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 these curves and using them to solve open problems. The Mordell-Weil theorem says that the points of an elliptic curve over a number field form a finitely generated group. The maximum 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 elliptic curves of arbitrarily large rank but so far the largest known rank is 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 [21].

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 a natural 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 smallest possible factors in these decompositions are elliptic curves (abelian varieties of dimension one). Decompositions of Jacobian varieties of genus 2 curves have been well studied and curves whose Jacobians decompose into two elliptic curves have special properties.

As one example, a newer intractable math problem that may be useful in cryptography is called the vector decomposition problem. Protocols have been proposed for signature schemes using a one-dimensional family of genus 2 curves over a finite field, whose Jacobians decompose into the product of two elliptic curves [4]. As another example, Howe, Leprévost, and Poonen [13] construct genus 2 and 3 curves with Jacobians 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. For
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 Jacobians of certain families of genus 2 curves [3]. There are also applications of decomposable Jacobians to questions of ranks of elliptic curves which are mentioned at the beginning of the next section.

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. The core of my research focuses on understanding decompositions of Jacobian varieties of higher genus curves.

1 Past Research

Much of my thesis research involved working toward answering the following question.

**Question.** 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 [5] find examples of curves $X$ of many genera up to 1297 with Jacobian $J_X \sim E_1 \times \cdots \times E_g$ where the $E_i$ are elliptic curves but which are not necessarily isogenous.

Answers to this question 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 $\phi : X \to E^t$. If $X$ has a point $P$ over some field $k$ then $\phi$ sends $P$ to $P_1 \times P_2 \times \cdots \times P_t$ 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, I developed a technique to decompose Jacobian varieties of a curve using a result of Kani and Rosen [14] 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 from my thesis 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 [8]. The first number is the order of the group. The dimension is the dimension of the family of curves of that genus with prescribed automorphism group inside the moduli space of all curves of that genus.

What follows is a brief sketch of the ideas of my thesis. 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 $\zeta_n$ will denote a primitive $n$th root of unity and $D_n$ and $C_n$ are the dihedral and cyclic groups of order $n$, respectively.
<table>
<thead>
<tr>
<th>Genus</th>
<th>Group</th>
<th>Dimension</th>
<th>Jacobian</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>$S_4 \times C_2$</td>
<td>0</td>
<td>$J_X \sim E^3$</td>
</tr>
<tr>
<td>4</td>
<td>(72, 40)</td>
<td>0</td>
<td>$J_X \sim E^4$</td>
</tr>
<tr>
<td>5</td>
<td>(160, 234)</td>
<td>0</td>
<td>$J_X \sim E^5$</td>
</tr>
<tr>
<td>6</td>
<td>(72, 15)</td>
<td>0</td>
<td>$J_X \sim E^6$</td>
</tr>
<tr>
<td>7</td>
<td>(32, 43)</td>
<td>1</td>
<td>$J_X \sim E_1^2 \times E_2^2 \times E_3^4$</td>
</tr>
<tr>
<td></td>
<td>$S_3 \times S_3$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>$S_3 \times D_8$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>(32, 18)</td>
<td>1</td>
<td>$J_X \sim E_1^2 \times E_2^2 \times A$</td>
</tr>
<tr>
<td>9</td>
<td>(192, 955)</td>
<td>0</td>
<td>$J_X \sim E_1^3 \times E_2^3$</td>
</tr>
<tr>
<td>10</td>
<td>(72, 40)</td>
<td>1</td>
<td>$J_X \sim E_1^2 \times E_2^2 \times E_3^4$</td>
</tr>
</tbody>
</table>

Table 1: Examples for Bounds on $t$

Given a curve $X$ of genus $g$ over $k$, 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 connecting idempotent relations in $\text{End}_0(J_X) = \text{End}(J_X) \otimes \mathbb{Q}$ to isogenies among images of $J_X$ under endomorphisms. If $\varepsilon_1$ and $\varepsilon_2$ are idempotents in $\text{End}_0(J_X)$ then $\varepsilon_1 \sim \varepsilon_2$ if $\chi(\varepsilon_1) = \chi(\varepsilon_2)$ for all characters $\chi$ in $\text{End}_0(J_X)$.

**Theorem.** (Theorem A, [14]) Let $\varepsilon_1, \ldots, \varepsilon_n, \varepsilon_1', \ldots, \varepsilon_m' \in \text{End}_0(J_X)$ be idempotents. Then the idempotent relation

\[
\varepsilon_1 + \cdots + \varepsilon_n \sim \varepsilon_1' + \cdots + \varepsilon_m'
\]

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

\[
\varepsilon_1(J_X) \times \cdots \times \varepsilon_n(J_X) \sim \varepsilon_1'(J_X) \times \cdots \times \varepsilon_m'(J_X).
\]

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 $\Delta_i$:

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

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

$$J_X \sim \bigoplus_{i,j} e(\pi_{i,j})J_X.$$  \hfill (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 [6] to compute the dimensions of these factors. We first define a representation of $G$.

**Definition.** The Hurwitz representation $V$ of a group $G$ is defined by the action of $G$ on $H_1(X,\mathbb{Z}) \otimes \mathbb{Q}$.

We are interested in the character of this representation which may be computed as follows. Given a map of curves from $X$ to $Y = X/G$ (where $Y$ has genus $g_Y$), branched at $s$ points with monodromy $g_1, \ldots, g_s \in G$, let $\chi(g_i)$ denote the character of $G$ induced from the trivial character of the subgroup of $G$ generated by $g_i$ (observe that $\chi_{(1_G)}$ is the character of the regular representation) and let $\chi_{\text{triv}}$ be the trivial character of $G$. The character of $V$ is defined as

$$\chi_V = 2\chi_{\text{triv}} + 2(g_Y - 1)\chi_{(1_G)} + \sum_i (\chi_{(1_G)} - \chi(g_i)).$$  \hfill (3)

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

$$\dim e(\pi_{i,j})J_X = \frac{1}{2} \dim_{\mathbb{Q}} \pi_{i,j}V = \frac{1}{2} \langle \chi_i, \chi_V \rangle.$$  \hfill (4)

See [6] for more information on the dimension computations.

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 search for sets of elements of the automorphism group which satisfy the monodromy conditions. We compute the Hurwitz character for this group and covering using (3) and finally compute the inner product of the irreducible $\mathbb{Q}$-characters with the Hurwitz character as in (4).

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

**Proposition.** [19] With notation as above, $e(\pi_{i,j_1})J_X \sim e(\pi_{i,j_2})J_X$ for any $1 \leq j_1, j_2 \leq n_i$. 

4
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 $n_\ell$). 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 $\ell$th place), the proposition above implies that the Jacobian variety decomposition consists of $n_\ell$ isogenous elliptic curves.

Maagard, Shaska, Shpectorov, and Völklein [16] 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 [15]. The rest of the results were new and, to my knowledge, 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 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.

Since finishing my thesis (and with a better understanding of some results from representation theory), I have applied the technique above to several families of hyperelliptic curves. Complete listings of automorphism groups and monodromy for hyperelliptic curves may be found in work of Shaska [22]. 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 [22]).

In particular, we find a genus 5 hyperelliptic curve with Jacobian isogenous to $E^5$ which, to my knowledge, is the first example of a hyperelliptic curve of genus 5 with such a decomposition. We also find a genus 8 curve with an improved bound for $t$ from that in Table 1.

A Different Project

During my postdoc I have had the opportunity to collaborate with Bourgain, Cochrane, and Pinner on an unrelated problem in number theory. Given an odd prime $p$, and integers $A$ and $d$ with $(d, p - 1) = 1$ and $p \nmid A$, we want to determine when the map $x \rightarrow Ax^d$ permutes the even residues in $\mathbb{Z}/p\mathbb{Z}$. If $p = 5$ and $A = d = 3$, for instance, then the map does permute the even residues mod $p$. Besides the trivial case where $A = d = 1$, there are five other examples of this for $p \leq 13$. It was first conjectured...
Table 2: Hyperelliptic Jacobian Decompositions

<table>
<thead>
<tr>
<th>Genus</th>
<th>Automorphism Group</th>
<th>Dimension</th>
<th>Jacobian Decomposition</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>$S_4 \times C_2$</td>
<td>0</td>
<td>$E^3$</td>
</tr>
<tr>
<td>4</td>
<td>$SL_2(3)$</td>
<td>0</td>
<td>$E_1^2 \times E_2^2$</td>
</tr>
<tr>
<td>5</td>
<td>$A_4 \times C_2$</td>
<td>1</td>
<td>$A_2 \times E^3$</td>
</tr>
<tr>
<td></td>
<td>$W_2$</td>
<td>0</td>
<td>$E_1^2 \times E_2^3$</td>
</tr>
<tr>
<td></td>
<td>$A_5 \times C_2$</td>
<td>0</td>
<td>$E^5$</td>
</tr>
<tr>
<td>6</td>
<td>$GL_2(3)$</td>
<td>0</td>
<td>$E_1^2 \times E_4^2$</td>
</tr>
<tr>
<td>7</td>
<td>$A_4 \times C_2$</td>
<td>1</td>
<td>$E \times A_3^2$</td>
</tr>
<tr>
<td>8</td>
<td>$SL_2(3)$</td>
<td>1</td>
<td>$A_{2,1}^2 \times A_{2,2}^2$</td>
</tr>
<tr>
<td></td>
<td>$W_3$</td>
<td>0</td>
<td>$A_3^2 \times E^4$</td>
</tr>
<tr>
<td>9</td>
<td>$A_4 \times C_2$</td>
<td>1</td>
<td>$A_3^2 \times E^3$</td>
</tr>
<tr>
<td></td>
<td>$W_2$</td>
<td>0</td>
<td>$E_1^1 \times E_2^2 \times A_3^2$</td>
</tr>
<tr>
<td></td>
<td>$A_5 \times C_2$</td>
<td>0</td>
<td>$E_1^4 \times E_5^2$</td>
</tr>
<tr>
<td>10</td>
<td>$SL_2(3)$</td>
<td>1</td>
<td>$A_2^2 \times A_3^2$</td>
</tr>
</tbody>
</table>

by Goresky and Klapper [11] that for primes greater than 13 the map above does not permute the even residues, except in the trivial case where $A = d = 1$.

This conjecture is motivated by an equivalent conjecture concerning binary $\ell$-sequences based on $p$: sequences $a = \{a_i\}_i$ of zeros and ones with $a_i \equiv (2^{-i} \mod p) \mod 2$. These sequences come from the study of pseudo-random binary sequences with good cross-correlation. The conjecture would produce large families of cyclically distinct sequences with ideal arithmetic cross-correlation. In our work, we prove the following theorem.

**Theorem.** [2] For any prime $p > 2.26 \times 10^{55}$, the map $x \rightarrow Ax^d$ does not permute the even residues mod $p$ unless $A = d = 1$.

An exhaustive computer search of primes less than 2 million has proven the conjecture for these cases as well [12]. The proof of the theorem uses methods of finite Fourier series and bounds for exponential sums. Many more details about this problem and the techniques used to solve it may be found here:

2 Current and Future Research

Broadly, my current research interests 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. A complete understanding of Jacobian decompositions will most probably not come out of that work alone though 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 ranks or the ranks of twists, as in the motivational example in Section 1?

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 [18]. In general however, trying to answer the question in the beginning of Section 1 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 [9] as well as results on $\mathbb{Q}$-curves [3]. Similarly, Pries and Glass answered questions about $p$-torsion in characteristic $p$ by studying the moduli space of curves of a given genus [10].

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 [13] produce genus 3 curves with Jacobians 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 with this property 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 [7] 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 \( x \) (\( \pi(x) \) is the number of primes less than or equal to \( x \)). In genus 1 and 2 they show their bound is sharp. I am 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 genus 1.

III. It is not just the elliptic factors of Jacobian varieties which are interesting. Given a covering of curves \( X \to Y \) then \( J_X \sim J_Y \times P \) 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 \( k \) (the field of definition). The curve \( X \) has automorphism group \( D_{12} \) and let \( Y \) 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 investigate 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 themselves Jacobian varieties of some lower genus curve? In [1] Achter is interested in the following property a curve \( X \) might have: if \( X \to Y \) is a finite cover, then \( Y \) 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. I do not believe this to be true for all curves. If there is some finite cover \( X \to Y \) such that the genus of \( Y \) is greater than 0 then \( J_Y \) will appear as a factor of \( J_X \). So, to find a curve of higher genus which is not simple but has no finite cover \( X \to Y \) (except if the genus of \( Y \) is 0), I will examine when factors of dimension greater than 1 are not themselves Jacobians. These factors are determined by images of \( J_X \) by endomorphisms, recall this from (2).

Even if a factor in \( J_X \) for some curve \( X \) is the Jacobian variety of some curve \( Y \), this does not imply that there is a map from \( X \) to \( Y \). The question of when this map exists is another question I would like to explore in conjunction with the property above.
IV. For a complete picture of the problem of Jacobian decompositions, a more general understanding of which curves have simple Jacobians and which decompose would be important. I am particularly interested in questions involving the endomorphism rings of Jacobian varieties. A corollary to Poincare’s complete reducibility theorem connects the decomposition of $J_X$ to the decomposition of $\text{End}_0(J_X)$ and Mumford [17] gives a classification of the structure of $\text{End}_0(J_X)$ for simple Jacobian varieties $J_X$. As such, a better understanding of the endomorphism ring in non-simple cases could lead to a better understanding of Jacobian decompositions.

References


