ON p-ADIC REPRESENTATIONS OF $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ WITH OPEN IMAGE

KEENAN KIDWELL

1. Introduction

Let p be a prime. Recently Greenberg has given a novel representation-theoretic criterion for an absolutely irreducible representation $\overline{\rho} : G_{\mathbf{Q}} \to \mathrm{GL}_n(\mathbf{F}_p)$ with $p \nmid |\mathrm{im}(\overline{\rho})|$ to admit lifts $G_{\mathbf{Q}} \to \mathrm{GL}_n(\mathbf{Z}_p)$ with open image (see [Gre16, Proposition 7.1.1] as well as [Gre16, Proposition 6.1.1] for an alternative approach which applies to reducible residual representations). A crucial hypothesis for the applicability of Greenberg's criterion is that the residual representation $\overline{\rho}$ factors through $\mathrm{Gal}(L/\mathbf{Q})$ for a finite Galois extension L of $\mathbf{Q}$ which is *p-rational*. The field L is p-rational if, for $L_{\Sigma_p}(p)$ the maximal pro-p extension of L unramified outside the set Σ_p of primes above p, the Galois group $\mathrm{Gal}(L_{\Sigma_p}(p)/L)$ is free pro-p of rank $r_2(L)+1$, where as usual $r_2(L)$ denotes the number of complex primes of L. This condition on L, which includes the Leopoldt conjecture for p and L, seems difficult to verify in practice, especially for number fields of large degree. By contrast, it is simple to exhibit many examples of finite Galois extensions $L/\mathbf{Q}_p$ which satisfy the natural local analogue of p-rationality. Namely, if $L(p)$ denotes the maximal pro-p extension of L, then $G_L(p) = \mathrm{Gal}(L(p)/L)$ is free pro-p of rank $[L : \mathbf{Q}_p] + 1$ as long as L does not contain a primitive p-th root of unity ([Ser02, Theorem II.5.3]). This observation led us to derive a local analogue of Greenberg's result, i.e., a representation-theoretic criterion for an absolutely irreducible representation $\overline{\rho} : G_{\mathbf{Q}_p} \to \mathrm{GL}_n(\mathbf{F}_p)$ with $p \nmid |\mathrm{im}(\overline{\rho})$ to admit lifts $G_{\mathbf{Q}_p} \to \mathrm{GL}_n(\mathbf{Z}_p)$ with open image (in fact the lifts whose existence is ensured by our criterion have image containing the congruence subgroup $\Gamma_n(\mathbf{Z}_p) = \ker(\mathrm{GL}_n(\mathbf{Z}_p) \to \mathrm{GL}_n(\mathbf{F}_p))$). While the assumption that $p \nmid |\mathrm{im}(\overline{\rho})|$ seems absolutely essential to our method, we can, in the local case, replace the analogue of p-rationality (the condition that the splitting field $\mathbf{Q}_p(\overline{\rho}) = \overline{\mathbf{Q}}_p^{\ker(\overline{\rho})}$ of $\overline{\rho}$ does not contain a primitive p-th root of unity) with the weaker condition that the residual representation $\overline{\rho}$ is *unobstructed* in the sense that $H^2(G_{\mathbf{Q}_p}, \mathrm{Ad}(\overline{\rho})) = 0$. This condition holds in particular if $L = \mathbf{Q}_p(\overline{\rho})$ does not contain a primitive p-th root of unity (in addition to the assumption that $p \nmid |\mathrm{im}(\overline{\rho})| = [L : \mathbf{Q}_p]$). When $p = 2$, every absolutely irreducible representation $\overline{\rho} : G_{\mathbf{Q}_p} \to \mathrm{GL}_n(\mathbf{F}_2)$ is obstructed, so our results only apply to odd primes.

Greenberg's lifting criterion is proved via a group-theoretic argument in which lifts of $\overline{\rho}$ are related to certain continuous homomorphisms from pro-p Galois groups to $\Gamma_n(\mathbf{Z}_p)$ which are equivariant for the action of a finite Galois group (an idea which originated in Boston's thesis, appeared in [BM89] and [Bos91] in the global case, and has been used extensively by Böckle in the local case to describe the structure of (uni)versal deformation rings of 2-dimensional mod p representations of G_K for K a p-adic field (cf. [Böc00] and [Böc10])). We note that while the works just cited use this group-theoretic approach to obtain structural information (e.g. presentations) for (uni)versal deformation rings, as well as constraints on the shapes of the corresponding (uni)versal deformations, as far as we know, Greenberg's article

Date: October 27, 2017.

[Gre16] is the first instance where the approach has been used to prove the existence of lifts (and Greenberg's main proofs do not actually make use of deformation-theoretic language). Our argument is similar to Greenberg's, but follows the slightly more deformation-theoretic variant outlined in [Gre16, §7.2] which is applicable in our local setting due to the fact that the universal deformation ring of an n-dimensional residual representation $\overline{\rho}$ satisfying our hypotheses is a power series ring over $\mathbf{Z}_p$ in n^2+1 variables (specifically this holds because $\overline{\rho}$ is absolutely irreducible and unobstructed). Exploiting the deformation-theoretic point of view, even in this simple situation in which the universal deformation ring is formally smooth over $\mathbf{Z}_p$, allows us to say somewhat more than we are able to utilizing the purely group-theoretic argument of Greenberg. Moreover, while the lifting method via either argument is very much non-constructive, we feel that the deformation-theoretic interpretation may be more conducive to obtaining additional information about the lifts whose existence it supplies (e.g. whether or not some of them may satisfy reasonable p-adic Hodge-theoretic properties).

After presenting our lifting criterion in §2 (Theorem 3), we state in §3 a theorem (Theorem 4) which furnishes the existence of an abundance of absolutely irreducible residual representations of $G_{\mathbf{Q}_p}$ of large dimension satisfying the criterion, which therefore admit (many inequivalent) lifts to characteristic zero having open image.

2. The Lifting Criterion

Although the terminology is somewhat abusive, we will say that a residual representation $\overline{\rho} : G_{\mathbf{Q}_p} \to \mathrm{GL}_n(\mathbf{F}_p)$ is *tame* if $p \nmid |\mathrm{im}(\overline{\rho})|$. Recall that a residual representation (tame or not) is said to be *unobstructed* if $H^2(G_{\mathbf{Q}_p}, \mathrm{Ad}(\overline{\rho})) = 0$. When $\overline{\rho}$ is absolutely irreducible and unobstructed, we have the following well-known structural result for its universal deformation ring $R_{\overline{\rho}}$.

Proposition 1. *If $\overline{\rho} : G_{\mathbf{Q}_p} \to \mathrm{GL}_n(\mathbf{F}_p)$ is absolutely irreducible and unobstructed, then $R_{\overline{\rho}}$ is isomorphic as a $\mathbf{Z}_p$-algebra to $\mathbf{Z}_p[[T_0, \ldots, T_{n^2}]]$.*

Proof. The fact that the universal deformation ring $R_{\overline{\rho}}$ is a power series ring over $\mathbf{Z}_p$ follows from the general formalism of deformation theory of Galois representations. That the relative dimension of $R_{\overline{\rho}}$ over $\mathbf{Z}_p$ is n^2+1 follows from an application of Tate's formula for the local Euler-Poincaré characteristic of $\mathrm{Ad}(\overline{\rho})$ ([Ser02, Theorem II.5.5]), taking into account that $H^2(G_{\mathbf{Q}_p}, \mathrm{Ad}(\overline{\rho})) = 0$ and that $H^0(G_{\mathbf{Q}_p}, \mathrm{Ad}(\overline{\rho})) = \mathbf{F}_p$ (the former being the definition of "unobstructed," and the latter being a consequence of the absolute irreducibility of $\overline{\rho}$). □

If $\overline{\rho} : G_{\mathbf{Q}_p} \to \mathrm{GL}_n(\mathbf{F}_p)$ is any residual representation, the *splitting field* $\mathbf{Q}_p(\overline{\rho})$ of $\overline{\rho}$ is the fixed field $\overline{\mathbf{Q}}_p^{\ker(\overline{\rho})}$ of the kernel of $\overline{\rho}$.

Proposition 2. *Let $\overline{\rho} : G_{\mathbf{Q}_p} \to \mathrm{GL}_n(\mathbf{F}_p)$ be tame with splitting field L. If L does not contain a primitive p-th root of unity, then $\overline{\rho}$ is unobstructed.*

Proof. Let $L(p)$ be the maximal pro-p extension of L, and $G_L(p) = \mathrm{Gal}(L(p)/L)$. The assumption that L does not contain a primitive p-th root of unity implies that $G_L(p)$ is free pro-p ([Ser02, Theorem II.5.3]). Note that since G_L acts trivially on $\mathrm{Ad}(\overline{\rho})$, we also have an induced (trivial) action of $G_L(p)$ on $\mathrm{Ad}(\overline{\rho})$. By [Ser02, Proposition II.5.20], the inflation map $H^2(G_L(p), \mathrm{Ad}(\overline{\rho})) \to H^2(G_L, \mathrm{Ad}(\overline{\rho}))$ is an isomorphism, which implies that the target $H^2(G_L, \mathrm{Ad}(\overline{\rho}))$ vanishes because the source does (the latter vanishing due to the fact that

$G_L(p)$ is free pro-p, cf. [Ser02, Corollary I.4.2]). Finally, since we have made the assumption that the index of G_L in $G_{\mathbf{Q}_p}$ is of order prime to p (because $G_{\mathbf{Q}_p}/G_L = \mathrm{Gal}(L/\mathbf{Q}_p) \simeq \mathrm{im}(\overline{\rho})$), the restriction map $H^2(G_{\mathbf{Q}_p}, \mathrm{Ad}(\overline{\rho})) \to H^2(G_L, \mathrm{Ad}(\overline{\rho})) = 0$ is injective by [Ser02, Proposition I.2.9], which proves that $\overline{\rho}$ is indeed unobstructed. □

We now state our main lifting theorem.

Theorem 3. *Let $\overline{\rho} : G_{\mathbf{Q}_p} \to \mathrm{GL}_n(\mathbf{F}_p)$ be absolutely irreducible, tame, and unobstructed, with splitting field L. Assume there exists a surjective $\mathbf{F}_p[\mathrm{Gal}(L/\mathbf{Q}_p)]$-module homomorphism*

$$\mathbf{F}_p[\mathrm{Gal}(L/\mathbf{Q}_p)] \to \mathrm{Ad}(\overline{\rho}).$$

Then there exist uncountably many $\mathbf{Z}_p$-inequivalent lifts $\rho : G_{\mathbf{Q}_p} \to \mathrm{GL}_n(\mathbf{Z}_p)$ of $\overline{\rho}$ with $\Gamma_n(\mathbf{Z}_p) \le \mathrm{im}(\rho)$. In particular these lifts have open image in $\mathrm{GL}_n(\mathbf{Z}_p)$.

Proof. We follow the strategy outlined in [Gre16, §7.2]. Let $\widetilde{L}$ be the maximal abelian extension of L of exponent p, which is of finite degree over L by local class field theory (in fact the local reciprocity map yields a canonical isomorphism $L^\times/(L^\times)^p \simeq \mathrm{Gal}(\widetilde{L}/L)$). Since $\mathrm{Gal}(L/\mathbf{Q}_p)$ has order prime to p due to the tameness assumption on $\overline{\rho}$, the exact sequence

$$1 \to \mathrm{Gal}(\widetilde{L}/L) \to \mathrm{Gal}(\widetilde{L}/\mathbf{Q}_p) \to \mathrm{Gal}(L/\mathbf{Q}_p) \to 1 \tag{2.1}$$

splits by the Schur-Zassenhaus theorem. By the same result (or using standard results in representation theory of finite groups), we may choose a lift $\nu : \mathrm{Gal}(L/\mathbf{Q}_p) \to \mathrm{GL}_n(\mathbf{Z}_p)$ of $\overline{\rho}$ via which $\mathrm{Gal}(L/\mathbf{Q}_p)$ acts on any closed normal subgroup of $\mathrm{GL}_n(\mathbf{Z}_p)$ by conjugation. The $\mathbf{F}_p[\mathrm{Gal}(L/\mathbf{Q}_p)]$-module $\mathrm{Gal}(\widetilde{L}/L) \simeq L^\times/(L^\times)^p$ has a submodule of $\mathbf{F}_p$-dimension 2 or 1 according as L does or doesn't contain a primitive p-th root of unity, and the corresponding quotient is isomorphic to the regular representation $\mathbf{F}_p[\mathrm{Gal}(L/\mathbf{Q}_p)]$ ([Böc00, Theorem 4.1]). On the other hand, $\mathrm{Ad}(\overline{\rho})$ is isomorphic as an $\mathbf{F}_p[\mathrm{Gal}(L/\mathbf{Q}_p)]$-module to the Frattini quotient

$$\widetilde{\Gamma_n(\mathbf{Z}_p)} = \Gamma_n(\mathbf{Z}_p)/\Gamma_n^2(\mathbf{Z}_p)$$

of $\Gamma_n(\mathbf{Z}_p)$, where $\Gamma_n^2(\mathbf{Z}_p) = \ker(\mathrm{GL}_n(\mathbf{Z}_p) \to \mathrm{GL}_n(\mathbf{Z}/p^2\mathbf{Z}))$. We have a canonical injection $\widetilde{\Gamma_n(\mathbf{Z}_p)} \hookrightarrow \mathrm{GL}_n(\mathbf{Z}/p^2\mathbf{Z})$ whose image is the image in $\mathrm{GL}_n(\mathbf{Z}/p^2\mathbf{Z})$ under the reduction map $\mathrm{GL}_n(\mathbf{Z}_p) \to \mathrm{GL}_n(\mathbf{Z}/p^2\mathbf{Z})$ of the congruence subgroup $\Gamma_n(\mathbf{Z}_p)$. Thus an $\mathbf{F}_p[\mathrm{Gal}(L/\mathbf{Q}_p)]$-module surjection as in the statement of the theorem yields a $\mathrm{Gal}(L/\mathbf{Q}_p)$-equivariant homomorphism

$$\tau_2 : \mathrm{Gal}(\widetilde{L}/L) \to \mathrm{GL}_n(\mathbf{Z}/p^2\mathbf{Z})$$

with image $\widetilde{\Gamma_n(\mathbf{Z}_p)}$. Using a splitting of the exact sequence (2.1) above, we may extend τ_2 to $\mathrm{Gal}(\widetilde{L}/\mathbf{Q}_p)$ and inflate to obtain a continuous homomorphism

$$\rho_2 : G_{\mathbf{Q}_p} \twoheadrightarrow \mathrm{Gal}(\widetilde{L}/\mathbf{Q}_p) \to \mathrm{GL}_n(\mathbf{Z}/p^2\mathbf{Z})$$

which lifts $\overline{\rho}$ and has image containing $\widetilde{\Gamma_n(\mathbf{Z}_p)}$. The strict equivalence class of this lift corresponds to a unique local $\mathbf{Z}_p$-algebra homomorphism $\psi_2 : R_{\overline{\rho}} \to \mathbf{Z}/p^2\mathbf{Z}$, where $R_{\overline{\rho}}$ is the universal deformation ring of $\overline{\rho}$. Due to the description of $R_{\overline{\rho}}$ as a power series ring of relative dimension $n^2 + 1$ over $\mathbf{Z}_p$ from Proposition 1, it is clear that there are uncountably many distinct local $\mathbf{Z}_p$-algebra homomorphisms $\psi : R_{\overline{\rho}} \to \mathbf{Z}_p$ which lift ψ_2. Each such ψ corresponds by specialization of the universal deformation to a lift $\rho : G_{\mathbf{Q}_p} \to \mathrm{GL}_n(\mathbf{Z}_p)$ of ρ_2 (hence also of $\overline{\rho}$), in fact an entire strict equivalence class of such liftings. Moreover, because the reduction modulo p^2 of such a ρ has image containing $\widetilde{\Gamma_n(\mathbf{Z}_p)}$, the image of such a ρ itself contains $\Gamma_n(\mathbf{Z}_p)$ by [DdSMS91, 1.9 Proposition]. This completes the proof. $\square$

3. Residual representations satisfying the lifting criterion

In seeking residual representations $\overline{\rho} : G_{\mathbf{Q}_p} \to \mathrm{GL}_n(\mathbf{F}_p)$ which satisfy the hypotheses of Theorem 3, we have not attempted an exhaustive enumeration of all the possibilities. (This might be feasible however, as the finite Galois groups whose representation theory must be analyzed are metacyclic, and in fact can always be assumed to be split metacyclic. The irreducible $\overline{\mathbf{F}}_p$-representations of such groups are all induced from explicit characters of explicit subgroups, and can be parametrized in a pleasantly number-theoretic manner. By Galois descent one obtains a parameterization of the irreducible $\mathbf{F}_p$-representations. See [Dal16, §2] for a lucid exposition.) Instead, we sought cases in which the numerology governing the structure of the Galois group and its representations was such that (a) the Galois group would admit an irreducible $\mathbf{F}_p$-representation of the maximal possible dimension and (b) the (ultimately numerical) representation-theoretic condition imposed on the adjoint representation in Theorem 3 could be verified directly. The family of representations which we found is described in the following theorem.

Theorem 4. *Let (e, f) be a pair of integers where $e = \ell^d$ is a power of an odd prime ℓ, $f = \varphi(\ell^d) = \ell^{d-1}(\ell - 1)$, and suppose that*

1. *$p \neq \ell$,*
2. *$p \nmid \ell - 1$, and*
3. *p is a primitive root modulo ℓ^d (i.e. the residue class of p in $\mathbf{Z}/\ell^d\mathbf{Z}$ generates the cyclic group $(\mathbf{Z}/\ell^d\mathbf{Z})^\times$).*

Set $L = \mathbf{Q}_p(\zeta_{p^f-1}, p^{1/e})$. Then L is a Galois extension of $\mathbf{Q}_p$ of degree ef prime to p and its Galois group $\mathrm{Gal}(L/\mathbf{Q}_p)$ admits a unique absolutely irreducible $\mathbf{F}_p$-representation τ_{can} of dimension f. If $\overline{\rho} : G_{\mathbf{Q}_p} \to \mathrm{GL}_f(\mathbf{F}_p)$ is the inflation of τ_{can} to $G_{\mathbf{Q}_p}$, then $\overline{\rho}$ satisfies the hypotheses of Theorem 3, and therefore admits uncountably many $\mathbf{Z}_p$-inequivalent lifts $\rho : G_{\mathbf{Q}_p} \to \mathrm{GL}_f(\mathbf{Z}_p)$ with $\Gamma_f(\mathbf{Z}_p) \leq \mathrm{im}(\rho)$. In particular these lifts have open image in $\mathrm{GL}_f(\mathbf{Z}_p)$.

Proof. We only give an outline of the proof here. Let $H = \mathrm{Gal}(L/\mathbf{Q}_p)$ and let $T = \mathrm{Gal}(L/\mathbf{Q}_p(\zeta_{p^f-1}))$ be the inertia subgroup of H (which is cyclic and normal). The existence and uniqueness of τ_{can} is a consequence of the classification of mod p representations of H described in [Dal16, §2]. Since $p \nmid |H|$, $\overline{\rho}$ is tame, and since L does not contain a primitive p-th root of unity (as $p-1$ does not divide the ramification index $e = \ell^d$ of L over $\mathbf{Q}_p$), $\overline{\rho}$ is unobstructed by Proposition 2.

Thus it remains to verify the representation-theoretic condition in Theorem 3 for $\mathrm{Ad}(\overline{\rho})$. Note that we are viewing the adjoint as a representation of $\mathrm{Gal}(L/\mathbf{Q}_p)$, and that we may work with L instead of the (potentially smaller) splitting field of $\overline{\rho}$, as the condition on the adjoint is insensitive to this change. Moreover, due to the semisimplicity of the mod p representation theory of H and the behavior of irreducible $\mathbf{F}_p$-representations of H under extension of scalars to a finite extension k of $\mathbf{F}_p$ which is a splitting field for H (i.e. for which every irreducible k-representation of H is absolutely irreducible), we may verify the representation-theoretic condition after extending scalars to such a field k (we take k to be the extension of the residue field $\mathbf{F}_{p^f}$ of L obtained by adjoining a primitive f-th root of unity). Then τ_{can} can be realized explicitly as $\mathrm{Ind}_T^H(\theta)$, where $\theta : T \to k^\times$ is the *canonical faithful character* of order e which sends $t \in T$ to the image of $t(p^{1/e})/p^{1/e}$ in $k^\times$ (this is only canonical up to the choice of the uniformizer p for $\mathbf{Q}_p$, but the terminology still seems reasonable to us).

The fact that p is a primitive root modulo ℓ^d ensures that $\mathrm{Ind}_T^H(\theta)$ is self-dual, so we can realize the adjoint representation as $\mathrm{Ind}_T^H(\theta) \otimes_k \mathrm{Ind}_T^H(\theta)$, which decomposes according to Mackey's tensor product decomposition theorem ([CR81, (10.18)]) as the direct sum of the representations $\mathrm{Ind}_T^H(\theta^{1+i})$, where i runs through the integers in $[1, e-1]$ relatively prime to e. The problem now is to show that the multiplicity of any irreducible k-representation of H in this direct sum is bounded above by its multiplicity in the regular representation, which is the dimension of the representation (since k is a splitting field for H). Using a variant of Frobenius reciprocity ([CR81, (10.21) Proposition]) together with Mackey's theorem on the decomposition of the restriction of an induced representation to a subgroup ([CR81, (10.13)]), we can give the decomposition of $\mathrm{Ind}_T^H(\theta^{1+i})$ into irreducible representations and show in particular that $\mathrm{Ind}_T^H(\theta^{1+i})$ is multiplicity-free. Finally, using the usual form of Frobenius reciprocity, we can show that the number of summands $\mathrm{Ind}_T^G(\theta^{1+i})$ in which a given irreducible k-representation of H may appear is at most its dimension (and indeed this bound cannot be improved as we have explicit examples where it is attained). Combining this with the fact that each summand $\mathrm{Ind}_T^H(\theta^{1+i})$ is multiplicity-free gives the desired bound. □

Remark 5. Although the majority of the work in proving Theorem 4 depends only on standard results on induced representations of finite groups, the fact that the multiplicity bounds we are able to obtain for the adjoint cannot generally be improved suggests that our choice to focus on pairs (e, f) of the form in the theorem, the corresponding tamely ramified Galois extension, and what we have called the canonical representation of H, is a fairly judicious one. This choice is informed by the aforementioned elementary number-theoretic qualities of the parameterization of irreducible k-representations of H described in [Dal16, §2] and our desire to have representations of large dimension. An additional feature of the canonical representation of H which distinguishes it from general irreducible k-representations of H is that it is induced from T, a *normal* subgroup of H. This normality simplifies the applications of Mackey's theorems which are essential to the proof.

Remark 6. Although we do not know whether or not, for a fixed (odd) prime p, a pair (e, f) as in Theorem 4 always exists, if we instead fix a pair (e, f) of the form $(\ell^d, \ell^{d-1}(\ell-1))$ for an odd prime ℓ, then the set of odd primes p satisfying the three conditions in Theorem 4 relative to this pair has positive density by Chebotarev.

We close with a corollary which follows from using the representations of Theorem 4 as inputs to Theorem 3.

Corollary 7. *For $p \in [3, 31]$, the set of integers n for which there exist residually absolutely irreducible representations $\rho : G_{\mathbf{Q}_p} \to \mathrm{GL}_n(\mathbf{Z}_p)$ with $\Gamma_n(\mathbf{Z}_p) \leq \mathrm{im}(\rho)$ is unbounded. More generally, this holds for any odd prime p such that there exists an odd prime $\ell \neq p$, $p \nmid \ell - 1$, for which p is a primitive root modulo ℓ^d for all $d \geq 1$. (Note that if p is a primitive root modulo ℓ, then it will also be a primitive root modulo ℓ^d for all $d \geq 1$ provided $p^{\ell-1}$ is not congruent to 1 modulo ℓ^2.)*

Proof. If p is an odd prime for which there exists an odd prime $\ell \neq p$ as in the statement of the corollary, then by Theorem 4, the set of integers in question contains $\ell^{d-1}(\ell-1)$ for all $d \geq 1$, and hence is clearly unbounded. For the first assertion of the theorem, one can easily check that for each $p \in [3, 31]$, there is a prime $\ell \in [3, 31]$ with the necessary properties. $\square$

Remark 8. It's clear from Corollary 7 that the coarse quantitative properties of the set of representations $\rho : G_{\mathbf{Q}_p} \to \mathrm{GL}_n(\mathbf{Z}_p)$ with $\Gamma_n(\mathbf{Z}_p) \leq \mathrm{im}(\rho)$ whose existence we have established depend on elementary (but presumably not known) properties of primitive roots modulo primes (and prime powers). It seems reasonable to expect that the condition in Corollary 7 holds for every odd prime p, although as far as we know, this is unknown. Also relevant to this issue is a special case of Artin's conjecture on primitive roots which asserts that for a fixed (odd) prime p, the set of odd primes $\ell \neq p$ such that p is a primitive root modulo ℓ, is infinite (and even has positive density). It is known by work of Heath-Brown ([HB86]) that there are at most two primes p for which the infinitude in Artin's conjecture may fail (GRH has been shown to imply that there are no such exceptional primes). However, even for the non-exceptional primes p, it is not immediately clear to us whether the set of (odd) primes $\ell \neq p$ modulo which p is a primitive root *and* for which $p \nmid \ell - 1$ is still infinite. If this holds for a given prime p, then we would again obtain the unboundedness statement in Corollary 7 for p, even restricting to dimensions of the form $\ell - 1$ for primes ℓ.

References

[BM89] N. Boston and B. Mazur. Explicit universal deformations of Galois representations. In *Algebraic number theory*, volume 17 of *Adv. Stud. Pure Math.*, pages 1–21. Academic Press, Boston, MA, 1989.

[Böc00] Gebhard Böckle. Demuškin groups with group actions and applications to deformations of Galois representations. *Compositio Math.*, 121(2):109–154, 2000.

[Böc10] Gebhard Böckle. Deformation rings for some mod 3 Galois representations of the absolute Galois group of $\mathbf{Q}_3$. *Astérisque*, (330):529–542, 2010.

[Bos91] Nigel Boston. Explicit deformation of Galois representations. *Invent. Math.*, 103(1):181–196, 1991.

[CR81] Charles W. Curtis and Irving Reiner. *Methods of representation theory. Vol. I.* John Wiley & Sons, Inc., New York, 1981. With applications to finite groups and orders, Pure and Applied Mathematics, A Wiley-Interscience Publication.

[Dal16] Chandan Singh Dalawat. $\mathbf{F}_p$-representations over p-adic fields. *arXiv preprint math/1608.04181*, 2016.

[DdSMS91] J. D. Dixon, M. P. F. du Sautoy, A. Mann, and D. Segal. *Analytic pro-p-groups*, volume 157 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1991.

[Gre16] Ralph Greenberg. Galois representations with open image. *Ann. Math. Qué.*, 40(1):83–119, 2016.

[HB86] D. R. Heath-Brown. Artin's conjecture for primitive roots. *Quart. J. Math. Oxford Ser. (2)*, 37(145):27–38, 1986.

[Ser02] Jean-Pierre Serre. *Galois cohomology.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, english edition, 2002. Translated from the French by Patrick Ion and revised by the author.