\end{aligned}$$

which rearranges to

$$\begin{aligned}
&\sum_{\lambda \neq 0} [g\left(\begin{smallmatrix} p & [\lambda] \\ 0 & 1 \end{smallmatrix}\right), (r-1)px^{r-1}y] \\
&+ [g\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right), y^r] + [g, ax^{r-1}y] \\
&+ \sum_{s \geq 1} [g\left(\begin{smallmatrix} p^{s} & 0 \\ 0 & 1 \end{smallmatrix}\right), -pa^{s-1}x^{r-1}y] \\
&+ \sum_{s \geq 1} [g\left(\begin{smallmatrix} p^{s} & 0 \\ 0 & 1 \end{smallmatrix}\right), a^{s+1}y^r] \\
&+ \sum_{s \geq 1} [g\left(\begin{smallmatrix} p^{s} & 0 \\ 0 & 1 \end{smallmatrix}\right), -a^{s+1}y^r + a^{s+1}x^{r-1}y]
\end{aligned}$$

where we have changed variables from j to s to make all the sums involve $g\left(\begin{smallmatrix} p^s & 0 \\ 0 & 1 \end{smallmatrix}\right)$, and put two of the "initial" terms into the sums. Pressing on, we get two terms in the sums cancelling and we are left with

$$\begin{aligned}
&\sum_{\lambda \neq 0} [g\left(\begin{smallmatrix} p & [\lambda] \\ 0 & 1 \end{smallmatrix}\right), (r-1)px^{r-1}y] \\
&+ [g\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right), y^r] + [g, ax^{r-1}y] \\
&+ \sum_{s \geq 1} [g\left(\begin{smallmatrix} p^{s} & 0 \\ 0 & 1 \end{smallmatrix}\right), a^{s-1}(a^2 - p)x^{r-1}y]
\end{aligned}$$

By the definition of t_0 we have $ap(r-1) \equiv 0 \pmod{p^{t_0}}$ and $a^2 - rp \equiv 0 \pmod{p^{t_0}}$, so we see that if $s \geq 2$ we have $a^{s-1}(a^2 - p) \equiv a^{s-2}(a(a^2 - rp) + ap(r-1)) \equiv 0$

(mod p^{t_0}). Thus we can simplify further to

$$\begin{aligned}&\sum_{\lambda\neq 0}[g\left(\begin{smallmatrix}p & [\lambda]\\ 0 & 1\end{smallmatrix}\right),(r-1)px^{r-1}y]\\&+[g\left(\begin{smallmatrix}1 & 0\\ 0 & p\end{smallmatrix}\right),y^r]+[g,ax^{r-1}y]\\&+[g\left(\begin{smallmatrix}p & 0\\ 0 & 1\end{smallmatrix}\right),(a^2-p)x^{r-1}y].\end{aligned}$$

Finally, since $a^2\equiv rp \pmod{p^{t_0}}$, the last term can be inserted into the sum by allowing $\lambda=0$. □

Lemma 4.5. *Assume that $p>2$ and that $r>p$ with $r\equiv 1 \pmod{p-1}$. If*

$$\varphi=-p\varphi_1+\sum_{\mu\in\mathbb{F}_p}a\varphi_{\left(\begin{smallmatrix}p & [\mu]\\ 0 & 1\end{smallmatrix}\right)}+[1,\sum_{\mu\in\mathbb{F}_p}([\mu]x+y)^r-rpx^{r-1}y]$$

(where φ_g is as in the statement of Lemma 4.4), and if $t_1=t_0+\min\{v(a),1-v(a)\}>t_0$, then

$$\begin{aligned}(T-a)\varphi\equiv&\sum_{\lambda,\mu\in\mathbb{F}_p}[\left(\begin{smallmatrix}p^2 & p[\lambda]+[\mu]\\ 0 & 1\end{smallmatrix}\right),a(r-1)px^{r-1}y]\\&+[1,ap(r-1)x^{r-1}y]\\&+\sum_{\lambda\in\mathbb{F}_p}[\left(\begin{smallmatrix}p & [\lambda]\\ 0 & 1\end{smallmatrix}\right),(a^2-rp)x^{r-1}y] \pmod{p^{t_1}}.\end{aligned}$$

Proof. First we note that $t+2\geq t_1$ (because $t+2=t+1+v(a)+(1-v(a))\geq t_0+(1-v(a))\geq t_1$). By Lemma 2.2 we have $r\geq t+3$ and hence $r\geq t_1+1>t_1$, so $p^r\equiv 0 \pmod{p^{t_1}}$. We also see from Lemma 2.1 and the inequality $r-1\geq t_1$ that

$$\sum_{\mu\in\mathbb{F}_p}([\mu]px+y)^r\equiv py^r \pmod{p^{t_1}}.$$

Using these facts and Lemma 4.4 (for the first two terms in the definition of φ) and (☎) (for the final term), we see that modulo p^{t_1}, we have

$$\begin{aligned}(T-a)\varphi\equiv&\left[\left(\begin{smallmatrix}1 & 0\\ 0 & p\end{smallmatrix}\right),-py^r\right]+\left[1,-pax^{r-1}y\right]\\&+[1,a\sum_{\mu\in\mathbb{F}_p}([\mu]x+y)^r]+\sum_{\mu\in\mathbb{F}_p}\left[\left(\begin{smallmatrix}p & [\mu]\\ 0 & 1\end{smallmatrix}\right),a^2x^{r-1}y\right]\\&+\sum_{\lambda,\mu\in\mathbb{F}_p}\left[\left(\begin{smallmatrix}p^2 & p[\lambda]+[\mu]\\ 0 & 1\end{smallmatrix}\right),a(r-1)px^{r-1}y\right]\\&+[1,-a\sum_{\lambda\in\mathbb{F}_p}([\lambda]x+y)^r+arpx^{r-1}y]\\&+\sum_{\lambda\in\mathbb{F}_p}\left[\left(\begin{smallmatrix}p & [\lambda]\\ 0 & 1\end{smallmatrix}\right),\left(\sum_{\mu\in\mathbb{F}_p}([\mu]x-[\lambda]x+py)^r\right)-rpx^{r-1}(-[\lambda]x+py)\right]+[\left(\begin{smallmatrix}1 & 0\\ 0 & p\end{smallmatrix}\right),py^r].\end{aligned}$$

Now some terms cancel, and we get

$$\sum_{\lambda,\mu\in\mathbb{F}_p}[\left(\begin{smallmatrix} p^2 & p[\lambda]+[\mu] \\ 0 & 1\end{smallmatrix}\right), a(r-1)px^{r-1}y]$$
$$+[1, ap(r-1)x^{r-1}y]$$
$$+\sum_{\lambda\in\mathbb{F}_p}\left[\left(\begin{smallmatrix} p & [\lambda] \\ 0 & 1\end{smallmatrix}\right), \left(\sum_{\mu\in\mathbb{F}_p}([\mu]x-[\lambda]x+py)^r\right)+a^2x^{r-1}y-rpx^{r-1}(-[\lambda]x+py)\right].$$

Again noting that $t+2\geq t_1$, by Corollary 2.6 we have

$$\sum_{\mu\in\mathbb{F}_p}([\mu]x-[\lambda]x+py)^r\equiv -[\lambda]rpx^r+rp(p-1)x^{r-1}y \pmod{p^{t_1}},$$

and the result follows. □

Corollary 4.6. *Assume that $p>2$ and that $r>p$ with $r\equiv 1 \pmod{p-1}$, and that $0<v(a)<1$.*

(1) *If $v(r-1)+1+v(a)>v(a^2-rp)$, then $\overline{\Theta}_{k,a}$ is a quotient of $I(\det\otimes\mathrm{Symm}^{p-2}\overline{\mathbb{F}}_p^2)/T$.*
(2) *If $v(r-1)+1+v(a)\leq v(a^2-rp)$, then $\overline{\Theta}_{k,a}$ is a quotient of $I(\det\otimes\mathrm{Symm}^{p-2}\overline{\mathbb{F}}_p^2)/(T^2-\overline{\tau}T+1)$ where $\tau=\frac{rp-a^2}{ap(r-1)}$.*

Proof. Set $\psi=p^{-t_0}\varphi$, with φ as in Lemma 4.5. By the definition of t_0, we see that both $v(a(r-1)p)$, and $v(a^2-rp)$ are at least t_0, so that $(T-a)\psi$ is integral, by Lemma 4.5. Thus $\overline{(T-a)\psi}$ is in the kernel of the natural map $I(\mathrm{Symm}^r\overline{\mathbb{F}}_p^2)\twoheadrightarrow\overline{\Theta}_{k,a}$. We will now compute $\Psi(\overline{(T-a)\psi})$ in both cases, and hence deduce the claim.

(1) If $v(r-1)+1+v(a)>v(a^2-rp)$, then we see from Lemma 4.5 that $\overline{(T-a)\psi}$ is a unit times $\sum_{\lambda\in\mathbb{F}_p}[\left(\begin{smallmatrix} p & [\lambda] \\ 0 & 1\end{smallmatrix}\right), x^{r-1}y]$. By Lemma 4.1(3) and Lemma 4.2(1), we see that $\Psi(\overline{(T-a)\psi})$ is a unit times $T[1,X^{p-2}]$ and the result follows. (Note that $\det\otimes\mathrm{Symm}^{p-2}\overline{\mathbb{F}}_p^2$ is irreducible, and in particular is generated by X^{p-2}.)
(2) If $v(r-1)+1+v(a)\leq v(a^2-rp)$, then writing $\tau=\frac{rp-a^2}{ap(r-1)}$, we see that $\overline{(T-a)\psi}$ is a unit times

$$\sum_{\lambda,\mu\in\mathbb{F}_p}[\left(\begin{smallmatrix} p^2 & p[\lambda]+[\mu] \\ 0 & 1\end{smallmatrix}\right), x^{r-1}y]$$
$$+[1,x^{r-1}y]$$
$$-\overline{\tau}\sum_{\lambda\in\mathbb{F}_p}[\left(\begin{smallmatrix} p & [\lambda] \\ 0 & 1\end{smallmatrix}\right), x^{r-1}y].$$

By Lemma 4.1(3) and Lemma 4.2, we see that $\Psi(\overline{(T-a)\psi})$ is a unit times $(T^2-\overline{\tau}T+1)[1,X^{p-2}]$, as required.

□

Corollary 4.7. *Assume that $p>2$ and that $r>p$ with $r\equiv 1 \pmod{p-1}$, and that $0<v(a)<1$.*

(1) *If $v(r-1)+1+v(a)>v(a^2-rp)$, then $\overline{V}_{k,a}\cong\mathrm{ind}(\omega_2^2)$ is irreducible.*

(2) *If* $v(r-1)+1+v(a) \leq v(a^2-rp)$, *then* $\omega^{-1} \otimes \overline{V}_{k,a}$ *is unramified, and the trace of* Frob_p *on this representation is* $\bar{t}$, *where* $t = \frac{rp-a^2}{ap(r-1)}$.

Proof. This is immediate from Lemma 3.2 and Corollary 4.6. □

References

[AS86] Avner Ash and Glenn Stevens, *Modular forms in characteristic l and special values of their L-functions*, Duke Math. J. **53** (1986), no. 3, 849–868.

[BB10] Laurent Berger and Christophe Breuil, *Sur quelques représentations potentiellement cristallines de* $\mathrm{GL}_2(\mathbf{Q}_p)$, Astérisque (2010), no. 330, 155–211.

[Ber10] Laurent Berger, *Représentations modulaires de* $\mathrm{GL}_2(\mathbf{Q}_p)$ *et représentations galoisiennes de dimension 2*, Astérisque (2010), no. 330, 263–279.

[Ber11] ———, *La correspondance de Langlands locale p-adique pour* $\mathrm{GL}_2(\mathbf{Q}_p)$, Astérisque (2011), no. 339, Exp. No. 1017, viii, 157–180, Séminaire Bourbaki. Vol. 2009/2010. Exposés 1012–1026.

[Ber12] ———, *Local constancy for the reduction mod p of 2-dimensional crystalline representations*, Bulletin of the London Mathematical Society (to appear) (2012).

[BG09] Kevin Buzzard and Toby Gee, *Explicit reduction modulo p of certain two-dimensional crystalline representations*, Int. Math. Res. Not. IMRN (2009), no. 12, 2303–2317.

[BL94] L. Barthel and R. Livné, *Irreducible modular representations of* GL_2 *of a local field*, Duke Math. J. **75** (1994), no. 2, 261–292.

[Bre03] Christophe Breuil, *Sur quelques représentations modulaires et p-adiques de* $\mathrm{GL}_2(\mathbf{Q}_p)$*. II*, J. Inst. Math. Jussieu **2** (2003), no. 1, 23–58.

E-mail address: buzzard@imperial.ac.uk

Department of Mathematics, Imperial College London

E-mail address: toby.gee@imperial.ac.uk

Department of Mathematics, Imperial College London