Research Statement

Hilary (Smallwood) Freese

1. Introduction

In algebraic geometry one is interested in studying the zero sets of polynomial equations. In number theory one is typically concerned with answering questions over arithmetically interesting fields. As a pair these two subjects form the intersection, arithmetic geometry. Here one studies the zero sets of polynomials over different rings and fields, such as the integers, the rational numbers or finite fields. The problems studied in arithmetic geometry usually have relatively simple statements. My research focuses on counting abelian surfaces that have real multiplication by a particular real quadratic field.

2. Undergraduate Research

As a researcher it is always a pleasure to collaborate with others, and in particular I am looking forward to working with undergraduates on research projects. In number theory many interesting questions can be presented at a very basic level, and can be worked on and explored with only a basic understanding of number theory. Such problems lend themselves well to undergraduates early in their mathematical careers. One class of problems in particular that undergraduates can explore comes from the study of elliptic curves. An elliptic curve can be described by the affine equation $y^2 = p(x)$ where $p(x)$ is a cubic polynomial, and a designated point at infinity. The points (x, y) that satisfy the defining equation of an elliptic curve form a group under a special addition law. Thus, problems about elliptic curves can have ties to group theory, finite fields or number fields, and number theory. Many questions regarding elliptic curves can also be explored computationally since the defining equations can be given explicitly and other properties, such as the addition law, can be explicitly described as well. There are a handful of computer programs, such as Sage and GAP, that allow for such computations to be done in bulk and with ease. The use of such computer systems would also allow for learning and practice of some basic programming skills. One nice application of elliptic curves is to cryptography. Possible research projects here could involve creating new schemes for encoding and sending messages using elliptic curves. Some of the most common elliptic curve cryptosystems in use now are analogues of preexisting cryptosystems.

3. Research Synopsis

My research focuses on two-dimensional abelian varieties, abelian surfaces. These are the higher dimensional analogues of elliptic curves. I take the Lang-Trotter Conjecture, initially a conjecture about elliptic curves, and attempt to formulate a similar conjecture for abelian surfaces. Even if a proof of the conjecture is out of reach, I can adduce evidence in support of it.

3.1. **Motivation: The Elliptic Curve Case.** Given an elliptic curve E one can define a map from E to itself. Such a map is called an endomorphism. Most of the time the ring of endomorphisms of E, denoted $\mathrm{End}(E)$, is the integers. Here each element $[m]$ represents the multiplication by m map, which takes a point P on E to $mP = P + P + ... + P$. However, there are instances where the endomorphism ring is bigger; when this happens E is said to have complex multiplication. As an example, the elliptic curve $E : y^2 = x^3 - x$ has an extra endomorphism that takes $(x, y) \mapsto (-x, iy)$, so $\mathrm{End}(E) \cong \mathbb{Z}[i]$, and E is said to have complex multiplication by $\mathbb{Z}[i]$. In general, let $\mathrm{End}(E)^0 = \mathrm{End}(E) \otimes \mathbb{Q}$.

Over a finite field $\mathbb{F}_q$, every elliptic curve E, admits an extra endomorphism, namely the Frobenius endomorphism $\mathrm{Frob}_q : (x, y) \mapsto (x^q, y^q)$. The action of Frob_q can be represented as a matrix in $\mathrm{GL}(2, \mathbb{Q})$, by looking the action of Frob_q on the torsion points of E. Thus associated to this endomorphism is a characteristic polynomial, specifically the characteristic polynomial of the matrix. This polynomial has the form $f_E(T) = T^2 - a_qT + q$, where $a_q = q + 1 - N_q$, and N_q is the number of points of E defined over $\mathbb{F}_q$. Let π_q be a root of $f_E(T)$. Then $\mathbb{Z}[\pi_q] \subset \mathrm{End}(E)$, and $\mathbb{Q}(\pi_q) \subset \mathrm{End}(E)^0$, and $\mathrm{End}(E)^0$ is either the quadratic imaginary field $\mathbb{Q}(\pi_q)$ or a quaternion algebra.

Now for E defined over $\mathbb{Q}$, consider the reduction $E_p = E \bmod p$ defined over $\mathbb{F}_p$. Then E_p admits a Frobenius endomorphism, Frob_p, with π_p as a root of the corresponding characteristic polynomial $f_{E_p}(T)$. A question one might ask is, for a fixed quadratic imaginary field K, when does $\mathbb{Q}(\pi_p) = K$?

In 1976 Serge Lang and Hale Trotter made the following conjecture [2]

Conjecture 1. *Let E be an elliptic curve defined over $\mathbb{Q}$ without complex multiplication and let K be a given quadratic imaginary field. Define $N_{K,E}(x)$ to be the number of primes $p \leq x$ such that $\mathbb{Q}(\pi_p) = K$. Then there is a constant $C(K, E) > 0$ such that*

$$N_{K,E}(x) \approx C(K, E)\frac{\sqrt{x}}{\log x}.$$

The plausibility of the Lang-Trotter conjecture hinges on the following ideas. First, one can approximate the number of elliptic curves E defined over $\mathbb{F}_p$ with $\mathbb{Q}(\pi_p) = K$ to be on the order of $\sqrt{p}$. Then one might guess that $N_{K,E}(x)$ could be approximated by the sum:

$$\sum_{p \leq x} \text{Prob(random } E/\mathbb{F}_p \text{ has } \mathbb{Q}(\pi_p) = K).$$

From the approximation above Prob(random $E/\mathbb{F}_p$ has $\mathbb{Q}(\pi_p) = K) \approx \dfrac{c\sqrt{p}}{p} = \dfrac{c}{\sqrt{p}}$, since there are approximately p elliptic curves defined over $\mathbb{F}_p$. Thus the sum can be rewritten as

$$\sum_{p \leq x} \frac{c}{\sqrt{p}}.$$

Now rather than sum over only the primes, sum over all integers. In order to do this, use the prime number theorem which informally states, that if a random integer is selected in the range of zero to some large integer x, the probability that the selected integer is prime is about $\dfrac{1}{\ln(x)}$. Thus, $N_{K.E}(x)$ can be approximated as follows:

$$\sum_{n \leq x} \frac{c'}{\sqrt{n}\ln(n)} \approx \int_2^x \frac{c'}{\sqrt{z}\ln(z)} \approx \frac{C\sqrt{x}}{\ln(x)}.$$

While a proof of the Lang-Trotter Conjecture may be inaccessible, it is interesting work to get upper bounds on $N_{K,E}(x)$. Some of the better results have been obtained through the use of various sieve techniques. One such upper bound is given by Cojocaru, Fouvry, and Murty, using a square sieve [1]:

$$N_{K,E}(x) \leq \frac{x(\log(\log(x)))^{13/12}}{(\log(x))^{25/24}}(1 + \#\{p \,:\, p \text{ ramifies in } K\}).$$

Which can be improved to

$$N_{K,E}(x) \leq x^{17/18}\log(x)$$

under a Generalized Riemann Hypothesis.

3.2. **A Generalization to Abelian Surfaces.** Since abelian surfaces are just the higher dimensional analogue of elliptic curves a natural progression would be to pose a similar question regarding the number of abelian surfaces with specified endomorphism ring structure.

The endomorphisms of an abelian surface also form a ring $\text{End}(A)$, and as before define $\text{End}(A)^0 = \text{End}(A) \otimes \mathbb{Q}$. Then if A is simple, $\text{End}(A)^0$ contains a unique, totally real quadratic subfield K, and in this instance we say A has real multiplication by K.

In a manner similar to that of Lang and Trotter we conjecture there is some sort of asymptotic behavior for the number of primes for which an abelian surface A when reduced mod p will have real multiplication by a specified field K.

Conjecture 2. *Let A be an abelian surface defined over $\mathbb{Q}$, with $End_{\mathbb{Q}}(A) \cong \mathbb{Z}$. Consider the reduction $A_p = A \bmod p$. Let K be a given real quadratic field, and define $N_{K,A}(x)$ to be the number of primes $p \leq x$ such that A_p has real multiplication by K. Then there is a constant $C(K,A) > 0$ such that*

$$N_{K,A}(x) \approx C(K,A)\frac{\sqrt{x}}{\log x}.$$

My research aims to give heuristics to justify the claim made in this conjecture and to give an upper bound for $N_{K,A}(x)$. The first part of my research looks at the question regarding the number of principally polarized abelian surfaces defined over $\mathbb{F}_q$ that have real multiplication by a specific real quadratic field K. This allows for a heuristic derivation, as with the Lang-Trotter conjecture, of the probability that a random principally polarized abelian surface defined over $\mathbb{F}_q$ has real multiplication by K. The second part of my research looks at obtaining an upper bound on $N_{K,A}(x)$ and involves the use of a large sieve to do so.

The following theorem summarizes the results of the first part of my research.

Theorem 1. *(H. Smallwood) Suppose that assumption $(\star)$ holds. Fix $d \in \mathbb{Z}_{>0}$, and let X_q be the set of principally polarized abelian surfaces A defined over $\mathbb{F}_q$ such that $K \subset End(A)^0$ for some fixed totally real quadratic field K. Then there exist constants C_1 and C_2 such that*

$$C_1 q^{5/2} \leq \#X_q \leq C_2 q^{5/2}.$$

$(\star)$ The size of an isogeny class can be approximated by the Sato-Tate measure.

The proof of this theorem relies on the following facts about abelian surfaces:

(i) $A/\mathbb{F}_q$ admits a Frobenius endomorphism which can be represented as a matrix in $\mathrm{GSp}_4(\mathbb{Z}_\ell) = \{\gamma \in \mathrm{GL}_4(\mathbb{Z}_\ell) : \gamma^T J \gamma = mJ,\, m \in (\mathbb{Z}_\ell)^\times\}$, where J is some skew-symmetric bilinear form.

(ii) The Frobenius matrix has a characteristic polynomial of the form $f_A(T) = T^4 - aT^3 + bT^2 - aqT + q^2$, with a, $b \in \mathbb{Z}$.

(iii) Two abelian surfaces A and B have the same characteristic polynomial of Frobenius if and only if A and B are isogenous (i.e. there exists a map between A and B which is surjective and has finite kernel) [3].

(iv) The coefficients of $f_A(T)$ determine the real quadratic subfield inside $\mathrm{End}(A)^0$, in the sense that $a^2 - 4b + 8q = \Delta_L$ where Δ_L is the discriminant of the totally real field $L \subset \mathrm{End}(A)^0$.

Armed with these facts, in order to get an approximation for $\#X_q$, one must determine which pairs of coefficients (a, b) permit real multiplication by this particular field K (i.e. which pairs (a, b) are such that $a^2 - 4b + 8q = \Delta_K$). Second, it must be determined how many abelian surfaces correspond to each characteristic polynomial with appropriate coefficients (i.e. what is the size of the isogeny class of principally polarized abelian surfaces corresponding to the characteristic polynomial with coefficients (a, b) that satisfy $a^2 - 4b + 8q = \Delta_K$). These two steps have been done, and the result is Theorem 1. This approximation is then used to say that the probability that a random $A/\mathbb{F}_q$ has real multiplication by K is $\approx \dfrac{Cq^{5/2}}{q^3} = \dfrac{C}{\sqrt{q}}$, since there are approximately q^3 abelian surfaces defined over $\mathbb{F}_q$. From here the arguments follow as with the Lang-Trotter conjecture described above, and thus support the reasonableness of Conjecture 2. Further work to be done here includes computations to explicitly determine the sizes of isogeny classes of abelian surfaces over finite fields, in order to support the Sato-Tate assumption.

The second part of my research focuses on obtaining an upper bound for $N_{K,A}(x)$. Work here begins with the observation that if A_p has real multiplication by K, then for any prime $\ell \neq p$, the action of Frob_p on the ℓ-torsion points of A_p must be compatible with real multiplication by K. Let $g_\ell(T) = f_{A_p}(T) \bmod \ell$, and define $g_\ell^+(T) \in \mathbb{Z}/\ell\,[T]$ to be the real quadratic polynomial associated to $g_\ell(T)$. Then the compatibility can be phrased in this way: if A_p has real multiplication by K, then for each $\ell \neq p$, $g_\ell^+(T)$ factors mod ℓ if and only if K splits at ℓ. Now, for ℓ fixed, $\{\mathrm{Frob}_p : p < x, p \neq \ell\}$, as matrix representations, are equidistributed in $\mathrm{GSp}_4(\mathbb{Z}/\ell)$, provided $x \gg \ell$. Thus for a fixed ℓ, one can expect that a matrix corresponding to Frob_p, for some p, behaves like a random matrix in $\mathrm{GSp}_4(\mathbb{Z}/\ell)$. I have determined that half of the matrices in $\mathrm{GSp}_4(\mathbb{Z}/\ell)$ have real quadratic polynomials which factor mod ℓ. It is also well known that K will split at about half the primes ℓ. Given this local data at ℓ, a sieve will be used over all ℓ to determine an upper bound for $N_{K,A}(x)$.

4. Conclusion

The work I have done in my years as a graduate student at Colorado State University has been both challenging and enjoyable. As I begin a career as a math professional I look forward to collaboration with colleagues on related research, as well as the opportunity to work with undergraduates on research projects about elliptic curves or abelian surfaces.

References

[1] Alina Carmen Cojocaru, Etienne Fouvry, and M. Ram Murty. The square sieve and the Lang-Trotter conjecture. *Canad. J. Math.*, 57(6):1155–1177, 2005.

[2] Serge Lang and Hale Trotter. *Frobenius distributions in* GL_2*-extensions.* Lecture Notes in Mathematics, Vol. 504. Springer-Verlag, Berlin, 1976. Distribution of Frobenius automorphisms in GL_2-extensions of the rational numbers.

[3] John Tate. Endomorphisms of abelian varieties over finite fields. *Invent. Math.*, 2:134–144, 1966.