http://dx.doi.org/10.1090/conm/487/09529

Contemporary Mathematics
Volume **487**, 2009

Hyperelliptic Curves, L-polynomials, and Random Matrices

Kiran S. Kedlaya and Andrew V. Sutherland

Abstract. We analyze the distribution of unitarized L-polynomials $\bar{L}_p(T)$ (as p varies) obtained from a hyperelliptic curve of genus $g \leq 3$ defined over $\mathbb{Q}$. In the generic case, we find experimental agreement with a predicted correspondence (based on the Katz-Sarnak random matrix model) between the distributions of $\bar{L}_p(T)$ and of characteristic polynomials of random matrices in the compact Lie group $USp(2g)$. We then formulate an analogue of the Sato-Tate conjecture for curves of genus 2, in which the generic distribution is augmented by 22 exceptional distributions, each corresponding to a compact subgroup of $USp(4)$. In every case, we exhibit a curve closely matching the proposed distribution, and can find no curves unaccounted for by our classification.

1. Introduction

For C a smooth projective curve of genus g defined over $\mathbb{Q}$ and each prime p where C has good reduction, we consider the polynomial $L_p(T)$, the numerator of the zeta function $Z(C/\mathbb{F}_p; T)$. This polynomial is intimately related to many arithmetic properties of the curve, appearing in the Euler product of the L-series

$$L(C, s) = \prod_p L_p(p^{-s})^{-1},$$

the characteristic polynomial of the Frobenius endomorphism,

$$\chi_p(T) = T^{2g} L_p(T^{-1}),$$

and the order of the group of $\mathbb{F}_p$-rational points on the Jacobian of C,

$$\#J(C/\mathbb{F}_p) = L_p(1).$$

In genus 1, C is an elliptic curve, and $L_p(T) = pT^2 - a_pT + 1$ is determined by the trace of Frobenius, a_p. The distribution of a_p as p varies has been and remains a subject of considerable interest, forming the basis of several well known conjectures, including those of Lang-Trotter [**36**] and Sato-Tate [**52**]. Considerable progress has been made on these questions, particularly the latter, much of it quite recently [**4, 5, 6, 21, 38**].

2000 *Mathematics Subject Classification.* Primary 11G40; Secondary 11G30, 05E15.
Key words and phrases. Sato-Tate conjecture, trace of Frobenius, zeta function, Haar measure, moment sequence.
Kedlaya was supported by NSF CAREER grant DMS-0545904 and a Sloan Research Fellowship.

Licensed to AMS.

©2009 American Mathematical Society

In genus 2, C is a hyperelliptic curve, and the study of $L_p(T)$ may be viewed as a natural generalization of these questions (we also consider hyperelliptic curves of genus 3). Our first objective is to understand the shape of the distribution of $L_p(T)$, which leads us to focus primarily on Sato-Tate type questions.

The random matrix model developed by Katz and Sarnak provides a ready generalization of the Sato-Tate conjecture to higher genera. They show (see Theorems 10.1.18.3 and 10.8.2 in [**27**]) that over a universal family of hyperelliptic curves of genus g, the distribution of *unitarized* L-polynomials, $\bar{L}_p(T) = L_p(p^{-1/2}T)$, corresponds to the distribution of characteristic polynomials $\chi(T)$ in the compact Lie group $USp(2g)$ (the group of $2g \times 2g$ complex matrices that are both unitary and symplectic). By also considering infinite compact subgroups of $USp(2g)$, we are able to frame a generalization of the Sato-Tate conjecture applicable to any smooth curve defined over $\mathbb{Q}$.[1]

To test this conjecture, we rely on a collection of highly efficient algorithms to compute $L_p(T)$, described by the authors in [**28**]. The performance of these algorithms has improved dramatically in recent years (due largely to an interest in cryptographic applications [**13**]). For a hyperelliptic curve, it is now entirely practical to compute $L_p(T)$ for all $p \le N$ (where the curve has good reduction), with N on the order of 10^8 in genus 2 and more than 10^7 in genus 3. Alternatively, for much smaller N (less than 10^4) one can perform similar computations with 10^{10} curves or more.

We characterize the otherwise overwhelming abundance of data with *moment statistics*. If $\{x_p\}$ is a set of unitarized values derived from $\bar{L}_p(T)$, say $x_p = a_p/\sqrt{p}$, we compute the first several terms of the sequence

$$\mathrm{m}(x_p),\ \ \mathrm{m}(x_p^2),\ \ \mathrm{m}(x_p^3),\ \ \ldots, \tag{1}$$

where $\mathrm{m}(x_p^k)$ denotes the mean of x_p^k over p. Under the conjecture, the moment statistics converge, term by term, to the *moment sequence*

$$\mathbf{E}[X],\ \ \mathbf{E}[X^2],\ \ \mathbf{E}[X^3],\ \ \ldots, \tag{2}$$

where the corresponding random variable X is derived from the characteristic polynomial $\chi(T)$ of a random matrix A, say $X = \mathrm{tr}(A)$. In all the cases of interest to us, the moments $\mathbf{E}[X^n]$ exist and determine the distribution of X. Furthermore, they are integers. The distributions we encounter can typically be distinguished by the first eight terms of (2). It will be convenient to begin our sequences with $\mathbf{E}[X^0] = 1$.

To apply this approach we must determine these moment sequences explicitly. This is an interesting problem in its own right, with applications to representation theory and combinatorics. The particular cases we consider include the elementary and Newton symmetric functions (power sums) of the eigenvalues of a random matrix in $USp(2g)$. We derive explicit formulae for the corresponding moment generating functions. Our results intersect other work in this area, most notably that of Grabiner and Magyar [**18**], and also Eric Rains [**42**]. We take a somewhat different approach, relying on the Haar measure to encode the combinatorial structure of the group.

With moment sequences for $USp(2g)$ in hand, we then survey the distributions of $\bar{L}_p(T)$. The case $g = 1$ is easily described, and we do so here. The polynomial

[1]With the generous assistance of Nicholas Katz.

Licensed to AMS.

$\bar{L}_p(T) = p + a_1 T + 1$ is determined by the coefficient $a_1 = -a_p/\sqrt{p}$, and there are two distributions of a_1 that arise.

For elliptic curves without complex multiplication, the moment statistics of a_1 converge to the corresponding moment sequence in $USp(2)$:

$$1,\ 0,\ 1,\ 0,\ 2,\ 0,\ 5,\ 0,\ 14,\ 0,\ 42,\ \ldots,$$

whose $(2n)$th term is the nth Catalan number. Convergence follows from the Sato-Tate conjecture, which for curves with multiplicative reduction at some prime (almost all curves) is now proven, thanks to the work of Clozel, Harris, Shepherd-Barron, and Taylor [**9, 21, 53**] (see Mazur [**38**] for an overview). Testing at least one example of every curve with conductor less than 10^7 (including all the curves in Cremona's tables [**11, 50**]) revealed no apparent exceptions among curves with purely additive reduction.

For elliptic curves with complex multiplication, the moment statistics of a_1 converge instead to the sequence:

$$1,\ 0,\ 1,\ 0,\ 3,\ 0,\ 10,\ 0,\ 35,\ 0,\ 126,\ \ldots,$$

whose $(2n)$th term is $\binom{2n}{n}/2$ for $n > 0$. This is the moment sequence of a compact subgroup of $USp(2)$, specifically, the normalizer of $SO(2)$ in $SU(2) = USp(2)$. The elements with nonzero traces have uniformly distributed eigenvalue angles, and for elliptic curves with complex multiplication, convergence follows from a theorem of Deuring [**12**] and known equidistribution results for Hecke characters [**35**, Ch. XV]. The only other infinite compact subgroup of $USp(2)$ (up to conjugacy) is $SO(2)$, and its moment sequence does not appear to correspond to the moment statistics of any elliptic curve (such a curve would necessarily contradict the Sato-Tate conjecture).

The main purpose of the present work is to undertake a similar study in genus 2. We also lay some groundwork for genus 3, but consider only the case of a typical hyperelliptic curve. Already in genus 2 we find a much richer set of possible distributions.

For the typical hyperelliptic curve in genus 2 (resp. 3), when computed for suitably large N, the moment statistics closely match the corresponding moment sequences in $USp(4)$ (resp. $USp(6)$), as predicted. In genus 2 we can make a stronger statement. In a family of one million curves with randomly chosen coefficients, every single one appeared to have the $\bar{L}_p(T)$ distribution of characteristic polynomials in $USp(4)$. Under reasonable assumptions, we can reject alternative distributions with a high level of statistical confidence.

To find exceptional distributions in genus 2 we must cast our net wider, searching very large families of curves with constrained coefficient values, as well as examples taken from the literature. Such a search yielded over 30,000 nonisomorphic exceptional curves, but among these we find only 22 clearly distinct distributions, each with integer moments (Table 11, p. 29). For each of these distributions we are able to identify a specific compact subgroup H of $USp(4)$ with a matching distribution of characteristic polynomials (Table 13, p. 34). The method we use to construct these subgroups is quite explicit, and a converse statement is very nearly true. Of the subgroups we can construct, only two do not correspond to a distribution we have found; we can rule out one of these and suspect the other can be ruled out also (§ 7.2). We believe we have accounted for all possible L-polynomial distributions of a genus 2 curve.

Licensed to AMS.

2. Some Motivating Examples

We work throughout with smooth, projective, geometrically irreducible algebraic curves defined over $\mathbb{Q}$. Recall that for a curve C with good reduction at p, the zeta function $Z(C/\mathbb{F}_p;T)$ is defined by the formal power series

$$Z(C/\mathbb{F}_p;T) = \exp\left(\sum_{k=1}^{\infty} N_k T^k/k\right),$$

where N_k counts the (projective) points on C over $\mathbb{F}_{p^k}$. From the seminal work of Emil Artin [**3**], we know that $Z(C/\mathbb{F}_p;T)$ is a rational function of the form

$$Z(C/\mathbb{F}_p;T) = \frac{L_p(T)}{(1-T)(1-pT)},$$

where the monic polynomial $L_p(T) \in \mathbb{Z}[T]$ has degree $2g$ (g is the genus of C) and constant coefficient 1.

By the Riemann hypothesis for curves (proven by Weil [**56**]), the roots of $L_p(T)$ lie on a circle of radius $p^{-1/2}$ about the origin of the complex plane. To study the distribution of $L_p(T)$ as p varies, we use the unitarized polynomial

$$\bar{L}_p(T) = L_p(p^{-1/2}T),$$

which has roots on the unit circle. As $\bar{L}_p(T)$ is a real polynomial of even degree with $\bar{L}_p(0) = 1$, these roots occur in conjugate pairs. We may write

$$\bar{L}_p(T) = T^{2g} + a_1T^{2g-1} + a_2T^{2g-2} + \cdots + a_2T^2 + a_1T + 1.$$

Since $\bar{L}_p(T)$ has unitary roots, we know that

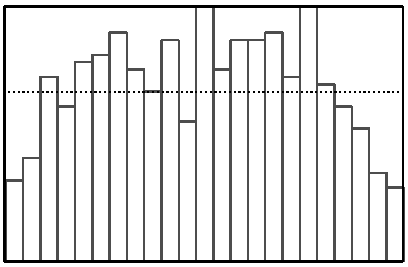
$$|a_i| \le \binom{2g}{i}, \tag{3}$$

and ask how a_i is distributed within this interval as p varies.

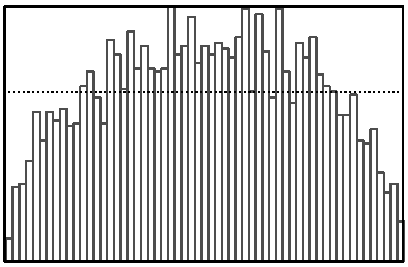
The next three pages show the distribution of a_1 for arbitrarily chosen curves of genus 1, 2, and 3 and various values of N. The coefficient a_1 is the negative sum of the roots of $\bar{L}_p(T)$, and may be written as $a_1 = -a_p/\sqrt{p}$, where a_p is the trace of Frobenius.

Each graph represents a histogram of nearly $\pi(N)$ samples (one for each prime where C has good reduction) placed into approximately $\sqrt{\pi(N)}$ buckets which partition the interval $[-2g, 2g]$ determined by (3). The horizontal axis spans this interval, and the vertical axis has been suitably scaled, with the height of the uniform distribution, $1/(4g)$, indicated by a dotted line.

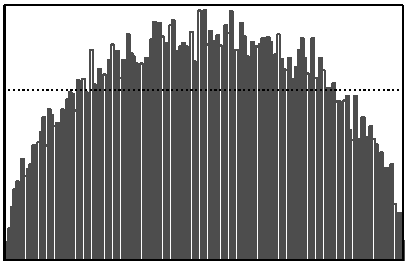
Licensed to AMS.



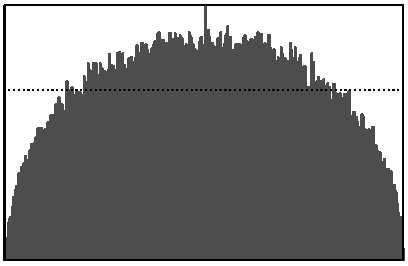
$N = 2^{12}$



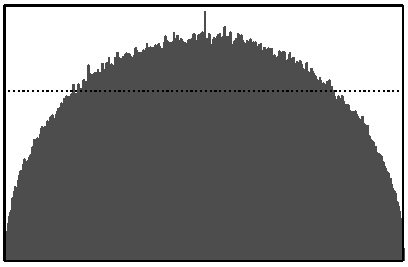
$N = 2^{15}$



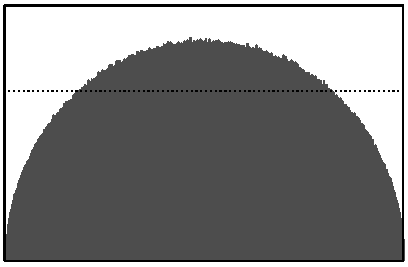
$N = 2^{18}$



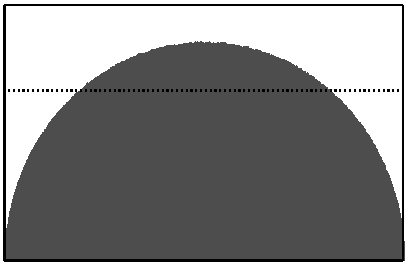
$N = 2^{21}$



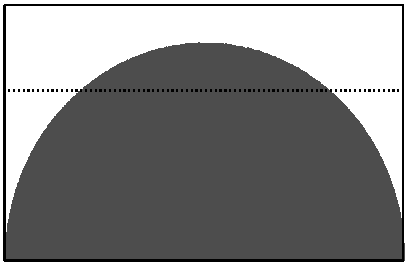
$N = 2^{24}$



$N = 2^{27}$



$N = 2^{30}$

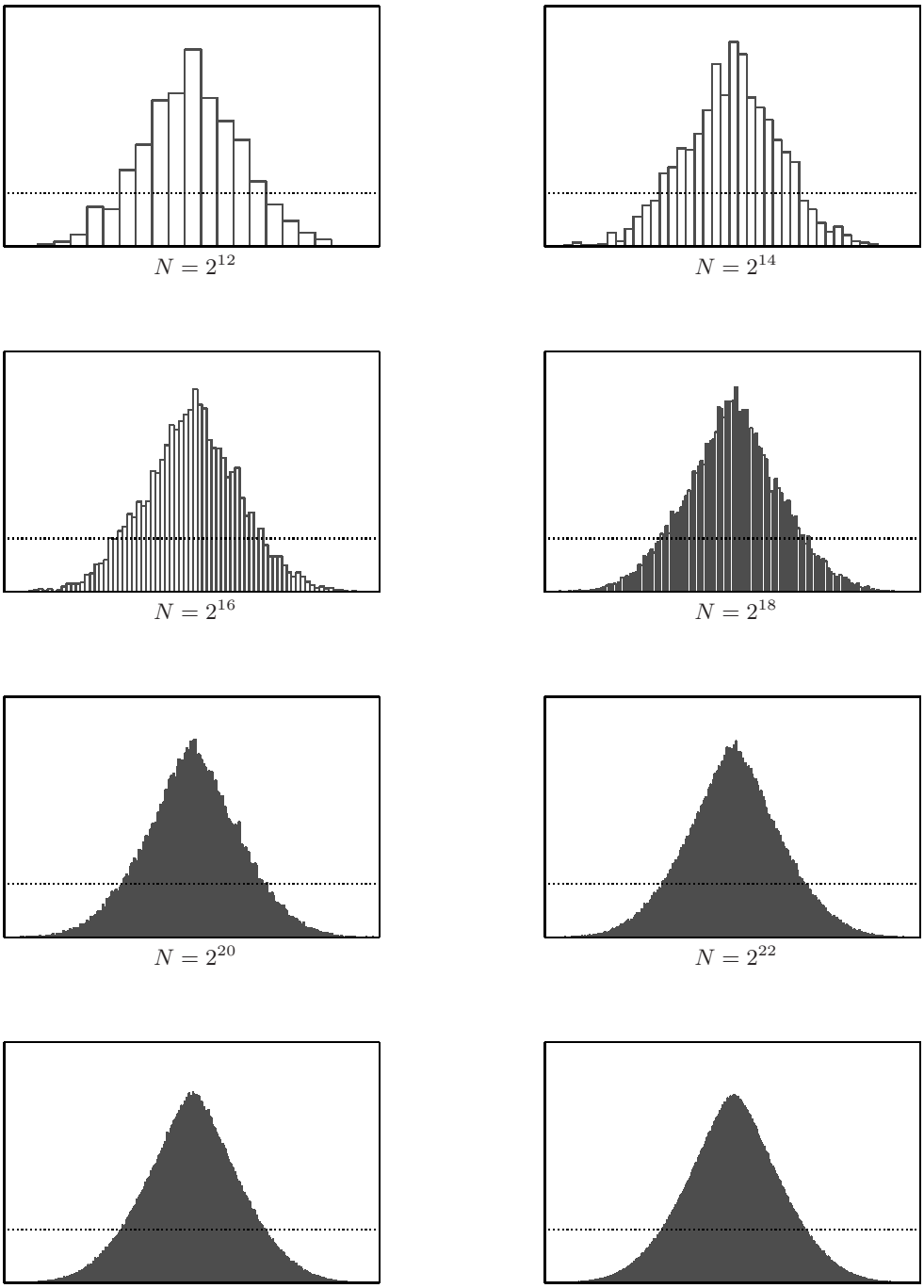


$N = 2^{33}$

Distribution of $a_1 = -a_p/\sqrt{p}$ for $p \leq N$ with good reduction.

$$y^2 = x^3 + 314159x + 271828.$$

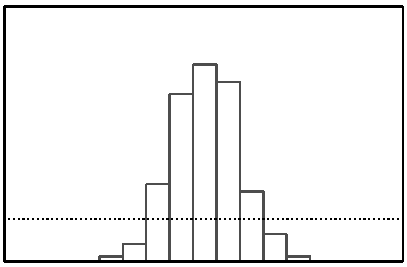
Licensed to AMS.



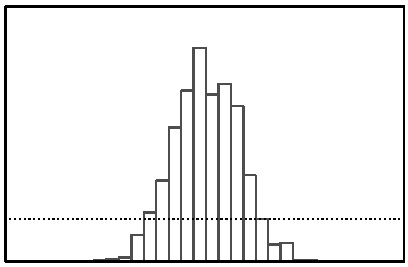
Distribution of $a_1 = -a_p/\sqrt{p}$ for $p \leq N$ with good reduction.

$$y^2 = x^5 + 314159x^3 + 271828x^2 + 1644934x + 57721566.$$

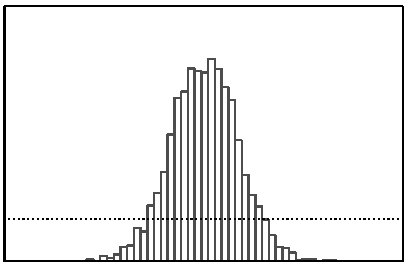
Licensed to AMS.



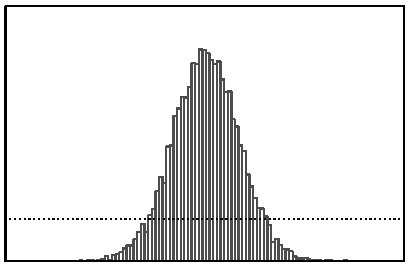
$N = 2^{11}$



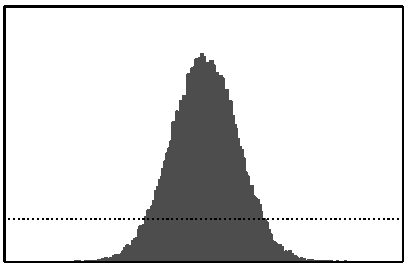
$N = 2^{13}$



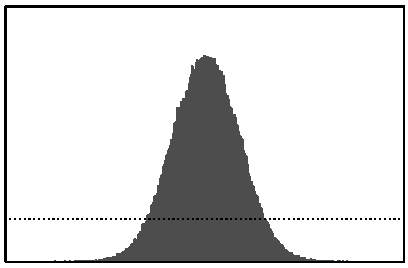
$N = 2^{15}$



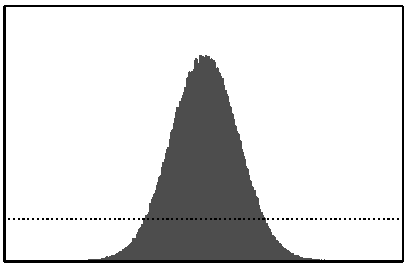
$N = 2^{17}$



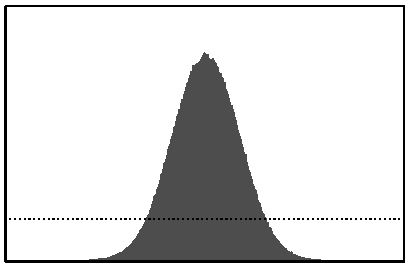
$N = 2^{19}$



$N = 2^{21}$



$N = 2^{23}$



$N = 2^{25}$

Distribution of $a_1 = -a_p/\sqrt{p}$ for $p \leq N$ with good reduction.

$$y^2 = x^7 + 314159x^5 + 271828x^4 + 1644934x^3 + 57721566x^2 + 1618034x + 141021.$$

Licensed to AMS.

The familiar semicircular shape in genus 1 is the Sato-Tate distribution. The examples in higher genera also appear to converge to distinct distributions. Provided the curve is "typical" (a notion we will define momentarily) this distribution is the same for every curve of a given genus. Even in atypical cases, there is (empirically) a small distinct set of distributions that arise for a given genus. In genus 1, only one exceptional distribution for a_1 is known, exhibited by all curves with complex multiplication:

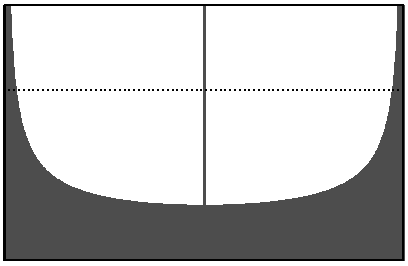


Fig. 1: Distribution of a_1 for $y^2 = x^3 - 15x + 22$.

The central spike has area 1/2 (asymptotically), arising from the fact that a curve with CM-field $\mathbb{Q}[\sqrt{D}]$ has $a_p = 0$ precisely when D is a not a quadratic residue in $\mathbb{F}_p$ [**12**].

In higher genera, a richer set of exceptional distributions arises. Below is an example for a genus 2 curve whose Jacobian splits as the product of two elliptic curves (one with complex multiplication). Histograms for several other exceptional genus 2 distributions are provided in Appendix II.

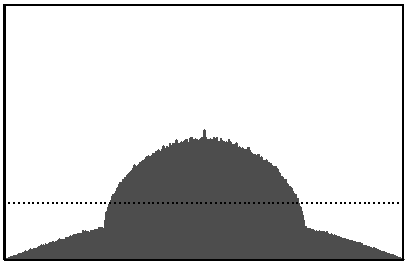


Fig. 2: Distribution of a_1 for $y^2 = x^5 + 20x^4 - 26x^3 + 20x^2 + x$.

3. A Generalized Sato-Tate Conjecture

We wish to give a conjectural basis for these distributions, both in the typical and atypical cases. The formulation presented here follows the model developed by Katz and Sarnak [**27**] and relies heavily on additional detail provided by Nicholas Katz [**26**], whom we gratefully acknowledge. Most of the statements below readily generalize to abelian varieties, but we restrict ourselves to curves defined over $\mathbb{Q}$.

We begin with the Sato-Tate conjecture, which may be stated as follows:

Conjecture 1 (Sato-Tate). *For an elliptic curve without complex multiplication, the distribution of the roots $e^{i\theta}$ and $e^{-i\theta}$ of $\bar{L}_p(T)$ for $p \le N$ converges (as $N \to \infty$) to the distribution given by the measure $\mu = \frac{2}{\pi}\sin^2\theta d\theta$ over $\theta \in [0, \pi]$.*

Licensed to AMS.

As noted earlier, this has been proven for elliptic curves with multiplicative reduction at some prime [**21**]. Using $a_1 = -2\cos\theta$, one finds that

$$\Pr[a_1 \le x] = \frac{1}{2\pi}\int_{-2}^{x}\sqrt{4-t^2}dt,$$

giving the familiar semicircular distribution.

An equivalent formulation of Conjecture 1 is that the distribution of $\bar{L}_p(T)$ corresponds to the distribution of the characteristic polynomial of a random matrix in $USp(2)$. More generally, the Haar measure on $USp(2g)$ provides a natural distribution of unitary symplectic polynomials of degree $2g$: the eigenvalues of a unitary matrix lie on the unit circle and the symplectic condition ensures that they occur in conjugate pairs (giving a polynomial with real coefficients). Conversely, each unitary symplectic polynomial corresponds to a conjugacy class of matrices in $USp(2g)$.

Let the eigenvalues of a random matrix in $USp(2g)$ be $e^{\pm i\theta_1}, \ldots, e^{\pm i\theta_g}$, with $\theta_j \in [0,\pi]$. The joint probability density function on $(\theta_1,\ldots,\theta_g)$ given by the Haar measure on $USp(2g)$ is

$$\mu(USp(2g)) = \frac{1}{g!}\Big(\prod_{j<k}(2\cos\theta_j - 2\cos\theta_k)\Big)^2\prod_j\left(\frac{2}{\pi}\sin^2\theta_j d\theta_j\right), \tag{4}$$

as shown by Weyl [**57**, Thm. 7.8B, p. 218] (also see [**27**, 5.0.4, p. 107]). For $g = 1$, we obtain the Sato-Tate distribution above.

In view of the atypical examples in the previous section, we cannot expect every curve to achieve the distribution given by $\mu(USp(2g))$. One might impose a restriction comparable to that of Sato-Tate by requiring that $\mathrm{End}_{\mathbb{C}}(J(C)) = \mathbb{Z}$, i.e. that the Jacobian have minimal endomorphism ring. While necessary, it is not clear that this restriction is sufficient in general. A stronger condition uses the ℓ-adic representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ induced by the Galois action on the Tate module $T_\ell(C)$ (the inverse limit of the ℓ^n-torsion subgroups of $J(C)$). Specifically, we require that the image of the representation

$$\rho_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(T_\ell(C)) \cong GL(2g,\mathbb{Z}_\ell)$$

be Zariski dense in $GSp(2g,\mathbb{Z}_\ell) \subset GL(2g,\mathbb{Z}_\ell)$. We know from results of Serre ([**46**, Sec. 7, Thm 3] and [**44**, p. 104]) that if this is achieved for any ℓ, then it holds for all ℓ, and we say such a curve has *large Galois image*.

Each of the conditions below suffices for C to have large Galois image.

(1) C is a genus g curve with g odd, 2, or 6, and $\mathrm{End}_{\mathbb{C}}(J(C)) = \mathbb{Z}$ (Serre [**46, 45**]). This does not hold in genus 4 (Mumford [**40**]).
(2) C is a hyperelliptic curve $y^2 = f(x)$ with $f(x)$ of degree $n \ge 5$ and the Galois group of $f(x)$ is isomorphic to S_n or A_n (Zarhin [**58**]).
(3) C is a genus g curve with good reduction outside of a set of primes S and the mod ℓ reduction of the image of ρ_ℓ is equal to $GSp(2g,\mathbb{Z}/\ell\mathbb{Z})$ for some $\ell \ge c(g,S)$ (Faltings [**14**], Serre [**46, 44**]).

Condition 3 was suggested to us by Katz. The constant $c(g,S)$ depends only on g and S. From Faltings [**14**, Thm. 5], we know that for a given g and S, there are only finitely many nonisomorphic Jacobians of genus g curves with good reduction outside of S. Each such curve has large Galois image if and only if for all $\ell > c$ the mod ℓ image of ρ_ℓ is $GSp(2g,\mathbb{Z}/\ell\mathbb{Z})$, for some constant c. By the results of

Licensed to AMS.

Serre cited above, it suffices to find one such ℓ, and taking the maximum of c over the finite set of Jacobians gives the desired $c(g, S)$. At present, effective bounds on $c(g, S)$ are known only in genus 1 [**10, 32**]. Even without effective bounds, Condition 3 gives an easily computable heuristic that is useful in practice.[2]

We now consider the situation for a curve which does not have large Galois image. The simplest case is an elliptic curve with complex multiplication. For such a curve the distribution of a_1 clearly does not match the distribution of traces in $USp(2)$ (see Fig. 1 above). In particular, the density of primes for which $a_1 = -a_p/\sqrt{p} = 0$ is one half. There is, however, a compact subgroup of $USp(2)$ which gives the correct distribution. Consider the subgroup

$$H = \left\{ \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}, \begin{pmatrix} i\cos\theta & i\sin\theta \\ i\sin\theta & -i\cos\theta \end{pmatrix} : \theta \in [0, 2\pi] \right\}.$$

H contains $SO(2)$ as a subgroup of index 2 (it is in fact the normalizer of $SO(2)$ in $USp(2)$). The elements of H not in $SO(2)$ all have zero traces, giving the desired density of 1/2. The Haar measure on $SO(2)$ gives uniformly distributed eigenvalue angles, matching the distribution of nonzero traces for elliptic curves with complex multiplication. Note that H is disconnected. This is a common (but not universal) feature among the subgroups we wish to consider.

For an elliptic curve with complex multiplication, the mod ℓ Galois image lies in the normalizer of a Cartan subgroup (see Lang [**34**, Thm 3.2]). For sufficiently large ℓ, one finds that is in fact equal to the normalizer of a Cartan subgroup. There is then a correspondence with the subgroup H above, which is the normalizer of the Cartan subgroup $SO(2)$ in $SU(2) = USp(2)$.

In general, we anticipate a relationship between the ℓ-adic Galois image of a curve C, call it G_ℓ (a subgroup of $GSp(2g, \mathbb{Z}_\ell)$), and a compact subgroup H of $USp(2g)$ whose distribution of characteristic polynomials matches the distribution of unitarized L-polynomials $\bar{L}_p(T)$ of C. One can (conjecturally) describe this relationship, albeit in a nonexplicit manner. Briefly, one takes the Zariski closure of G_ℓ through a series of embeddings:

$$GSp(2g, \mathbb{Z}_\ell) \to GSp(2g, \mathbb{Q}_\ell) \to GSp(2g, \overline{\mathbb{Q}}_\ell) \to GSp(2g, \mathbb{C}).$$

The last step is justified by the fact that $\overline{\mathbb{Q}}_\ell$ and $\mathbb{C}$ are algebraically closed fields containing $\mathbb{Q}$ of equal cardinality, hence isomorphic, and we choose a particular embedding of $\overline{\mathbb{Q}}_\ell$ in $\mathbb{C}$. One then takes the intersection with $Sp(2g)$, obtaining a reductive group over $\mathbb{C}$. After dividing by $\sqrt{p}$, the image of each Frobenius element lies in this intersection, as a diagonalizable matrix with unitary eigenvalues. We now consider a maximal compact subgroup of the intersection, H, lying in $USp(2g)$. Each unitarized Frobenius element is conjugate to some element of H (unique up to conjugacy in H) whose characteristic polynomial is $\bar{L}_p(T)$. When G_ℓ is Zariski dense in $GSp(2g, \mathbb{Z}_\ell)$, we obtain $H = USp(2g)$, but in general, H is some compact subgroup of $USp(2g)$.

There is an analogous construction involving the Mumford-Tate group $\mathrm{MT}(A)$ of an abelian variety A, which contains G_ℓ. The result is the Hodge group $\mathrm{Hg}(A)$, corresponding to our subgroup H above. For simple abelian varieties of low dimension (up to genus 5) the possibilities for $\mathrm{Hg}(A)$ have been classified by Moonen and

[2]A fourth condition has recently been proven by Hall [**20**]. In the same paper, Kowalski proves that almost all hyperelliptic curves have large Galois image.

Licensed to AMS.

Zarhin [**39**].[3] For genus 2 curves we consider the classification of H in Section 7, and give what we believe to be a complete list of the possibilities (most of these do not correspond to simple Jacobians). We note here that curves with nonisomorphic Hodge groups may have identical L-polynomial distributions, so the notions are not equivalent.

We can now state the conjecture.

Conjecture 2 (Generalized Sato-Tate). *For a curve C of genus g, the distribution of $\bar{L}_p(T)$ converges to the distribution of characteristic polynomials $\chi(T)$ in an infinite compact subgroup $H \subseteq USp(2g)$. Equality holds if and only if C has large Galois image.*

We say that the subgroup H *represents* the L-polynomial distribution of C.

4. Moment Sequences Attached to L-polynomials

Let $P_C(N)$ denote the set of primes $p \leq N$ for which the curve C has good reduction. We may compute $\bar{L}_p(T)$ for all $p \in P_C(N)$, and if x is a quantity derived from $\bar{L}_p(T)$ (e.g., the coefficients a_k or some function of the a_k), we consider the mean value $m(x^n)$ over $p \in P_C(N)$ as an approximation of the nth moment $E[X^n]$ of a corresponding random variable X. Under Conjecture 2, we assume there is a compact subgroup $H \subseteq USp(2g)$ which represents the L-polynomial distribution of C. If X is a real random variable defined as a polynomial of the eigenvalues of an element of H, it clearly has bounded support under the Haar measure on H (the eigenvalues lie on the unit circle). Therefore its moments all exist. Further, one may determine absolute bounds on X depending only on g, which we regard as fixed. Carleman's condition [**31**, p. 126] then implies that the moment sequence for X uniquely determines its distribution. We summarize this argument with the following proposition.

Proposition 1. *Under Conjecture 2, let H be a compact subgroup of $USp(2g)$ which represents the L-polynomial distribution of a curve C. Let x_p be a real-valued polynomial of the roots of $\bar{L}_p(T)$, and let the random variable X be the corresponding polynomial of the eigenvalues of a random matrix in H. Then the moments of X exist and determine the distribution of X. For all nonnegative integers n, the mean value of x_p^n over $p \in P_C(N)$ converges to $E[X^n]$ as $N \to \infty$.*

We now consider random variables X that are symmetric functions (polynomials) of the eigenvalues, with integer coefficients. In this case, it is easy to see that the moments of X must be integers.

Proposition 2. *Let V be a vector space of finite dimension over $\mathbb{C}$. Let the random variable X be a symmetric polynomial with integer coefficients over the eigenvalues of a random matrix in a compact group $G \subseteq GL(V)$, distributed with Haar measure. Then $E[X^n] \in \mathbb{Z}$ for all nonnegative integers n.*

Proof. The sum of the eigenvalues, e_1, is the trace of the standard representation V of G, and $E[e_1] = \int_G \operatorname{tr}(A)dA$ counts the multiplicity of the trivial representation in V, an integer. Similarly, the kth symmetric function e_k is the trace of the kth exterior power $\Lambda^k V$, hence $E[e_k]$ must be an integer. The product of the traces of two representations is the trace of their tensor product, hence $E[e_k^n]$

[3]We thank David Zywina for bringing this to our attention.

Licensed to AMS.

is an integer, as are the moments of any product of elementary symmetric functions. Linearity of expectation implies that $\mathbb{Z}$-linear combinations of products of elementary symmetric functions also have integer moments, and every symmetric polynomial with integer coefficients may be expressed in this way. $\square$

Proposition 2 is quite useful in practice, particularly when H is unknown. We can "determine" $E[X^n]$ for small n by computing the mean of x_p^n up to a suitable bound N. The value obtained is purely heuristic of course, depending both on Conjecture 2 and an assumption about the rate of convergence. Nevertheless, the consistency of the results so obtained are quite compelling.

For most curves (those with large Galois image) we expect $H = USp(2g)$, and we may compute the distribution of X using the measure μ defined in (4).

4.1. Moment Generating Functions in $USp(2g)$. Let $\chi(T) = \sum a_k T^k$ be the characteristic polynomial of a random matrix in $USp(2g)$ with eigenvalues $e^{\pm i\theta_1}, \ldots, e^{\pm i\theta_g}$. Up to a sign $(-1)^k$, the a_k are the elementary symmetric functions of the eigenvalues. We also define

$$s_k = \sum_j (e^{ki\theta_j} + e^{-ki\theta_j}) = \sum_j 2\cos k\theta_j,$$

the kth power sums of the eigenvalues (Newton symmetric functions).

We wish to compute the (integer) sequence $M[X] = (1, E[X], E[X^2], \ldots)$, where X is a_k or s_k. We first consider s_k (including $a_1 = -s_1$).[4] We have

$$M[s_k](n) = E[s_k^n] = \int_V \Big(\sum_j 2\cos k\theta_j\Big)^n \mu, \tag{5}$$

where $V = [0,\pi]^g$ denotes the volume of integration. If we expand (5) using the formula for μ in (4), we need only consider univariate integrals of the form

$$C_k^m(n) = \frac{1}{\pi}\int_0^\pi (2\cos k\theta)^n (2\cos\theta)^m (2\sin^2\theta) d\theta. \tag{6}$$

We regard C_k^m as a sequence indexed by $n \in \mathbb{Z}^+$ (in fact, an integer sequence), and define the exponential generating function (egf) of C_k^m by

$$\mathcal{C}_k^m(z) = \sum_{n=0}^\infty C_k^m(n)\frac{z^n}{n!}.$$

Similarly, $\mathcal{M}[s_k]$, the egf of $M[s_k]$, is the moment generating function of s_k. We will compute C_k^m in terms of sequences B_ν, defined by[5]

$$B_\nu(n) = \binom{n}{\frac{n+\nu}{2}}, \tag{7}$$

where the binomial coefficient is zero when $(n+\nu)/2$ is not an integer in the interval $[0,n]$. With this understanding, we allow ν to take arbitrary values, with B_ν identically zero for $\nu \notin \mathbb{Z}$. Letting $\mathcal{B}_\nu(z) = \sum_{n=0}^\infty B_\nu(n)\frac{z^n}{n!}$, we find that

$$\mathcal{B}_\nu(z) = \mathcal{I}_\nu(2z) = \sum_{n=0}^\infty \frac{z^{2n+\nu}}{n!(n+\nu)!}, \qquad \text{for } \nu \in \mathbb{Z}. \tag{8}$$

[4]The other a_k are addressed in Section 4.4 (for $g \le 3$).

[5]$B_\nu(n)$ counts paths of length n from 0 to ν on the real line using step set $\{\pm 1\}$.

Licensed to AMS.

The function $\mathcal{I}_\nu(z)$ is a hyperbolic Bessel function (of the first kind, of order ν) [**49**, Ch. 49-50]. Hyperbolic Bessel functions are defined for nonintegral values of ν (and are not identically zero), so the condition $\nu \in \mathbb{Z}$ in (8) should be duly noted.

We can now state a concise formula for $\mathcal{M}[s_k]$.

THEOREM 1. *Let s_k denote the kth power sum of the eigenvalues of a random element of $USp(2g)$. The moment generating function of s_k is*

$$\mathcal{M}[s_k] = \det_{g\times g}\left(\mathcal{C}_k^{i+j-2}\right), \tag{9}$$

where $\mathcal{C}_k^m(z)$ is given by

$$\mathcal{C}_k^m = \sum_j \binom{m}{j}\left(\mathcal{B}_{(2j-m)/k} - \mathcal{B}_{(2j-m+2)/k}\right), \tag{10}$$

with $\mathcal{B}_\nu$ defined as above.

We postpone the proof until Section 4.2.

The determinantal formula in Theorem 1 contains some redundancy (e.g., when $g = 3$ the term $C_k^1 C_k^2 C_k^3$ appears twice), but we find the simple form of Theorem 1 well suited to both hand and machine computation. For example, when $g = 2$ and $k = 1$ we have

$$\mathcal{M}[s_1] = \mathcal{C}_1^0\mathcal{C}_1^2 - \mathcal{C}_1^1\mathcal{C}_1^1 = (\mathcal{B}_0 - \mathcal{B}_2)(\mathcal{B}_0 - \mathcal{B}_4) - (\mathcal{B}_1 - \mathcal{B}_3)^2.$$

From (15) of Section 4.3, we obtain the identity[6]

$$M[s_1](2n) = c(n)c(n+2) - c(n+1)^2, \tag{11}$$

where $c(n)$ is the nth Catalan number. The odd moments are zero and the even moments form sequence A005700 in the On-line Encyclopedia of Integer Sequences (OEIS) [**47**]. A complete list of the sequences $M[s_k]$ and $g \le 3$ can be found in Section 4.3.

The sequence A005700 = (1, 1, 3, 14, 84, 594, ...) is well known. It counts lattice paths of length $2n$ in $\mathbb{Z}^2$ with step set $\{(\pm 1, 0), (0, \pm 1)\}$ that return to the origin and are constrained by $x_1 \ge x_2 \ge 0$. In general, the sequence $M[s_1]$ counts returning lattice paths in $\mathbb{Z}^g$ which remain in the region $x_1 \ge \ldots \ge x_g \ge 0$. This follows from a general result of Grabiner and Magyar[7] which relates the decomposition of tensor powers of certain Lie group representations to lattice paths in a chamber of the associated Weyl group [**18**]: as in the proof of Proposition (2), interpret $E[s_1^n]$ as the multiplicity of the trivial representation in $V^{\otimes n}$, where V is the standard representation of $USp(2g)$, then apply Theorem 2 of [**18**].

For the group $USp(2g)$ and $k = 1$, our results intersect those of [**18**], where an equivalent determinantal formula is obtained by counting lattice paths in the Weyl chamber of the corresponding Lie algebra. By contrast, we compute $\mathcal{M}[s_k]$ directly from the measure $\mu(USp(2g))$, using only elementary methods. The Haar measure, via the Weyl integration formula, effectively encodes the relevant combinatorial content. Particularly when $k > 1$, this is simpler than a combinatorial or

[6]The similarity of $\mathcal{C}_1^0\mathcal{C}_1^2 - \mathcal{C}_1^1\mathcal{C}_1^1$ and $c(n)c(n+2) - c(n+1)^2$ is somewhat misleading, both expressions involve Catalan numbers, but the terms do not correspond.

[7]As explained to us by Arun Ram, this equality may be interpreted in terms of crystal bases, which leads directly to analogues for groups other than $USp(2g)$.

Licensed to AMS.

representation-theoretic approach. More generally, Haar measure, and moment sequences in particular, can provide convenient access to the combinatorial structure of compact groups.

Determinantal formulas of the type above arise in many combinatorial questions related to lattice paths and Young tableaux (see [**16, 8**] for examples). One might ask what the moment sequences for s_k count when $k > 1$. For $g = 2$, some answers may be found in the OEIS (see links in Table 2).

Before proving Theorem 1, we note the following corollary.

Corollary 1. *For all $k > 2g$, the random variables s_k are identically distributed with moment generating function $\mathcal{M}[s_k] = (\mathcal{B}_0)^g$.*

Proof. From (9) of Theorem 1, $\mathcal{M}[s_k]$ is a polynomial expression in $\mathcal{C}_k^m$ with $m \le 2g-2$. From (10), it follows that $\mathcal{C}_k^m = \binom{m}{m/2}\mathcal{B}_0 - \binom{m}{m/2-1}\mathcal{B}_0$ for all $k > m+2$, since B_ν is zero for nonintegral ν. Thus $\mathcal{M}[s_k]$ is an integer multiple of $\mathcal{B}_0^g$, and $\mathcal{M}[s_k]$ must be equal to $\mathcal{B}_0^g$, since $M[s_k](0) = 1 = B_0(0)$.[8] □

The distribution of s_k given by Corollary 1 corresponds to the trace of a random matrix under a uniform distribution of $\theta_1, \dots, \theta_g$. This is a special case of a general phenomenon first noticed by Eric Rains, who has proven similar results for all the compact classical groups [**41, 42**]. The sudden transition to a fixed distribution is quite startling when first encountered; one might naïvely expect the distribution of s_k to gradually converge as $k \to \infty$. There is, however, an elementary explanation (see the proof of Lemma 3 below).

4.2. Proof of Theorem 1. We rearrange the integral for $M[s_k](n) = E[s_k^n]$ to obtain a determinantal expression in C_k^m. Lemma 3 then evaluates $C_k^m(n)$.

Proof of Theorem 1. Let $w_j = 2\cos k\theta_j$ for $1 \le j \le g$. Then $s_k = \sum w_j$ and the integral for $M[s_k](n)$ in (5) becomes

$$M[s_k](n) = \int_V \Big(\sum_j w_j\Big)^n \mu = \sum_v n_v \int_V \prod_j w_j^{v_j} \mu \tag{12}$$

where $V = [0,\pi]^g$ is the volume of integration, μ is the Haar measure on $USp(2g)$ defined in (4), v ranges over vectors of g nonnegative integers, and $n_v = \binom{n}{v_1,\dots,v_g}$. Now let $x_j = 2\cos\theta_j$ and $y_j = 2\sin^2\theta_j$ so that (4) becomes

$$\mu = \frac{1}{g!\pi^g}\prod_{i<j}(x_i - x_j)^2 \prod_j (y_j d\theta_j).$$

By Lemma 1, we may write this as

$$\mu = \frac{1}{g!\pi^g}\sum_\sigma \det_{g\times g}\Big(x_{\sigma(j)}^{i+j-2}\Big)\prod_j (y_j d\theta_j), \tag{13}$$

where σ ranges over permutations of $\{1,\dots,g\}$. From the definition of $C_k^m(n)$ in (6) we have $C_k^m(n) = \frac{1}{\pi}\int_0^\pi w_j^n x_j^m y_j d\theta_j$, for any j. Combining (12) and (13),

$$M[s_k](n) = \sum_v n_v \frac{1}{g!}\sum_\sigma \det_{g\times g}\Big(C_k^{i+j-2}(v_j)\Big) = \sum_v n_v \det_{g\times g}\Big(C_k^{i+j-2}(v_j)\Big).$$

[8] In fact, for $k > 2g$, factoring out $\mathcal{B}_0$ from $\mathcal{M}[s_k]$ leaves the Hankel determinant of the sequence $c(0)$, 0, $c(1)$, 0, $c(2)$, …, which is 1 (see [**1**]).

Licensed to AMS.

In terms of egfs (by Lemma 2), we then have the desired expression

$$\mathcal{M}[s_k] = \det_{g\times g}\left(\mathcal{C}_k^{i+j-2}\right).$$

Applying Lemma 3 to evaluate the integral $C_k^m(n)$ completes the proof. □

Lemmas (1) and (2) are elementary facts; lacking a ready reference, we provide short proofs.

LEMMA 1. *If $r_1, \ldots, r_g$ are indeterminates in a commutative ring, then*

$$\prod_{j<k}(r_j - r_k)^2 = \sum_{\sigma} \det_{g\times g}\left(r_{\sigma(j)}^{i+j-2}\right),$$

where σ ranges over permutations of $\{1,\ldots,g\}$.

PROOF. Recall that $\prod_{j<k}(r_j - r_k)$ is the Vandermonde determinant [**29**, p. 71]. Define $r^\alpha = \prod_j r_j^{\alpha(j)}$ for any function $\alpha : \{1,\ldots,g\} \to \mathbb{Z}^+$, and for a permutation σ let $r_\sigma = (r_{\sigma(1)},\ldots,r_{\sigma(g)})$. Then $\prod_{j<k}(r_j - r_k)^2$ is given by

$$\begin{aligned}\left(\det\left(r_i^{j-1}\right)\right)^2 &= \left(\sum_{\pi}\operatorname{sgn}(\pi) r^{\pi-1}\right)^2 = \sum_{\pi,\phi}\operatorname{sgn}(\pi)\operatorname{sgn}(\phi) r^{\pi+\phi-2}\\ &= \sum_{\pi,\phi}\operatorname{sgn}(\pi\phi) r_\phi^{\pi(\phi^{-1})+\mathrm{id}-2} = \sum_{\pi,\phi}\operatorname{sgn}(\pi\phi^{-1}) r_\phi^{\pi(\phi^{-1})+\mathrm{id}-2}\\ &= \sum_{\sigma}\sum_{\phi}\operatorname{sgn}(\phi) r_\sigma^{\phi+\mathrm{id}-2} = \sum_{\sigma}\det\left(r_{\sigma(j)}^{i+j-2}\right),\end{aligned}$$

and the lemma is proven. □

LEMMA 2. *For $1 \le i,j \le m$, let $\mathcal{A}_{i,j} \in \mathbb{C}[[z]]$. Then*

$$[n]\det_{m\times m}(\mathcal{A}_{i,j}) = \sum_{n_1,\ldots,n_m}\binom{n}{n_1,\ldots,n_m}\det_{m\times m}\big([n_j]\mathcal{A}_{i,j}\big),$$

where $[n]\mathcal{F}$ denotes the coefficient of $z^n/n!$ in $\mathcal{F} \in \mathbb{C}[[z]]$.

PROOF. For any $\mathcal{F}_1,\ldots,\mathcal{F}_m \in \mathbb{C}[[z]]$ we have

$$[n]\prod_j \mathcal{F}_j = \sum_{n_1,\ldots,n_m}\binom{n}{n_1,\ldots,n_m}\prod_j [n_j]\mathcal{F}_j.$$

It follows that

$$\begin{aligned}[n]\det_{m\times m}(\mathcal{A}_{i,j}) &= \sum_{\sigma}\operatorname{sgn}(\sigma)\sum_i [n]\prod_j \mathcal{A}_{\sigma(i),j}\\ &= \sum_{\sigma}\operatorname{sgn}(\sigma)\sum_i\sum_{n_1,\ldots,n_m}\binom{n}{n_1,\ldots,n_m}\prod_j [n_j]\mathcal{A}_{\sigma(i),j}\\ &= \sum_{n_1,\ldots,n_m}\binom{n}{n_1,\ldots,n_m}\det_{m\times m}\big([n_j]\mathcal{A}_{i,j}\big),\end{aligned}$$

as desired. □

Licensed to AMS.

Lemma 3 computes the integral C_k^m.

LEMMA 3. *Define* $C_k^m(n) = \frac{1}{\pi}\int_0^\pi (2\cos k\theta)^n (2\cos\theta)^m (2\sin^2\theta)d\theta$, *for positive integers* k *and nonnegative integers* m *and* n, *and let* $B_\nu(n) = \binom{n}{\frac{n+\nu}{2}}$. *Then*

$$C_k^m(n) = \sum_j \binom{m}{j}\big(B_{(2j-m)/k}(n) - B_{(2j-m+2)/k}(n)\big)$$

for all nonnegative integers n.

PROOF. We may write $C_k^m(n)$ as

$$\frac{1}{\pi}\int_0^\pi \left(e^{ik\theta}+e^{-ik\theta}\right)^n \left(e^{i\theta}+e^{-i\theta}\right)^m \left(1-\left(e^{2i\theta}+e^{-2i\theta}\right)/2\right)d\theta.$$

In terms of $\delta(t) = \frac{1}{\pi}\int_0^\pi e^{it\theta}d\theta$, one finds that $C_k^m(n)$ is equal to

$$\sum_r\sum_j \binom{n}{r}\binom{m}{j}\delta(k(2r-n)+2j-m)$$
$$-\frac{1}{2}\sum_r\sum_j \binom{n}{r}\binom{m}{j}\delta(k(2n-r)+2j-m+2)$$
$$-\frac{1}{2}\sum_r\sum_j \binom{n}{r}\binom{m}{j}\delta(k(2n-r)+2j-m-2).$$

As $C_k^m(n)$ is a real number, we need only consider the real parts of the sums above. For real t, the real part of $\delta(t)$ is nonzero only when $t=0$, in which case it is 1. Hence, in Iverson notation, $\Re(\delta(t)) = [t=0]$ holds for all $t\in\mathbb{R}$.[9]

The real parts of the second two sums are equal, since we may replace j with $m-j$ and r with $n-r$ in the last sum and then apply $[t=0]=[-t=0]$. Interchanging the order of summation we obtain

$$\sum_j\sum_r \binom{m}{j}\binom{n}{r}\Big([k(2r-n)+2j-m=0]-[k(2n-r)+2j-m+2=0]\Big).$$

We now note that

$$\sum_r \binom{n}{r}[2r-n=\nu] = \binom{n}{\frac{n+\nu}{2}} = B_\nu(n),$$

for all nonnegative integers n and arbitrary ν. Thus we have

$$C_k^m(n) = \sum_j \binom{m}{j}\big(B_{(m-2j)/k}(n) - B_{(m-2j-2)/k}(n)\big).$$

Applying the identity $B_\nu = B_{-\nu}$ completes the proof. □

4.3. Explicit Computation of $M[s_k]$ in $USp(2g)$, for $g\le 3$. For $g\le 3$, Theorem 1 gives:

g=1: $M[s_k] = C_k^0$;
g=2: $M[s_k] = C_k^0C_k^2 - C_k^1C_k^1$;
g=3: $M[s_k] = C_k^0C_k^2C_k^4 + 2C_k^1C_k^2C_k^3 - C_k^0C_k^3C_k^3 - C_k^1C_k^1C_k^4 - C_k^2C_k^2C_k^2$.

We will compute these moment sequences explicitly.

[9]The function $[P]$ is 1 when the boolean predicate P is true and 0 otherwise, see [**30**].

Licensed to AMS.

$k\backslash m$	0	1	2	3	4	5	6
1	$\mathcal{C}$	$\mathbf{D}\mathcal{C}$	$\mathbf{D}^2\mathcal{C}$	$\mathbf{D}^3\mathcal{C}$	$\mathbf{D}^4\mathcal{C}$	$\mathbf{D}^5\mathcal{C}$	$\mathbf{D}^6\mathcal{C}$
2	$\mathcal{A}$	0	$\mathcal{C}$	0	$(\mathbf{D}+2)\mathcal{C}$	0	$(\mathbf{D}+2)^2\mathcal{C}$
3	$\mathcal{B}$	$-\mathcal{D}$	$\mathcal{B}$	$-\mathcal{D}$	$\mathcal{B}+\mathcal{C}$	$-\mathcal{D}$	$\mathcal{B}+4\mathcal{C}$
4	$\mathcal{B}$	0	$\mathcal{A}$	0	$2\mathcal{A}$	0	$4\mathcal{A}+\mathcal{C}$
5	$\mathcal{B}$	0	$\mathcal{B}$	$-\mathcal{D}$	$2\mathcal{B}$	$-3\mathcal{D}$	$5\mathcal{B}$
6	$\mathcal{B}$	0	$\mathcal{B}$	0	$\mathcal{A}+\mathcal{B}$	0	$4\mathcal{A}+\mathcal{B}$
7	$\mathcal{B}$	0	$\mathcal{B}$	0	$2\mathcal{B}$	$-\mathcal{D}$	$5\mathcal{B}$
8	$\mathcal{B}$	0	$\mathcal{B}$	0	$2\mathcal{B}$	0	$5\mathcal{B}-\mathcal{D}$
9	$\mathcal{B}$	0	$\mathcal{B}$	0	$2\mathcal{B}$	0	$5\mathcal{B}$

TABLE 1. Exponential Generating Functions $\mathcal{C}_k^m$.

For convenience, define

$A = B_0 - B_1$ A126930=(1, -1, 2, -3, 6, -10, 20, -35, 70, -126, ...),
$B = B_0$ A126869=(1, 0, 2, 0, 6, 0, 20, 0, 70, 0, 252, ...),
$C = B_0 - B_2$ A126120=(1, 0, 1, 0, 2, 0, 5, 0, 14, 0, 42, ...),
$D = B_1$ A138364=(0, 1, 0, 3, 0, 10, 0, 35, 0, 126, 0, ...),

and let $\mathcal{A}, \mathcal{B}, \mathcal{C}$, and $\mathcal{D}$ denote the corresponding egfs.

LEMMA 4. *Let* $\mathbf{D}$ *denote the derivative operator.*

1. $\mathcal{C}_1^m = \mathbf{D}^m\mathcal{C}$.
2. $\mathcal{C}_2^m = (\mathbf{D}+2)^{(m-2)/2}\mathcal{C}$, *for even* $m > 0$.
3. $\mathcal{C}_k^m = 0$, *for* m *odd and* k *even.*
4. $\mathcal{C}_k^m = C(m)\mathcal{B}$, *for* $k = m+1 > 1$, *or* $k > m+2$.

PROOF. Recall from (10) of Theorem 1 that

$$\mathcal{C}_k^m = \sum_j \binom{m}{j} \left(\mathcal{B}_{(2j-m)/k} - \mathcal{B}_{(2j-m+2)/k}\right).$$

By Pascal's identity, we have

$$\mathbf{D}\mathcal{B}_\nu = \mathcal{B}_{\nu+1} + \mathcal{B}_{\nu-1}. \tag{14}$$

The proofs of statements 1 and 2 are then straightforward inductions on m. Statements 3 and 4 follow immediately from Lemma 3. □

Applying Lemmas 3 and 4, we compute Table 1. From Table 1 and (9) of Theorem 1 we obtain a closed form for $\mathcal{M}[s_k]$ in terms of $\mathcal{A}, \mathcal{B}, \mathcal{C}$, and $\mathcal{D}$. To determine $M[s_k](n)$ we must compute linear combinations of multinomial convolutions of various B_j. This is reasonably efficient for small values of g and n, however we can speed up the process significantly with the following lemma.

Licensed to AMS.

LEMMA 5. *Let* $\mathcal{B}_\nu(z) = \sum_{n=0}^{\infty} B_\nu(n) z^n/n!$, *where* $B_\nu(n) = \binom{n}{\frac{n+\nu}{2}}$. *Then*

$$\mathcal{B}_a(z)\mathcal{B}_b(z) = \sum_{n=0}^{\infty} B_{a+b}(n) B_{a-b}(n) \frac{z^n}{n!}$$

for all $a, b \in \mathbb{Z}$.

PROOF. The coefficient of $z^n/n!$ on both sides of the equality count lattice paths from $(0,0)$ to (a,b) in $\mathbb{Z}^2$ with step set $\{(\pm 1, 0), (0, \pm 1)\}$. This is immediate for the LHS. A simple bijective proof for the RHS appears in [**19**]. □

In genus 2, Lemma 5 gives us a closed form for $\mathcal{M}[s_k](n)$ in terms of binomial coefficients (or Catalan numbers). For example, from

$$\mathcal{M}[s_1] = \mathcal{C}_1^0\mathcal{C}_1^2 - \mathcal{C}_1^1\mathcal{C}_1^1 = (\mathcal{B}_0 - \mathcal{B}_2)(\mathcal{B}_0 - \mathcal{B}_4) - (\mathcal{B}_1 - \mathcal{B}_3)^2,$$

we obtain

$$\begin{aligned} M[s_1] &= B_0^2 - B_4^2 - B_2^2 + B_2B_6 - B_0B_2 + 2B_2B_4 - B_0B_6 \\ &= (B_0 - B_2)(2(B_0 - B_4) + B_2 - B_6) - (B_0 - B_4)^2. \end{aligned}$$

This may be expressed more compactly as

$$M[s_1](n) = C(n)C(n+2) - C(n+4). \tag{15}$$

Here $C(2n) = c(n)$ is the nth Catalan number, giving the identity (11) noted earlier. Similar formulas for the other $M[s_k]$ in genus 2 are listed in Table 2. In higher genera we do not obtain a closed form, but computation is considerably faster with Lemma 5; in genus 4 we use $O(n)$ multiplications to compute $M[s_k](n)$, rather than $O(n^3)$.

By Corollary 1, the sequences for $k > 2g$ are all the same, so it suffices to consider $k \le 2g+1$. For even $k \le 2g$ we find that $E[s_k] = -1$, hence we also consider $M[s_k + 1] = M[s_k^+]$, the sequence of central moments. These may be obtained by computing the binomial convolution of $M[s_k]$ with the sequence $(1, 1, 1, \ldots)$. In genus 1 we obtain

$M[s_2^+] = (1,\ 0,\ 1,\ 1,\ 3,\ 6,\ 15,\ 36,\ 91,\ 232,\ 603,\ 1585,\ \ldots)$ A005043,

and in genus 2 we find

$M[s_2^+] = (1,\ 0,\ 2,\ 1,\ 11,\ 16,\ 95,\ 232,\ 1085,\ 3460,\ 14820\ \ldots)$ A138351,

$M[s_4^+] = (1,\ 0,\ 3,\ 1,\ 21,\ 26,\ 215,\ 493,\ 2821,\ 9040,\ 43695,\ \ldots)$ A138354.

4.4. Explicit Computation of $M[a_k]$ in $USp(2g)$ for $g \le 3$. To complete our study of moment sequences, we now consider the coefficients a_k of the characteristic polynomial $\chi(T)$ of a random matrix in $USp(2g)$. We have already addressed $a_1 = -s_1$. For $k > 1$, the Newton identities allow us to express a_k in terms of s_1, $\ldots$, s_k, however this does not allow us to easily compute $M[a_k]$ from the sequences $M[s_j]$ (the covariance among the s_j is nonzero). Instead, we note that by writing

$$\chi(T) = \prod_j \Big((T - e^{i\theta_j})(T - e^{-i\theta_j})\Big) = \prod_j (T^2 - 2\cos\theta_j T + 1), \tag{16}$$

Licensed to AMS.

g	k	$M[s_k](n) = E[s_k^n]$	OEIS
1	1	$C(n)$	
		1, 0, 1, 0, 2, 0, 5, 0, 14, 0, 42, 0, 132, 0, 429, ...	A126120
	2	$A(n)$	
		1, -1, 2, -3, 6, -10, 20, -35, 70, -126, 252, -462, 924, ...	A126930
	3	$B(n)$	
		1, 0, 2, 0, 6, 0, 20, 0, 70, 0, 252, 0, 924, 0, 3432, ...	A126869
2	1	$C(n)C(n+4) - C(n+2)^2$	
		1, 0, 1, 0, 3, 0, 14, 0, 84, 0, 594, 0, 4719, 0, 40898, ...	A138349
	2	$C(n)D(n+1) - D(n)C(n+1)$	
		1, -1, 3, -6, 20, -50, 175, -490, 1764, -5292, 19404, ...	A138350
	3	$B(n)C(n)$	
		1, 0, 2, 0, 12, 0, 100, 0, 980, 0, 10584, 0, 121968, ...	A000888*
	4	$B(n)^2 - D(n)^2$	
		1, -1, 4, -9, 36, -100, 400, -1225, 4900, -15876, 63504, ...	A018224*
	5	$B(n)^2$	
		1, 0, 4, 0, 36, 0, 400, 0, 4900, 0, 63504, 0, 853776, ...	A002894*

TABLE 2. Moment Sequences $M[s_k]$ for $g \leq 2$.

X	$M[X](n) = E[X^n]$	OEIS
s_1	1, 0, 1, 0, 3, 0, 15, 0, 104, 0, 909, 0, 9449, 0, 112398, ...	A138540
s_2	1, -1, 3, -7, 24, -75, 285, -1036, 4242, -16926, 73206, ...	A138541
s_2^+	1, 0, 2, 0, 11, 1, 95, 36, 1099, 982, 15792, 25070,...	A138542
s_3	1, 0, 3, 0, 26, 0, 345, 0, 5754, 0, 110586, 0, 2341548 ...	A138543
s_4	1, -1, 4, -9, 42, -130, 660, -2415, 12810, -51786, 281736, ...	A138544
s_4^+	1, 0, 3, 1, 27, 26, 385, 708, 7231, 20296, 164277, ...	A138545
s_5	1, 0, 4, 0, 42, 0, 660, 0, 12810, 0, 281736, 0, 6727644, ...	A138546
s_6	1, -1, 6, -15, 90, -310, 1860, -7455, 44730, -195426, ...	A138547
s_6^+	1, 0, 5, 1, 63, 46, 1135, 1800, 25431, 66232, 666387, ...	A138548
s_7	1, 0, 6, 0, 90, 0, 1860, 0, 44730, 0, 1172556, ...	A002896

TABLE 3. Moment Sequences $M[s_k]$ and $M[s_{2k}^+]$ for $g = 3$.†

*The OEIS sequence differs slightly.

† The notation X^+ denotes the random variable $X + 1$.

Licensed to AMS.

each a_k may be expressed as a polynomial in $2\cos\theta_1, \ldots, 2\cos\theta_g$. It follows that we may compute $M[a_k]$ in terms of the sequences C_1^m already considered. The following proposition addresses the cases that arise for $g \le 3$.

PROPOSITION 3. *Let $C(n) = B_0(n) - B_2(n)$ as above and let a_k be the coefficient of T^k in $\chi(T)$, the characteristic polynomial of a random matrix in $USp(2g)$. For $g = 2$ we have*

$$E[(a_2 - 2)^n] = C(n)C(n+2) - C(n+1)^2, \tag{17}$$

and if $g = 3$ then

$$E[(a_2 - 3)^n] = \sum_{n_1,n_2,n_3} \binom{n}{n_1, n_2, n_3} \det_{3\times 3} C(n - n_j + i + j - 2). \tag{18}$$

Also for $g = 3$ we have

$$E[a_3^n] = \sum_{n_1,n_2,n_3,m} \binom{n}{n_1, n_2, n_3, m} 2^{n-m} \det_{3\times 3} C(m + n_j + i + j - 2). \tag{19}$$

PROOF. In genus 2, equation (16) gives $a_2 - 2 = (2\cos\theta_1)(2\cos\theta_2)$ and we have

$$E[(a_2 - 2)^n] = \int_0^\pi \int_0^\pi (2\cos\theta_1)^n (2\cos\theta_2)^n \mu. \tag{20}$$

By Lemma 3, we note that

$$C(n+m) = C_1^m(n) = \frac{1}{\pi} \int_0^\pi (2\cos\theta)^n (2\cos\theta)^m (2\sin^2\theta) d\theta. \tag{21}$$

Expanding (20) and applying (21) yields (17). In genus 3 we write

$$a_2 - 3 = (2\cos\theta_1)(2\cos\theta_2) + (2\cos\theta_1)(2\cos\theta_3) + (2\cos\theta_2)(2\cos\theta_3),$$

and apply Lemma 1 to write the expanded integral for $E[(a_2 - 3)^n]$ in determinantal form to obtain (18) (we omit the details). For (19), note that

$$a_3 = (2\cos\theta_1)(2\cos\theta_2)(2\cos\theta_3) + 2(2\cos\theta_1 + 2\cos\theta_2 + 2\cos\theta_3),$$

and proceed similarly. □

Taking the binomial convolution of $M[a_2 - g]$ with the sequence $(1, g, g^2, \ldots)$ gives the moment sequence for a_2 in genus g. One finds that $E[a_2] = 1$, hence we also consider the sequence of central moments, $M[a_2 - 1]$. Table 4 gives the complete set of moment sequences for a_k in genus $g \le 3$, including $a_1 = -s_1$.

5. Moment Statistics of Hyperelliptic Curves

Having computed moment sequences attached to characteristic polynomials of random matrices in $USp(2g)$, we now consider the corresponding moment statistics of a hyperelliptic curve. Under Conjecture 2, the latter should converge to the former, provided the curve has large Galois image. Tables 5-7 list moment statistics of a hyperelliptic curves known to have large Galois image.

These tables were constructed by computing $\bar{L}_p(T)$ to determine sample values of a_k and s_k for each p (the a_k are the coefficients, the s_k are derived via the Newton identities). Central moment statistics of $X = a_k - E[a_k]$ and $X = s_k - E[s_k]$ were then computed by averaging X^n over all $p \le N$ where the curve has good reduction.

Licensed to AMS.

g	X	$M[X](n) = E[X^n]$	OEIS
1	a_1	1, 0, 1, 0, 2, 0, 5, 0, 14, 0, 42, 0, 132, ...	A126120
2	a_1	1, 0, 1, 0, 3, 0, 14, 0, 84, 0, 594, 0, 4719, ...	A138349
	a_2	1, 1, 2, 4, 10, 27, 82, 268, 940, 3476, 13448, ...	A138356
	a_2^-	1, 0, 1, 0, 3, 1, 15, 15, 105, 190, 945, 2410,...	A095922
3	a_1	1, 0, 1, 0, 3, 0, 15, 0, 104, 0, 909, 0, 9449, ...	A138540
	a_2	1, 1, 2, 5, 16, 62, 282, 1459, 8375, 52323 ...	A138549
	a_2^-	1, 0, 1, 1, 5, 16, 75, 366, 2016, 11936, 75678, ...	A138550
	a_3	1, 0, 2, 0, 23, 0, 684, 0, 34760, 0, 2493096, ...	A138551

TABLE 4. Moment Sequences $M[a_k]$ and $M[a_{2k}^-]$ for $g \leq 3$.†

†The notation X^- denotes the random variable $X - 1$.

The values of $E[a_k]$ and $E[s_k]$ are as determined in the previous two sections, 0 for k odd or $k > 2g$ and ± 1 otherwise.

Using central moments, we find the moment statistic M_1 (the mean of x) very close to zero ($|M_1| < 0.001$), so we list only $M_2, \ldots, M_{10}$ for each x. Beneath each row the corresponding moments for $USp(2g)$ are listed. Note that the value of N is not the same in each table (we are able to use larger N in lower genus), and the number of sample points is approximately $\pi(N) \approx N/\log N$.

Tables 8 and 9 show the progression of the moment statistics in genus 2 and 3 as N increases, giving a rough indication of the rate of convergence and the degree of uncertainty in the higher moments.

The agreement between the moment statistics listed in Tables 5-7 and the moment sequences computed in Sections 4.3-4.4 is consistent with Conjecture 2. Indeed, on the basis of these results we can quite confidently reject certain alternative hypotheses.

As an example, consider the fourth moment of a_1 in genus 2. The value $M_4 = 3.004$ represents the average of 3,957,807 data points ($\approx \pi(2^{26})$). A uniform distribution on a_1 would imply the mean value of a_1^4 is greater than 50. The probability of then observing $M_4 = 3.004$ over a sample of nearly four million data points is astronomically small. A uniform distribution on the eigenvalue angles gives a mean of 36 yielding a similarly improbable event. In fact, let us suppose only that a_1^4 has a distribution with integer mean not equal to 3. We can then bound the standard deviation by 256 (since $a_1^8 \leq 256^2$) and apply a Z-test to obtain an event probability less than one in a trillion.

Licensed to AMS.

X	M_2	M_3	M_4	M_5	M_6	M_7	M_8	M_9	M_{10}
a_1	1.000	0.000	2.000	0.000	5.000	0.001	14.000	0.002	42.000
	1	0	2	0	5	0	14	0	42
s_2^+	1.000	1.000	3.000	6.000	15.001	36.003	91.010	232.03	603.11
	1	1	3	6	15	36	91	232	603
s_3	2.000	0.000	6.000	0.000	20.000	0.000	69.998	0.000	252.00
	2	0	6	0	20	0	70	0	252
s_4	2.000	0.000	6.000	0.000	20.000	0.000	70.001	-0.001	252.00
	2	0	6	0	20	0	70	0	252

TABLE 5. Central moment statistics of a_k and s_k in genus 1, $N = 2^{35}$.

$$y^2 = x^3 + 314159x + 271828$$

.

X	M_2	M_3	M_4	M_5	M_6	M_7	M_8	M_9	M_{10}
a_1	1.001	-0.001	3.004	-0.006	14.014	-0.031	84.041	-0.178	594.02
	1	0	3	0	14	0	84	0	594
a_2^-	1.001	0.000	3.003	0.997	15.013	14.964	105.10	190.00	947.38
	1	0	3	1	15	15	105	190	945
s_2^+	2.001	1.002	11.014	16.044	95.247	232.90	1089.3	3476.4	14891
	2	1	11	16	95	232	1085	3460	14820
s_3	2.002	0.001	12.014	-0.001	100.14	-0.147	981.54	-2.850	10603
	2	0	12	0	100	0	980	0	10584
s_4^+	3.004	1.010	21.049	26.150	215.66	500.32	2830.6	9075.6	43836
	3	1	21	26	215	493	2821	9040	43695
s_5	3.996	-0.015	35.958	-0.211	399.62	-3.152	4897.2	-47.602	63492
	4	0	36	0	400	0	4900	0	63504
s_6	3.999	-0.002	35.983	-0.023	399.81	-0.490	4898.0	-9.460	63487
	4	0	36	0	400	0	4900	0	63504

TABLE 6. Central moment statistics of a_k and s_k in genus 2, $N = 2^{26}$.

$$y^2 = x^5 + 314159x^3 + 271828x^2 + 1644934x + 57721566.$$

Licensed to AMS.

X	M_2	M_3	M_4	M_5	M_6	M_7	M_8	M_9	M_{10}
a_1	0.999	-0.007	2.995	-0.046	14.968	-0.343	103.76	-2.723	906.67
	1	0	3	0	15	0	104	0	909
a_2^-	0.999	0.996	4.992	15.982	75.049	366.87	2023.7	11990	75992
	1	1	5	16	75	366	2016	11936	75678
a_3	1.996	-0.034	22.940	-0.950	684.23	-22.334	34938	2360.8	2512126
	2	0	23	0	684	0	34760	0	2493096
s_2^+	2.000	0.001	10.998	0.969	94.977	35.182	1099.5	966.05	15812
	2	0	11	1	95	36	1099	982	15792
s_3	2.996	0.008	25.953	0.129	344.64	2.935	5759.4	73.138	111003
	3	0	26	0	345	0	5754	0	110586
s_4^+	3.002	0.980	27.023	25.574	384.80	697.45	7207.4	20004	163235
	3	1	27	26	385	708	7231	20296	164277
s_5	3.995	-0.036	41.906	-0.719	658.28	-16.625	12776	-428.23	281027
	4	0	42	0	660	0	12810	0	281736
s_6^+	5.001	0.968	63.005	45.334	1134.1	1782.0	25376	65650	663829
	5	1	63	46	1135	1800	25431	66232	666387
s_7	6.000	0.002	90.015	0.356	1860.6	13.010	44746	380.75	1172844
	6	0	90	0	1860	0	44730	0	1172556

TABLE 7. Central moment statistics of a_k and s_k in genus 3, $N = 2^{25}$.

$$y^2 = x^7 + 314159x^5 + 271828x^4 + 1644934x^3 + 57721566x^2 + 1618034x + 141021.$$

Licensed to AMS.

N	M_1	M_2	M_3	M_4	M_5	M_6	M_7	M_8
2^{11}	-0.071	1.031	-0.276	3.167	-2.295	15.250	-21.145	97.499
2^{12}	-0.036	1.112	-0.087	3.565	-0.475	17.251	-4.539	105.082
2^{13}	-0.067	1.085	-0.249	3.407	-1.567	16.537	-12.893	103.344
2^{14}	-0.046	1.029	-0.232	3.181	-1.529	15.795	-13.309	104.558
2^{15}	-0.044	1.031	-0.121	3.256	-0.428	16.325	-2.396	107.173
2^{16}	-0.025	1.022	-0.069	3.143	-0.251	15.251	-1.673	96.837
2^{17}	-0.016	1.011	-0.041	3.079	-0.204	14.594	-1.717	88.871
2^{18}	-0.009	1.002	-0.022	3.041	-0.138	14.441	-1.456	88.636
2^{19}	-0.002	1.003	-0.013	3.031	-0.108	14.259	-1.023	86.288
2^{20}	0.001	0.998	0.001	3.003	-0.041	14.126	-0.687	85.815
2^{21}	-0.000	1.003	-0.002	3.016	-0.045	14.088	-0.577	84.746
2^{22}	0.002	1.002	0.009	3.013	0.037	14.058	0.101	84.166
2^{23}	0.001	1.001	0.002	3.006	0.001	13.999	-0.103	83.715
2^{24}	0.000	1.001	0.001	3.002	0.008	13.964	0.036	83.346
2^{25}	0.000	1.000	-0.000	2.995	-0.010	13.950	-0.120	83.500
2^{26}	0.000	1.001	-0.001	3.004	-0.006	14.014	-0.031	84.041

TABLE 8. Convergence of moment statistics for a_1 in genus 2 as N increases.

$$y^2 = x^5 + 314159x^3 + 271828x^2 + 1644934x + 57721566.$$

N	M_1	M_2	M_3	M_4	M_5	M_6	M_7	M_8
2^{11}	0.033	0.942	0.204	2.611	1.313	11.365	9.198	62.068
2^{12}	0.009	0.921	0.092	2.447	0.649	10.149	4.617	52.838
2^{13}	0.015	0.961	0.075	2.676	0.535	11.971	4.345	69.641
2^{14}	-0.011	0.983	-0.060	2.893	-0.245	14.316	0.704	99.690
2^{15}	-0.005	1.011	-0.018	3.134	-0.067	16.286	0.836	116.675
2^{16}	-0.017	1.007	-0.054	3.154	-0.105	16.813	2.952	127.212
2^{17}	-0.006	0.993	-0.024	3.027	-0.041	15.431	1.622	109.717
2^{18}	-0.005	0.996	-0.026	3.006	-0.110	15.196	0.239	106.901
2^{19}	-0.001	0.999	-0.013	2.985	-0.087	14.793	-0.418	101.662
2^{20}	0.000	0.989	-0.007	2.934	-0.072	14.440	-0.759	98.109
2^{21}	0.003	0.997	0.003	2.979	-0.017	14.796	-0.562	101.690
2^{22}	0.002	0.999	0.005	3.003	0.038	15.098	0.446	105.733
2^{24}	0.000	1.001	0.001	3.015	-0.005	15.138	-0.102	105.418
2^{24}	0.000	0.999	-0.004	2.990	-0.043	14.916	-0.397	103.271
2^{25}	0.000	0.999	-0.007	2.995	-0.046	14.968	-0.343	103.755

TABLE 9. Convergence of moment statistics for a_1 in genus 3 as N increases.

$$y^2 = x^7 + 314159x^5 + 271828x^4 + 1644934x^3 + 57721566x^2 + 1618034x + 141021.$$

Licensed to AMS.

#	N	%	ΔM_1	ΔM_2	ΔM_3	ΔM_4	ΔM_5	ΔM_6	ΔM_7	ΔM_8
10^6	2^{16}	50	0.008	0.012	0.031	0.072	0.204	0.563	1.685	5.104
		90	0.020	0.029	0.076	0.177	0.497	1.371	4.120	12.397
		99	0.032	0.045	0.120	0.277	0.781	2.156	6.512	19.633
10^4	2^{20}	50	0.002	0.003	0.009	0.020	0.057	0.159	0.470	1.433
		90	0.006	0.008	0.021	0.049	0.138	0.384	1.154	3.485
		99	0.009	0.013	0.033	0.078	0.214	0.604	1.801	5.432
10^2	2^{24}	50	0.001	0.001	0.002	0.005	0.017	0.044	0.138	0.424
		90	0.002	0.002	0.006	0.013	0.035	0.101	0.277	0.933
		99	0.002	0.003	0.008	0.019	0.054	0.165	0.543	1.519

TABLE 10. Moment deviations for families of random genus 2 curves.

After perusing the data in Tables 5-9, several questions come to mind:

(1) What is the rate of convergence as N increases?
(2) Are these results representative of typical curves?
(3) Can we distinguish exceptional distributions that may arise?

Question 1 has been considered in genus 1 (but not, to our knowledge, in higher genera). For an elliptic curve without complex multiplication, the conjectured discrepancy between the observed distribution and the Sato-Tate prediction is $O(N^{-1/2})$ (see Conjecture 1 of [**2**] or Conjecture 2.2 of [**38**]). This conjecture implies that the generalized Riemann Hypothesis then holds for the L-series of the curve [**2**, Theorem 2]. We will not attempt to address this question here, other than noting that the figures listed in Tables 8 and 9 are not inconsistent with a convergence rate of $O(N^{-1/2})$.

5.1. Random Families of Genus 2 Curves. We can say more about Questions 2 and 3, at least in genus 2. To address Question 2 we tested over a million randomly generated curves of the form

$$y^2 = x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0,$$

with the integer coefficients $f_0, \ldots, f_5$ obtained from a uniform distribution on the interval $[-2^{63}+1, 2^{63}-1]$.

Table 10 describes the distribution of moment statistics for a_1 over three sets of computations: one million curves with $N = 2^{16}$, ten thousand curves with $N = 2^{20}$, and one hundred curves with $N = 2^{24}$. The rows list bounds on the deviation from the moment sequence for a_1 in $USp(2g)$ that apply to $m\%$ of the curves, with m equal to 50, 90, or 99. One sees close agreement with the predicted moment statistics, with ΔM_n decreasing as N increases. The maximum deviation in M_4 observed for any curve was 0.56 with $N = 2^{16}$.

We also looked for exceptional distributions among the outliers, considering the possibility that one or more curves in our random sample might not have large Galois image. From our initial family of one million random curves we selected one thousand curves whose moment statistics showed the greatest deviation from the predicted values. We recomputed the a_1 moment statistics of these curves, with the bound N increased from 2^{16} to 2^{20}. In each and every case, we saw convergence

Licensed to AMS.

toward the moment sequence for a_1 in $USp(4)$,

$$M[a_1] = 1,\ 0,\ 1,\ 0,\ 3,\ 0,\ 14,\ 0,\ 84,\ 0,\ 594,\ \ldots, \tag{A138349}$$

as predicted by Conjecture 2 for curves with large Galois image. An additional test of one hundred of the most deviant curves from within this group with $N = 2^{24}$ yielded further convergence, with $\Delta M_n < 1$ for all $n \leq 8$. This is strong evidence that all the curves in our original random sample had large Galois image; every exceptional distribution we have found for a_1 in genus 2 has $\Delta M_8 > 200$.

One may ask whether convergence of the a_1 moment statistics to $M[a_1]$ is enough to guarantee that the L-polynomial distribution of the curve is represented by $USp(2g)$, since we have not examined the distribution of a_2. If we assume the distribution of $\bar{L}_p(T)$ is given by some infinite compact subgroup of $USp(4)$ (as in Conjecture 2), then it suffices to consider a_1. In fact, under this assumption, much more is true: if the fourth moment statistic of a_1 converges to 3, then the distribution of $\bar{L}_p(T)$ converges to the distribution of $\chi(T)$ in $USp(4)$. This remarkable phenomenon is a consequence of *Larsen's alternative* [**37, 25**].

5.2. Larsen's Alternative. To apply Larsen's alternative we need to briefly introduce a representation theoretic definition of "moment" which will turn out to be equivalent to the usual statistical moment in the case of interest to us. Here we parallel the presentation in [**25**, Section 1.1], but assume G to be compact rather than reductive. Let V be a complex vector space of dimension at least two and $G \subset GL(V)$ a compact group. Define

$$M_{a,b}(G, V) = \dim_{\mathbb{C}}(V^{\otimes a} \otimes \check{V}^{\otimes b})^G, \tag{22}$$

and set $M_{2n}(G, V) = M_{n,n}(G, V)$. Let $\chi(A) = \mathrm{tr}(A)$ denote the character of V as a G-module (the standard representation of G). We then have

$$M_{2n}(G, V) = \int_G \chi(A)^n \bar{\chi}(A)^n dA = \int_G |\chi(A)|^{2n} dA.$$

We now specialize to the case $V = \mathbb{C}^{2g}$ and suppose $G \subset USp(2g)$. Then

$$M_{2n}(G, V) = \int_G (\mathrm{tr}(A))^{2n} dA = E[(\mathrm{tr}(A))^{2n}] = M[a_1](2n),$$

where $a_1 = -\mathrm{tr}(A)$ and $M[a_1](n) = E[a_1^n]$ as usual. We can now state Larsen's alternative as it applies to our present situation.

THEOREM 2 (Larsen's Alternative). *Let V a complex vector space of even dimension greater than 2 and suppose G is a compact subgroup of $USp(V)$. If $M_4(G, V) = 3$, then either G is finite or $G = USp(V)$.*

This is directly analogous to Part 3 of Theorem 1.1.6 in [**25**], and the proof is the same.

COROLLARY 2. *Let C be a curve of genus $g > 1$. Under Conjecture 2, the distribution of $\bar{L}_p(T)$ converges to the distribution of $\chi(T)$ in $USp(2g)$ if and only if the fourth moment statistic of a_1 converges to 3.*

The corollary provides a wonderfully effective way for us to distinguish curves with exceptional $\bar{L}_p(T)$ distributions.

Licensed to AMS.

6. Exceptional $\bar{L}_p(T)$ Distributions in Genus 2

While we were unable to find *any* exceptional $\bar{L}_p(T)$ distributions among random genus 2 curves with large coefficients, if one restricts the size of the coefficients such cases are readily found. We tested every curve of the form $y^2 = f(x)$, with $f(x)$ a monic polynomial of degree 5 with coefficients in the interval $[-64, 64]$, more than 2^{35} curves. As not every hyperelliptic curve of genus 2 can be put in this form, we also included curves with $f(x)$ of degree 6 (not necessarily monic) and coefficients in the interval $[-16, 16]$. With such a large set of curves to test, we necessarily used a much smaller value of N, approximately 2^{12}. We computed the moment statistics of a_1 using parallel point-counting techniques described in [**28**] to process 32 curves at once.

To identify exceptional curves, we applied a heuristic filter to bound the deviation of the fourth and sixth moment statistics from the $USp(2g)$ values $M[a_1](4) = 3$ and $M[a_1](6) = 14$. By Larsen's alternative, it suffices only to consider the fourth moment, however we found the sixth moment also useful as a distinguishing metric: the smallest sixth moment observed among any of the exceptional distributions was 35, compared to 14 in the typical case. A combination of the two moments proved to be most effective.

Searching for a small subset of exceptional curves in a large family using a statistical test necessarily generates many false positives: nonexceptional curves which happen to deviate significantly from the $USp(2g)$ distribution for $p \leq N$. The filter criteria were tuned to limit this, at the risk of introducing more false negatives (unnoticed exceptional curves). After filtering the entire family with $N \approx 2^{12}$, the remaining curves were filtered again with $N = 2^{16}$ to remove false positives. Finally, we restricted the resulting list to curves with distinct Igusa invariants [**24**], leaving a set of some 30,000 nonisomorphic curves with (apparently) exceptional distributions.

One additional criterion used to distinguish distributions was the ratio $z(C, N)$ of zero traces, that is, the proportion of primes p for which $a_p = 0$, among $p \leq N$ where C has good reduction. For a typical curve, $z(C, N) \to 0$ as $N \to \infty$, but for many exceptional distributions, $z(c, N)$ converges to a nonzero rational number. In most cases where this arises, one can readily compute

$$\lim_{N\to\infty} z(C, N) = z(C), \tag{23}$$

using the Hasse-Witt matrix. This is described in detail in [**51**], and the following is a typical example. One can show that the curve $y^2 = x^6 + 2$ has $a_p = 0$ unless p is of the form $p = 6n + 1$, in which case

$$a_p \equiv \binom{3n}{n} 2^n (2^n + 1) \mod p. \tag{24}$$

It follows that for $p = 6n + 1$ we have $a_p = 0$ if and only if $2^n \equiv -1 \bmod p$. The integer $2^n = 2^{(p-1)/6}$ is necessarily a sixth root of unity mod p, and exactly one of these is congruent to -1. By the Čebotarev density theorem, this occurs for a set of density 1/6 among primes of the form $p = 6n + 1$. Combine this with the fact that $a_p = 0$ when p is not of this form and we obtain $z(C) = 7/12$.

Licensed to AMS.

Under Conjecture 2, one can show that for any curve C (of arbitrary genus), $z(C)$ must exist and is a rational number, however we need not assume this here.[10] For each nonzero $z(C)$ in Table 11, we have identified a specific curve exhibiting the distribution for which one can show of $\lim_{N\to\infty} z(C,N) = z(C)$. Typically, the Hasse-Witt matrix gives a lower bound on $\liminf_{N\to\infty} z(C,N)$, and by computing $G[\ell]$, the mod ℓ image of the Galois representation in $GSp(2g, Z/\ell z)$, one obtains the density of nonzero traces mod ℓ, establishing an upper bound on $\limsup_{N\to\infty} z(c,N)$. It is generally not difficult to find an ℓ for which these two bounds are equal (the Čebotarev density theorem is invoked on both sides of the argument).

After sorting the sequences of moment statistics and considering the values of $z(C)$ among our set of more than 30,000 exceptional curves, we were able to identify only 22 distributions that were clearly distinct (within the precision of our computations). We also tested a wide range of genus 2 curves taken from the literature [**7, 15, 17, 22, 23, 33, 43, 48, 54, 55**], most with coefficient values outside the range of our search family. In every case the a_1 moment statistics appeared to match one of our previously identified distributions. Conversely, several of the distributions found in our search did not arise among the curves we tested from the literature.

Table 11 lists the 23 distinct distributions for a_1 we found for genus two curves, including the typical case, which is listed first. The value of $z(C)$ and the first six moments of a_1 suffice to distinguish every distribution we have found. We also list the eighth moment statistic, which, while not accurate to the nearest integer, is almost certainly within one percent of the "true" value. We list only the moment statistics of a_1. Histograms of the first twelve a_1 distributions can be found in Appendix II. Additional a_1 histograms, along with moment statistics and histograms for a_2 and s_k are available at `http://math.mit.edu/~drew/`.

The third distribution in Table 11 went unnoticed in our initial analysis (we later found several examples that had been misclassified) and is not a curve taken from the literature. We constructed the curve

$$(C) \qquad y^2 = x^5 + 20x^4 - 26x^3 + 20x^2 + x$$

to have a split Jacobian, isogenous to the product of the elliptic curve

$$(E_1) \qquad y^2 = x^3 - 11x + 14,$$

which has complex multiplication, and the elliptic curve

$$(E_2) \qquad y^2 = x^3 + 4x^2 - 4x,$$

which does not. For every p where C has good reduction, the trace of Frobenius is simply the sum of the traces of E_1 and E_2. As E_1 and E_2 are not isogenous (over $\mathbb{C}$), we expect their a_1 distributions to be uncorrelated.[11] It follows that the moment sequence of a_1 for the curve C is simply the binomial convolution of the moment sequences of a_1 for the curves E_1 and E_2. Thus we expect the moment

[10] A compact subgroup of $USp(2g)$ has a finite number of connected components. The density of zero trace elements must be zero or one on each component.

[11] The genus 1 traces may be correlated in a way that does not impact $a_1 = -a_p/\sqrt{p}$, e.g., both curves might have the property that p mod 3 determines a_p mod 3.

Licensed to AMS.

#	$z(C)$	M_2	M_4	M_6	M_8	$f(x)$
1	0	1	3	14	84	x^5+x+1
2	0	2	10	70	588*	$x^5-2x^4+x^3+2x-4$
3	0	2	11	90	888*	$x^5+20x^4-26x^3+20x^2+x$
4	0	2	12	110	1203*	$x^5+4x^4+3x^3-x^2-x$
5	0	4	32	320	3581*	$x^5+7x^3+32x^2+45x+50$
6	1/6	2	12	100	979*	$x^5-5x^3-5x^2-x$
7	1/4	2	12	100	1008*	$x^5+2x^4+2x^2-x$
8	1/4	2	12	110	1257*	$x^5-4x^4-2x^3-4x^2+x$
9	1/2	1	5	35	293*	$x^5-2x^4+11x^3+4x^2+4x$
10	1/2	1	6	55	601*	$x^5-2x^4-3x^3+2x^2+8x$
11	1/2	2	16	160	1789*	x^5+x^3+x
12	1/2	2	18	220	3005*	$x^5-3x^4+19x^3+4x^2+56x-12$
13	1/2	4	48	640	8949*	x^6+1
14	7/12	1	6	50	489*	$x^5-4x^4-3x^3-7x^2-2x-3$
15	7/12	2	18	200	2446*	x^6+2
16	5/8	1	6	50	502*	x^5+x^3+2x
17	5/8	2	18	200	2515*	$x^5-10x^4+50x^2-25x$
18	3/4	1	8	80	894*	x^5-2x^3-x
19	3/4	1	9	100	1222*	x^5-1
20	3/4	1	9	110	1501*	$11x^6+11x^3-4$
21	3/4	2	24	320	4474*	x^5+x
22	13/16	1	9	100	1254*	x^5+3x
23	7/8	1	12	160	2237*	x^5+2x

TABLE 11. Moments of a_1 for genus 2 curves $y^2=f(x)$ with $N=2^{26}$.

Column $z(C)$ is the density of zero traces (a_p values). The starred values indicate uncertainty in the eighth moment statistic. In each case, if $T_8=\lim_{N\to\infty}M_8$, we estimate that $-0.005\le 1-M_8/T_8\le 0.01$ with very high probability (the larger uncertainty on the positive side is primarily due to an observed excess of zero traces for small values of N, we expect $M_8\le T_8$ in most cases). See Table 13 for predicted values of T_8 and T_{10}.

statistics of a_1 for C to converge to

(A138552*) $\qquad 1,\ 0,\ 2,\ 0,\ 11,\ 0,\ 90,\ 0,\ 889,\ 0,\ 9723,\ \ldots,$

which is the binomial convolution of the sequences $(1,0,1,0,3,0,10,0,35,\ldots)$ and $(1,0,1,0,2,0,5,0,14,\ldots)$ mentioned in the introduction. These are the a_1 moment sequences of elliptic curves with and without complex multiplication. In terms of moment generating functions, we simply have

$$\mathcal{M}_C[a_1]=\mathcal{M}_{E_1}[a_1]\mathcal{M}_{E_2}[a_1].$$

Licensed to AMS.

Provided the covariance between the a_1 distributions of E_1 and E_2 is zero, one can prove the a_1 moment statistics of C converge to the sequence above using known results for genus 1 curves (note that E_1 has complex multiplication and E_2 has multiplicative reduction at $p = 107$).

Many of the distributions in Table 11 can be obtained from genus 1 moment sequences by constructing an appropriate genus 2 curve with split Jacobian, as shown in the next section. It is important to note that a curve whose Jacobian is simple (not split over $\overline{\mathbb{Q}}$) may still have an L-polynomial distribution matching that of a split Jacobian. Distribution #2, for example, corresponds to a Jacobian which splits as the product of two nonisogenous elliptic curves without complex multiplication. This distribution also arises for some genus 2 curves with simple Jacobians, including

$$y^2 = x^5 - x^4 + x^3 + x^2 - 2x + 1.$$

This is a modular genus 2 curve which appears as $C_{188,A}$ in [**17**], along with many similar examples.

We speculate that simple Jacobians with Distribution #2 are all of type I(2) in the classification of Moonen and Zarhin [**39**], corresponding to Jacobians whose endomorphism ring is isomorphic to the ring of integers in a real quadratic extension of $\mathbb{Q}$. A similar phenomenon occurs with Distribution #11, which arises for split Jacobians that are isogenous to the product of an elliptic curve and its twist, but also for simple Jacobians of type II(1) in the Moonen-Zarhin classification (these are QM-curves, see [**22**] for examples). The remaining two types of simple genus 2 Jacobians in the Moonen-Zarhin classification are type I(1), which is the typical case (Jacobians with endomorphism ring $\mathbb{Z}$), and type IV(2,1), which occurs for curves with complex multiplication over a quartic CM field (with no imaginary quadratic subfield). These correspond to Distributions #1 and #19 respectively (examples of the latter can be found in [**54**]). The remaining distributions appear to arise only for curves with split Jacobians.

7. Representation of Genus 2 Distributions in $USp(4)$

Conjecture 2 implies that each distribution in Table 11 is represented by the distribution of characteristic polynomials in some infinite compact subgroup H of $USp(4)$. In this section we will exhibit such an H for each distribution. We do not claim that each H we give is the "correct" subgroup for every curve with the corresponding distribution, in the sense of corresponding to the Galois image G_ℓ, as discussed in Section 3.[12] Rather, for each H we show that its density of zero traces and moment sequence are compatible with the corresponding data in Table 11. In most cases we also have evidence that suggests H is the correct subgroup for the particular corresponding curve listed in Table 11 (see Section 7.1).

For all but two cases we will construct H using two subgroups of $USp(2)$ that represent distributions of genus 1 curves: $G_1 = USp(2)$ for an elliptic curve without complex multiplication, and $G_2 = N(SO(2))$, the normalizer of $SO(2)$ in $SU(2)$, for an elliptic curve with complex multiplication. We will construct each $H \subset USp(4)$ from G_1 and/or G_2 explicitly as a group of matrices, however the motivation behind these constructions are split Jacobians.

[12]Indeed, a single H for each distribution would not suffice. As noted above, two curves may share the same $\bar{L}_p(T)$ distribution for different reasons.

Licensed to AMS.

The most obvious cases correspond to the product of two nonisogenous elliptic curves, and we have the groups $G_1 \times G_1$, $G_1 \times G_2$, and $G_2 \times G_2$ as groups of block diagonal 2×2 matrices in $USp(4)$. These correspond to Distributions #2, #3, and #8 in Table 11, and their moment sequences are easily computed via binomial convolutions of the appropriate genus 1 moment sequences (the example of the previous section corresponds to $G_1 \times G_2$).

To obtain additional distributions, we also consider the product of two isogenous elliptic curves. We may, for example, pair an elliptic curve with an isomorphic copy of itself, or with one of its twists.[13] For two isomorphic curves, the corresponding subgroup H_i contains block diagonal matrices of the form

$$B = \begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix}$$

where A is an element of G_i ($i = 1$ or 2). To pair a curve with its twist we also include block diagonal matrices with A and $-A$ on the diagonal to obtain the subgroup H_i^-.

We now generalize this idea. Let $G = G_1$ (resp. G_2) be a compact subgroup of $USp(2)$, and let G^* be the subgroup of $U(2)$ obtained by extending G by scalars and taking the subgroup of elements whose determinants are kth roots of unity (for some positive integer k). For $A \in G^*$, let $\overline{A}$ denote the complex conjugate of A and define the block diagonal matrix

$$B = \begin{pmatrix} A & 0 \\ 0 & \overline{A} \end{pmatrix}.$$

The matrix B is clearly unitary, and one easily verifies that it is also symplectic, hence $B \in USp(4)$. The set of all such B forms our subgroup H. As a topological group, H has k (resp. $2k$) connected components, each a closed set consisting of elements with A having a fixed determinant, thus H is compact. The identity component is isomorphic to $USp(2)$ (resp. $SO(2)$), embedded diagonally.

We may write $A \in G^*$ as $A = \omega^j A_0$ with $A_0 \in G \subseteq USp(2)$, ω a primitive $2k$th root unity, and $1 \le j \le k$. We then have

$$\mathrm{tr}(B) = \mathrm{tr}(A) + \mathrm{tr}(\overline{A}) = \omega^j \mathrm{tr}(A_0) + \omega^{-j}\mathrm{tr}(\overline{A}_0) = (\omega + \omega^{-j})\mathrm{tr}(A_0),$$

since $\mathrm{tr}(\overline{A}_0) = \mathrm{tr}(A_0)$ for any $A_0 \in USp(2)$. It follows that

$$\mathbf{E}_H[(\mathrm{tr}(B))^n] = \left(\frac{1}{k}\sum_{j=1}^{k}(\omega^j + \omega^{-j})^n\right)\mathbf{E}_G[(\mathrm{tr}(A_0))^n] \tag{25}$$

where $\mathbf{E}_G[X]$ denotes the expectation of a random variable X over the Haar measure on G.

The term $(\omega^j + \omega^{-j})^n \mathbf{E}_G[(\mathrm{tr}(A_0))^n]$ corresponds to the nth moment of the trace distribution on a component of H. These moments will all be integers precisely when $k \in \{1, 2, 3, 4, 6\}$ (they are zero for n odd). In fact, these are the only values of k for which H plausibly represents the distribution of $\bar{L}_p(T)$ for a genus 2 curve defined over $\mathbb{Q}$, as we now argue.

[13] See [**7**, Ch. 14] and [**33**] for explicit methods of constructing such curves.

Licensed to AMS.

H	$k=1$	$k=2$	$k=3$	$k=4$	$k=6$
H_1^k	5	11	4	7	6
$J(H_1^k)$	11	17	10	16	14
H_2^k	13	21	12	18	15
$J(H_2^k)$	21	23	20	22	*

TABLE 12. Distributions matching H_i^k or $J(H_i^k)$.

Consider an L-polynomial $L_p(T)$ for which $\bar{L}_p(T) = L_p(p^{-1/2}T)$ is the characteristic polynomial of some $B \in H$. We may factor $L_p(T)$ as

$$L_p(T) = (\chi(p)pT^2 - \alpha T + 1)(\overline{\chi}(p)pT^2 - \overline{\alpha}T + 1), \tag{26}$$

where $\alpha \in \mathbb{Z}[\zeta]$, with ζ a primitive kth root of unity, and $\chi(p)$ is a kth root of unity equal to the determinant of A in the component of H containing B. For the elliptic curve we have in mind as a factor of the Jacobian, $\chi(p)p$ is the determinant of its Frobenius element and α is the trace. Since $L_p(T)$ has integer coefficients, α must lie in a quadratic extension of $\mathbb{Q}$, giving $k \in \{1, 2, 3, 4, 6\}$.

For each of these k we can easily compute closed forms for the parenthesized expression in (25). Assuming $n > 0$ is even, we obtain

$$2^n, \quad 2^n/2, \quad (2^n + 2)/3, \quad (2^n + 2^{n/2+1})/4, \quad (2^n + 2 \cdot 3^{n/2} + 2)/6,$$

for $k = 1, 2, 3, 4, 6$, respectively. Since $\mathbf{E}_G[(\mathrm{tr}(A_0))^n]$ is zero for odd values of n, these expressions may be used in (25) for all positive n. For even values of k, the density $z(H)$ of zero traces in H is $1/k$ (resp. $1/2 + 1/k$), and $z(H)$ is zero (resp. $1/2$) for k odd.

For any of the subgroups H constructed as above, we may also consider the group $J(H)$ generated by H and the block diagonal matrix

$$J = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}. \tag{27}$$

The group $J(H)$ contains H as a subgroup of index 2, with the nonidentity coset having all zero traces. For $n > 0$, the nth moment of the trace distribution in $J(H)$ is simply half that of H, and $z(J(H)) = (z(H) + 1)/2$.

For $i = 1$ or 2 and $k \in \{1, 2, 3, 4, 6\}$, let H_i^k denote the group H constructed using G_i and k. By also considering $J(H_i^k)$, we can construct a total of 20 groups, 18 of which have distinct eigenvalue distributions. With the sole exception of $J(H_2^6)$, each of these matches one of the distributions in Table 11 to a proximity well within the accuracy of our computational methods. Note that $H_i^1 = H_i$, and the group H_i^2 has the same eigenvalue distribution as H_i^- (but is not conjugate).

We may also consider $J(G_1 \times G_1)$, which corresponds to Distribution #9. This construction does not readily apply to $G_1 \times G_2$ (in fact $J(G_1 \times G_2) = J(G_1 \times G_1)$). The group $J(G_2 \times G_2)$ does give a new distribution (it is the normalizer of $SO(2) \times SO(2)$ in $USp(4)$), but it does not correspond to any we have found. However, the group $J(G_2 \times G_2)$ contains a subgroup K not equal to $G_2 \times G_2$ which matches Distribution #19. The group K has identity component $SO(2) \times SO(2)$ and a cyclic component group, of order 4 (this determines K).

Licensed to AMS.

Of all the groups we have constructed, only K does not correspond, in some fashion, to a split Jacobian. As noted above, Distribution #19 arises for curves with simple Jacobians and complex multiplication over a quartic CM field, and in fact all nineteen such curves documented by van Wamelen have this distribution [**54, 55**]. The only remaining group to consider is $USp(4)$ itself, which of course gives Distribution #1.

Table 13 gives a complete list of the subgroups of $USp(4)$ we have identified, one for each distribution in Table 11, and also entries for $J(H_2^6)$ and $J(G_2 \times G_2)$. These last two distributions appear to be spurious; see § 7.2.

7.1. Supporting Evidence. Aside from closely matching the trace distributions we have found, there is additional data that supports our choice of the subgroups H appearing in Table 13. First, we find that these H not only match the distribution of the a_1 coefficient in $\bar{L}_p(T)$, they also appear to give the correct distribution of a_2. We should note that for the three curves in Table 11 where $f(x)$ has degree 6, the available methods for computing $L_p(T)$ are much less efficient, so we did not attempt this verification in these three cases.[14]

More significantly, the disconnected groups in Table 13 also appear to give the correct distribution of a_1 (and a_2 for $f(x)$ of degree 5) on each of their components. If we partition the components of H according to their distributions of characteristic polynomials, for a given curve we can typically find a partitioning of primes into sets of corresponding density with matching $\bar{L}_p(T)$ distributions.

Taking Distribution #10 as an example, we have $H = J(H_1^3)$ in Table 13 and the corresponding curve in Table 11 is given by

$$y^2 = f(x) = x^5 - 2x^4 - 3x^3 + 2x^2 + 8x = x(x-2)(x^3 - 3x - 4).$$

The cubic $g(x) = x^3 - 3x - 4$ has Galois group S_3. The set of primes P_3 for which $g(x)$ splits into three factors in $\mathbb{F}_p[x]$ has density $1/6$, and corresponds to the identity component of $J(H_1^3)$.[15] The set of primes P_2 where $g(x)$ splits into two factors has density $1/2$, and corresponds to the nonidentity coset of H_1^3 in $J(H_1^3)$, containing three components with identical eigenvalue distributions. The remaining set of primes P_1 for which $g(x)$ is irreducible has density $1/3$ and corresponds to the set of elements of H_1^3 for which the determinant of the block diagonal matrix A is not 1 (this includes two of the six components of $J(H_1^3)$). Table 14 lists the moment statistics for a_1 and a_2, restricted to the sets P_1, P_2, and P_3, with values for the corresponding subset of $J(H_1^3)$ beneath.

A similar analysis can be applied to the other disconnected groups in Table 13, however the definition of the sets P_i varies. For Distribution #11 the group H_1^- has two components, and for the curve $y^2 = f(x) = x^5 + x^3 = x$ the correct partitioning of primes simply depends on the value of p modulo 4, not on how $f(x)$ splits in $\mathbb{F}_p[x]$ (in fact, the set of primes where $f(x)$ splits intersects both partitions). In other cases both a modular constraint and a splitting condition may apply. In general there is some partitioning of primes which corresponds to a partitioning of the components of H, and the corresponding distributions appear to agree.

In addition to verifying the distribution of $\bar{L}_p(T)$ over sets of primes, for each group corresponding to a split Jacobian, one can also check whether $L_p(T)$ admits

[14]The a_1 coefficient can be computed reasonably efficiently in the degree 6 case by counting points on C in $\mathbb{F}_p$, but the group law on the Jacobian is much slower.

Licensed to AMS.

[15]We thank Dan Bump for suggesting this approach.

#	H	d	$c(H)$	$z(H)$	M_2	M_4	M_6	M_8	M_{10}
1	$USp(4)$	10	1	0	1	3	14	84	594
2	$G_1 \times G_1$	6	1	0	2	10	70	588	5544
3	$G_1 \times G_2$	4	2	0	2	11	90	889	9723
4	H_1^3	3	3	0	2	12	110	1204	14364
5	H_1	3	1	0	4	32	320	3584	43008
6	H_1^6	3	6	1/6	2	12	100	980	10584
7	H_1^4	3	4	1/4	2	12	100	1008	11424
8	$G_2 \times G_2$	2	4	1/4	2	12	110	1260	16002
9	$J(G_1 \times G_1)$	6	2	1/2	1	5	35	294	2772
10	$J(H_1^3)$	3	6	1/2	1	6	55	602	7182
11	H_1^-	3	2	1/2	2	16	160	1792	21504
12	H_2^3	1	6	1/2	2	18	220	3010	43092
13	H_2	1	2	1/2	4	48	640	8960	129024
14	$J(H_1^6)$	3	12	7/12	1	6	50	490	5292
15	H_2^6	1	12	7/12	2	18	200	2450	31752
16	$J(H_1^4)$	3	8	5/8	1	6	50	504	5712
17	H_2^4	1	8	5/8	2	18	200	2520	34272
18	$J(H_1^-)$	3	4	3/4	1	8	80	896	10752
19	K	2	4	3/4	1	9	100	1225	15876
20	$J(H_2^3)$	1	12	3/4	1	9	110	1505	21546
21	H_2^-	1	4	3/4	2	24	320	4480	64512
22	$J(H_2^4)$	1	16	13/16	1	9	100	1260	17136
23	$J(H_2^-)$	1	8	7/8	1	12	160	2240	32256
*	$J(G_2 \times G_2)$	2	8	5/8	1	6	55	630	8001
*	$J(H_2^6)$	1	24	19/24	1	9	100	1225	15876

TABLE 13. Candidate subgroups of $USp(4)$.

Row numbers correspond to the distributions in Table 11. Column d lists the real dimension of H, and $c(H)$ counts its components. The column $z(H)$ gives the density of zero traces, and $M_n = \mathbf{E}_H[(\mathrm{tr}(B))^n]$ for a random $B \in H$. The last two rows are not known to match the L-polynomial distribution of a genus 2 curve.

a factorization of the expected type. For the product groups we expect $L_p(T)$ to factor into two quadratics with coefficients in $\mathbb{Z}$. For the groups H_i^k we expect a factorization of the form given in (26), and a similar form applies to H_i^-.[16] For each curve in Table 11 with $f(x)$ of degree 5 corresponding to such a group, we

[16] As previously noted, there are curves with simple Jacobians matching distributions #2 and #11 for which this would not apply, but they don't appear in Table 11.

Licensed to AMS.

Set	X	M_1	M_2	M_3	M_4	M_5	M_6	M_7	M_8
P_1	a_1	0.000	1.001	-0.002	2.002	-0.007	5.005	-0.027	14.01
		0	1	0	2	0	5	0	14
	a_2	0.001	1.001	1.001	3.002	6.005	15.01	36.03	91.10
		0	1	1	3	6	15	36	91
P_2	a_1	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
		0	0	0	0	0	0	0	0
	a_2	1.000	2.010	3.001	6.003	10.00	20.01	35.02	70.05
		1	2	3	6	10	20	35	70
P_3	a_1	-0.002	3.999	-0.045	31.95	-0.590	319.3	-7.69	3574
		0	4	0	32	0	320	0	3584
	a_2	2.999	9.995	36.97	149.8	652.7	3005	14404	71160
		3	10	37	150	654	3012	14445	71398

TABLE 14. Component distributions of a_1 and a_2 for curve #10.

verified the existence of the expected factorization for primes $p \leq 10^6$. For groups with multiple components, we partitioned the primes appropriately (note that for groups of the form $J(H)$ we do not expect a factorization for primes corresponding to components with off-diagonal elements).

The final piece of evidence we present is much less precise, and of an entirely different nature. By computing the group structure of the Jacobian and determining the rank of its ℓ-Sylow subgroup for many p, one can estimate the size of the mod ℓ Galois image $G[\ell]$ in $GSp(2g, \mathbb{Z}/\ell\mathbb{Z})$. The primes for which the ℓ-Sylow subgroup has rank $2g$ correspond to the identity element in $G[\ell]$. The group $GSp(2g, \mathbb{Z}/\ell\mathbb{Z})$ has size $O(\ell^{11})$, and this corresponds to the real dimension of $USp(2g)$ which is 10 (the reduction in dimension arises from unitarization). For all but the first group in Table 13. the real dimension is at most 6. We should expect correspondingly small $G[\ell]$, at most $O(\ell^7)$ in size. By computing

$$d = \frac{\log(\#G[\ell_1]) - \log(\#G[\ell_2])}{\log \ell_1 - \log \ell_2} \tag{28}$$

for various $\ell_1 \neq \ell_2$ we obtain a general estimate for $\#G[\ell] = O(\ell^d)$. The value $d-1$ is then an estimate of the real dimension of H. This is necessarily a rather crude approximation, and one must take care to avoid exceptional values of ℓ. We performed this computation for each exceptional curve in Table 11 where $f(x)$ has degree 5 for $p \leq N = 2^{24}$ and ℓ ranging from 3 to 19. The results agreed with the corresponding dimensions in Table 11 to within ± 1.

7.2. Nonexistence Arguments. We wish to thank Jean-Pierre Serre (private communication) for suggesting the following argument to rule out the case $H = J(G_2 \times G_2)$. Let E be the endomorphism algebra of the Jacobian of the curve over $\overline{\mathbb{Q}}$. Then $E \otimes \mathbb{Q}$ must be a commutative $\mathbb{Q}$-algebra of rank 4; more precisely, it must be either $K \otimes_{\mathbb{Q}} K'$ for some nonisomorphic imaginary quadratic fields K, K',

Licensed to AMS.

or a quartic CM-field. (We cannot have $K \cong K'$ or else H would be forced to have dimension 1 rather than 2.) In either case, $\mathrm{Aut}(E \otimes \mathbb{Q})$ has at most 4 elements, so the elements of H are defined over a field of degree at most 4 over $\mathbb{Q}$. However, $J(G_2 \times G_2)$ has 8 connected components, so this is impossible.

We do not yet have an analogous argument to rule out $H = J(H_2^6)$. However, Serre suggests that it should be possible to give such an argument based on the following data: the algebra $E \otimes \mathbb{Q}$ must be a (possibly split) quaternion algebra over a quadratic field, and the image of Galois in $\mathrm{Aut}(E \otimes \mathbb{Q})$ must have order 24.

8. Conclusion

Based on the results presented in Section 6, we now state a more explicit form of Conjecture 2 for genus 2 curves.

Conjecture 3. *Let C be a genus 2 curve. The distribution of $\bar{L}_p(T)$ over $p \leq N$ converges (as $N \to \infty$) to the distribution of $\chi(T)$ in one of the first 23 subgroups of $USp(4)$ listed in Table 13. For almost all curves, this group is $USp(4)$.*

It would be interesting to carry out a similar analysis in genus 3, but it is not immediately clear from the genus 2 results how many exceptional distributions one should expect. An exhaustive search of the type undertaken in genus 2 may not be computationally feasible in genus 3.

We end by once again thanking Nicholas Katz for his invaluable support throughout this project, and David Vogan for several helpful conversations. We also thank Zeev Rudnick for his feedback on an early draft of this paper, and Jean-Pierre Serre for his remarks in § 7.2.

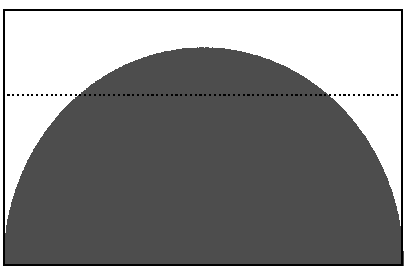
Licensed to AMS.

9. Appendix I - Distributions of s_k

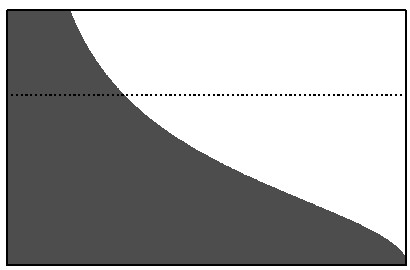
This appendix is a gallery of distributions of s_k for hyperelliptic curves of genus 1, 2, and 3 with large Galois image. The s_k are the kth power sums (Newton symmetric function) of the roots of the unitarized L-polynomial $\bar{L}_p(T)$ defined in Section 2.

Each figure represents a histogram of approximately $\pi(N)$ values derived from $\bar{L}_p(T)$ for $p \leq N$ where the curve has good reduction. The horizontal axis ranges from $-\binom{2g}{k}$ to $\binom{2g}{k}$, divided into approximately $\sqrt{\pi(N)}$ buckets. The vertical axis is scaled to fit the data, with the height of the uniform distribution indicated by a dotted line.

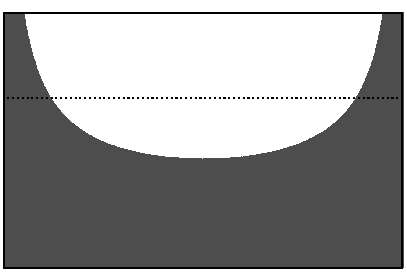
9.1. Genus 1. $N = 2^{35}$; $\quad y^2 = x^3 + 314159x + 271828$.



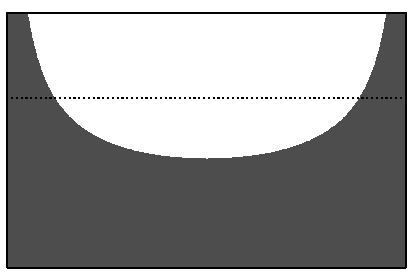
s_1



s_2



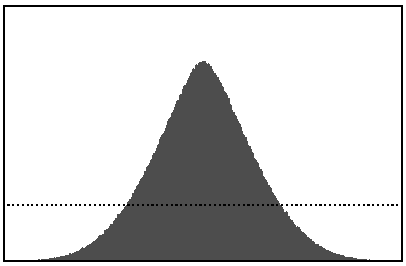
s_3



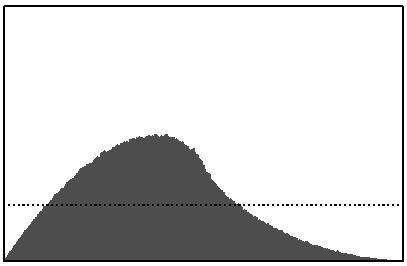
s_4

Licensed to AMS.

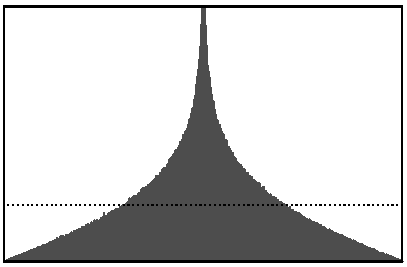
9.2. Genus 2. $N = 2^{26}$;
$y^2 = x^5 + 314159x^3 + 271828x^2 + 1644934x + 57721566.$



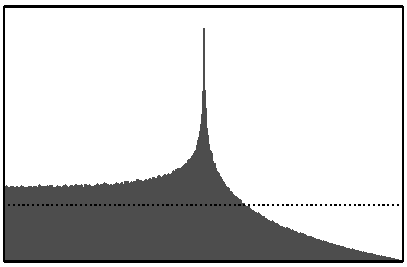
s_1



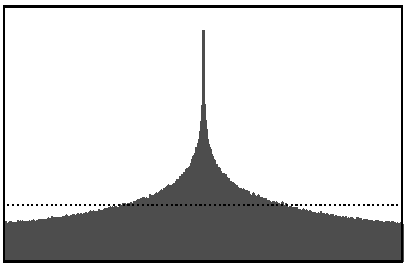
s_2



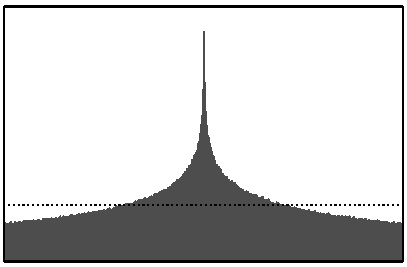
s_3



s_4



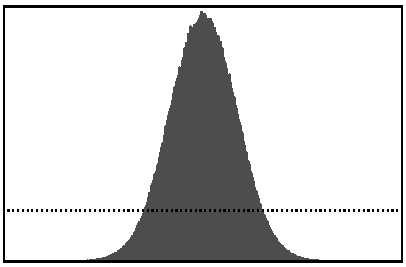
s_5



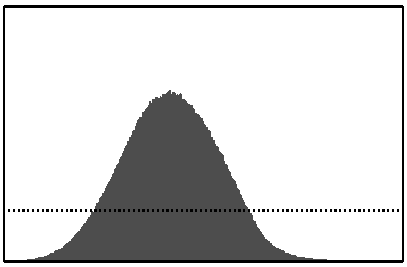
s_6

Licensed to AMS.

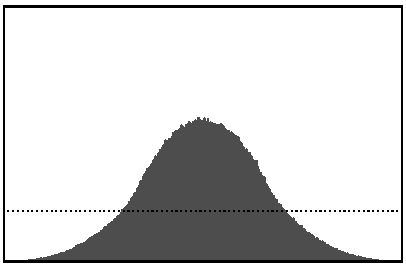
9.3. Genus 3. $N = 2^{25}$;
$y^2 = x^7 + 314159x^5 + 271828x^4 + 1644934x^3 + 57721566x^2 + 1618034x + 141021.$



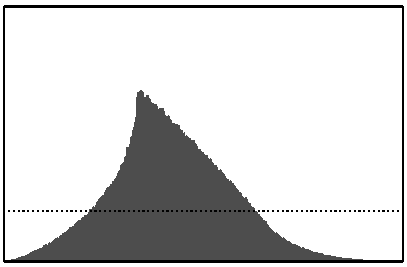
s_1



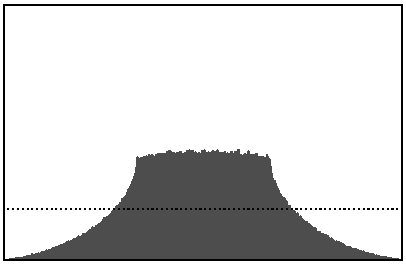
s_2



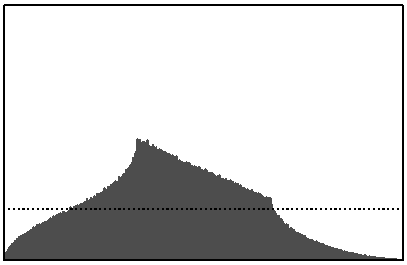
s_3



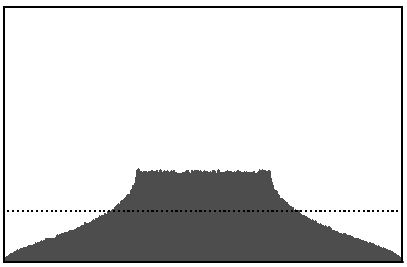
s_4



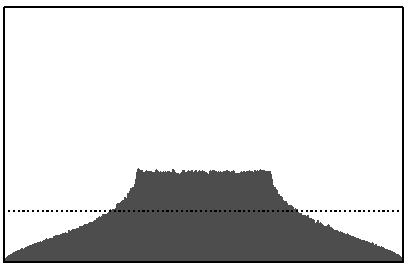
s_5



s_6



s_7

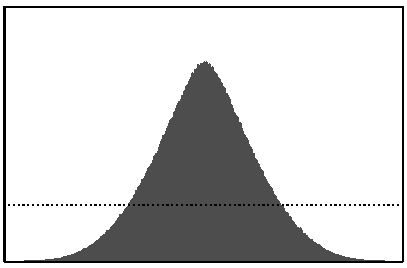


s_8

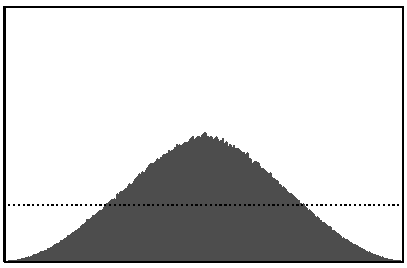
Licensed to AMS.

10. Appendix II - Distributions of a_1 in Genus 2

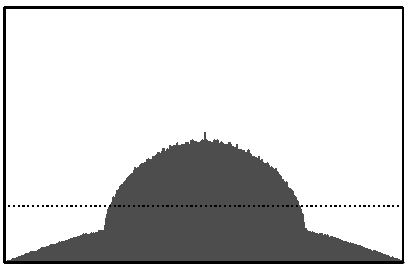
This appendix contains a_1 histograms for each of the first 12 curves listed in Table 11, computed with $N = 2^{26}$. The approximate area of the central spike is given by $z(C)$ in Table 11, corresponding to primes for which $a_p = 0$. The secondary spikes at $a_1 = \pm 2$ appearing in distributions #8 and #12 have approximately zero area.



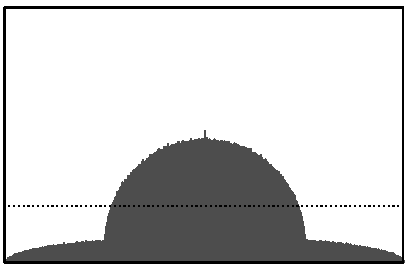
#1



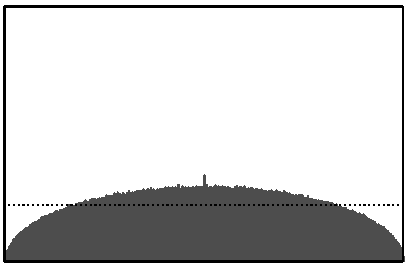
#2



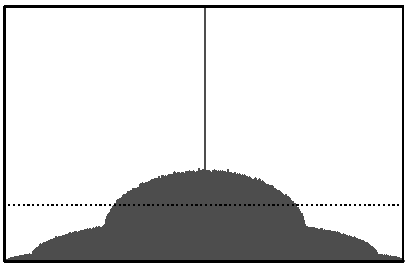
#3



#4

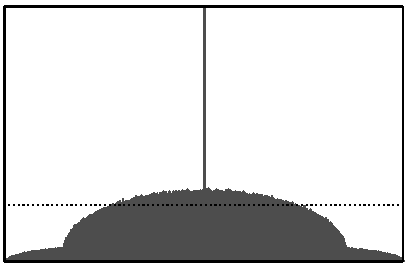


#5

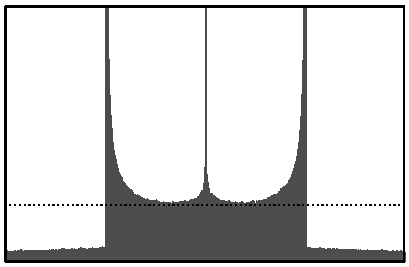


#6

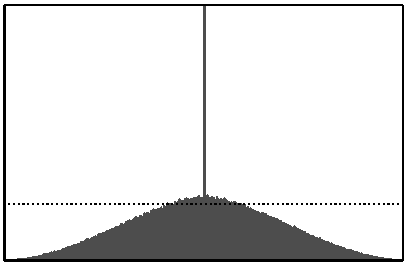
Licensed to AMS.



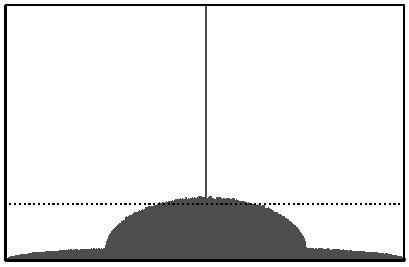
#7



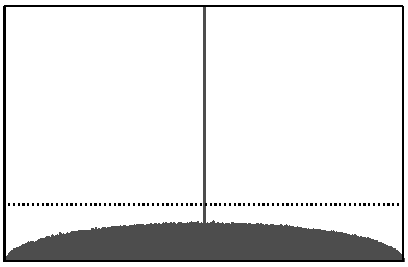
#8



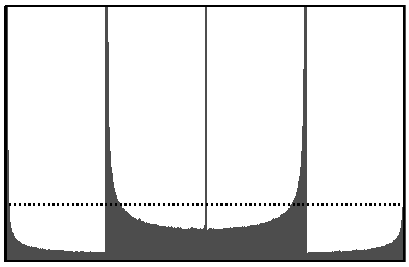
#9



#10



#11



#12

Licensed to AMS.

References

1. Martin Aigner, *Catalan and other numbers: a recurrent theme*, Algebraic combinatorics and computer science, a tribute to Gian-Carlo Rota, Springer, 2001, pp. 347–390.
2. Shigeki Akiyama and Yoshio Tanigawa, *Calculation of values of L-functions associated to elliptic curves*, Mathematics of Computation **68** (1999), no. 227, 1201–1231.
3. Emil Artin, *Quadratische Körper in gebiete der höheren Kongruenzen. I, II*, Mathematische Zeitschrift **19** (1924), 153–246.
4. Stephan Baier, *A remark on the conjectures of Lang-Trotter and Sato-Tate on average*, 2007, preprint, `http://arxiv.org/abs/0708.2535v3`.
5. Stephan Baier and Lianyi Zhao, *The Sato-Tate conjecture on average for small angles*, 2007, to appear, `http://arxiv.org/abs/math/0608318v4`.
6. William D. Banks and Igor E. Shparlinski, *Sato-Tate, cyclicity, and divisibility statistics on average for elliptic curves of small height*, 2007, to appear, `http://arxiv.org/abs/math/0609144`.
7. J. W. S. Cassels and E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus 2*, London Mathematical Society Lecture Note Series, vol. 230, Cambridge University Press, 1996.
8. William Y.C. Chen, Eva Y.P. Deng, Rosena R.X. Du, Richard P. Stanley, and Catherine H. Yan, *Crossings and nestings of matchings and partitions*, Transactions of the American Mathematical Society **359** (2007), 1555–1575.
9. Laurent Clozel, Michael Harris, and Richard Taylor, *Automorphy for some l-adic lifts of automorphic mod ℓ Galois representations*, 2006, preprint, `http://www.math.harvard.edu/~rtaylor/twugnew.pdf`.
10. Alina Carmen Cojocaru, *On the surjectivity of the Galois representations associated to non-CM elliptic curves*, Canadian Mathematics Bulletin **48** (2005), no. 1, 16–31, With an appendix by Ernst Kani.
11. John Cremona, *The elliptic curve database for conductors to 130000*, Algorithmic Number Theory Symposium–ANTS VII, Lecture Notes in Computer Science, vol. 4076, 2006, pp. 11–29.
12. Max Deuring, *Die Klassenkörper der komplexen Multiplication*, Enzyklopädie der mathematischen Wissenschaften, vol. 12 (Book 10, Part II), B.G. Teubner Verlagsgesellschaft, Stuttgart, 1958.
13. Henri Cohen (Ed.) et al., *Handbook of elliptic and hyperelliptic curve cryptography*, Chapman and Hall, 2006.
14. Gerd Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. [Finiteness theorems for abelian varieties over number fields]*, Inventiones Mathematicae **73** (1983), no. 3, 349–366. MR 718935 (85g:11026a) reviewed by James Milne.
15. Gerhard Frey and Michael Müller, *Arithmetic of modular curves and applications*, Algorithmic algebra and number theory (Matzat et al., ed.), Springer-Verlag, 1999, pp. 11–48.
16. Ira M. Gessel, *Symmetric functions and P-recursiveness*, Journal of Combinatorial Theory A **53** (1990), 257–285.
17. Enrique González-Jiménez and Josep González, *Modular curves of genus 2*, Mathematics of Computation **72** (2003), no. 241, 397–418.
18. David J. Grabiner and Peter Magyar, *Random walks in Weyl chambers and the decomposition of tensor powers*, Journal of Algebraic Combinatorics **2** (1993), no. 3, 239–260.
19. Richard K. Guy, Christian Krattenthaler, and Bruce Sagan, *Lattice paths, reflections and dimension-changing bijections*, Ars Combinatorica **34** (1992), 3–15.
20. Chris Hall, *An open image theorem for a general class of abelian varieties*, 2008, preprint, `http://arxiv.org/abs/0803.1682v1`.
21. Michael Harris, Nick Shepherd-Barron, and Richard Taylor, *A family of Calabi-Yau varieties and potential automorphy*, May 2006, preprint, `http://www.math.harvard.edu/~rtaylor/`.
22. Ki-Ichiro Hashimoto and Hiroshi Tsunogai, *On the Sato-Tate conjecture for QM-curves of genus two*, Mathematics of Computation **68** (1999), no. 228, 1649–1662.
23. Everett W. Howe, Franck Leprévost, and Bjorn Poonen, *Large torsion subgroups of split jacobians of curves of genus two or three*, Forum Mathematicum **12** (2000), no. 3, 315–364.
24. Jun-Ichi Igusa, *Arithmetic variety of moduli for genus two*, Annals of Mathematics **2** (1960), no. 72, 612–649.

Licensed to AMS.

25. Nicholas M. Katz, *Larsen's alternative, moments, and the monodromy of Lefschetz pencils*, Contributions to automorphic forms, geometry, and number theory, Johns Hopkins University Press, 2004, pp. 521–560.
26. _____, 2008, e-mail correspondence.
27. Nicholas M. Katz and Peter Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, American Mathematical Society, 1999.
28. Kiran S. Kedlaya and Andrew V. Sutherland, *Computing L-series of hyperelliptic curves*, Algorithmic Number Theory Symposium–ANTS VIII, Lecture Notes in Computer Science, vol. 5011, Springer, 2008, pp. 312–326.
29. Anthony W. Knapp, *Basic algebra*, Birkhäuser, 2006.
30. Donald E. Knuth, *Two notes on notation*, American Mathematical Monthly **99** (1992), no. 5, 403–422.
31. Paul Koosis, *The logarithmic integral I*, Cambridge University Press, 1998.
32. Alain Kraus, *Une remarque sur les points de torsion des courbes elliptiques*, C. R. Acad. Sci. Paris Sér. I Math. **321** (1995), no. 9, 1143–1146.
33. Masato Kuwata, *Quadratic twists of an elliptic curve and maps from a hyperelliptic curve*, Mathematics Journal of Okayama University **47** (2005), 85–97.
34. Serge Lang, *Introduction to modular forms*, Springer, 1976.
35. _____, *Algebraic number theory*, second ed., Springer, 1994.
36. Serge Lang and Hale Trotter, *Frobenius distributions in GL_2 extensions*, Lecture Notes in Mathematics, vol. 504, Springer-Verlag, 1976.
37. Michael Larsen, *The normal distribution as a limit of generalized Sato-Tate measures*, early 1990s, preprint, `http://mlarsen.math.indiana.edu/~larsen/papers/gauss.pdf`.
38. Barry Mazur, *Finding meaning in error terms*, Bulletin of the American Mathematical Society **45** (2008), no. 2, 185–228.
39. B.J.J. Moonen and Yu. G. Zarhin, *Hodge classes on abelian varieties of low dimension*, Mathematische Annalen **315** (1999), 711–733.
40. David Mumford, *A note of Shimura's paper "Discontinuous groups and abelian varities"*, Mathematische Annalen **181** (1969), 345–351.
41. Eric M. Rains, *High powers of random elements of compact Lie groups*, Probability Theory and Related Fields **107** (1997), 219–241.
42. _____, *Images of eigenvalue distributions under power maps*, Probability Theory and Related Fields **125** (2003), no. 4, 522–538.
43. Fernando Rodriguez-Villegas, *Explicit models of genus 2 curves with split CM*, Algorithmic Number Theory Symposium–ANTS IV, Lecture Notes in Computer Science, vol. 1838, Springer-Verlag, 2000, pp. 505–514.
44. Jean-Pierre Serre, *Groupes linéaires modulo p et points d'ordre fini des variétés abéliennes*, 1986, Collège de France course notes by Eva Bayer-Fluckiger, `http://alg-geo.epfl.ch/~bayer/files/Serre-cours.pdf`.
45. _____, *Propriétés conjecturales des groupes de Galois motiviques et des représentations l-adiques*, Motives (Seattle, WA, 1991), Proceedings of Symposia in Pure Mathematics, vol. 55, American Mathematical Society, 1994, pp. 377–400. MR 1265537 (95m:11059)
46. _____, *Lettre a Marie-France Vigneras*, Oeuvres, Collected Papers, Springer, 2000, pp. 38–55.
47. N. J. A. Sloane, *The on-line encyclopedia of integer sequences*, 2007, `www.research.att.com/~njas/sequences/`.
48. N.P. Smart, *S-unit equations, binary forms and curves of genus 2*, Proceedings of the London Mathematical Society **75** (1997), no. 2, 271–307.
49. Jerome Spanier and Keith B. Oldham, *An atlas of functions*, Hemisphere, 1987.
50. William A. Stein and Mark Watkins, *A database of elliptic curves–first report*, Algorithmic Number Theory Symposium–ANTS V, Lecture Notes in Computer Science, vol. 2369, Springer, 2002, pp. 267–275.
51. Andrew V. Sutherland, *Notes on the Hasse-Witt matrix and the density of zero Frobenius traces*, 2008, in preparation.
52. J. T. Tate, *Algebraic cycles and poles of zeta functions*, Arithmetical Algebraic Geometry, Harper and Row, 1965.
53. Richard Taylor, *Automorphy for some ℓ-adic lifts of automorphic mod ℓ Galois representations II*, 2006, preprint, `http://www.math.harvard.edu/~rtaylor/twugk6.pdf`.

Licensed to AMS.

54. Paul van Wamelen, *Examples of genus two CM curves defined over the rationals*, Mathematics of Computation **68** (1999), no. 225, 307–320.
55. ———, *Proving that a genus 2 curve has complex multiplication*, Mathematics of Computation **68** (1999), no. 228, 1663–1677.
56. André Weil, *Numbers of solutions of equations in finite fields*, Bulletin of the American Mathematical Society **55** (1949), 497–508.
57. Hermann Weyl, *Classical groups*, second ed., Princeton University Press, 1946.
58. Yuri G. Zarhin, *Hyperelliptic jacobians with complex multiplication*, Mathematical Research Letters **7** (2000), no. 1, 123–132.

Department of Mathematics, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, MA 02139

E-mail address: (kedlaya|drew)@math.mit.edu

Licensed to AMS.