NEW RATIONAL POINTS OF ALGEBRAIC CURVES

BARRY MAZUR AND KARL RUBIN

This is just a very rough draft of notes written jointly with Karl Rubin. I presented a small bit of this material at the conference — Journée Gretchen et Barry Mazur*—held on July 5 2019 at the IHES.*

Contents

1. Some thoughts about the early IHES

I first visited the IHES roughly six decades ago, on the very first year it established itself in Bures-sur-Yvette. The Résidence de l'Ormaille hadn't been set up yet. Professors and visitors were all lodged in the Résidence Gratien. Thom was expanding our understanding of the fundamental notion of singularities in differential topology, of structural stability and of morphogenesis. Grothendieck was transforming algebraic geometry, and—en passage—an impressive amount of the vocabulary of mathematics, and of its practice.. A favorite phrase of his was: "X" (i.e., whatever he began his discussion with) "n'est rien d'autre que Y" often thereby changing a point of view in some essential way.

And—at the same time—there were so many other important things going on in this extraordinarily inspiring place. I'm so grateful for having had the chance of learning a good amount of my mathematics here, and am happy that the IHES continues to thrive, and to inspire.

And, of course, I'm overwhelmed by Will Hearst's creation of a visiting professorship chair at the IHES in Gretchen's name and mine. I don't see that we deserve this extraordinary honor, but I do see this development as, yet again, an example of Will's wonderful generous spirit for the grand culture of mathematics, for his devotion to our subject, as he is even more broadly devoted to the world of science, literature, and the arts.

How wonderful it is for me to see that Sasha Goncharov will be the first recipient of this chair, and to see so many great friends here at this event. Much thanks to Bernard Saint-Donat and Emmanuel Ullmo for organizing it.

Part 1. Questions

2. Differently quantified questions regarding Diophantine stability

A. New points. This lecture is a survey of questions and issues that Karl Rubin and I are currently are thinking about. The general topic is 'the appearance of new rational points on a variety, upon extension of the base field.' Much of this project is empirical: computations to develop a sense of the nature of certain distributions[1] that are—conjecturally—connected to the issues we want to understand.

Definition 1. *A variety V defined over K is* **Diophantine stable** *(DS) for the field extension L/K if V 'acquires no new rational points when one extends the base from K to L. This is, if $V(L) = V(K)$.*

For example, if V contains the nonconstant image of an open subscheme in $\mathbb{P}^1_{/K}$, then *no nontrivial extension L/K is DS.* Is the converse true?

B. Quantification. If one formulates questions regarding a single notion, but quantifies the fundamental data differently, the questions can have quite different characters. The data regarding Diophantine stability consists of:

- the variety $V_{/K}$,
- the extension L/K and
- the isomorphism class of the Galois group G of the Galois closure of L/K.

C. The question of Diophantine Instability for a fixed variety and fixed isomorphism class of the Galois group G of the extension L/K.

This is somewhat akin to the "Inverse Galois Problem" of classical Galois Theory.

Definition 2. *Let G be a finite group, and V a variety over a number field K. Say that V is* **significantly (Diophantine) stable** *for G if there are only finitely many Galois extensions L/K with Galois group isomorphic to G, relative to which V is Diophantine unstable.*

[1] of values of certain appropriately normalized "θ-coefficients"

Moreover, if $V = A$ is an abelian variety over K, and L/K is Galois with group G, this relative question (Diophantine stability or instability) has variants, such as ignoring torsion and considering

$$A(K) \otimes \mathbb{Q} \subset A(L) \otimes \mathbb{Q},$$

and—fixing a given (irreducible, say) representation G with character χ—asking whether for infinitely many Galois extensions L/K with Galois group isomorphic to G the specific character χ occurs in the G-representation $A(K) \otimes \mathbb{Q} \subset A(L) \otimes \mathbb{Q}$.

Proposition 2.1. *Fix any positive integer n, any elliptic curve E, and any number field K. There are infinitely many Galois extensions L/K with Galois group isomorphic to the symmetric group S_n such that if χ is the character of the 'standard representation' of S_n, χ occurs in the S_n-representation $E(L) \otimes \mathbb{Q}$. (So, following Definition 2) E is Diophantine unstable for S_n.*

Remarks 1. (i) *The proof of Proposition 2.1 is given first by combining the two files*[2]*:*

- *simple.branching.lemma.pdf sent to us by Joe Harris, and*
- *For.S_n.result.*

and then by applying the triple of results: The Hilbert Irreducibility Theorem, Faltings' Theorem and the (proved) Manin-Mumford Conjecture. See a bit more about this in Section 4 below.

(ii) *One has a similar conclusion for abelian varieties—but not as sharp:*

Proposition 2.2. *Fix an abelian variety A over a number field K. For $n \gg_A 0$ there are infinitely many Galois extensions L/K with Galois group isomorphic to the symmetric group S_n such that if χ is the character of the 'standard representation' of S_n, χ occurs in the S_n-representation $A(L) \otimes \mathbb{Q}$.*

For more, see Section 4 below.

(iii) *We don't know whether the same is true for the Alternating groups A_n. But we're trying to prove:*

Proposition 2.3. *(?) For any algebraic j-invariant j_0 and any positive odd integer n there is an elliptic curve E over a number field K with j-invariant equal to j_0 for which there*

[2] that I will include in the next draft of these notes

are infinitely many Galois A_n-extensions L/K such that the standard representation of A_n occurs in the A_n-representation space $E(L) \otimes \mathbb{Q}$.

For the idea behind the hoped-for proof of this, see Section 4 below. See also Corollary 6.14 below for an explicit example over an explicit number field.

(iv) *For the question of whether there are elliptic curves that are Diophantine unstable relative to certain fixed Galois extensions (of low degree) see* [25].

(v) *The above type of question, framed in arithmetic language, has, conjecturally, a closely related question framed in analytic language.*

Specifically, letting $L(A_{/K}, \chi; s)$ be the Hasse-Weil L-function of the abelian variety A twisted by the character χ, then—conjecturally—the character χ occurs in the G-representation $A(K) \otimes \mathbb{Q} \subset A(L) \otimes \mathbb{Q}$ if and only if $L(A_{/K}, \chi; 1) = 0$.

D. The question for varying curves of genus > 1, and a fixed Galois extension L/K.

In [6], Lucia Caporaso, Joe Harris and I made a conjecture[3] that implies the following:

Conjecture 1. *Let K be a number field and $g > 1$. Then for any Galois extension L/K with simple Galois group of order $|\mathrm{Gal}(L/K)| \gg 0$, only finitely many curves of genus g defined over K are diophantine unstable for the extension L/K.*

We include the possibility that $\mathrm{Gal}(L/K)$ is cyclic of prime order.

E. The question of Diophantine Stability for a fixed curve (of genus > 0) and cyclic Galois extensions.

[3] In our paper [6] (published over a quarter of a century ago) we claimed to show that our conjecture follows from the "Strong Lang Conjecture," but thanks to correspondence with Jacob Stix we see that the argument published was not correct, or at the very least: incomprehensible. We're actually currently preparing a revision of [6]. Nevertheless we *do believe* the truth of our conjecture.

Karl Rubin and I proved—a few years ago—the following theorem (stated for a given *single* curve of positive genus or abelian variety; see [20]).

Theorem 2.4. *Let C be a (smooth geometrically irreducible projective) curve of genus > 0 over a number field K_0; let—respectively— A be any geometrically simple abelian variety over K_0. There is a finite extension K/K_0 and a 'Cebotarev class' (and consequently a class of positive density) of prime numbers ℓ (both K/K_0 and the arithmetic progression depending on C—respectively, on A) such that for any positive integer n there are infinitely many cyclic (Galois) extensions L/K with Galois group isomorphic to $\mathbb{Z}/\ell^n\mathbb{Z}$ for which C—respectively, A—is Diophantine stable.*

We expect that a good deal more than this is true. (See Conjecture 3 below.)

Note: A corollary (an easy exercise) of Theorem 2.4 is that for any elliptic curve E over K there are uncountably many fields of algebraic numbers M/K for which $E(M)$, the group of M-rational points of E, is finitely generated. This implies, for example, that there are uncountably many fields of algebraic numbers for which Hilbert's Tenth Problem has a negative solution.

F. The question of Diophantine Stability for elliptic curves and cyclic field extensions.

For cyclic Galois extensions of degree $d \geq 2$ prime, let $N^{\mathrm{arith}}_{E,d}(X)$ denote the number of such extensions in $\bar{\mathbb{Q}}$ and of conductor $< X$ for which an elliptic curve E acquires a higher Mordell-Weil rank; i.e., higher than *rank* $E(\mathbb{Q})$.

G. Quantitative guesses. The classical BSD conjecture would have

$$N^{\mathrm{arith}}_{E,d}(X) \stackrel{?}{=} N^{\mathrm{anal}}_{E,d}(X) := \frac{1}{d-1}|\{\chi \text{ of order } d;\ \mathrm{cond}(\chi) < X \mid L(E,\chi,1) = 0\}|.$$

The following conjecture is due to Conrey, Keating, Rubinstein, and Snaith [8] for $p = 2$, and David, Fearnley, and Kisilevsky [9, 10] for p odd.

Conjecture 2 ([8, 9, 10])**.**

(i) $N^{\mathrm{anal}}_{E,2}(X) \ll_E X^{3/4}\log(X)^{c_{E,2}}$, *with* $c_{E,2} \in \mathbb{R}$ *depending on* E,

(ii) $N_{E,3}^{\mathrm{anal}}(X) \ll_E \sqrt{X}\log(X)^{c_{E,3}}$, *with* $c_{E,3} \in \mathbb{R}$ *depending on* E,
(iii) $N_{E,5}^{\mathrm{anal}}(X) \ll_E \log(X)^{3/2}$,
(iv) $N_{E,p}^{\mathrm{anal}}(X)$ *is bounded independently of* X *if* $p \geq 7$.

Remark 2.5. These conjectures stated for $N_{E,d}^{\mathrm{anal}}(X)$ imply (unconditionally) the corresponding conjectures for $N_{E,d}^{\mathrm{alg}}(X)$.

H. The question for abelian Galois groups G. The question is open, for example, for cyclic groups of prime order. The conjecture (2 above) of David-Fearnley-Kisilevsky that (in effect) for any elliptic curve over $\mathbb{Q}$ a cyclic group of prime order p is significantly unstable if and only if $p \leq 5$ is based on random matrix heuristics.

Inspired by their result (and dependent on a certain naive heuristic related to modular symbols—see Part 2 below)—a heuristic supported by computations regarding our conjectured distributions of θ-coefficients (Section 2 below) suggests:

Conjecture 3. *Any elliptic curve over* $\mathbb{Q}$ *has finitely generated Mordell-Weil group over any abelian field that contains only finitely many subfields of order* < 7.

3. Pencils of Diophantine instability

In seeking examples of varieties and isomorphism classes of groups G for which they are *significantly unstable* (as in Definition 2 above) it is natural to look for rationally parametrized Galois coverings; i.e., maps $C \to \mathbb{P}^1$ with Galois group isomorphic to G (for which C admits a (nonconstant) K-rational map to the variety in question). There are a few different ways of searching for such structures, and we will discuss two such ways below—restricting attention to the case where the variety is an elliptic curve E.

A. G-pencil coverings of E. Let G be a finite group and M a free abelian group of finite rank r, with a linear G-action. We view M as $\mathbb{Z}[G]$ module. Set $V := M \otimes_{\mathbb{Z}} \mathbb{Q}$. Assume that $V = M \otimes \mathbb{Q}$ is an irreducible G-representation, and let χ denote its character.

If E is an elliptic curve over a number field K, form $\mathcal{X}(E, M) := E \otimes_{\mathbb{Z}} M$, the r-dimensional abelian variety with G-action defined in the evident way, noting that any choice of $\mathbb{Z}$-basis of M allows us to pinpoint an isomorphism

$$E \otimes_{\mathbb{Z}} M \simeq E^r.$$

Now form the r-dimensional quotient variety over K,

$$E \otimes_{\mathbb{Z}} M \quad \xrightarrow{\pi} \quad Y(E,M) := E \otimes_{\mathbb{Z}} M/\{\text{action of } G\}.$$

If $y = \mathrm{Spec}(K) \hookrightarrow Y(E,M)$ is a K-valued point, let

$$\begin{array}{ccc} \mathcal{X}_y & \longrightarrow & \mathcal{X} = E \otimes_{\mathbb{Z}} M \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathrm{Spec}(K) = y & \xrightarrow{\hookrightarrow} & Y(E,M). \end{array} \tag{3.1}$$

be the corresponding Cartesian diagram, the top line being, naturally, a G-equivariant mapping.

If, in addition, y is not a branch point of $\mathcal{X} \xrightarrow{\pi} Y(E,M)$, i.e., if $\mathcal{X}_y = \mathrm{Spec}(A)$ where A is an étale K-algebra of rank $|G|$, write $A = \prod_{j=1}^{\nu} K_j$ where K_j/K are field extensions. We have the natural action of G on

$$\mathrm{Spec}(A) = \sqcup_{j=1}^{\nu} \mathrm{Spec}(K_j) = \sqcup_{j=1}^{\nu} \xi_j \hookrightarrow \mathcal{X}$$

For $j = 1, 2, \ldots, \nu$, denote by $G_j \subset G$ the isotropy subgroup of G relative to $\mathrm{Spec}(K_j) = \xi_j$; that is $G_j := \{g \in G \mid g \cdot \xi_j = \xi_j\}$. So we have a natural injection $\eta_j : G_j \hookrightarrow \mathrm{Aut}_K(K_j)$. By comparing the rank of A over K and the order of G we see that these injections η_j must be isomorphisms, i.e., the extensions K_j/K are all Galois and the η_j can be interpreted as natural isomorphisms

$$G_j \simeq \mathrm{Gal}(K_j/K). \tag{3.2}$$

Proposition 3.3. *Suppose there exists a K-rational point $y \in Y(E,M)$. (With the notation as above) suppose further that the set*

$$\xi_j \otimes_{\mathrm{Spec}(K)} (\mathbb{C}) \subset E \otimes_{\mathbb{Z}} M(\mathbb{C})$$

does not consist of torsion points, Then the $\mathrm{Gal}(K_j/K)$-representation $E \otimes_{\mathbb{Z}} M(K_j)$ contains a (positive) number of copies of the restriction of χ to $\mathrm{Gal}(K_j/K)$.

Corollary 3.4. *Suppose, in addition to (and in the notation of) Proposition 3.3 that—relative to the point y, $\nu = 1$ or equivalently $A = K_1$; and so, by 3.2, we have*

$$G = Aut_K(A) = \mathrm{Gal}(K_1/K) = G_1. \tag{3.5}$$

The set $\xi_j \otimes_{\mathrm{Spec}(K)} (\mathbb{C}) \subset E \otimes_{\mathbb{Z}} M(\mathbb{C})$ does not consist of torsion points. Then, denoting again by χ the character on $G_K := \mathrm{Gal}\bar{K}/K)$ induced by χ on $\mathrm{Gal}(K_1/K) = G$ via the isomorphism 3.5,we have that χ occurs in the G_K-action on the Mordell-Weil group of E over K_1.

Now suppose that $Y(E,M)$ contains $\mathcal{P}$, the birational image of a projective line over K, and let $\mathbb{P}^1 \to \mathcal{P} \simeq Y(E,M)$ be the corresponding (nonconstant) mapping. Suppose, further, that $\mathcal{P}$ contains a point y satisfying the hypothesis in Corollary 3.4. Consider the projective smooth curve C over K that is the normalization of the inverse image in $E \otimes_{\mathbb{Z}} M$:

$$\begin{array}{ccc} C & \xrightarrow{j} & E \otimes_{\mathbb{Z}} M \simeq E^r \\ \downarrow \pi & & \downarrow \\ \mathbf{P}^1 & \longrightarrow & Y(E,M) \end{array} \tag{3.6}$$

Remark 3.7. Here, the curve $C_{/K}$ is stable under the action of G, and (using diagram 3.1) the corresponding total quotient ring of $C_{/K}$ is a field F. More specifically, letting t denote a parameter for $\mathbb{P}^1$ so that the total quotient ring of $\mathbb{P}^1_{/K}$ is $K(t)$ then $F/K(t)$ is a Galois extension with Galois group G.

Projecting to the first factor in E^r we get:

$$\begin{array}{ccc} C & \xrightarrow{j} & E \\ \downarrow \pi & & \\ \mathbf{P}^1 \simeq C/G & & \end{array} \tag{3.8}$$

Definition 3. *By a* G**-pencil covering** E *let us mean a diagram such as 3.8 (defined over a number field* K*; and where* C *is a smooth projective* **geometrically irreducible** *curve with* G *action).*

We are in a position to apply the classical Hilbert Irreducibility Theorem[4] to the Galois extension of curves $C \xrightarrow{i} C/G \simeq \mathbb{P}^1$ over K, the Galois group being G.

It follows that:

3.9. *There are infinitely many* K*-rational points* $y_j \in \mathbb{P}^1(K)$ *such that* $\pi^{-1}(y_j) = \mathrm{Spec}(L_j)$ *with* L_j/K *a Galois field extension with Galois group isomorphic to* G*; and as long as* $\pi^{-1}(y)$ *does not consist of torsion points the* G*-representation space* $E(L_j) \otimes \mathbb{Q}$ *contains the irreducible representation corresponding to the character* χ*.*

[4]*noting that the Irreducibility theorem does not require* C *to be geometrically irreducible. For related issues regarding the arithmetic of branched coverings of* $\mathbf{P}^1$*, see* [3].

At this point one should distinguish between the cases where C is of genus 1, and of genus > 1

(i) C is of genus 1.

discussion to be included

(ii) C is of genus > 1.

In this case, that there are only finitely many y such that $\pi^{-1}(y) \subset C$ is torsion follows from the Manin-Mumford Conjecture—the form of it proved by Michael McQuillan (see [27], [21]). For L_j (any $j = 1, 2, \dots$) there are only finitely many L_j-rational points on C by Faltings Theorem—consequently that must be infinitely many different extensions L_j/K. This shows that in the above situation we have:

Corollary 3.10. *If E has a G-pencil covering as in Definition 3, E is significantly Diophantine unstable for G.*

B. G-pencils arising from rational functions on E.

Digression 1. *Let f be a nonconstant K-rational function f on E. We can view f as a mapping $E \xrightarrow{f} \mathbb{P}^1$ of curves over K; and also as an element $f \in K(E)$ the field of fractions of E, this element being transcendental over K. Forming the Galois closure $\mathcal{L}/K(f)$ of the field extension $K(E)/K(f)$ and passing to $C :=$ the integral closure of $\mathrm{Spec}(\mathcal{L}) \to \mathrm{Spec}(K(f))$ over $\mathbf{P}^1$ we can view $\mathcal{L}$ as $K(C)$, the total quotient ring of C. One obtains a diagram:*

(3.11)
$$\begin{array}{ccc} C & \xrightarrow{\ j\ } & E \\ \downarrow{\scriptstyle \pi} & \swarrow{\scriptstyle f} & \\ \mathbf{P}^1 \simeq C/G & & \end{array}$$

Here $G = \mathrm{Gal}(K(C)/K(f))$.

Hypothesis 3.12. *Suppose that there is no nontrivial finite étale extension of K in $K(C)$ or—equivalently—that C is geometrically irreducible.*

If Hypothesis 3.12 holds and the diagram 3.11 came—as 3.6—from a mapping of $\mathbf{P}^1$ to $Y(E, M)$ for some character χ of G we would get an explicit description of the corresponding Galois representation on the Mordell-Weil groups E over the extension fields L_j discussed above. The (possible) advantage of these G-pencils covering elliptic

curves that come from rational functions f on E (leading to diagrams such as 3.1 above) is that these may well occur in families of elliptic curves of varying j-invariant. Specifically, viewing 3.1 as a diagram of Riemann surfaces:

$$\begin{array}{ccc} C(\mathbb{C}) & \xrightarrow{\ j\ } & E(\mathbb{C}) \\ \Big\downarrow{\scriptstyle \pi} & \swarrow{\scriptstyle f} & \\ \mathbf{P}^1(\mathbb{C}) \simeq C(\mathbb{C})/G & & \end{array} \tag{3.13}$$

and composing f with a diffeomorphism

$$\mathbf{P}^1(\mathbb{C}) = S^2 \xrightarrow{\ h\ } S^2 = \mathbb{P}^1(\mathbb{C}),$$

an application of the Riemann Existence Theorem ([13]) yields a new analytic structure on E and on C leading to an interesting variation of 3.1 dependent on h in the group of diffeomorphisms of S^2:

$$\begin{array}{ccc} C^h & \xrightarrow{\ j\ } & E^h \\ \Big\downarrow{\scriptstyle \pi} & \swarrow{\scriptstyle f} & \\ \mathbf{P}^1 \simeq C^h/G & & \end{array} \tag{3.14}$$

Here $h \mapsto E^h$ may or may not provide a variation over the moduli stack $\mathcal{M}_1$.[5]

4. Regarding the standard representation of the symmetric groups

We thank Joe Harris for explaining this to us.

First note that for any integer n, any elliptic curve E over (say) any number field K admits an embedding into a projective space $\mathbb{P}^r$ as a curve of degree n (this embedding being defined over K).

Theorem 4.1. *If $X \subset \mathbb{P}^r$ is a smooth curve over a field K of characteristic 0 and $\Lambda \simeq \mathbb{P}^{r-2} \subset \mathbb{P}^r$ a general codimension 2 plane in $\mathbb{P}^r$ then the projection map from Λ,*

$$f = f_\Lambda : X \to \mathbb{P}^1,$$

[5] I want to thank Curt McMullen for explaining to us that if ν is the number of branch points in $\mathbf{P}^1(\mathbb{C})$ of the mapping π in the diagram 6.12 then $h \mapsto E^h$ comes from a mapping

$$\mathcal{M}'_{0,\nu} \longrightarrow \mathcal{M}_1,$$

where $\mathcal{M}'_{o,\nu}$ is a finite cover of the moduli stack $\mathcal{M}_{0,\nu}$.

is simply branched.

Note: We can attach Joe Harris's one-page proof of this (*simple.branching.lemma.pdf*) as an appendix—or perhaps there's a published reference for it.

Proposition 4.2. *A simply branched mapping, f_Λ, as guaranteed to exist by Theorem 4.1, has 'Galois group' S_n.*

The proof of this is in the file: *For.S_n.result.*

If E is an elliptic curve over K we therefore can find an S_n-pencil covering E (Definition 3 above):

$$C \to E \xrightarrow{f_\Lambda} \mathbb{P}^1$$

where $C \to \mathbb{P}^1$ is the Galois closure of $E \xrightarrow{f_\Lambda} \mathbb{P}^1$ for Λ rational over K and 'general .' We can apply Corollary 3.10 finishing the proof of Proposition 2.1.

The proof of Proposition 2.2 is similar. Let $A_{/K}$ be an abelian variety. We can find a K-rational curve (irreducible over K—*can we find such that is geometrically irreducible?*—passing through the origin in A. Letting $\mathcal{E}$ be the normalization of this curve, and n greater than the genus of $\mathcal{E}$ plus 2, we take $D = n \cdot \text{origin}$ and apply Riemann-Roch to find an embedding of $\mathcal{E}$ in some projective space $\mathbb{P}^r$ as a curve of degree n, and then proceed as in the proof of Proposition 2.1.

5. Regarding the standard representation of the alternating groups

Here we'll *almost* be proving Proposition 2.3: For any algebraic j-invariant j_0 and any positive *odd* integer n there is an elliptic curve E over a number field K with j-invariant equal to j_0 for which there are infinitely many Galois S_n-extensions L/K such that the standard representation of A_n occurs in the A_n-representation space $E(L) \otimes \mathbb{Q}$.

Proof: Our proof is actually over the field of complex numbers and even more: purely complex analytic. We'll consider algebraicity (and number fields as fields of definition) afterwards.

Let $U := \mathbb{P}^1$ *minus four (distinct) points:* $\{u_1, u_2, u_3, u_4\}$. The fundamental group of U is free on three generators, but it is better to think of it—in the usual way— as having four generators x_1, x_2, x_3, x_4 with the single relation:

$$x_1.x_2.x_3.x_4 = 1.$$

One chooses these x_i again in the usual way: by fixing a base point $u \in U$ and (nonintersecting) paths γ_i from u to u_i (for $i = 1, 2, 3, 4$). Define x_i to be the class in the fundamental group represented by the closed loop in U obtained by following γ_i from u to a neighborhood of u_i; then circling u_i clockwise; then returning to u via the path γ_i.

Now S_n is generated by $g_1 := (1, 2)$ and $g_3 := (1, 2, 3, 4, ..., n)$. so if we set $g_2 = g_1^{-1} = (1, 2)$ and $g_4 = g_3^{-1} = (n, ..., 3, 2, 1)$ we have that

$$g_1.g_2.g_3.g_4 = 1$$

so the rule: $x_i \mapsto g_i$ $(i = 1, 2, 3, 4)$ gives us a surjective homomorphism

$$\pi_1(U) \longrightarrow S_n. \tag{5.1}$$

The induced cover $C \to \mathbb{P}_1$ (i.e., the smooth projective curve containing, as Zariski dense open, the quotient of the universal cover of U by the kernel of 5.1) is ramified at the four points $\{x_i; i = 1, 2, 3, 4\}$ in $\mathbb{P}_1$ with Galois group S_n and inertial groups at the x_i generated by the g_i.

Note that if n is odd, then g_3 and g_4 are both in A_n so we have that the quotient C/A_n is ramified over $\mathbb{P}^1$ only over x_1 and x_2, and hence is of genus 0.

Consider $S_{n-1} \subset S_n$ (for notational convenience, suppose that it is the S_{n-1} that fixes $1 \in \{1, 2, ..., n\}$). Let E denote the quotient of C by S_{n-1} so the induced map $h : E \to \mathbb{P}^1$ is of degree n.

Lemma 5.2. *:*

(i) *The mapping h is simply branched at x_1 and x_2.*
(ii) *The mapping h is totally ramified at x_3 and x_4.*

Proof: The ramification subgroups at x_1 and x_2 are the cyclic groups of order two generated by $(1, 2), (2, 3), (3, 4)$ etc. All but one of these lie in our S_{n-1}. This shows (1). On the other hand S_{n-1} is disjoint from the subgroup generated by g_3 "or" g_4, showing (2).

Now, using Riemann-Hurwitz we compute the Euler-characteristic of E to be

$$2n - 1 - 1 - (n - 1) - (n - 1) = 0$$

This construction depends on the relative homotopy classes of the paths γ_i in $\pi_1(U; u, u_i)$ and hence so does the elliptic curve E. Now let $j(\gamma_1, \gamma_2, \gamma_3, \gamma_4) \in \mathbb{C}$ denote the j-invariant of E. To finish the proof of Proposition 2.3 it remains to show:

Lemma 5.3. *?? The function $j(\gamma_1, \gamma_2, \gamma_3, \gamma_4)$ is not constant.*

and

Lemma 5.4. *If the points x_i are algebraic, the curves and mappings $C \to E \to \mathbb{P}^1$ are defined over some field K of finite degree over $\mathbb{Q}$.*

I think that Lemma 5.3 must be true; but why?

6. Cyclic groups

Let G be a cyclic group of order d, and χ the irreducible representation of G over $\mathbb{Q}$ of dimension $\phi(d)$ (Euler's function). Let E be an elliptic curve over $\mathbb{Q}$, and let $Y(E, M)$ the $\phi(d)$-fold as defined in Section 3 above.

A. The case $\phi(d) = 2$.

A.1. $d = 3$. This case is beautifully discussed in [12]. Here $Y(E, M)$ is a surface over K that is a twist of the double cover over the plane of the (degree six) dual curve to E. This surface has nine singularities, and when desingularized, yields a K3 surface of Picard number 19. It would be of interest to find K-rational rational curves in $Y(E, M)$ for *any* elliptic curve over K.

Points of $Y(E, M)$ are the image of triples of points (P, Q, R) of E such that $P + Q + R = 0$. These are then in correspondence with lines in $\mathbf{P}^2$. This represents $Y(E, M)$ as a double cover of the dual space of $\mathbb{P}^2$. The ramification locus of this double cover consist of elements of $(\mathbb{P}^2)^*$ corresponding to the image of triples of points $(P, P, -2P)$ of E, i.e., tangent lines to E. So:

Lemma 6.1. *The ramification locus of the double cover*

$$Y(E, M) \to (\mathbb{P}^2)^*$$

is $E^* \subset (\mathbb{P})^*$, the dual curve to E in $(\mathbb{P}^2)^*$. The curve E^* is a sextic with nine singular points corresponding the the points (P, P, P) for $P \in E[3]$.

Remark: If $E = E_{a,b} : y^2 = x^3 + ax + b$, then $Y(E, M)$ is given by the equation $w^2 = \Delta(u, v)$ where

$$\Delta(u, v) = -4a^3 + a^2(u^4 + 24uv) + a(-18bu^2 - 4u^5v - 30u^2v^2)$$
$$-27b^2 + b(4u^6 + 36u^3v + 54v^2) - 4u^3v^3 - 27v^4.$$

For example, for $E : y^2 = x^3 - 9x + 9$ (i.e., $a = -9, b = 9$) and $r(t) := 8(t^2 - 162t)/(t^2 + 8748)$ one computes to find that the points (x, y) on

the curve E with $y = 3x + r(t)$ for rational values of t parametrize cubic cyclic points on E.

Problem: Find K-rational rational lines in $Y(E, M)$ for any E over K.

Lemma 6.2. *If E admits a cyclic 3-isogeny over K, then E is covered by a cyclic pencil of degree 3 (but possibly only defined over a quadratic extension of K).*

Proof. (Or, at least, a sketch of a proof:) Let $Z \subset E[3] \subset E^*$ be the cyclic group of order 3 which is the kernel of that isogeny. Draw the straight line in the dual projective plane that contains the image of the two nonzero points in Z. The inverse image of this line splits into two genus zero curves in $Y(E, M)$. □

A.2. $d = 4$. Again $Y(E, M)$ when desingularized, yields a K3 surface... that we should study, but haven't yet.

B. The case $d = 5$. The classical "Bring's Curve" $\mathcal{C}$ (cf. [5], [11], [16]) is defined over $\mathbb{Q}$ and will provide an example (e.g., over the field of Gaussian numbers $\mathbb{Q}[i]$) of a cyclic pencil of genus 4 for a certain elliptic curve $\mathcal{E}$. "Bring's curve" is the (smooth, projective) curve in $\mathbf{P}^4$ defined by three equations—in the five homogenous variables $(x_1, x_2, x_3, x_4, x_5)$:

$$\sum_i x_i^n = 0 \text{ for } n = 1, 2, 3. \tag{6.3}$$

Visibly $\mathcal{C}$ admits the symmetric group S_5 as group of automorphisms (all of this defined over $\mathbb{Z}$) the action being by permutation of the five variables. The group S_5 is the entire group of its automorphisms since $\mathcal{C}$ is a curve of genus 4. Also, $\mathcal{C}$ has no real points since its quadratic defining equation has none.

Let $\tau := (12345)$, and $\sigma := (1234)$ be the indicated 5- and 4- cycles, respective.

Proposition 6.4. (i) *There are exactly four fixed points of τ in $\mathcal{C}$. Namely: $\{(1, \zeta, \zeta^2, \zeta^3, \zeta^4)\}$ where ζ runs through the nontrivial fifth roots of 1. These are the only points of ramification for the mapping*

$$\mathcal{C} \to \mathcal{C}/\{\text{action of } \tau\}.$$

(ii) *There are exactly two ramified points for the mapping*

$$\mathcal{C} \to \mathcal{C}/\{\text{action of } \sigma\}.$$

Namely: $\{(1, \pm i, -1, \mp i, 0)\}$. *These two points are all fixed points of* σ*; i.e., they are 'totally ramified.'*

Proof. Taking the indices $1, 2, 3, 4, 5$ mod 5, for a ($\mathbb{C}$-valued) point $(x_1, x_2, x_3, x_4, x_5)$ to be a fixed point of τ we must have, for some $\lambda \in \mathbb{C}$ that $x_{k+1} = \lambda x_k$ for all $k \in \mathbb{Z}/5\mathbb{Z}$ which forces λ to be a fifth root of unity, and by the linear equation in 6.3 it must be a nontrivial fifth root of unity. For each such λ there is exactly one such point, proving (1).

For (2):

Lemma 6.5. *If* $x = (x_1, x_2, x_3, x_4, x_5)$ *is a fixed point of* $\sigma^2 = (13)(24)$*, then* $x_5 = 0$*.*

Proof. If x is such a fixed point, then there is a $\lambda \in \mathbb{C}$ such that $\sigma^2(x)_k = \lambda \cdot x_k$ for all five coordinates x_k. In particular,

$$x_3 = \lambda x_1;\ x_4 = \lambda x_2; x_5 = \lambda x_5.$$

By the latter equality (if $x_5 \neq 0$) it would follow that $\lambda = 1$. That is, $x = (a, b, a, b, c)$ for some a, b, c, with $c \neq 0$. The linear equation in 6.3 gives $c = -2(a + b)$ so a and b cannot both be zero. Without loss of generality, suppose that $a \neq 0$, and scale it so that $a = 1$. So, the linear equation in 6.3 gives

$$c = -2(b + 1) \tag{6.6}$$

and combined with the quadratic equation in 6.3,
i.e., $c^2 = -2(a^2 + b^2)$, we get that

$$b = \frac{5}{3} \text{ or } \frac{11}{3}. \tag{6.7}$$

Now comparing 6.6 with the cubic equation in 6.3 gives the relation $b^3 + 1 = 4(b + 1)^3$ and neither value in 6.7 satisfies this. □

Now let $x = (x_1, x_2, x_3, x_4, 0)$ be a fixed point of $\sigma^2 = (13)(24)$. Such a point satisfies the relations $x_3 = \lambda x_1$ and $x_4 = \lambda x_2$ for $\lambda \in \{\pm 1\}$. Again, without loss of generality we may suppose that $x_1 \neq 0$, and scaling suitably, $x_1 = 1$. So, putting $x_2 = b$, our point is of the form $x = (1, b, \lambda, \lambda b, 0)$. The linear equation in 6.3 then gives: $(1+\lambda)(1+b) = 0$; i.e., either $b = -1$ in which case the quadratic equation in 6.3 is violated, or else $\lambda = -1$ and the quadratic equation in 6.3 tells us that $b = \pm i$. Therefore $\{(1, \pm i, -1, \mp i, 0)\}$ are the only fixed points of $\sigma^2 = (13)(24)$.

Noting that $\{(1, \pm i, -1, \mp i, 0)\}$ are actually fixed under σ concludes the proof of Proposition 6.4. □

Corollary 6.8. *Let $\mathcal{P}$ (resp: $\mathcal{E}$) denote the quotient of $\mathcal{C}$ (over the field $\mathbb{Q}$) by the action of $\tau = (12345)$ (resp: $\sigma = (13)(24)$). Then $\mathcal{P}$ is of genus 0 and $\mathcal{E}$ is of genus 1.*

Proof. Recall that the Euler characteristic of Bring's curve is -6. If u and v denotes the Euler characteristics of $\mathcal{P}$ and $\mathcal{E}$ respectively, the Riemann-Hurwitz formula and Proposition 6.4 give:

$$-6 = 5u - 4 \cdot 4 \quad \text{and} -6 = 4v - 2 \cdot 3 \tag{6.9}$$

That is: $u = 2$ and $v = 0$. □

If K is a number field over which $\mathcal{C}$ has a K-rational point, then $\mathcal{P} \simeq \mathbf{P}^1$ (over K) and taking the image of that point in $\mathcal{E}$ as the 'origin' we view $\mathcal{E}$ as an elliptic curve over K. The structure

$$\mathcal{P} \underset{\pi}{\leftarrow} \mathcal{C} \xrightarrow{j} \mathcal{E} \ , \tag{6.10}$$

is a cyclic pencil of degree 5 (and genus 4) for the elliptic curve $\mathcal{E}$ over K. Moreover, it induces a mapping of $\mathcal{P}$ into $Y(\mathcal{E}, \chi)$ where χ is the character of the irreducible representation of dimension 4 (over $\mathbb{Q}$) of the cyclic group of order 5.

As a consequence we have that $\mathcal{E}_{/K}$ is significantly Diophantine unstable for a cyclic group of order 5.

Question 6.11. *Are there cyclic pencils of degree 5 (and genus 4) for other elliptic curves?*

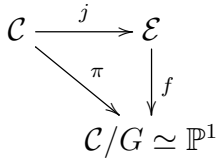
Note that since $\tau = (12345)$ and $:\sigma = (13)(24)$ are both in the alternating group $A_5 \subset S_5$, if we pass to the quotient of $\mathcal{C}$ by the action of A_5 we get a diagram:

(6.12)

$$\begin{array}{ccccc} & & \mathcal{C} & \xrightarrow{j} & \mathcal{E} \\ & \swarrow & \downarrow{\scriptstyle \pi} & \swarrow{\scriptstyle f} & \\ \mathcal{C}/\{\tau\} \simeq \mathcal{P} & \longrightarrow & \mathcal{C}/G & & \end{array}$$

with $G = A_5$.

It follows that $\mathcal{C}/G$ is of genus zero, and more specifically , $\mathcal{C}/G_{/K} \simeq \mathbb{P}^1$, so 6.12 is a diagram of the 3.1 type:

(6.13)


as discussed in Section 3 above.

Corollary 6.14. *$\mathcal{E}_{/K}$ is significantly Diophantine unstable for (the standard representation of) the alternating group A_5.*

Part 2. Some comments about heuristics

For E an elliptic over $\mathbb{Q}$, $F/\mathbb{Q}$ a Galois extension, and χ a character of an irreducible representation of $\mathrm{Gal}(F/\mathbb{Q})$, a standard conjecture asserts that χ occurs in the $\mathrm{Gal}(F/\mathbb{Q})$-representation space $E(F) \otimes \mathbb{Q}$ if and only if $L(E, \chi, 1) = 0$ (where $L(E, \chi, s)$ is the Hasse-Weil L-function of E twisted by χ).

So, $F/\mathbb{Q}$ is Diophantine unstable for E if and only if either $L(E, \chi, 1) = 0$ or else E has more F-rational torsion points than $\mathbb{Q}$-rational ones. That is, the frequency of vanishing of $L(E, \chi, 1)$ for varying χ is *largely* indicative of Diophantine stability.

In fact the conjectures we alluded to above, as formulated in [8] and [9], [10], were phrased (analytically) in terms of vanishing of $L(E, \chi, 1)$ rather than arithmetically in terms of acquisition of rational points. Those conjectures were supported, as we mentioned, by random matrix heuristics.

Karl Rubin and I have been considering another (perhaps more naive) heuristic based (in effect) on the distribution of values of $L(E, \chi, 1)$. Our predictions are qualitatively in accord with those bolstered by random matrix statistics. Our heuristic takes off from the fact that the values of $L(E, \chi, 1)$ are expressible in terms of (certain sums of) modular symbols. The statistics for modular symbols has great interest in itself, results about it having recently been achieved by three different collaborations (working independently, and focusing on different aspects of the general problem: [23], [24]; [18]; [4]).

Let E be an elliptic curve over $\mathbb{Q}$. To give the basic idea we will only discuss here the case where E is semistable. Consider fields $F/\mathbb{Q}$ that are finite cyclic extension of odd degree d.

The **θ-element**[6] (over F, associated to E) is an element in the integral group ring,

$$\theta_F \in \mathbb{Z}[\mathrm{Gal}(F/\mathbb{Q})]$$

We have

$$\theta_F = \sum_{\gamma \in \mathrm{Gal}(F/\mathbb{Q})} c_{F,\gamma} \cdot \gamma \in \mathbb{Z}[\mathrm{Gal}(F/\mathbb{Q})] \tag{6.15}$$

We will refer to the $c_{F,\gamma} \in \mathbb{Z}$ as *θ-coefficients*.

The basic feature of theta elements of interest to us is the following:

Proposition 6.16. *Suppose $F/\mathbb{Q}$ is a finite real cyclic extension of conductor m and $\chi : \mathrm{Gal}(F/\mathbb{Q}) \to \mathbb{C}^*$ is a character Then*

$$\bar{\chi}(\theta_F) = (\text{a nontrivial factor}) \cdot L(E, \chi, 1) \tag{6.17}$$

[7]

Note the simple proposition (following from 6.17):

Proposition 6.18. *These are equivalent:*

- *$\bar{\chi}(\theta_F) = 0$ for some nontrivial character χ cutting out F (equivalently for all such characters).*
- *$L(E, \chi, 1) = 0$ for some nontrivial character χ cutting out F (equivalently for all such characters).*
- In the case where the degree $d = p$ is prime *the above two bullets are equivalent to the statement that θ-coefficients are all equal; i.e.,*

  $$c_{F,\gamma} = c_{F,\gamma'}$$

  for all $\gamma, \gamma' \in \mathrm{Gal}(F/\mathbb{Q})$.

These are strong constraints for vanishing of $L(E, \chi, 1) = 0$—e.g., the last item of the above proposition.

C. 'Regularities'. Of course there are other relevant relations between the theta coefficients... e.g., as imposed on them via various structures, for example:

(i) *The sum of all the θ-coefficients of a given θ-element:*

[6]—cf. *** for an exposition of this material and in a more general context

[7] E.g., when $\chi : \mathrm{Gal}(F/\mathbb{Q}) \hookrightarrow \mathbb{C}^*$, then $\bar{\chi}(\theta_F) = (\delta_E \frac{\tau(\bar{\chi}))L(E,\chi,1)}{\Omega}$ where δ_E is the l.c.m. of the orders of the rational torsion points of E times the Manin Constant [1]. on E) and $\Omega := \Omega_E$ is the real period of E.

Let $F/\mathbb{Q}$ be cyclic of order $p > 2$ and of conductor m with Galois group G. Suppose, further that:

(*) m is squarefree and relatively prime to the conductor of E.

Then one has:

$$\sum_{\gamma \in G} c_{F,\gamma} = \prod_{\ell \mid m} (a_\ell - 2) \cdot u_E. \tag{6.19}$$

where a_ℓ is the ℓ-th Fourier coefficient of the newform f_E attached to the elliptic curve E and where u_E is a rational number, dependent only on E, and zero if and only if $L(E,1) = 0$.

Note that when **(*)** holds, the equivalent conditions of 6.18 are also equivalent to the statement that:

(**) the value of all the θ-coefficients $c_{F,\gamma}$ is equal to

$$\frac{1}{p} \cdot \prod_{\ell \mid m} (a_\ell - 2) \cdot u_E,$$

allowing us the side-comment that if $p \gg_E 0$ then for any character χ of order p, of squarefree conductor m prime to the conductor of E then $L(E,\chi;1) = 0$ implies that there exists a prime divisor ℓ of m such that $a_\ell \equiv 2 \mod p$.

(ii) *A duality coming from the classical functional equation—or equivalently the Atkin-Lehner relation:*

Namely, for $F/\mathbb{Q}$ cyclic of prime degree, let

$$e := g.c.d.(N, m),$$

where $m :=$ the conductor of F and (recall:) $N =$ the conductor of E. There is an involution (*of sets, not necessarily of groups*), $\iota_e : \mathrm{Gal}(F/\mathbb{Q}) \to \mathrm{Gal}(F/\mathbb{Q})$ such that if $\gamma' := \iota_e(\gamma)$ for $\gamma \in \mathrm{Gal}(F/\mathbb{Q})$, then

$$c_{F,\gamma} \quad = \quad -w_e \cdot c_{F,\gamma'} \tag{6.20}$$

where $w_e \in \{\pm 1\}$ is the eigenvalue of the Atkin-Lehner operator W_e acting on the modular form f_E.

Definition 4. *In the above context an element $\gamma \in \mathrm{Gal}(F/\mathbb{Q})$ is called* **generic** *if $\iota_e(\gamma) \neq \gamma$ and* **special** *if it is fixed by ι_e.*

Note that one might expect somewhat different statistical behavior for the data consisting of the values $c_{F,\gamma}$ when γ is special, in contrast to when γ is generic. For example, if $w = 1$ we see from Equation 6.20 that $c_{F,\gamma} = 0$ when γ is special.

7. The distributions

For every odd $d > 1$, let $\Sigma_d^{\text{generic}}$ denote the collection of data

$$\Sigma_d^{\text{generic}} := \left\{ \frac{c_{F,\gamma}\sqrt{d}}{\sqrt{\varphi(m)\log(m)}} : F/\mathbb{Q} \text{ real, cyclic of degree } d, \right. \\ \left. m = \text{cond}(F),\ \gamma \in \text{Gal}(F/\mathbb{Q}) \textit{ generic} \right\},$$

ordered by increasing m. If the Atkin-Lehner eigenvaue w that appears in Equation 6.20 is equal to -1, let $\Sigma_d^{\text{special}}$ be defined in the same way, for γ special. instead of generic.

A side-comment: In the case when $d = p$ is a prime and **(*)** holds, we have that $L(E, \chi, 1) = 0$ if and only if **(**)** above holds, so that the normalized data coming from such θ-coefficients is given by the equation:

$$\frac{c_{F,\gamma}\sqrt{p}}{\sqrt{\varphi(m)\log(m)}} = \frac{\prod_{\ell \mid m}(a_\ell - 2)}{\sqrt{p \cdot \varphi(m)\log(m)}} \cdot u_E. \tag{7.1}$$

The size of these terms is bounded in absolute value by a constant times

$$\prod_{\ell \mid m} \frac{2(\sqrt{\ell}+1)}{\sqrt{\ell - 1}} \cdot \frac{1}{\sqrt{\log m}}.$$

I think that this tends to zero as m goes to infinity. If so, of particular interest to us would be the statistics of the data $\Sigma_d^{\text{generic}}$ near 0.

Conjecture 7.2. (i) *For every $d \geq 2$, the collections of data $\Sigma_d^{\text{generic}}$ and $\Sigma_d^{\text{special}}$, ordered by increasing m, have limiting distribution functions $\Lambda_{E,d}^{\text{generic}}(t)$ and $\Lambda_{E,d}^{\text{special}}(t)$.*

(ii) *The distribution functions $\Lambda_{E,d}^{\text{generic}}(t)$ and $\Lambda_{E,d}^{\text{special}}(t)$ are continuous except possibly at $t = 0$.*

(iii) $\Lambda_{E,d}(t)^{\text{generic}}$ *is bounded near* $t = 0$ *by a constant times* $|\log(t)|^{\alpha_d}$ *for some* α_d. *Moreover,* $\lim_{d\to\infty} \alpha_d = 0$.

(iv) *For large* d, $\Lambda_{E,d}(t)^{\text{generic}}$ *and* $\Lambda_{E,d}^{\text{special}}(t)$ *are continuous for all* t. *As* d *grows,* $\Lambda_{E,d}^{\text{generic}}(t)$ *(resp.,* $\Lambda_{E,d}^{\text{special}}(t)$*) converges to a normal distribution with variance* $2\mathcal{C}_E$ *(resp.,* $4\mathcal{C}_E$*), where*

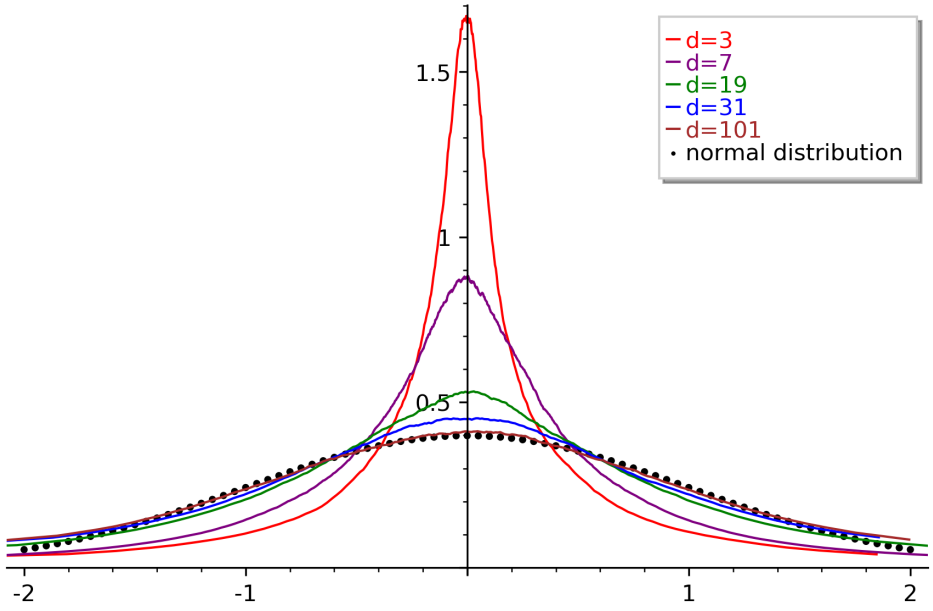
$$\mathcal{C}_E := 6/\pi^2 \prod_{\ell \mid m=cond(F)} (1+\ell^{-1})^{-1} L(\mathrm{Sym}^2(E), 1).$$

These (conjectured) distributions seem interesting enough as concepts of their own.

Question 7.3. *Can we find (even conjecturally) an explicit formula for the distribution* $\Lambda_{E,d}^{\text{generic}}(t)$, *depending—as it does—only on* d *and the Fourier coefficients of the newform* f_E*?*

Our heuristic makes use of only gross features of the distributions $\Lambda_{E,d}(t)$. For example: we need only understanding the behavior of $\Lambda_{E,d}(t)^{\text{generic}}$ and $\Lambda_{E,d}^{\text{special}}(t)$ (we call it a *growth bound*) in some germ about $t = 0$.

We do, however, depend on the relative *lack of correlation* in the values of the different θ-coefficients of a given θ-element. The *strict correlation* as described in Subsection **C** suggests that there are at most roughly $\phi(d)/2$ statistically independent coefficients—but our heuristic would suggest qualitatively similar conjectures even if there were roughly $\log(d)$ statistically independent coefficients.



8. Conjectures

As a result of this—and the data we have gathered— we make the following conjecture:

Conjecture 8.1. *Let $\mathcal{X}$:= the set of all even Dirichlet characters of order at least 7 and different from 8, 10, or 12. Then the set $\{\chi \in \mathcal{X} : L(E, \chi, 1) = 0\}$ is finite.*

An arithmetic conjecture analogous to (and conjecturally equivalent to) Conjecture 8.1 is:

Conjecture 8.2. *Let E be an elliptic curve over $\mathbb{Q}$ and M an abelian (Galois) field of algebraic numbers that contains only finitely many subfields of order $2, 3$ or 5. Then $E(M)$, the Mordell-Weil group of E over M, is finitely generated.*

.

In connection with this conjecture, recall the classical result of Kato, Ribet and Rohrlich that guarantees the same conclusion for E an elliptic curve over $\mathbb{Q}$ and M any abelian (Galois) field of algebraic numbers that is unramified except at finitely many primes. For more about these matters, see [19].

References

[1] A. Agashe, K. Ribet and W. A. Stein, The Manin Constant *Pure and Applied Mathematics Quarterly* Volume 2, **2** 617-636 (2006).

[2] T. Apostol, Introduction to Analytic Number Theory. *Undergraduate Texts in Math.,* Springer, New York (1976).

[3] S. Beckmann, Is every extension of $\mathbb{Q}$ the specialization of a branched covering? J. Algebra **164** (1994) 430-451.

[4] S. Bettin, S. Drappeau, Limit laws for rational continued fractions and value distributions of quantum modular forms, `http://sary-aurelien.drappeau.perso.luminy.univ-amu.fr/documents/LL-cfrac.pdf`

[5] E. S. Bring, Erland Samuel; S. G. Sommelius, Meletemata qudam mathematica circa transformationem quationem algebraicarum, Promotionschrift, University of Lund (1786)

[6] L. Caporaso, J. Harris, and B. Mazur, Uniformity of rational points. J. Amer. Math. Soc., **10** 1-5 (1997)

[7] K. Conrad, Recognizing Galois groups S_n and A_n, `https://kconrad.math.uconn.edu/blurbs/galoistheory/galoisSnAn.pdf`

[8] B. Conrey, J. Keating, M. Rubinstein, N. Snaith, On the frequency of vanishing of quadratic twists of modular L-Functions. In: *Number Theory for the Milennium* I. Natick, MA: A K Peters, Ltd., (2002) 301?315.

[9] C. David, J. Fearnley, H. Kisilevsky, On the vanishing of twisted L-functions of elliptic curves, *Experiment. Math.* **13**, (2004) 185–198.

[10] C. David, J. Fearnley, H. Kisilevsky, Vanishing of L-functions of elliptic curves over number fields. In: Ranks of elliptic curves and random matrix theory, *London Math. Soc. Lecture Note Ser.* **341**, Cambridge Univ. Press, Cambridge (2007) 247–259.

[11] W. L. Edge, "Bring's curve," Journal of the London Mathematical Society, **18** (3): 539-545 (1978)

[12] J. Fearnley, H. Kisilevsky, M. Kuwata, Vanishing and non-vanishing Dirichlet twists of L-functions of elliptic curves, *J. London Math. Soc.* (2) **86** (2012) 539–557.
[13] D.Harbater, Riemann's Existence Theorem, `https://www.math.upenn.edu/~harbater/RETppr.pdf`
[14] G. H. Hardy, E. M. Wright, An Introduction to the Theory of Numbers. Fourth Edition. Oxford University Press: London (1960).
[15] M. Kim, H-S. Sun, Modular symbols and modular L-values with cyclotomic twists, preprint.
[16] F. Klein, Lectures on the icosahedron and the solution of equations of the fifth degree, [1884] Dover Phoenix Editions, New York: Dover Publications, (2003)
[17] T. Kubota, Density in a family of abelian extensions, *Proceedings of the international symposium on algebraic number theory*, Tokyo & Nikko (1955) 77–91. Science Council of Japan, Tokyo, 1956.
[18] J. Lee, H-S. Sun, Dynamics of continued fractions and distribution of modular symbols, preprint.
[19] A. Lozano-Robledo, Ranks of abelian varieties over infinite extensions of the rationals,`https://alozano.clas.uconn.edu/wp-content/uploads/sites/490/2014/01/lozano-robledo_abelian_revised_web.pdf`
[20] B. Mazur, K. Rubin, Diophantine stability, *American J. Math.* **140**, (2018) 571–616.
[21] M. McQuillan, Division points on semi-abelian varieties, Invent. Math. **120** (1995), no. 1, 143-159.
[22] W. Narkiewicz, Elementary and analytic theory of algebraic numbers. Third Edition. *Springer Monographs in Mathematics*, Springer (2004).
[23] T. N. Petridis, M. S. Risager, Modular symbols have a normal distribution. *Geom. funct. anal.* **14** (2004) 1013-1043.
[24] T. N. Petridis, M. S. Risager, Arithmetic statistics of modular symbols, *Invent. math.* **212** (2018) 997-1053.
[25] D. E. Rohrlich, Realization of some Galois representations of low degree in Mordell-Weil groups, Mathematical Research Letters **4** (1997) 123-130
[26] T. Shioda, Mordell-Weil lattices and Galois representation. I,II,III Proc. Japan Acad., **65A**, 268-271; 296-299; 300-303 (1989)
[27] P. Tzermias, The Manin-Mumford conjecture: a brief survey `http://swc.math.arizona.edu/aws/1999/99Tzermias.pdf`