Every 7-Dimensional Abelian Variety over $\mathbb{Q}_p$ has a Reducible ℓ-adic Galois Representation

Lambert A'Campo

June 15, 2020

Abstract

Let K be a complete, discretely valued field with finite residue field and G_K its absolute Galois group. The subject of this note is the study of the set of positive integers d for which there exists an absolutely irreducible ℓ-adic representation of G_K of dimension d with rational traces on inertia. Our main result is that non-Sophie Germain primes are not in this set when the residue characteristic of K is > 3. The result stated in the title is a special case.

Over a number field one expects a 'generic' abelian variety to be irreducible. For instance [Zar00] proves a result in this direction and provides us with abelian varieties A of any dimension such that $\mathrm{End}(A) = \mathbb{Z}$. By Faltings isogeny theorem the Tate module of such an abelian variety is an absolutely irreducible Galois representation.

Over local fields with residue characteristic p, the situation is very different. The dimensions which appear in absolutely irreducible ℓ-adic Galois representations with rational traces on inertia form a proper subset of the positive integers. We are not able to give a full description of this subset, however we prove some restrictions, namely we show that if the representation is tamely ramified, then its dimension is a value of the Euler totient function, see Proposition 2. In the case of wild ramification we can only conclude that $(p-1)$ divides the dimension, see Proposition 4. Nevertheless, this is still enough to show

Theorem 1. *Let $p \neq 2, 3$, $K/\mathbb{Q}_p$ a finite extension and $\ell \neq p$ a prime. If d is a prime such that $2d+1$ is not prime, then there is no abelian variety A/K of dimension d whose associated Galois representation*

$$V_\ell A := \left(\varprojlim_{n \geq 1} A[\ell^n](\overline{K}) \right) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$$

is absolutely irreducible. In particular, the conclusion holds for all primes $d \equiv 1 \pmod 3$.

Prime numbers d, such that $2d+1$ is not prime are non-Sophie Germain primes. The first few are $d = 7, 13, 17, 19, 31 \ldots$ [OEIS, A053176]. The set of non-Sophie Germain primes is infinite since for any prime $d \equiv 1 \pmod 3$, 3 divides $2d+1$. Thus every prime $\equiv 1 \pmod 3$ is not a Sophie Germain prime and the theorem applies. Moreover, non-Sophie Germain primes should contain 100% of all primes by the following probabilistic heuristic. The events 'n is prime' and '$2n+1$ is prime' should occur independently with probabilities $1/\log n$ and $1/\log(2n+1)$, respectively. Thus the number of Sophie Germain primes up to x is of order $x/(\log x)^2$ which is easily seen to be 0% of primes as $x \to \infty$ by the prime number theorem.

Our results continue the observation [AD19, footnote 2] which shows that it is difficult to attack the inverse Galois problem for the groups $\mathrm{GSp}_{2n}(\mathbb{F}_p)$ by constructing an abelian variety over $\mathbb{Q}$ with suitable reductions as one can easily do with elliptic curves for $n = 1$.

We fix some notations. Let K be a complete, discretely valued field with finite residue field k of characteristic p and cardinality q. So K is either a finite extension of $\mathbb{Q}_p$ or a finite extension of $\mathbb{F}_p((t))$. The former is the most interesting case since in the latter all ramification is tame. The absolute Galois group G_K of the field K is a split extension

$$1 \to I_K \to G_K \to G_k \to 0,$$

where I_K is the inertia group of K [CF67, I. §7]. The representations we consider are continuous representations $\rho : G_K \to \mathrm{GL}_n(\overline{\mathbb{Q}_\ell})$, where $\ell \neq p$ and for all $g \in I_K$, $\mathrm{tr}(\rho(g)) \in \mathbb{Q}$. In particular, this should include the class of 'geometric' ℓ-adic representations which occur as the Tate module of an abelian variety A/K or more generally as the ℓ-adic cohomology of a variety X/K. For example see [ST68, Theorem 2] for a proof that the Tate module of an abelian variety over K with potentially good reduction has rational traces on inertia. With these notations, our precise results are the two following propositions.

Proposition 2. *Let V be a continuous, irreducible, tamely ramified $\overline{\mathbb{Q}_\ell}$-representation of G_K such that the trace of any $h \in I_K$ is rational, then either $\dim V = 1, 2$ or there exists an odd prime $v \neq p$, such that $\dim V = (v-1)v^a$, for some $a \geq 0$ such that q generates $(\mathbb{Z}/v^{a+1}\mathbb{Z})^\times$. In particular, $\dim V = \varphi(m)$ for some positive integer m. Moreover, each of these dimensions is realised by such a representation.*

Example 3. Let C be the genus 11 hyperelliptic curve $y^2 = x^{23} - 5^2$ over $\mathbb{Q}_5$ and J its Jacobian. Then C obtains good reduction over $\mathbb{Q}_5(5^{1/23})$ and so the inertia group of $\mathbb{Q}_5$ acts on $T_\ell J$ through a quotient of order 23. This realises a 22 dimensional, irreducible, tamely ramified $\overline{\mathbb{Q}_\ell}$-representation of $G_{\mathbb{Q}_5}$ as promised by Proposition 2 with $v = 23$ and $q = p = 5$.

Proposition 4. *Let V be a continuous, irreducible, wildly ramified $\overline{\mathbb{Q}_\ell}$-representation of G_K such that the trace of any $h \in I_K$ is rational, then $(p-1) \mid \dim V$.*

For the proofs we fix a geometric Frobenius element $\phi_K \in G_K$, i.e. an element which reduces to $\mathrm{Frob}_k^{-1} \in G_k$, where $\mathrm{Frob}_k(x) = x^q$ and $q = |k|$. Moreover, recall that I_K has a unique pro-p Sylow subgroup P_K, called the wild inertia group which is also a normal subgroup of G_K. There is an isomorphism $I_K/P_K \cong \prod_{v \neq p} \mathbb{Z}_v$ such that $\phi_K^{-1} x \phi_K = x^q$ for all $x \in I_K/P_K$ and we fix a projection $t_\ell : I_K/P_K \to \mathbb{Z}_\ell$ which is the maximal pro-ℓ quotient of I_K/P_K. See [CF67, I.§8] for proofs of these facts.

Proof of Proposition 2. Since G_K/P_K is topologically generated by two elements, we can assume that V is defined over a finite extension $F/\mathbb{Q}_\ell$. Then the Grothendieck Monodromy Theorem [ST68, Appendix] shows that there is an open subgroup $H < I_K$ and a nilpotent operator $N \in \mathrm{End}(V)$ such that $h \in H$ acts as $\exp(t_\ell(h)N)$. Since V is irreducible, we must have $N = 0$ and so I_K acts through a finite quotient. The tame inertia group is pro-cyclic and so I_K acts on V through $\mathbb{Z}/m\mathbb{Z}$ for some integer m which we choose to be minimal. Let $\tau \in I_K$ be a generator of this action, then the eigenvalues of $\rho(\tau)$ are mth roots of unity. Suppose one of the eigenvalues is not a primitive root of unity. Then there is $n < m$ such that $\rho(\tau)^n$ has a non-zero fixed subspace. The relation $\phi_K^{-1}\tau\phi_K = \tau^q$ implies that this is an invariant subspace of the whole representation. However, it is not the whole representation since $\rho(\tau)$ has order m by the minimality of m. This contradicts the irreducibility of V.

Thus all eigenvalues of $\rho(\tau)$ are primitive mth roots of unity and so $\det(X\,\mathrm{id} - \rho(\tau)) = \Phi_m(X)^t$ for some t, where Φ_m is the mth cyclotomic polynomial. Moreover, finite group representation theory applied to $\mathbb{Z}/m\mathbb{Z}$ shows that $\rho(\tau)$ is diagonalisable. The relation $\phi_K^{-1}\tau\phi_K = \tau^q$ shows that ϕ_K maps the λ-eigenspace to the λ^q-eigenspace. So by choosing an appropriate basis we can decompose $V = \oplus_{i=1}^t V_i$ where V_i contains each eigenvalue with multiplicity one. By absolute irreducibility we conclude that $t = 1$ and so $\dim V = \varphi(m) = |\{\zeta \in \overline{\mathbb{Q}_\ell} : \zeta \text{ is a primitive } m\text{th root of unity}\}|$.

Moreover, for every integer m which is coprime to p, there is a unique quotient of the tame inertia group of order m and we can realise the above representation explicitly as $\overline{\mathbb{Q}_\ell} \cdot S$, where

S is the set of primitive mth roots of unity, ϕ_K acts on S by sending $\lambda \mapsto \lambda^q$ and a generator τ of the quotient acts as $\tau(a \cdot \lambda) = \lambda a \cdot \lambda$. This representation is irreducible if and only if q acts transitively on the primitive mth roots of unity, i.e. if and only if q generates $(\mathbb{Z}/m\mathbb{Z})^\times$. This is only possible when $m = 2, 4$, $m = v^{a+1}$ or $m = 2v^{a+1}$, where v is an odd prime. Hence $\dim V = 1, 2$ or $\dim V = (v-1)v^a$. □

Lemma 5. *Let G be a compact group and $\rho : G \to \mathrm{GL}_n(F)$ a continuous homomorphism, where F is a discretely valued field of characteristic 0 with valuation $v : F^\times \to \mathbb{Z}$ and ring of integers $R = \{x \in F : v(x) \geq 0\}$. Then ρ is conjugate to a continuous homomorphism $G \to \mathrm{GL}_n(R)$.*

Proof. Note that $R = \{x \in F : v(x) > 1/2\}$ is an open subset of F. Consequently $\mathrm{GL}_n(R)$ is an open subgroup of $\mathrm{GL}_n(F)$ and its preimage $H = \rho^{-1}(\mathrm{GL}_n(R))$ is open as well. By the compactness of G, G/H is finite and so $GR^n \subset F^n$ is a finitely generated, torsion free R-submodule which is G-invariant by definition. Since R is a discrete valuation ring, GR^n is free of rank n. So with respect to a basis of GR^n, ρ takes values in $\mathrm{GL}_n(R)$. □

Proof of Proposition 4. The result is trivial for $p = 2$ so we assume $p \geq 3$. Then by [JW82], G_K is topologically finitely generated and so V is defined over a finite extension $F/\mathbb{Q}_\ell$.[1] By lemma 5, we can assume that G_K acts on V by a continuous homomorphism $\rho : G_K \to \mathrm{GL}_n(\mathcal{O}_F)$, where $n = \dim V$ and $\mathcal{O}_F$ is the ring of integers of F. The reduction $\overline{\rho} : G_K \to \mathrm{GL}_n(\mathcal{O}_F/\mathfrak{m}_F\mathcal{O}_F)$ has finite image. As the kernel of $\mathrm{GL}_n(\mathcal{O}_F) \to \mathrm{GL}_n(\mathcal{O}_F/\mathfrak{m}_F\mathcal{O}_F)$ is a pro-ℓ-group we conclude that P_K acts faithfully through a finite quotient G on V. Since P_K is a normal subgroup of G_K we can apply Clifford's theorem [Cli37, §1] to decompose the restriction of V to G into irreducibles. Thus there is an isomorphism of G-representations $V \cong \bigoplus_i V_i$, where the V_i are irreducible G-representations which are all conjugate, i.e. if $\rho_i : G \to \mathrm{GL}(V_i)$ is the corresponding homomorphism, then for all j, $\rho_j(x) = \rho_i(gxg^{-1})$ for some $g \in G$.

Note that $V^G < V$ is a subrepresentation since $P_K < G_K$ is a normal subgroup. Thus $V^G = 0$ since otherwise V is tamely ramified. Consequently all the V_i are non-trivial. Let $G_i = G/\ker \rho_i$ be the quotient of G which acts faithfully on V_i. Since G_i is a p-group, there is a non-trivial element g_i in the center of G_i which acts as a scalar λ_i on V_i. As G_i acts faithfully we find that λ_i is a non-trivial p^tth root of unity for some $t \geq 1$. Hence the Galois orbit of the character of V_i contains $p^{t-1}(p-1)$ elements. Since the character of V is defined over $\mathbb{Q}$, this implies that the decomposition of V contains all these Galois conjugates and in particular that $(p-1) \mid \dim V$. □

Proof of Theorem 1. Suppose A was such an abelian variety A/K of dimension d. Combining the irreducibility assumption with the Grothendieck Monodromy Theorem [ST68, Appendix], we see that I_K must act through a finite quotient on $V_\ell A$, i.e. A has potentially good reduction and the characteristic polynomials of elements $h \in I_K$ have integral coefficients independent of ℓ by [ST68, Theorem 2]. If $V_\ell A$ is tamely ramified then proposition 2 shows that $2d = \dim V_\ell A = \varphi(m)$ for some m. Absurd. See [OEIS, A005277] for more examples of even integers which are not a value of φ. If $V_\ell A$ is wildly ramified, then proposition 4 shows that $(p-1) \mid 2d$, so $p \in \{2, 3, d+1, 2d+1\}$ contradicting the hypothesis that $p \neq 2, 3$ and $2d+1$ is not prime. □

Acknowledgments. I thank Vladimir Dokchitser for suggesting this subject to me and for encouraging me to write this note. He patiently discussed many (wrong) versions of Proposition 4 with me and provided lots of essential advice and ideas. Moreover, I thank my father and Jesse Pajwani for reading an early version of this text.

[1] In practice one does not need the strong result of [JW82] since most representations already come defined over a finite extension of $\mathbb{Q}_\ell$. For example all Tate modules are defined over $\mathbb{Q}_\ell$.

References

[AD19] Samuele Anni and Vladimir Dokchitser. "Constructing Hyperelliptic Curves with Surjective Galois Representations". In: *Transactions of the American Mathematical Society* 373.2 (2019), pp. 1477–1500. DOI: 10.1090/tran/7995.

[CF67] John William Scott Cassels and Albrecht Fröhlich. *Algebraic number theory: proceedings of an instructional conference*. Academic Press, 1967.

[Cli37] A. H. Clifford. "Representations Induced in an Invariant Subgroup". In: *The Annals of Mathematics* 38.3 (1937), p. 533. DOI: 10.2307/1968599.

[JW82] Uwe Jannsen and Kay Wingberg. "Die Struktur der Absoluten Galoisgruppe $\mathfrak{p}$-adischer Zahlkörper". In: *Inventiones Mathematicae* 70.1 (1982), pp. 71–98. DOI: 10.1007/bf01393199.

[OEIS] OEIS Foundation Inc. (2020). *The On-Line Encyclopedia of Integer Sequences*. URL: https://oeis.org/.

[ST68] Jean-Pierre Serre and John Tate. "Good Reduction of Abelian Varieties". In: *The Annals of Mathematics* 88.3 (1968), p. 492. DOI: 10.2307/1970722.

[Zar00] Yuri G. Zarhin. "Hyperelliptic Jacobians without Complex Multiplication". In: *Mathematical Research Letters* 7.1 (2000), pp. 123–132. DOI: 10.4310/mrl.2000.v7.n1.a11.