

RESEARCH STATEMENT

Jennifer Paulhus

My primary research interests lie in two distinct branches of number theory. I explore decompositions of Jacobian varieties of curves and related arithmetic geometry problems. I also study questions about the parity of k th powers of residues in $\mathbb{Z}/p\mathbb{Z}$ for primes p and related topics on exponential sum bounds and finite Fourier series. Brief overviews of both of these areas may be found immediately below and greater detail about each may be found in subsequent sections.

1 Brief Overview

Arithmetic geometry is a field of mathematics sitting at the cusp of number theory and algebraic geometry. As in algebraic geometry, we primarily study varieties (solutions to systems of polynomial equations) but while algebraic geometers tend to ask questions about varieties over the complex numbers, we are interested in varieties over rings that are in the purview of number theory: \mathbb{Z} , \mathbb{Q} , and number fields (finite extensions of \mathbb{Q}). Traditionally much of the work focused on elliptic curves with stunning results (Fermat's Last Theorem being perhaps the best known example).

Points on elliptic curves have a natural group structure which is integral to the success in understanding elliptic curves and using them to solve open problems. One generalization of elliptic curves is higher genus curves. Unfortunately, higher genus curves do not have a natural group structure on their points so a variety associated to the curve which does have such a group structure is defined. This variety is called the Jacobian variety of the curve and we can ask many of the same questions which have been asked about elliptic curves.

Like other mathematical objects, one fruitful way to study Jacobian varieties is to try to factor them into smaller abelian varieties and use knowledge about these smaller pieces to study the Jacobian. The core of my research in this area focuses on understanding decompositions of Jacobian varieties of higher genus curves. I discuss my past and future work on this area in Sections 2 and 4.

During my postdoc I have had the opportunity to collaborate with Bourgain, Cochrane, and Pinner. Our work has focused on several questions about the parity of images of elements in $\mathbb{Z}/p\mathbb{Z}$ under certain permutations. We began by working on the following problem. Given an odd prime p , and integers A and d with $\gcd(d, p-1) = 1$ and $p \nmid A$, determine when the map $x \mapsto Ax^d$ permutes the even residues $\mathbb{E} := \{0, 2, 4, \dots, p-1\}$ in $\mathbb{Z}/p\mathbb{Z}$. If $p = 5$ and $A = d = 3$, for instance, then the map does permute the even residues. There are five other examples of this for $p \leq 13$. It was first conjectured by Goresky and Klapper [12] that for primes greater than 13 the map above does not permute the even residues. In our work, we prove this conjecture is true for sufficiently large primes.

This conjecture was motivated by an equivalent conjecture concerning binary ℓ -sequences based on p : sequences $\mathbf{a} = \{a_i\}_i$ of zeros and ones where $a_i := (2^{-i} \bmod p) \pmod{2}$. These sequences come from the study of pseudo-random binary sequences. The conjecture of Goresky

and Klapper would imply that these ℓ -sequences give large families of cyclically distinct sequences with ideal arithmetic cross-correlation.

The problem above is related to a question D.H. Lehmer posed [14]: given a prime p , determine the number N_{-1} of even residues in $\mathbb{Z}/p\mathbb{Z}$ with odd multiplicative inverse. Intuitively, one expects about one quarter of all residues in $\mathbb{Z}/p\mathbb{Z}$ will satisfy this and, in fact, Zhang [24] proved $N_{-1} \sim p/4$. This question may be restated as asking about the parity of the image of the map $x \mapsto x^{-1}$. In the work discussed above, we proved that $N_d := \#\{x \in \mathbb{E} \mid Ax^d \in \mathbb{O}\}$ is non-zero for sufficiently large p (where \mathbb{O} denotes the odd residues $\{1, 3, 5, \dots, p-2\}$). In a sequel, we consider the more general problem of determining N_d . In this more general setting, it is not always true that $N_d \sim p/4$. These results use methods of finite Fourier series and bounds for exponential sums. More details may be found in Section 3.

2 Jacobian Variety Decompositions

Decomposable Jacobian varieties have many interesting applications. Decompositions of Jacobians of genus 2 curves have been well studied and curves whose Jacobians decompose into two elliptic curves have special properties. As one example, Howe, Leprévost, and Poonen [15] construct genus 2 and 3 curves with large torsion subgroups. Their construction specifically relies on the curves having split Jacobians.

In the other direction, the elliptic curves that appear in these decompositions are better understood because of their presence as a factor of a certain Jacobian. As an example, \mathbb{Q} -curves (elliptic curves defined over a number field which are isogenous to their Galois conjugates) of degree 2 and 3 are precisely the elliptic factors of certain families of genus 2 curves [4]. Little is known beyond the genus 2 case. The success in genus 2 suggests a better understanding of Jacobian decompositions in higher genus is warranted.

Much of my past research involved working towards answering the following question.

Question 1. *For a fixed genus g , what is the largest positive integer t such that there is some curve X of that genus whose Jacobian J_X is isogenous to the product of t copies of an elliptic curve E and some other abelian variety A , denoted $J_X \sim E^t \times A$.*

The largest t could be is g , the genus of the curve. Ekedahl and Serre [6] find examples of curves X of many genera up to 1297 with Jacobian $J_X \sim E_1 \times \dots \times E_g$ where E_i are elliptic curves but which are not necessarily isogenous.

The Mordell-Weil theorem says that the points of an elliptic curve over a number field form a finitely generated group. The maximal number of \mathbb{Z} -linearly independent points is called the rank of the curve. Rank is still a quite mysterious object. Over the rationals, for instance, it is conjectured that there are curves of arbitrarily large rank but so far the largest known rank is of a curve with at least 28 linearly independent points, hence of rank at least 28. There are several major open conjectures about rank such as the Birch and Swinnerton-Dyer conjecture and the Parity conjecture. Rubin and Silverberg have a nice survey paper about rank and related questions [22].

Answers to Question 1 have consequences for questions of ranks of elliptic curves and their twists. If there is some curve X such that $J_X \sim E^t \times A$ then there is a map $\phi : X \rightarrow E^t$. If X has a point P over some field k then ϕ sends P to $P_1 \times P_2 \times \dots \times P_t$ where the $P_i \in E$.

If we are able to show the P_i are \mathbb{Z} -linearly independent then E would have rank at least t over k .

To find partial answers to the question posed above, in my thesis I developed a technique to decompose Jacobian varieties of a curve using a result of Kani and Rosen [16] which connects idempotent relations in the group ring $\mathbb{Q}[G]$ (where G is the automorphism group of the curve) to isogeny relations among the Jacobian and images of the Jacobian under endomorphisms. Then I use representation theory to determine if the factors in the decomposition are isogenous elliptic curves. Some results are summarized in Table 1. The automorphism group of a curve is given by its number in the table of small groups from the computer algebra package GAP [9]. The first of these number is the order of the group.

Genus	Automorphism Group	Jacobian Decomposition	Genus	Automorphism Group	Jacobian Decomposition
3	$S_4 \times C_2$	$J_X \sim E^3$	7	(504, 156)	$J_X \sim E^7$
4	(72, 40)	$J_X \sim E^4$	8	(336, 208)	$J_X \sim E^8$
5	(160, 234)	$J_X \sim E^5$	9	(192, 955)	$J_X \sim E_1^3 \times E_2^6$
6	(72, 15)	$J_X \sim E^6$	10	(360, 118)	$J_X \sim E^{10}$

Table 1: Examples for Bounds on t

What follows is a sketch of the ideas of this technique to decompose Jacobian varieties. Throughout k will be an algebraically closed field of characteristic 0. The technique works generally for any field but it relies on knowing the automorphism group of the curve which is dependent on the field we work over. Also ζ_k will denote a primitive k th root of unity and D_n and C_n are the dihedral and cyclic groups of order n , respectively.

Given a curve X of genus g over a field k , the automorphism group G of X is the automorphism group of the field extension $k(X)$ over k , where $k(X)$ is the function field of X . This group will always be finite for $g \geq 2$.

Kani and Rosen prove a result tying idempotent relations in $\text{End}_0(J_X) := \text{End}(J_X) \otimes_{\mathbb{Z}} \mathbb{Q}$ to isogenies among images of J_X under endomorphisms. If ε_1 and ε_2 are idempotents in $\text{End}_0(J_X)$ then $\varepsilon_1 \sim \varepsilon_2$ if $\chi(\varepsilon_1) = \chi(\varepsilon_2)$ for all characters χ in $\text{End}_0(J_X)$.

Theorem 1. (Theorem A, [16]) *Let $\varepsilon_1, \dots, \varepsilon_n, \varepsilon'_1, \dots, \varepsilon'_m \in \text{End}_0(J_X)$ be idempotents. Then the idempotent relation*

$$\varepsilon_1 + \dots + \varepsilon_n \sim \varepsilon'_1 + \dots + \varepsilon'_m$$

holds in $\text{End}_0(J_X)$ if and only if we have the isogeny relation

$$\varepsilon_1(J_X) \times \dots \times \varepsilon_n(J_X) \sim \varepsilon'_1(J_X) \times \dots \times \varepsilon'_m(J_X).$$

There is a natural \mathbb{Q} -algebra homomorphism e from $\mathbb{Q}[G]$ to $\text{End}_0(J_X)$. It is a well known result of Wedderburn that any group ring of the form $\mathbb{Q}[G]$ has a decomposition into the direct sum of matrix rings over division rings Δ_i :

$$\mathbb{Q}[G] = \bigoplus_i M_{n_i}(\Delta_i). \tag{1}$$

Define $\pi_{i,j}$ to be the idempotent in $\mathbb{Q}[G]$ which is the zero matrix for all components except the i th component where it is the matrix with a 1 in the (j, j) position and zeros elsewhere. The following equation is an idempotent relation in $\mathbb{Q}[G]$:

$$1_{\mathbb{Q}[G]} = \bigoplus_{i,j} \pi_{i,j}.$$

Applying the map e and Theorem 1 to it gives

$$J_X \sim \bigoplus_{i,j} e(\pi_{i,j})J_X. \quad (2)$$

The primary goal in my thesis was to study isogenous elliptic curves that appear in the decomposition above. In order to identify which summands in (2) have dimension 1, we use work in [7] to compute the dimensions of these factors.

If χ_i is the irreducible \mathbb{Q} -character associated to the i th component from (1), then the dimensions of the summands in (2) are

$$\dim e(\pi_{i,j})J_X = \frac{1}{2} \dim_{\mathbb{Q}} \pi_{i,j}V = \frac{1}{2} \langle \chi_i, \chi_V \rangle \quad (3)$$

where χ_V is the character of a special representation of G called the Hurwitz representation. χ_V may be computed from the monodromy of the cover X over $Y = X/G$ and induced characters.

Hence given an automorphism group G of a curve X and monodromy for the cover X over Y , to compute these dimensions we first determine the degrees of the irreducible \mathbb{Q} -characters of G , which will be the n_i values in (1). Next we compute the Hurwitz character for this group and covering, and finally compute the inner product of the irreducible \mathbb{Q} -characters with the Hurwitz character as in (3).

We are particularly interested in *isogenous* factors. The following proposition gives us a condition for the factors to be isogenous.

Proposition 1. [20] *With notation as above, $e(\pi_{i,j_1})J_X \sim e(\pi_{i,j_2})J_X$ for any j_1, j_2 .*

Suppose a curve of genus g has automorphism group with group ring decomposition as in (1) with at least one matrix ring of degree close to g (so one n_i value close to g – call it n_j). If the computations of dimensions of abelian variety factors outlined above lead to a dimension 1 variety in the place corresponding to that matrix ring (the j th place), Proposition 1 implies that the Jacobian variety decomposition consists of n_j isogenous elliptic curves.

Maagard, Shaska, Shpectorov, and Völklein [18] compute automorphism groups and monodromy for many curves up to genus 10. We applied the technique above to their data and were able to find the curves listed in Table 1. The genus 3 case in that table was already in the literature, although it was found using a different technique [17]. The genus 7 example is a Hurwitz curve called the MacBeath curve. Work of MacBeath, Jennifer Whitworth (a student of MacBeath), and Barry and Tretkoff showed, using special properties of this particular curve, that the Jacobian was isogenous to 7 copies of an elliptic curve [25]. The rest of the results in the table are new and the first known results of this kind.

Except for the genus 3 curve in Table 1 none of the curves are hyperelliptic (curves which are defined by an equation of the form $y^2 = f(x)$ where $f(x) \in k[x]$). Recall that one of the

Table 2: Jacobian Variety Decompositions

Genus	Auto. Group	Dim.	Jacobian Decomposition	Genus	Auto. Group	Dim.	Jacobian Decomposition
4	$\mathrm{SL}_2(3)$	0	$E_1^2 \times E_2^2$	8	$\mathrm{SL}_2(3)$	1	$A_{2,1}^2 \times A_{2,2}^2$
5	$A_4 \times C_2$	1	$A_2 \times E^3$		W_3	0	$A_2^2 \times E^4$
	W_2	0	$E_1^2 \times E_2^3$	9	$A_4 \times C_2$	1	$A_3^3 \times E^3$
	$A_5 \times C_2$	0	E^5		W_2	0	$E_1 \times E_2^2 \times A_2^3$
6	$\mathrm{GL}_2(3)$	0	$E_1^2 \times E_2^4$		$A_5 \times C_2$	0	$E_1^4 \times E_2^5$
7	$A_4 \times C_2$	1	$E \times A_2^3$	10	$\mathrm{SL}_2(3)$	1	$A_2^2 \times A_3^3$

motivations for the question posed at the beginning of this section was to find elliptic curves with large rank. If X were a hyperelliptic curve with $J_X \sim E^t \times A$ then there is an infinite number of quadratic extensions where X has a point (for any $s \in \mathbb{Q}$ square-free, if $k = \mathbb{Q}(\sqrt{f(s)})$ then the point $(s, \sqrt{f(s)})$ will be on the curve over k) and so there is the potential for an elliptic curve of rank at least t over an infinite family of quadratic fields. It would be helpful to have results similar to those in Table 1 for hyperelliptic curves.

More recently (and with a better understanding of some results from representation theory), I have applied the technique above to several families of hyperelliptic curves. These results may be found in Table 2, where W_2 and W_3 are groups of order 48 defined by the relations: $W_2 = \langle u, v \mid u^4, v^3, vu^2v^{-1}u^2, (uv)^4 \rangle$ and $W_3 = \langle u, v \mid u^4, v^3, u^2(uv)^4, (uv)^8 \rangle$ (we use notation for these groups as in [23]). The dimension is the dimension of the family of curves of that genus with prescribed automorphism group inside the module space of all curves of that genus.

In particular, we find a genus 5 hyperelliptic curve with Jacobian isogenous to E^5 which is the first example of a hyperelliptic curve of genus 5 with such a decomposition.

3 Parity of Residues modulo p

Let p be an odd prime, $\mathbb{E} := \{0, 2, 4, \dots, p-1\}$ and $\mathbb{O} := \{1, 3, 5, \dots, p-2\}$ the set of even and odd residues, respectively in $\mathbb{Z}/p\mathbb{Z}$. Goresky and Klapper [12] conjectured the following:

Conjecture (Generalized G-K). *Given a prime $p > 13$ and integers d and A such that $\mathrm{gcd}(d, p-1) = 1$ and $p \nmid A$, the map on $\mathbb{Z}/p\mathbb{Z}$ sending x to Ax^d does not fix the even residues unless it is the identity map ($A \equiv 1 \pmod{p}$, $d \equiv 1 \pmod{p-1}$).*

As was mentioned in the introduction, this conjecture has implications to sequences with ideal arithmetic cross-correlation. An exhaustive computer search of primes less than 2 million has proven the conjecture for these cases as well [13]. Bourgain, Cochrane, Pinner, and I prove this conjecture for sufficiently large primes.

Theorem 2. [3] *For any prime $p > 2.26 \times 10^{55}$ and integers d, A with $\mathrm{gcd}(d, p-1) = 1$ and $p \nmid A$, the map $x \mapsto Ax^d$ does not permute the even residues modulo p unless it is the identity map.*

In a sequel, we improve the theorem above by removing the gcd condition on d .

Given $M := \#\{x_1, x_2, x_3, x_4 \in \mathbb{Z}/p\mathbb{Z} \mid x_1 + x_2 = x_3 + x_4, x_1^d + x_2^d = x_3^d + x_4^d\}$, the main idea of the proof is to show that if $M < .000823p^3$, then the conjecture above is true. To prove this we show there is a solution (x, y) to $A(2x)^d = 2y - 1$ over $\mathbb{Z}/p\mathbb{Z}$ with $(x, y) \in I_1 \times I_2$ with $I_1 = \{0, 1, 2, \dots, \frac{p-1}{2}\}$ and $I_2 = I_1 - \{0\}$. We define a function $\alpha(x, y)$ which is the convolution of characteristic functions of subintervals of the intervals I_1 and I_2 such that α is supported on $I_1 \times I_2$. Special properties of the function's Fourier coefficients are then used to prove that when M is bounded $\sum_{A(2x)^d=2y-1} \alpha(x, y) > 0$.

One problem is that this bound for M is not true if $d_1 := \gcd(d-1, p-1) < .18(p-1)^{16/23}$. (See Cochrane and Pinner [5] for more details.) To rectify this, we use a different technique (utilizing multiplicative characters) to prove that if $d_1 > 10\sqrt{p}$ and $p > 2.1 \times 10^7$, then the Generalized G-K Conjecture is true. Combining these two results gives Theorem 2.

Suppose now for any integer k we define $N_k = N_k(A) := \#\{x \in \mathbb{E} \mid Ax^k \in \mathbb{O}\}$. The work above shows that if $\gcd(k, p-1) = 1$ then $N_k \neq 0$. For $k = -1$, Zhang [24] proved that $N_{-1} \sim p/4$. For general k , this asymptotic result is not necessarily true and depends on several special values: $d := \gcd(k, p-1)$, $d_1 := \gcd(k-1, p-1)$, as well as $s := \frac{p-1}{d}$ and $t := \frac{p-1}{d_1}$.

For instance, if t and $|A|$ are both small odd numbers, we show $N_k \sim \left(1 - \frac{1}{At}\right) \frac{p}{4}$, and thus there is some bias. There are, however, a number of situations where $N_k \sim p/4$. Let

$$e_p(\cdot) := e^{2\pi i \cdot / p} \text{ and let } \Phi(k) := \max_{\substack{a \in \mathbb{Z}/p\mathbb{Z} \\ a \neq 0}} \left| \sum_{x \neq 0} e_p(ax^k) \right|.$$

Theorem 3. [2] *Let k, A be any integers with $p \nmid A$.*

(a) *If k is odd, and t is even then*

$$\left| N_k - \frac{p}{4} \right| \ll p^{89/92} \log^2 p.$$

(b) *If k is odd and t is odd then*

$$\left| N_k - \frac{p}{4} \right| \ll d_1 + \frac{p}{\log p}.$$

(c) *If k is even then for $c > 1$*

$$\left| N_k - \frac{p}{4} \right| \ll \Phi(k) \log \left(\frac{cp}{\Phi(k)} \right).$$

Thus, when k is odd and $d_1 = o(p)$, or when k is even and $\Phi(k) = o(p)$, we get $N_k \sim p/4$. There has been much recent interest in bounding exponential sums, and the best estimates for $\Phi(k)$ are from work of Bourgain and Tao using breakthroughs in additive combinatorics.

The proof of Theorem 3 patches together several smaller theorems each contingent on the values of d_1 , s , and t . These smaller theorems utilize a variety of results. We use estimates for monomial and binomial exponential sums (in particular bounds on M as discussed above) and the Polya, Landau, Schur bound for incomplete character sums. Also, let $\{C_1, \dots, C_t\}$ be the

set of nonzero $(k-1)$ -st powers and for any $C \in \mathbb{Z}$ with $p \nmid C$, let $F(C) := \sum_x \chi_{\mathbb{E}}(x) \chi_{\mathbb{O}}(Cx)$ be the number of even residues x such that Cx is odd. We prove a bound on $\left| N_k - \frac{1}{t} \sum_{i=1}^t F(AC_i) \right|$. On average $F(C)$ will be $p/4$ so we study $\delta_C = F(C) - \frac{p}{4}$ to determine any discrepancy. This value δ_C depends on the distribution of points in the lattice $\{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid y \equiv Cx \pmod{p}\}$ and we are able to estimate $|\delta_C|$.

4 Current and Future Research

Broadly, my future research plans in arithmetic geometry involve understanding how Jacobian varieties of curves decompose. The technique from my thesis has not been exhausted yet so there is still work to be done in that direction. But, a complete understanding of Jacobian decompositions will not come out of that work alone and thus there are several other directions my research is heading as well.

I. In results obtained in my thesis and subsequent work on hyperelliptic curves, I prove that Jacobians of certain curves decompose into many isogenous elliptic curves but I do not yet know what these elliptic curves actually are. I am currently working to find equations for these curves. Once I have those, I will be able to study the arithmetic of these elliptic curves and ask various questions about them. Are they \mathbb{Q} -curves? What is their torsion? Are families of elliptic curves with certain properties identifiable in these factors? Can I prove interesting results about their rank or rank of twists, as in the motivational example in Section 2.

For several special families of automorphism groups of hyperelliptic curves I was able to prove decomposition results for any genus which has a curve of that automorphism group [19]. In general however, trying to answer the question in the beginning of Section 2 completely for higher genus will require alternative techniques. The moduli space of curves of a fixed genus may be a good place to start. In genus 2 studying how the families with fixed automorphism groups sit in the moduli space of curves of that genus led to complete classification of Jacobian decompositions based on automorphism groups [10] as well as results on \mathbb{Q} -curves [4]. Similarly, Pries and Glass answered questions about p -torsion in characteristic p by studying the moduli space of curves of a given genus [11].

II. Suppose that instead of fixing a genus and asking for many elliptic curves in the decomposition of the Jacobian of some curve of that genus, we fix an elliptic curve E over the field of complex numbers. Can we determine (or at least bound) the set of r such that E^r is isogenous to some Jacobian? Or, if we are also given a positive integer t , can we find the smallest genus such that E^t is a factor in the decomposition of the Jacobian of some curve of that genus? These questions lead us to special cases of the Schottky problem, that is we need to decide if certain principally polarized abelian varieties, obtained as the product of elliptic curves, correspond to the Jacobian of a curve.

Howe, Leprévost and Poonen [15] produce genus 3 curves with large torsion subgroups by finding elliptic curves with large torsion subgroups and proving that their product may be recognized as the Jacobian of a genus 3 curve. This method of starting with elliptic curves with

a desired property and showing their product is the Jacobian of a curve has been utilized with some limited success. It is, however, quite hard in general to determine if an abelian variety is actually a Jacobian. Starting with my results which give products of elliptic curves that are already known to be factors of Jacobians provides an alternative way to prove some of these results.

For example, Ford and Shparlinki [8] prove a lower bound for the largest order of elements in the Jacobian of a curve over the finite field with $q = p^r$ elements for all but $o(\pi(x))$ prime powers $q < x$ for a fixed x . In genus 1 and 2 they show their bound is sharp. I am currently working to find examples in genus 3, and perhaps higher genus, which attain this bound. The goal is to search for families of genus 3 curves whose Jacobians are known, by my work, to split into three elliptic curves which themselves attain the bound for elliptic curves.

III. It is not just the elliptic factors of Jacobian varieties which are interesting. Given a covering of curves $X \rightarrow C$ then $J_X \sim J_C \times P$ where P is called a Prym variety. Information about P may provide us with information about X or might help us decompose J_X . For instance, let X be the genus 3 curve $y^2 = x(x^6 + ax^3 + 1)$ for some a in k (which has automorphism group D_{12}) and Y be $y^2 = (x^2 - 4)(x^3 - 3x + a)$, the quotient of X by one order two element of its automorphism group. Our techniques cannot be used to decompose J_Y (since Y had no extra automorphisms) but we can use the techniques in two different ways to conclude that the Jacobian of X is isogenous to both $J_Y \times E_2$ and $E_1 \times E_2^2$, which means $J_Y \sim E_1 \times E_2$. This is a very simple example but this idea may be useful in high genus. I will explore this idea further with families of higher genus curves which have no extra automorphisms in the hopes of understanding the decompositions of their Jacobians better.

Also, are the abelian varieties which are non-elliptic factors even Jacobian varieties of some lower genus curve? In [1] Achter is interested in the following property a curve X might have: if $X \rightarrow C$ is a finite cover, then C has genus zero. If J_X is simple then X will have this property. The question is whether the converse of this statement is also true. For genus up to 6 the converse is true since most principally polarized abelian varieties are Jacobians. For higher genus it is unknown whether the converse is true and is one motivation for studying whether factors of Jacobians could be abelian varieties which are not Jacobian varieties.

References

- [1] J. D. Achter. Split reductions of simple abelian varieties. *Math. Res. Lett.*, 16(2):199–213, 2009.
- [2] J. Bourgain, T. Cochrane, J. Paulhus, and C. Pinner. On the parity of k th powers mod p : A generalization of a problem of Lehmer. In preparation.
- [3] J. Bourgain, T. Cochrane, J. Paulhus, and C. Pinner. Decimations of l -sequences and permutations of even residues mod p . *SIAM J. Discrete Math.*, 23(2):842–857, 2009.
- [4] G. Cardona. \mathbb{Q} -curves and abelian varieties of GL_2 -type from dihedral genus 2 curves. In *Modular curves and abelian varieties*, volume 224 of *Progr. Math.*, pages 45–52. Birkhäuser, Basel, 2004.
- [5] T. Cochrane and C. Pinner. An improved Mordell type bound for exponential sums. *Proc. Amer. Math. Soc.*, 133(2):313–320 (electronic), 2005.
- [6] T. Ekedahl and J.-P. Serre. Exemples de courbes algébriques à jacobienne complètement décomposable. *C. R. Acad. Sci. Paris Sér. I Math.*, 317(5):509–513, 1993.

- [7] J. S. Ellenberg. Endomorphism algebras of Jacobians. *Adv. Math.*, 162(2):243–271, 2001.
- [8] K. Ford and I. Shparlinski. On curves over finite fields with Jacobians of small exponent. *Int. J. Number Theory*, 4(5):819–826, 2008.
- [9] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.4*, 2006. (<http://www.gap-system.org>).
- [10] P. Gaudry and É. Schost. On the invariants of the quotients of the Jacobian of a curve of genus 2. In *Applied algebra, algebraic algorithms and error-correcting codes (Melbourne, 2001)*, volume 2227 of *Lecture Notes in Comput. Sci.*, pages 373–386. Springer, Berlin, 2001.
- [11] D. Glass and R. Pries. Hyperelliptic curves with prescribed p -torsion. *Manuscripta Math.*, 117(3):299–317, 2005.
- [12] M. Goresky and A. Klapper. Arithmetic crosscorrelations of feedback with carry shift register sequences. *IEEE Trans. Inform. Theory*, 43(4):1342–1345, 1997.
- [13] M. Goresky, A. Klapper, R. Murty, and I. Shparlinski. On decimations of l -sequences. *SIAM J. Discrete Math.*, 18(1):130–140 (electronic), 2004.
- [14] R. K. Guy. *Unsolved problems in number theory*. Problem Books in Mathematics. Springer-Verlag, New York, third edition, 2004.
- [15] E. W. Howe, F. Leprévost, and B. Poonen. Large torsion subgroups of split Jacobians of curves of genus two or three. *Forum Math.*, 12(3):315–364, 2000.
- [16] E. Kani and M. Rosen. Idempotent relations and factors of Jacobians. *Math. Ann.*, 284(2):307–327, 1989.
- [17] M. Kuwata. Quadratic twists of an elliptic curve and maps from a hyperelliptic curve. *Math. J. Okayama Univ.*, 47:85–97, 2005.
- [18] K. Magaard, T. Shaska, S. Shpectorov, and H. Völklein. The locus of curves with prescribed automorphism group. *Sūrikaisekikenkyūsho Kōkyūroku*, (1267):112–141, 2002. Communications in arithmetic fundamental groups (Kyoto, 1999/2001).
- [19] J. Paulhus. Elliptic factors in Jacobians of hyperelliptic curves with certain automorphism groups. Preprint. Available at: <http://www.math.ksu.edu/~paulhus>.
- [20] J. Paulhus. *Elliptic factors in Jacobians of low genus curves*. PhD thesis, University of Illinois at Urbana-Champaign, 2007.
- [21] J. Paulhus. Decomposing Jacobians of curves with extra automorphisms. *Acta Arith.*, 132(3):231–244, 2008.
- [22] K. Rubin and A. Silverberg. Ranks of elliptic curves. *Bull. Amer. Math. Soc. (N.S.)*, 39(4):455–474 (electronic), 2002.
- [23] T. Shaska. Determining the automorphism group of a hyperelliptic curve. In *Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation*, pages 248–254 (electronic), New York, 2003. ACM.
- [24] Z. Wenpeng. On a problem of D. H. Lehmer and its generalization. *Compositio Math.*, 86(3):307–316, 1993.
- [25] J. Wolfart. Regular dessins, endomorphisms of Jacobians, and transcendence. In *A panorama of number theory or the view from Baker’s garden (Zürich, 1999)*, pages 107–120. Cambridge Univ. Press, Cambridge, 2002.