AVERAGE MULTIPLICITIES

DAVID E. ROHRLICH

This note summarizes my talk at the ICERM workshop on Murmurations and Arithmetic, June 6 to June 8, 2023. The talk was based on the paper [14], to which the reader is referred for details and proofs. The two addenda at the end appeared neither in the talk nor in [14] but are complementary to both.

It is a pleasure to thank ICERM and the organizers of the workshop for inviting me to participate in a meeting that was both enjoyable and productive.

1. The talk

A lack of competence prevents me from saying anything about murmurations, but my hope is that those who do have the competence may perhaps find something worth exploring in my topic. We consider an irreducible Artin representation of $\mathbb{Q}$, say ρ, which should be thought of as fixed, together with an elliptic curve E over $\mathbb{Q}$, which should be thought of as varying. By definition, ρ is a continuous homomorphism $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(V)$, where V is a finite-dimensional vector space over $\mathbb{C}$, but we can always choose a finite Galois extension K of $\mathbb{Q}$ such that ρ is trivial on $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$, and then ρ becomes a complex representation of the finite group $\mathrm{Gal}(K/\mathbb{Q})$. Since E is defined over $\mathbb{Q}$, it is meaningful to talk about $E(K)$, the Mordell-Weil group of E over K. The natural action of $\mathrm{Gal}(K/\mathbb{Q})$ on $E(K)$ affords a representation of $\mathrm{Gal}(K/\mathbb{Q})$ on the finite dimensional complex vector space $\mathbb{C} \otimes E(K)$, where the tensor product is taken over $\mathbb{Z}$, and the multiplicity of the irreducible representation ρ in $\mathbb{C} \otimes E(K)$ will be denoted $\langle \rho, E \rangle$.

Let $1_{\mathbb{Q}}$ be the trivial one-dimensional representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Then $\langle 1_{\mathbb{Q}}, E \rangle$ is the rank of $E(\mathbb{Q})$. Current thinking about the rank seems to favor the conjecture that with probability 1,

$$\text{rank of } E(\mathbb{Q}) \leqslant 1 \tag{1}$$

as E varies over all elliptic curves over $\mathbb{Q}$ ordered in some reasonable way (see for example [1], [2], [3], [4], [8], and [17]). Since (1) can be written $\langle 1_{\mathbb{Q}}, E \rangle \leqslant 1$, it is tempting to speculate that for *any* fixed irreducible ρ and varying E,

$$\langle \rho, E \rangle \leqslant 1 \tag{2}$$

with probability 1. Nothing in this note is intended to cast doubt on (2). But there is a companion to (1) which predicts that the average rank of an elliptic curve over $\mathbb{Q}$ is $1/2$, and if we replace "average rank" by "average multiplicity" then the resulting conjecture is flatly inconsistent with (2) for certain ρ.

The first example of this inconsistency arises when K is a Galois extension of $\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q}) \cong Q$, the quaternion group of order 8. Then $\mathrm{Gal}(K/\mathbb{Q})$ has a unique (up to isomorphism) irreducible two-dimensional representation ρ, and elementary constructions show that there is an elliptic curve E over $\mathbb{Q}$ such that $\langle \rho, E \rangle \geqslant 1$ ([9], p. 129, Prop. 3) or even $\langle \rho, E \rangle \geqslant 2$ (see [12]). In fact a recent theorem of Suresh [16] implies that there are infinitely many such E with distinct j-invariants. But

the key point is that $\langle \rho, E\rangle$ is even for *any* E, because the natural representation of $\mathrm{Gal}(K/\mathbb{Q})$ on $\mathbb{C}\otimes E(K)$ is defined over $\mathbb{Q}$, whereas ρ is symplectic. Does the fact that $\langle \rho, E\rangle$ is even for all E and positive for infinitely many E contradict (2)? No, because we would simply infer from (2) that the set of isomorphism classes of elliptic curves E such that $\langle \rho, E\rangle > 0$ has density 0 in the set of all isomorphism classes. But this inference implies that the average multiplicity of ρ in E for varying E is 0, not 1/2.

The more general point here is that if ρ is any irreducible Artin representation of $\mathbb{Q}$ and $m(\rho)$ its Schur index then $m(\rho)$ divides $\langle \rho, E\rangle$ for every E. If ρ is symplectic as in the previous paragraph then $m(\rho) = 2$ and thus $\langle \rho, E\rangle$ is even, but long ago Brauer proved that for every positive integer m there exists a group G and an irreducible representation ρ of G such that $m(\rho) = m$ ([5], pp. 742-745). Given m, it is easy to construct a Galois extension K of $\mathbb{Q}$ such that $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to Brauer's G (cf. [13]), but for large m I have no idea how to show that ρ, now viewed as a representation of $\mathrm{Gal}(K/\mathbb{Q})$, occurs in $\mathbb{C}\otimes E(K)$ for some E and thus occurs with multiplicity $\geqslant m$. The main point though is that even if such elliptic curves E exist, they would presumably be of density 0 among all elliptic curves and so their existence would be compatible with (2).

More problematic are examples where $m(\rho) = 1$ but $\langle \rho, E\rangle$ is nonetheless even for all elliptic curves E over $\mathbb{Q}$. Such examples are at present conjectural, because they depend on the following variant of the Birch-Swinnerton-Dyer conjecture, which we shall refer to as "BSD with twist":

$$\mathrm{ord}_{s=1} L(s, E, \rho) = \langle \rho, E\rangle. \tag{3}$$

Here $L(s, E, \rho)$ is the L-function with local factors $\sigma'_{E/\mathbb{Q}_p}\otimes\rho_p$ (notation as in [10] or [11]; in particular, $\sigma'_{E/\mathbb{Q}_p}$ is the representation of the Weil-Deligne group associated to $E/\mathbb{Q}_p$). Although we have referred to (3) as a "variant" of the usual BSD conjecture, it is actually a consequence of the usual version together with the Deligne-Gross conjecture ([6], p. 323, Conjecture 2.7 (iii)). In the present setting, the latter predicts that

$$\mathrm{ord}_{s=1} L(s, E, \rho) = \mathrm{ord}_{s=1} L(s, E, \rho^\gamma) \tag{4}$$

for all automorphisms γ of the cyclotomic subfield of $\mathbb{C}$ generated by the traces of ρ, where ρ^γ denotes the representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that $\mathrm{tr}\,(\rho^\gamma) = (\mathrm{tr}\,\rho)^\gamma$. For a deduction of (3) from the usual BSD and (4) see [9], p. 127, Prop. 2. The conjectural functional equation of $L(s, E, \rho)$ relates $L(s, E, \rho)$ to $L(s, E, \rho^\vee)$, where $\rho^\vee$ the dual of ρ, so if ρ is self-dual then the root number $W(E, \rho)$ in the functional equation determines the parity of the order of vanishing at $s = 1$:

$$W(E, \rho) = (-1)^{\mathrm{ord}_{s=1} L(s,E,\rho)}.$$

It follows under (3) that

$$W(E, \rho) = (-1)^{\langle \rho, E\rangle}. \tag{5}$$

Henceforth we assume that ρ is self-dual, so that (5) is conjecturally valid.

Let us now return to the "problematic" phenomenon mentioned at the beginning of the previous paragraph. In view of (5) we may reformulate it as follows: There are irreducible self-dual Artin representations ρ of $\mathbb{Q}$ such that $W(E, \rho) = 1$ for all E over $\mathbb{Q}$ even though $m(\rho) = 1$. Such ρ are necessarily of even dimension and trivial determinant ([11], p. 338, Prop. 11), but examples do exist (cf. [11], p. 313,

Prop. D). The problem is that the examples in [11] are just too big – $\dim \rho = 16$ and $[K : \mathbb{Q}] \geqslant 80,080$ – to be nonvacuous in the strong sense that $\langle \rho, E \rangle$ is provably positive for at least one E.

The paper [14] is an attempt to remedy this defect. Let L and L' be Galois extensions of $\mathbb{Q}$ with relatively prime discriminants and Galois groups isomorphic to Q, so that the compositum $K = LL'$ has Galois group $Q \times Q$. Up to isomorphism there is a unique irreducible representation ρ of $\mathrm{Gal}(K/\mathbb{Q})$ of dimension 4, and ρ is self-dual with $m(\rho) = 1$. In fact ρ factors through a quotient of $\mathrm{Gal}(K/\mathbb{Q})$ of order 32, and it follows from the work of Suresh [16] that there are infinitely many elliptic curves E over $\mathbb{Q}$ with distinct j-invariants such that $\langle \rho, E \rangle > 0$. Presumably such E are of density 0, because in [14] we prove:

Theorem 1. *$W(E, \rho) = 1$ for all elliptic curves E over $\mathbb{Q}$.*

It is also shown in [14] that if the coprimality of the discriminants of L and L' is replaced by the weaker assumption that $L \cap L' = \mathbb{Q}$ then it can happen that $W(E, \rho) = -1$.

2. Addendum: Minimality

To recapitulate, given an irreducible self-dual Artin representation ρ of $\mathbb{Q}$, let us say that ρ has Property P if $W(E, \rho) = 1$ for all elliptic curves E over $\mathbb{Q}$. A necessary condition for ρ to have Property P is that $\dim \rho$ be even and $\det \rho$ be trivial, and the property itself is problematic – in the sense that it lacks an explanation – only if $m(\rho) = 1$. (By the Brauer-Speiser theorem, 1 and 2 are the only possible values of $m(\rho)$ for a self-dual ρ.) In Theorem 1, ρ has dimension 4 and factors through a Galois group of order 32. The following group-theoretic statement shows that the theorem is minimal among problematic instances of Property P:

Theorem 2. *Let G be a finite group and ρ an irreducible self-dual representation of G of even dimension, trivial determinant, and Schur index 1. Then $\dim \rho \geqslant 4$ and $|G| \geqslant 32$.*

Proof. In dimension 2 the symplectic and special linear groups coincide, because the bilinear form $\langle *, * \rangle$ given by $\langle (a, b), (c, d) \rangle = ad - bc$ is alternating and nondegenerate. Hence if $\dim \rho = 2$ then our hypothesis that $\det \rho$ is trivial implies that ρ is symplectic, whence $m(\rho) = 2$. Therefore $\dim \rho \geqslant 4$.

To show that $|G| \geqslant 32$, we will make frequent use of the fact that

$$|G| = \sum_{\beta} (\dim \beta)^2, \tag{6}$$

where β runs over a set of representatives for the distinct isomorphism classes of irreducible representations of G. In particular, if $\dim \rho \geqslant 6$ then $|G| \geqslant 36 > 32$. So we may assume that $\dim \rho = 4$, and we must show that $|G| \geqslant 32$.

Suppose on the contrary that $|G| < 32$. Since $\dim \rho = 4$ we have $|G| \geqslant 16$, and in fact $|G| \geqslant 17$ (taking account of the one-dimensional trivial representation). So $17 \leqslant |G| < 32$. But since $\dim \rho$ divides $|G|$ we find that $|G|$ is either 20 or 24 or 28.

First consider the possibility that $|G| = 28$. A Sylow 7-subgroup of G is normal and therefore unique; denote it N, and let P be a Sylow 2-subgroup. For any finite group X let $\mathrm{Aut}(X)$ denote the automorphism group of X. The action of P on N by conjugation determines a homomorphism

$$\varphi : P \to \mathrm{Aut}(N) \cong \mathbb{Z}/6\mathbb{Z},$$

and the kernel of φ contains a subgroup M of order 2 centralizing N. Then MN is an abelian normal subgroup of index 2 in G, whence every irreducible representation of G has dimension dividing 2 ([15], p. 61, Corollary). This is a contradiction, because $\dim \rho = 4$.

Next consider the case $|G| = 20$. A Sylow 5-subgroup is normal, and we denote it N; we also choose a Sylow 2-subgroup P. As before, the action of P on N by conjugation gives a homomorphism

$$\varphi : P \to \mathrm{Aut}(N) \cong \mathbb{Z}/4\mathbb{Z}.$$

If there is an element x of order 2 in the kernel of φ then the subgroup generated by N and x is abelian and normal of index 2 in G, so we get a contradiction as before. Otherwise φ is an isomorphism, and ρ is induced by a nontrivial character χ of N. According to the formula for the determinant of a monomial representation [7],

$$\det \rho = \mathrm{sign}_{G/N} \cdot (\chi \circ \mathrm{tran}_{G,N}),$$

where $\mathrm{sign}_{G/N}$ is the determinant of the permutation representation of G on the cosets of N in G and $\mathrm{tran}_{G,N}$ is the transfer from the abelianization G^{ab} of G to $N^{\mathrm{ab}} = N$. Since $|G^{\mathrm{ab}}| = |P| = 4$ and $|N| = 5$ the transfer is trivial, and $\det \rho = \mathrm{sign}_{G/N}$. Now the elements of P form a set of coset representatives for N in G, and thus the permutation representation of P on G/N is the regular representation. Since P is cyclic of *even* order, the determinant of its regular representation is nontrivial, whence $\mathrm{sign}_{G/N}$ is nontrivial also. Hence $\det \rho$ is nontrivial, contradicting our hypotheses.

There remains the case $|G| = 24$. In view of (6), there are two possibilities for the irreducible representations of G (counted up to isomorphism) in addition to ρ: Either there are 8 one-dimensional characters or there are 4 one-dimensional characters and in addition a two-dimensional representation.

Consider the first of these alternatives, that there are 8 one-dimensional characters. The commutator subgroup of G is then the Sylow 3-subgroup N of G. Let P be a Sylow 2-subgroup; as before we have a map

$$\varphi : P \to \mathrm{Aut}(N) \cong \mathbb{Z}/2\mathbb{Z}. \tag{7}$$

The kernel of φ contains a subgroup M of order 4 centralizing N, and MN is an abelian normal subgroup of index 2 in G. Thus we have a contradiction as before.

Finally, suppose that there are just 4 one-dimensional characters of G, so that the commutator subgroup H of G is a normal subgroup of order 6. Then either $H \cong \mathbb{Z}/6\mathbb{Z}$ or H is the symmetric group on 3 letters, but in either case, the subgroup N of order 3 in H is unique. Since H is normal in G so is N; in other words, the Sylow 3-subgroup N of G is normal. As before, let P be a Sylow 2-subgroup, and let φ be as in (7). The argument is now completed as in the previous paragraph. □

Remark. Since an irreducible self-dual representation is either orthogonal or symplectic, we can replace *self-dual* in the statement of the theorem by *orthogonal* if we like. But we would still need to retain the condition that $m(\rho) = 1$, because it is entirely possible for an irreducible orthogonal representation to have Schur index 2, even though the local Schur index at infinity would be 1.

3. Addendum: Coprimality of conductors

The proposal that (2) should hold with probability 1 for any elliptic curve E over $\mathbb{Q}$ strikes me as the most straightforward generalization of the corresponding conjecture about ranks. However one could argue that the correct generalization is more restrictive: With probability 1, the inequality (2) holds as E varies over elliptic curves with conductor *prime to the conductor of* ρ. Of course if $\rho = 1_{\mathbb{Q}}$ then the coprimality condition holds for all E. In this connection we recall that if ρ is self-dual and the conductors of E and ρ are relatively prime then there is a simple formula for $W(E, \rho)$ (cf. [11], p. 337, Proposition 10):

$$W(E, \rho) = \chi_\rho(-N_E)W(E)^{\dim \rho}, \tag{8}$$

where N_E is the conductor of E and χ_ρ is the determinant of ρ, viewed as a primitive Dirichlet character via class field theory. Also $W(E) = W(E, 1_{\mathbb{Q}})$. Note that χ_ρ is either quadratic or trivial since ρ is self-dual. The table below distinguishes between four cases of (8).

$\dim \rho$	$\det \rho$	$W(E, \rho)$
even	trivial	1
odd	trivial	$W(E)$
even	nontrivial	$\chi_\rho(-N_E)$
odd	nontrivial	$\chi_\rho(-N_E)W(E)$

Of particular note is the second row of the table, where ρ has odd dimension but trivial determinant. Now if we return to (1) for a moment, we may paraphrase the associated conjecture by saying that with probability 1, the rank of $E(\mathbb{Q})$ is determined by $W(E)$. And for a fixed self-dual ρ, a similar paraphrase applies to (2) with rank and $W(E)$ replaced by $\langle \rho, E \rangle$ and $W(E, \rho)$. But if these statements are true, then for a fixed ρ of odd dimension and trivial determinant we have

$$\langle \rho, E \rangle = \text{rank of } E(\mathbb{Q})$$

with probability 1 as E varies over elliptic curves over $\mathbb{Q}$ of conductor prime to the conductor of ρ.

References

[1] J. Balakrishnan, W. Ho, N. Kaplan, S. Spicer, W. Stein J. Weigandt, *Databases of elliptic curves ordered by height and distributions of Selmer groups and ranks*, LMS J. of Computation and Math. 19 Issue A (Algorithmic Number Theory Symposium XII) (2016), 351-370.

[2] B. Bektemirov, B. Mazur, W. Stein, M. Watkins, *Average ranks of elliptic curves: Tension between data and conjecture*, Bull. AMS 44 (2007), 233-254.

[3] M. Bhargava, A. Shankar, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, Ann. of Math. 181 (2015), 191-242.

[4] M. Bhargava, A. Shankar, *Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0*, Ann. of Math. 181 (2015), 587-621.

[5] R. Brauer, *Untersuchungen über die arithmetischen Eigenschaften von Gruppen linearer Substitutionen II*, Math. Zeitschrift 31 (1930) 733-747.

[6] P. Deligne, *Valeurs de fonctions L et périodes d'intégrales* In: *Automorphic Forms, Representations, and L-functions*, Proc. Symp. Pure Math. vol. XXXIII, Part 2, AMS (1979), 313-346.

[7] P. X. Gallagher *Determinants of representations of finite groups*, Abh. Math. Sem. Univ. Hamburg 28 (1965), 162-167

[8] D. Goldfeld, *Conjectures on elliptic curves over quadratic fields*, Number theory, Carbondale 1979 (Proc. Southern Illinois Univ. Carbondale, Ill. 1979) Lecture Notes in Math. 751) Springer (1979), 108-118.
[9] D. E. Rohrlich, *The vanishing of certain Rankin-Selberg convolutions*. In: Automorphic Forms and Analytic Number Theory, Les Publications CRM, Montreal (1990), 123 – 133.
[10] D. E. Rohrlich, *Elliptic curves and the Weil-Deligne group*. In: *Elliptic Curves and Related Topics*, HKisilevsky and M. R. Murty, eds, CRM Proceedings and Lecture Notes 4, Amer. Math. Soc. (1994), 125 – 157.
[11] D. E. Rohrlich, *Galois theory, elliptic curves, and root numbers*, Compos. Math. 100 (1996), 311 – 349.
[12] D. E. Rohrlich, *Realization of some Galois representations of low degree in Mordell-Weil groups*, Mathematical Research Letters 4 (1997), 123 - 130.
[13] D. E. Rohrlich, *Galois representations in Mordell-Weil groups of elliptic curves*, Cubo: Mat. Educacional 3 (2001), 149-160.
[14] D. E. Rohrlich, *Multiplicities in Mordell-Weil groups*, to appear.
[15] J.-P. Serre, *Linear Representations of Finite Groups*, Springer GTM 42 (1977).
[16] A. Suresh, *Realizing Galois representations in abelian varieties by specialization*, to appear.
[17] M. Watkins, *Some heuristics about elliptic curves*, Experimental Math. 17 (2008), 105-125.

Department of Mathematics and Statistics, Boston University, Boston, MA 02215
Email address: rohrlich@math.bu.edu