RESEARCH STATEMENT

KEVIN JAMES

1. Introduction

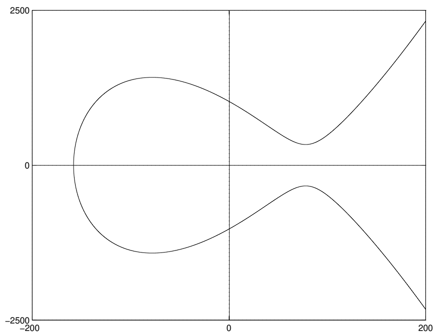
I have been exploring the arithmetic properties of the Fourier coefficients of modular forms of integral and half-integral weight from a theoretical and a computational point of view. My research has been especially focused on problems related to the Birch and Swinnerton-Dyer conjecture, Goldfeld's conjecture and to the Lang–Trotter conjecture. In the remainder of this section, I will introduce some of the basic definitions and terminology from this area. In the second section I will discuss some of my recent work and, in the final section, I will outline some ideas for further research.

Elliptic Curves. One of the fundamental questions of modern number theory is that of understanding Diophantine equations, particularly those of low degree. Linear equations in two variables are not difficult and quadratic equations are now pretty well understood. However, much effort is currently going into understanding degree 3 equations, especially elliptic curves. An elliptic curve can be thought of as the set of all solutions to an equation of the form:

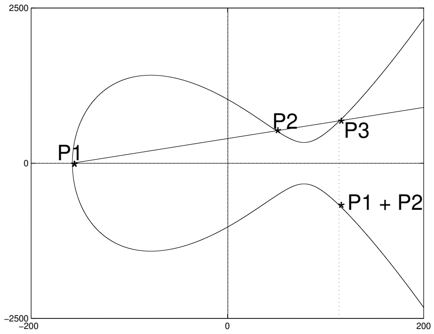
$$y^2 = x^3 + Ax + B. \tag{1}$$

One of the main objectives in the study of elliptic curves is to determine the number of rational solutions to these equations. Without loss of generality, we may assume that A and B are integers. Also, we will assume throughout that our curves have no singularities (ie. that our curves are "smooth" and do not intersect themselves).

If we turn our attention to real solutions, then the graph of a typical elliptic curve will look like:



Let E be an elliptic curve with equation (1). We will denote by $E(\mathbb{Q})$ the set of rational points $\{(x, y) \in \mathbb{Q}^2 : y^2 = x^3 + Ax + B\}$ of E. Given rational points P_1 and P_2 on E, we can draw the secant line passing through P_1 and P_2. It was known to Newton that this line must intersect the curve in exactly three places counting multiplicities, and that since P_1 and P_2 are rational the third point of intersection P_3 must also be a rational point on the curve.



Poincaré discovered that by defining $P_1 + P_2$ to be the reflection through the x-axis of the point P_3 mentioned above, the set of rational points on an elliptic curve forms an Abelian group with the identity being the point at infinity. It was later proven by Mordell that this group is finitely generated. Thus, we know that

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tor}} \oplus \mathbb{Z}^r, \tag{2}$$

where $E(\mathbb{Q})_{\text{tor}}$ denotes the torsion subgroup of $E(\mathbb{Q})$. There is now a complete characterization of the possible torsion groups given by Mazur, the largest of these groups having order 16. Thus the interesting question becomes that of determining the number r from (2). This number is referred to as the rank of E.

One surprisingly powerful way of studying the rank of elliptic curves is to study their associated L-functions. The L-function of an elliptic curve E is defined as follows. For each prime p let $N(p)$ denote the number of solutions to (1) modulo p. Put $a_p = p - N(p)$. Then we define

$$L(E, s) = \prod_{p \text{ prime, } p \mid \Delta} \frac{1}{1 - a_p p^{-s}} \prod_{p \text{ prime, } p \nmid \Delta} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}, \tag{3}$$

where Δ is the minimal discriminant of E (Δ is a certain divisor of $4A^3 + 27B^2$). The above Euler product can be shown to converge for $Re(s) > 2$. If E is a *modular* curve, then there is a function, generally known as the *analytic continuation* of $L(E, s)$, defined on the whole complex plane which agrees with $L(E, s)$ when $Re(s) > 2$ and which is an entire function. In fact, it is believed that all curves are modular. Indeed Wiles has proved this for a positive proportion of elliptic curves. We will assume throughout the rest of the discussion that all of our elliptic curves are modular. We can therefore think of $L(E, s)$ as being defined on the whole complex plane. Now, the Birch and Swinnerton-Dyer conjecture says that the rank of E should be equal to the order of vanishing of $L(E, s)$ at $s = 1$. In fact it is known that if $L(E, 1) \neq 0$ then the rank of E is zero, that is E has only a finite number of rational points.

One ancient problem that can be better understood through the theory of elliptic curves is the so called congruent number problem. A natural number n is said to be *congruent* if it is the area of a right triangle with rational side lengths. The congruent number problem is to determine which natural numbers are congruent. Since scaling the sides of a triangle by a factor of s changes the area of the triangle by a factor of s^2, we can restrict our attention to the square-free natural numbers, that is natural numbers which have no prime dividing them to a higher power than 1. It turns out that a square-free natural number n is congruent if and only if the elliptic curve with equation

$$E_n : y^2 = x^3 - n^2 x \tag{4}$$

has infinitely many points. In [12], Tunnell gives an unconditional criterion for determining that certain numbers are not congruent, and conjecturally his criterion completely characterizes congruent numbers.

The curves E_n given in (4) make up what is known as a family of quadratic twists. Given an elliptic curve with an equation as in (1), we say that the curve $E_n : y^2 = x^3 + An^2x + Bn^3$ is the n-th quadratic twist of E. As n varies over all square-free integers it is natural to wonder how often $E_n(\mathbb{Q})$ has rank zero. It is conjectured that for a positive proportion of the square-free integers n the rank of E_n should be zero. This is a consequence of Goldfeld's conjecture (see [Go]) for the L-series of modular forms.

Two other important groups which are associated to elliptic curves are the so called Selmer and Tate-Shafarevic groups. These groups arise from attempts to understand the failure of the local-global principle for elliptic curves. In the quadratic case, one can determine the existence of solutions to an equation by examining that equation modulo finitely many prime powers. Indeed, if a binary quadratic form has real solutions and has solutions modulo powers of p for all primes p dividing its discriminant then it has rational solutions. Elliptic curves do not enjoy this same local-global principle. In fact, there are elliptic curves with equations which have solutions over the reals and modulo every prime power and yet which have no rational solutions. The Selmer group of an elliptic curve E is constructed completely from local information and can be thought of as measuring the number of local solutions to the minimal equation for E (-ie. solutions modulo prime powers). The Tate-Shafarevic group of E measures the failure of the local-global principle for E in the following sense. If $S(E)_p$ and $\text{Ш}(E)[p]$ denote the subgroup of elements of order p in the Selmer and Tate-Shafarevic groups respectively, then we have the following exact sequence.

$$1 \to E(\mathbb{Q})/pE(\mathbb{Q}) \to S(E)_p \to \text{Ш}(E)[p] \to 1 \tag{5}$$

Thus, the rank of $\text{Ш}(E)[p]$ is equal to the rank of $S(E)_p$ (the local solutions) minus the rank of $E(\mathbb{Q})$ (the global solutions). In particular, the local global principle holds for E if and only if the Tate-Shafarevic group is trivial.

As for $E(\mathbb{Q})$, it is quite natural to study the behavior of these mysterious groups in families of quadratic twists. For instance, there has been some interest in the behavior of the size of these groups in families of quadratic twists of elliptic curves. Since $S(E)$ and $\text{Ш}(E)$ are groups it is natural to ponder not only their size but also their structure as well. For instance, computational studies suggest that the proportion of the natural numbers n for which $\text{Ш}(E_n)$ is or is not divisible by a given prime p should be positive. For example, let E_n be defined as in (4) and let $\delta(p, X)$ denote the proportion of square-free integers $1 \leq n \leq X$ for which p does not divide $\text{Ш}(E_n)$ and for which $L(E_n, 1) \neq 0$. Using the work of [12] and assuming the Birch and Swinnerton-Dyer conjecture, I was able to compute the following table.

X	$\delta(3, X)$	$\delta(5, X)$	$\delta(7, X)$	$\delta(11, X)$
1,000,000	0.32530	0.39535	0.42117	0.44022
5,000,000	0.32397	0.39543	0.42317	0.44420
10,000,000	0.32286	0.39556	0.42353	0.44542
15,000,000	0.32212	0.39567	0.42377	0.44617
20,000,000	0.32193	0.39564	0.42401	0.44672
25,000,000	0.32183	0.39565	0.42415	0.44710
30,000,000	0.32178	0.39573	0.42426	0.44740

Although, the above data is quite compelling, a proof that $\liminf_{X\to\infty} \delta(p, X) > 0$ still seems far away. Thus, we are still far from understanding the behavior of these groups in families of twists.

Modular Forms Many of the problems discussed above can be studied from the point of view of modular forms. In fact, much of my own work is phrased much more naturally in the language of modular forms. So, we will now turn our attention to describing some of the theory of modular forms.

The definition of a modular form is a little hard to take in at first glance. So, we postpone giving the definition for a couple of paragraphs. One of the main reasons that modular forms have been studied extensively over the past several years is to determine special values of their associated L-series. These values often contain arithmetic information. For example, we saw in section 1 that given an elliptic curve E, we can form its L-series $L(E, s)$. In the case that E is a *modular* curve we saw that conjecturally the behavior of $L(E, s)$ near $s = 1$ tells us about the rank of E. Saying that an elliptic curve is *modular* means that there is a modular form F whose associated L-series is $L(E, s)$. The fact that $L(E, s)$ is the L-series of a modular form is what guarantees the existence of the analytic continuation of $L(E, s)$ mentioned in section 1. Since we now know that many elliptic curves are modular, we can gain a great deal of arithmetic information by studying the L-series attached to modular forms.

A modular form F is a function on the upper complex half plane $\mathfrak{h}$, which transforms nicely under a finite index subgroup of the linear fractional transformations of $\mathfrak{h}$; that is there exists a formula which relates f's value at $\tau \in \mathfrak{h}$ to its value at $\frac{a\tau+b}{c\tau+d}$ for certain $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$. Also, modular forms are assumed to be holomorphic on $\mathfrak{h}$ and to behave nicely as τ approaches infinity or any rational number. These forms behave so nicely that it is a little surprising that any actually exist!

More precisely denote by $\Gamma_0(N)$ the set of 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ such that N divides c.

Definition 1.1. *Let k and N be positive integers, and let χ be a Dirichlet character modulo N. Letting $\mathfrak{h}$ denote the upper half complex plane, $\{\tau \in \mathbb{C} : Im(\tau) > 0\}$, we say that a function $F : \mathfrak{h} \to \mathbb{C}$ is a* modular form *of weight k, level N and character χ if it satisfies the following conditions*

1: *$F(\frac{a\tau+b}{c\tau+d}) = \chi(d)(c\tau + d)^k F(\tau)$, for all $\tau \in \mathfrak{h}$ and all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$.*

2: *F is holomorphic on $\mathfrak{h}/\Gamma_0(N)$.*

If in addition to the above conditions F also vanishes at the cusps of $\Gamma_0(N)$ then F is said to be a cusp form. *Denote the space of modular forms of weight k, level N and character χ and its subspace of cusp forms by $M_k(N, \chi)$ and $S_k(N, \chi)$ respectively. If the character χ is trivial then simply write $M_k(N)$ and $S_k(N)$.*

Note that by condition 1 above, $F(\tau + 1) = F(\tau)$, and hence F has a Fourier expansion of the form $F(\tau) = \sum_{n\geq 0} a_n q^n$, where $q = e^{2\pi i\tau}$. If F is a cusp form then $a_0 = 0$.

To any cusp form $F(\tau) = \sum_{n\geq 1} a_n q^n \in S_k(N, \chi)$, we can associate the L-series $L(F, s) = \sum_{n\geq 1} \frac{a_n}{n^s}$ which converges for $Re(s) > k/2 + 1$. One can show the existence of an entire function on the whole complex plane which is given by $L(F, s)$ for all s with $Re(s) > k/2+1$. Thus we can extend $L(F, s)$ to the whole complex plane. Also, there is a functional equation relating the value of $L(F, s)$ to the value of $L(F, k - s)$. So the values of $L(F, s)$ are particularly interesting when $k/2 - 1 \leq Re(s) \leq k/2 + 1$. We will be interested in the value of $L(F, s)$ at $s = k/2$ which is referred to as the central critical value.

Given a cusp form $F(\tau) = \sum_{n\geq 1} a_n q^n \in S_k(N,\chi)$ and a Dirichlet character ψ modulo M, define the *twist* of F by ψ to be $F_\psi(\tau) = \sum_{n\geq 1} a_n\psi(n)q^n$. Then $F_\psi \in S_k(NM^2, \chi\psi^2)$. We will be particularly interested in "quadratic twists" of cusp forms. that is twists by quadratic Dirichlet characters. Given any square-free integer t, denote by χ_t the Dirichlet character associated to the extension $\mathbb{Q}(\sqrt{t})/\mathbb{Q}$, that is $\chi_t(n) = (\frac{\Delta}{n})$, where Δ is the discriminant of $\mathbb{Q}(\sqrt{t})/\mathbb{Q}$ and $(\frac{D}{n})$ is the Kronecker-Legendre symbol. In fact, the notion of twisting for modular forms is related to the notion of twisting for elliptic curves. If E is a modular elliptic curve and F is the modular form associated to E then F_{χ_n} is the modular form associated to E_n. For a given cusp form F of weight k, it has been conjectured by Goldfeld [Go] that $L(F_{\chi_t}, k/2) \neq 0$ for precisely half of the square-free integers t and that $L(F_{\chi_t}, k/2) = 0$ for half of the positive square-free integers t.

2. Results

In order to describe some of my results, it will be convenient to use the following notation. We will write $f(x) >> g(x)$ if there exist some positive constant C and some lower bound B such that for all $x > B$, $f(x) > Cg(x)$. Also, the notation $f(x) \sim g(x)$ will mean that $\lim_{x\to\infty} f(x)/g(x) = 1$.

I have been successful in proving some results towards Goldfeld's conjecture (see [6, 1, 8]). More precisely, I was able to prove for elliptic curves E possessing rational points of order 3 and satisfying an additional rather technical hypothesis that

$$\#\{0 < D < X : L(E(-D), 1) \neq 0\} >> X.$$

To my knowledge, these were the first positive density results for the non-vanishing of modular L-series in families of quadratic twists and thus a significant step toward Goldfeld's conjecture. I list below for several such curves E, a Weierstrass equation for E, the conductor $N(E)$ of E, and a lower bound δ_E on the lower density of square-free natural numbers D such that $L(E_{-D}, 1) \neq 0$

E	N_E	δ_E
$y^2 = x^3 + 8$	576	1/4
$y^2 = x^3 + x^2 + 72x - 368$	14	7/64
$y^2 = x^3 + 1$	36	5/24
$y^2 = x^3 + 4x^2 - 144x - 944$	19	19/240
$y^2 = x^3 + x^2 + 4x + 4$	20	5/72
$y^2 = x^3 + x^2 - 72x - 496$	26	13/112
$y^2 = x^3 + x^2 + 24x + 144$	30	5/128
$y^2 = x^3 + x^2 - 48x + 64$	34	17/144
$y^2 = x^3 + x^2 + 3x - 1$	44	11/144
$y^2 = x^3 + 5x^2 - 200x - 14000$	50	5/24

For the curves mentioned in the previous result satisfying one additional hypothesis, I have also been able to prove (see [7]) that the following weak form of the Birch and Swinnerton-Dyer conjecture holds for a positive density of their quadratic twists E_n:

$$\frac{L(E_n,1)}{\Omega_{E_n}} \#E_n(\mathbb{Q})^2_{\mathrm{tor}} \equiv \#\text{Ш}(E_n) \prod_p c_p(E_n) \pmod 3, \tag{6}$$

where $L(E_n, s)$, Ω_{E_n}, $\text{Ш}(E_n)$ and $c_p(E_n)$ denote the L-series, real period, Tate-Shafarevic group and local Tamagawa factors of E_n respectively. It would be cumbersome to define Ω and the c_p's here but, suffice it to say that each of these can be computed simultaneously for each curve in a family of twists fairly quickly using an adaptation of an algorithm of Tate.

K. Ono and I have conducted investigations into the behavior of the Tate-Shafarevic groups in families of quadratic twists of Elliptic curves. We were able to prove the following general theorem.

Theorem 2.1. *(James–Ono [J-O]) If $E/\mathbb{Q}$ is a modular elliptic curve, then for every sufficiently large prime ℓ we have*

$$\#\{|D| < X \quad : \; D \text{ square-free and } Ш(E(D))[\ell] = \{1\}\} \gg_{E,\ell} \frac{\sqrt{X}}{\log X}.$$

Moreover, for all such D the rank of $E(D)$ is zero and thus $\S(E)_\ell$ is also trivial.

This theorem is still very far from the truth. However, it is the first unconditional result for a general modular curve of its kind. Previously, Kohnen and Ono had shown a similar result for elliptic curves with complex multiplication but all of the results of this kind for general modular curves were much weaker and depended on the truth of the Birch and Swinnerton-Dyer conjecture.

Along with K. Ono and D. Farmer I have also been exploring the characteristic polynomials of Hecke operators on a spaces of modular forms. More precisely, there is an algebra of self-adjoint commuting linear operators $\{T_n\}_{n\in\mathbb{N}}$ defined on each space of modular forms. These operators are called Hecke operators and there has been much interest in the literature in the characteristic polynomials of these operators. We will denote by $T_n(X)$ the characteristic polynomial of T_n. One amazing conjecture is that if we restrict our attention to the case of cusp forms of level one, then for any weight k and for any $n \in \mathbb{N}$, $T_n(X)$ is irreducible and has full Galois group (-ie the Galois group is S_d where d is the degree of $T_n(X)$).

In [11], K. Ono and I were able to prove a theorem which essentially says that if we fix a space of modular forms and primes p and ℓ then for a positive proportion of the primes q the characteristic polynomial of T_q is the same modulo ℓ as the one for T_p. In particular, if we specialize to the case of cusp forms of weight one, this says that if there exists one prime p for which $T_p(X)$ is irreducible modulo ℓ then for a positive proportion of the primes q, $T_q(X)$ is also irreducible.

More recently in [3], D. Farmer and I were able to extend this result in the case of level one cusp forms to the following theorem.

Theorem 2.2. *For every $k <= 2000$ for which the space S_k of cusp forms of level one and weight k is non-trivial, there exists a set of primes p consisting of at least $5/6$ of all of the primes and containing all primes less than 2000 such that the characteristic polynomial of T_p acting on S_k is irreducible and has full Galois group.*

Another problem of interest lately has been the Lang-Trotter conjecture and its generalization to modular forms. Given, an elliptic curve E and letting $a_p = p + 1 - \#E(\mathbb{F}_p)$, the Lang-Trotter conjecture predicts for any integer n the number of primes p up to X for which $a_p = n$. For example it predicts for any elliptic curve E that $\#\{p < X | a_p = 0\} \sim C_0(E)\sqrt{x}/\log x$, where $C_0(E)$ is an explicit constant depending only on E. This conjecture has been proved in an average sense by the works of Fouvry and Murty [4] and of David and Pappalardi [2]. Recently, K. Murty and I have been conducting extensive investigations into the generalizations of the Lang and Trotter conjecture from both a numerical and statistical point of view (see [J-M]). It is interesting to note that for certain elliptic curves our computed constant differs significantly from the one predicted by Lang and Trotter. So, even though the conjecture holds on average, it seems that for individual curves, it may not be true. This work is still in progress but I have included a very preliminary preprint of our work thus far (see [9]).

3. Further Research

I am planning to continue to explore the connections between modular forms and arithmetic geometry. In particular, I hope to better understand the structure of Tate–Shafarevic groups of elliptic curves and the distribution of the coefficients of modular forms of integral and half–integral weight. I plan to proceed with both numerical and theoretical investigations into these matters.

As stated in the previous section, K. Ono and I had some success in answering the question of how often Tate-Shafarevic groups of twists of elliptic curves are not divisible by a given prime. Next, I plan to attack the complementary question of divisibility of these groups.

I will conduct further investigations related to the Lang-Trotter conjecture in the following three directions. First, I would like to extend the conjecture to the case of half-integral weight forms, especially forms of weight 3/2. A better understanding of the behavior of the distribution of the Fourier coefficients of these forms would have a direct impact on our understanding of Tate-Shafarevic groups of quadratic twists of elliptic curves. Secondly, I plan to establish average Lang-Trotter type results for families of elliptic curves with prescribed torsion subgroups. Such results should shed some light on the discrepancies between the predictions of Lang and Trotter and the computational observations made by K. Murty and myself in [9]. Thirdly, I would like to investigate the extensions of this conjecture to modular forms of weight 3. All of the research on these conjectures, to my knowledge has been directed to the case of weight 2 forms. Cusp forms of weight 3 are related to the arithmetic of K3 surfaces which should allow one to establish average results analogous to those in [4, 2] at the very least.

An additional problem of interest, is to develop a better understanding of the behavior of the characteristic polynomials of the Hecke operators acting on spaces of modular forms. Such studies may lead to better upper bounds for the number of elliptic curves of a given conductor and perhaps shed light on a conjecture of Maeda concerning the irreducibility of the characteristic polynomials of the Hecke operators of level one.

References

[1] J. Bruinier, K. James, W. Kohnen, K. Ono, C. Skinner and V. Vatsal, *Central critical values of quadratic twists of modular L-functions and some applications*, in: Proceedings of Topics in Number Theory [Editors: G. Andrews, K. Ono], Kluer Acad. Publ., (1999) 115–125.

[2] C. David and F. Pappalardi, *Average Frobenius distributions of elliptic curves*, Internat. Math. Res. Notices (1999) no. 4, 165–183.

[3] D. Farmer and K. James, *On the irreducibility of Hecke polynomials of level one*, (preprint).

[4] E. Fouvry and M. R. Murty, *On the distribution of supersingular primes*, Canadian J. math. **48** (1996) 81–104.

[5] D. Goldfeld, *Conjectures on elliptic curves over quadratic fields*, Springer Lect. Notes **751** (1979), 108–118.

[6] K. James, *L-series with non-zero central critical value*, J. Amer. Math. Soc. **11** (1998), 635–641.

[7] *Elliptic curves satisfying the Birch and Swinnerton-Dyer conjecture mod 3*, J. Number Theory vol 76, (1999) 16–21.

[8] *An example of an elliptic curve with a positive density of prime quadratic twists which have rank zero*, in: Proceedings of Topics in Number Theory [Editors: G. Andrews, K. Ono], Kluer Acad. Publ. (1999) 223–227.

[9] K. James and K. Murty *Frobenius distributions and Galois representations – numerical evidence.*, (preprint).

[10] K. James and K. Ono, *Selmer groups of quadratic twists of elliptic curves*, Math. Ann. **314** (1999) 1–17.

[11] K. James and K. Ono, *On the irreducibility of Hecke Polynomails*, J. Number Theory vol. 73, (1998) pp. 527–532.

[12] J.B. Tunnell, *A classical Diophantine problem and modular forms of weight 3/2*, Invent. Math. **72** (1983) 323–334.