RESEARCH SUMMARY

Past Research Overview

Introduction. For over a hundred years number theory has been motivated by the study of L-series, as first introduced by P. G. Lejeune Dirichlet [13] in the study of primes in arithmetic progressions then generalized by Emil Artin [1] in his study of representations of finite Galois groups. In the 1930's, Artin conjectured that L-series associated to suitable types of Galois representations should have both an analytic continuation to the entire complex plane and a functional equation. While he was ultimately able to prove that the latter is always true, he conjectured the validity of the former.

In the past 40 years, there has been signifnicant progress made towards the validity of this conjecture. Robert Langlands [42] showed in the 1970's that in order to prove Artin's conjecture it suffices to somehow associate automorphic forms with the given representation. In fact, Langlands, along with a slight generalization by Jerrold Tunnell [48], was able to show in the 1980's that 2-dimensional representations of Galois groups with projective image isomorphic to either $A_4 \simeq PSL_2(\mathbb{F}_3)$ or $S_4 \simeq PGL_2(\mathbb{F}_3)$ do indeed satisfy Artin's conjecture.

In the past 15 years, the conjecture has taken on a "geometric" approach. Andrew Wiles [49], introduced elliptic curves into the picture in the 1990's by studying their 3-torsion in his celebrated proof of Fermat's Last Theorem. The basic idea was to relate their mod 3 representations with Galois representations into $PGL_2(\mathbb{F}_3)$. Soon thereafter Richard Taylor [7] expanded upon this idea by relating 5-torsion of elliptic curves with Galois representations into $A_5 \simeq PSL_2(\mathbb{F}_5)$. His approach to the icosahedral case of Artin's conjecture followed a program which used both geometric and analytic aspects: first associate the given Galois representation to the 5-torsion of some elliptic curve, then prove that the elliptic curve is associated to a modular form, and finally use the theory of deformations to conclude that the original Galois representation has analytic continuation.

Specific Goals. My research concerns this interplay of Galois representations, elliptic curves, and modular forms. I have spent some time studying the next two generalizations of Galois representations by considering $PSL_2(\mathbb{F}_\ell)$ for $\ell = 5$ and $\ell = 7$. My work has centered on two key questions in these cases.

> **Geometric Problem:** Given a polynomial with Galois group $PSL_2(\mathbb{F}_\ell)$ for $\ell =$ 5, 7, under what conditions can one find an elliptic curve such that the splitting field is associated to the ℓ-torsion of the curve?
>
> **Analytic Problem:** Given an elliptic curve over $\mathbb{Q}(\sqrt{(-1)^{(\ell-1)/2}\,\ell})$ with absolutely irreducible mod ℓ representation for $\ell = 5$, 7 can one construct explicit examples of Galois representations which satisfy Artin's conjecture?

The first problem requires an analysis of the formulas introduced in Klein [41] and [40]; I have considered these cases myself in my thesis [22], and later in [25] and [28]. The second problem is considerably more difficult, as the only such papers which use this approach seem to be the article by Taylor et al. [7] and as well as the work of Chandrashekhar Khare and Jean-Pierre Wintenberger [39] regarding Serre's conjecture.

Geometric Problem. We explain the relationship between $PSL_2(\mathbb{F}_\ell)$ and elliptic curves. Fix a complex vector space $V \simeq \mathbb{C}^n$, and consider a continuous homomorphism

$$\rho: \quad \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \longrightarrow GL(V).$$

We define the L-series associated to ρ as the complex analytic function

$$L(\rho, s) = \prod_p \det\left[1 - \left(\rho|_{V^{I_p}}\right)(\mathrm{Frob}_p) \cdot p^{-s}\right]^{-1}, \qquad \Re(s) > 1;$$

as the product over all rational primes p, where V^{I_p} denotes the subspace of V invariant under action by the inertia group I_p. When the vector space V is 1-dimensional and ρ is the trivial representation then $L(\rho, s) = \zeta(s)$ is the Riemann zeta function; it is well-known that this function has a pole at $s = 1$. It is conjectured that when ρ does not contain the trivial representation (i.e., V has no invariant subspaces where ρ acts trivially), the L-series has analytic continuation to the entire complex plane. The conjecture is known to be true when $\dim_{\mathbb{C}} V = 1$, so we consider irreducible vector spaces V with $\dim_{\mathbb{C}} V > 1$.

Some of these complex representations ρ have been classified. Denote $\widetilde{\rho}$ as the projective representation associated to ρ, i.e., the composition with the map which considers linear transformations modulo scalar multiplication. The continuity of such a representation means there exists a finite Galois extension K of $\mathbb{Q}$ which makes the following exact diagram commutative:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathrm{Gal}\left(\overline{\mathbb{Q}}/K\right) & \longrightarrow & \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) & \longrightarrow & \mathrm{Gal}\left(K/\mathbb{Q}\right) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow \rho & & \downarrow \widetilde{\rho} & & \\
1 & \longrightarrow & \mathbb{C}^{\times} & \longrightarrow & GL(V) & \longrightarrow & PGL(V) & \longrightarrow & 1
\end{array}$$

We identify the finite group $\mathrm{Gal}(K/\mathbb{Q})$ with the image of the projective complex representation $\widetilde{\rho}$. When $\dim_{\mathbb{C}} V = 2$ such images fall into one of five classes: it is either cyclic, dihedral, tetrahedral (i.e., $A_4 \simeq PSL_2(\mathbb{F}_3)$), octahedral (i.e., $S_4 \simeq PGL_2(\mathbb{F}_3)$), or icosahedral (i.e., $A_5 \simeq PSL_2(\mathbb{F}_5)$). When $\dim_{\mathbb{C}} V = 3$ such image may be heptaoctahedral (i.e., $G_{168} \simeq SL_3(\mathbb{F}_2) \simeq PSL_2(\mathbb{F}_7)$), although others are possible. Depending on the image of $\widetilde{\rho}$ as above, we call a 2-dimensional representation ρ cyclic, dihedral, tetrahedral, octahedral, or icosahedral; and a 3-dimensional representation heptaoctahedral. This conjecture is known to be true when ρ is either cyclic, dihedral, tetrahedral, or octahedral; but when I began my research in this area it was not known when ρ is either icosahedral or heptaoctahedral.

There are canonical ways to exhibit icosahedral and heptaoctahedral representations using elliptic curves. For $\ell = 5, 7$ there exist faithful group representations $\pi_\ell : \overline{\mathbb{F}}_\ell^{\times} \cdot SL_2(\mathbb{F}_\ell) \to GL_n(\mathbb{C})$ of dimension $n = (\ell - 1)/2$, so given an elliptic curve E over $\mathbb{Q}(\sqrt{(-1)^{(\ell-1)/2}\ell})$, the mod ℓ representation yields the continuous homomorphism

$$\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}(\sqrt{(-1)^n \ell})\right) \xrightarrow{\overline{\rho}_{E,\ell}} \overline{\mathbb{F}}_\ell^{\times} \cdot SL_2(\mathbb{F}_\ell) \xrightarrow{\pi_\ell} GL_n(\mathbb{C}).$$

Unfortunately, this complex Galois representation is defined over $\mathbb{Q}(\sqrt{(-1)^{(\ell-1)/2}\ell})$, not $\mathbb{Q}$. If E were a $\mathbb{Q}$-curve, then such a composition would be the twist of the restriction of a representation $\rho_E : \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \to GL_n(\mathbb{C})$. Moreover, if the mod ℓ representation $\overline{\rho}_{E,\ell}$ is absolutely irreducible then the complex representation ρ_E is either icosahedral or heptaoctahedral. The extension K_E associated with the projective representation $\widetilde{\rho}_E$ is contained in the field generated by the ℓ-torsion of the elliptic curve, i.e., $K_E \subseteq \mathbb{Q}(E[\ell])$. My work concerns studying those icosahedral and heptaoctahedral representations which arise this way.

Geometric Problem for Icosahedral Representations. Consider an icosahedral representation ρ, and denote the extension K as above such that $\mathrm{Gal}(K/\mathbb{Q}) \simeq PSL_2(\mathbb{F}_5)$. This extension must necessarily be the splitting field of a degree five polynomial defined over $\mathbb{Q}$. In 1786, Erland Bring (and independently in 1834, George Jerrard) showed that over some extension F of $\mathbb{Q}$ this quintic can be chosen to be of the form $x^5 + a\,x + b$. In 2003 [25], I showed that there exists a $\mathbb{Q}$-curve E defined over $\mathbb{Q}(\sqrt{5})$ such that $K = K_E$ whenever K is the splitting field of $x^5 + a\,x + b$

over $\mathbb{Q}$. In my doctoral thesis [22], I showed that whenever K is not totally real and there exists a totally real extension F such that (1) $[F:\mathbb{Q}]$ divides 6 and (2) $K\,F$ is the splitting field of $x^5+a\,x+b$ over F, then there exists a elliptic curve E defined over $F(\sqrt{5})$ such that (1) E is isogeneous to its $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$-conjugates, (2) $K\,F=K_E$, and (3) $\mathrm{Gal}\,(K\,F/F)\simeq PSL_2(\mathbb{F}_5)$. If K is not totally real, we say ρ is an odd representation. A goal of mine is to prove that such a field F always exists, thereby showing that every odd icosahedral representation is "geometric," i.e., may be associated with the 5-torsion of an elliptic curve defined over a totally real number field F.

Geometric Problem for Heptaoctahedral Representations. Consider a heptaoctahedral representation ρ, and denote K as above such that $\mathrm{Gal}(K/\mathbb{Q})\simeq PSL_2(\mathbb{F}_7)$. This extension must necessarily be the splitting field of a degree seven polynomial defined over $\mathbb{Q}$. Unfortunately, there is no "canonical" form which generalizes the Bring-Jerrard form for degree five polynomials, so it is unclear to me which is the correct family of polynomials to associate to an elliptic curve. A family of degree seven polynomials over $\mathbb{Q}$ has been shown to have Galois group $PSL_2(\mathbb{F}_7)$: the polynomials $x^7+d\,x+e$ were originally studied by Erbach, Fisher, and McKay [15]. However, I have been able to show that there is a considerably larger family once one considers polynomials over $\mathbb{Q}(\sqrt{-7})$: Let E be a $\mathbb{Q}$-curve over $\mathbb{Q}(\sqrt{-7})$ with invariant j, and fix $m,\,n\in\mathbb{Q}(\sqrt{-7})$. In [28], I show that $K_E(\sqrt{-7})$ is the splitting field of $x^7+a_{m,n,j}\,x^4+b_{m,n,j}\,x^3+c_{m,n,j}\,x^2+d_{m,n,j}\,x+e_{m,n,j}$ over $\mathbb{Q}(\sqrt{-7})$, where

$$
\begin{aligned}
a_{m,n,j} &= -\frac{7}{j}\left[\epsilon\,m^3+\frac{72\,m\,n^2+(2-\epsilon)\,n^3}{1728-j}\right]\\
b_{m,n,j} &= -\frac{7}{j}\left[\frac{-9\,(1+\epsilon)\,m^2\,n^2-m\,n^3}{1728-j}+\frac{(-54+81\,\epsilon)\,n^4}{(1728-j)^2}\right]\\
c_{m,n,j} &= -\frac{7}{j}\left[\frac{-2\,m^3\,n^2}{1728-j}+\frac{(36+9\,\epsilon)\,m\,n^4-\epsilon\,n^5}{(1728-j)^2}\right]\\
d_{m,n,j} &= -\frac{7}{j^2}\left[(-6+5\,\epsilon)\,m^6-16\,m^5\,n\right.\\
&\quad+\frac{-720\,(4+5\,\epsilon)\,m^4\,n^2-10\,(50+43\,\epsilon)\,m^3\,n^3-80\,\epsilon\,m^2\,n^4}{1728-j}\\
&\quad\left.+\frac{25920\,(-5+4\,\epsilon)\,m^2\,n^4+144\,(-26+5\,\epsilon)\,m\,n^5+5\,(14+37\,\epsilon)\,n^6}{(1728-j)^2}\right]\\
e_{m,n,j} &= -\frac{1}{j^2}\left[-12\,m^7+\frac{-126\,(7+12\,\epsilon)\,m^5\,n^2-119\,\epsilon\,m^4\,n^3}{1728-j}\right.\\
&\quad+\frac{189\,(570+167\,\epsilon)\,m^3\,n^4+1638\,(6+\epsilon)\,m^2\,n^5+7\,(50+41\,\epsilon)\,m\,n^6-12\,n^7}{(1728-j)^2}\\
&\quad\left.+\frac{95256\,(2-3\,\epsilon)\,m\,n^6-1323\,(2+11\,\epsilon)\,n^7}{(1728-j)^3}\right]
\end{aligned}
$$

in terms of $\epsilon=\frac{-1+\sqrt{-7}}{2}$. These formulas are a bit cumbersome, so consider the special case where K is the splitting field of $x^7+d\,x+e$ over $\mathbb{Q}$. I conjecture that there exists a $\mathbb{Q}$-curve E defined over $\mathbb{Q}(\sqrt{-7})$ such that $K=K_E$. The first degree seven polynomial ever known to have Galois group $PSL_2(\mathbb{F}_7)$ was the so-called Trinks polynomial $x^7-7\,x+3$. My goal, at the very least, is to show that it may be associated with the 7-torsion of some elliptic curve.

Analytic Problem. We explain the relationship with Artin's conjecture and modular forms. Given a modular form $f(\tau)=\sum_{n=1}^{\infty}a_n\,e^{2\pi i n\tau}$ we define the analytic function $L(f,s)=\sum_{n=1}^{\infty}a_n/n^s$

for $\Re(s) > 1$ as the L-series associated to f. It is well-known that there is a representation

$$\rho_f : \quad \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \longrightarrow GL(V)$$

for some ℓ-adic vector space $V \simeq \overline{\mathbb{Q}}_\ell^{\,2}$ such that $\operatorname{tr}\rho_f(\mathrm{Frob}_p) = a_p$ for almost all primes p. We say a 2-dimensional representation ρ is modular if there exists a modular form such that $\rho \simeq \rho_f$, i.e., $\operatorname{tr}\rho(\mathrm{Frob}_p) = a_p$ for almost all primes p. It is well-known that if ρ is modular then it satisfies Artin's conjecture. This motivates an approach to verify Artin's conjecture for higher dimensional representations.

Say ρ is either an icosahedral or heptaoctahedral representation. We may choose a basis for V such that ρ has image in $GL_n(\mathcal{O})$ for some ring $\mathcal{O} \hookrightarrow \overline{\mathbb{Z}}_\ell$ – recall $\ell = 5, 7$ and $n = (\ell-1)/2$ – so there exists a prime ideal λ such that $\mathcal{O}/\lambda$ is a finite extension of $\mathbb{F}_\ell$. We say that ρ is residually modular if there exists a modular form $f(\tau)$ such that the following diagram commutes:

$$\begin{array}{ccccc} \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) & \xrightarrow{\rho_f} & GL_2(\mathcal{O}) & \xrightarrow{\mathrm{mod}\,\lambda} & GL_2(\overline{\mathbb{F}}_\ell) \\ \big\downarrow = & & & & \big\downarrow \mathrm{Sym}^{n-1} \\ \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) & \xrightarrow{\rho} & GL_n(\mathcal{O}) & \xrightarrow{\mathrm{mod}\,\lambda} & GL_n(\overline{\mathbb{F}}_\ell) \end{array}$$

There are canonical ways to exhibit icosahedral and heptaoctahedral representations which are residually modular using modular elliptic curves. For $\ell = 5, 7$ there exist faithful group representations π_ℓ such that

$$\mathrm{Sym}^{n-1} : \quad \overline{\mathbb{F}}_\ell^{\times} \cdot SL_2(\mathbb{F}_\ell) \xrightarrow{\pi_\ell} GL_n(\mathcal{O}) \xrightarrow{\mathrm{mod}\,\lambda} GL_n(\overline{\mathbb{F}}_\ell).$$

If E is a modular $\mathbb{Q}$-curve then ρ_E is residually modular. In general, given a totally real field F, if E is an elliptic curve defined over $F(\sqrt{(-1)^{(\ell-1)/2}\ell})$ which is isogeneous to its $\mathrm{Gal}\left(\overline{\mathbb{Q}}/F\right)$-conjugates, then E may be associated to a Hilbert modular form; in this case ρ_E is again residually modular. My work concerns studying those icosahedral and heptaoctahedral representations which arise this way.

Analytic Problem for Icosahedral Representations. Let ρ be an icosahedral representation, and continue notation as above. In a preprint [27], I was able to show ρ is residually modular whenever K is the splitting field of $x^5 + a\,x + b$ over $\mathbb{Q}$. Morever, I have shown that as long as (1) K, the splitting field of $x^5 + a\,x + b$, is not totally real, (2) ρ is wildly ramified at 5, and (3) the image of $\mathrm{Gal}\left(\overline{\mathbb{Q}}_5/\mathbb{Q}_5\right)$ under $\widetilde{\rho}$ is a cyclic group, then ρ satisfies Artin's conjecture. In the last couple of years, Chandrashekhar Khare and Jean-Pierre Wintenberger [39] have proved Artin's conjecture for odd icosahedral representations, although I have come up with these results independently of their work. (My preprint [27] has been available for several years now; an earlier draft was submitted for publication as early as 2004. It is in preprint form now because it must be modified to mirror the recent developments due to Khare's work.)

Analytic Problem for Heptaoctahedral Representations. Let ρ be a heptaoctahedral representation, and continue notation as above. I have shown that there exists a representation ρ_0 such that the following diagram commutes:

$$\begin{array}{ccccc} \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) & \xrightarrow{\rho_0} & GL_2(\mathcal{O}) & \xrightarrow{\mathrm{mod}\,\lambda} & GL_2(\overline{\mathbb{F}}_7) \\ \big\downarrow = & & & & \big\downarrow \mathrm{Sym}^2 \\ \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) & \xrightarrow{\rho} & GL_3(\mathcal{O}) & \xrightarrow{\mathrm{mod}\,\lambda} & GL_3(\overline{\mathbb{F}}_7) \end{array}$$

Serre's conjecture [45] – now a theorem due to Khare and Wintenberger [39] – asserts that ρ_0 is modular whenever K is not totally real. The representation ρ_0 is not a complex Galois

representation, but rather a 7-adic Galois representation. This approach to consider the symmetric square is motivated by the work of Ash and Tiep [2]. As an example, consider the heptaoctahedral representation associated to the so-called Trinks polynomial $x^7 - 7\,x + 3$. Serre notes that ρ_0 can be chosen to be the 7-adic representation associated with a modular form of weight 3 and level 3^3, but I have found that it may also be associated with a modular form of weight 2 and level $3^3 \cdot 7$. The abelian variety A_f associated with this latter modular form has dimension 3, so it may be possible to write an explicit model for this variety, then study the 7-torsion points in order to show that $K \subseteq \mathbb{Q}(A_f[7])$.

Doctoral Thesis

Elliptic Curves and Icosahedral Galois Representations
Stanford University (1999)
[22], `http://homepage.mac.com/ehgoins/notes/thesis.pdf`

> In 1917, Hecke proved that one-dimensional complex Galois representations give rise to entire L-series. In the 1930's, Artin conjectured that a generalization of such a result should be true: n-dimensional irreducible complex projective representations of finite Galois groups should also give rise to entire L-series.
>
> The case of one-dimensional Galois representations was proved in full generality with the advent of Class Field Theory, and soon thereafter researchers began work on the case of irreducible two-dimensional representations. Klein showed that the only finite images in $PGL_2(\mathbb{C})$ correspond to regular polygons and polyhedra. Most of these cases of the conjecture have been answered in the affirmative: Irreducible cyclic and dihedral representations are induced from one-dimensional ones, while irreducible tetrahedral and octahedral representations were studied by Langlands and Tunnell. The first known example to verify Artin's conjecture for the icosahedral case did not surface until Buhler's work in 1977.
>
> One approach to the icosahedral case starts by realizing an icosahedral Galois extension $K/\mathbb{Q}$ as one which is contained in the field generated by the 5-torsion of an elliptic curve. The overall goal of this thesis is to show how the icosahedral representation constructed by Buhler is attached to a modular elliptic curve. Using the work of Klein, we find a $\mathbb{Q}$-curve E_B defined over $\mathbb{Q}(\sqrt{5})$ such that $K(\zeta_5) = \mathbb{Q}(E_B[5]_x)$ is the field generated by the x-coordinates of the 5-torsion, where $K/\mathbb{Q}$ is the icosahedral extension studied in Buhler's work. We also find a weight 2 modular form over $\mathbb{Q}$, associated to E_B which is a deformation of Buhler's weight 1 modular form.

Refereed Publications

Semi-Magic Squares and Elliptic Curves
Missouri Journal of Mathematical Sciences, Vol. 22 (2010), no. 2, pgs. 102 - 107.
[19], `http://arxiv.org/abs/0910.0049v1`

> We show that, for all odd natural numbers N, the N-torsion points on an elliptic curve may be placed in an $N \times N$ grid such that the sum of each column and each row is the point at infinity.

A Tasty Combination: Multivariable Calculus and Differential Forms
With Talitha Washington. The Pentagon: The Journal of Kappa Mu Epsilon, Fall 2009, pgs. 11-28.
[37], `http://arxiv.org/abs/0910.0047v1`

Differential Calculus is a staple of the college mathematics major's diet. Eventually one becomes tired of the same routine, and wishes for a more diverse meal. The college math major may seek to generalize applications of the derivative that involve functions of more than one variable, and thus enjoy a course on Multivariate Calculus. We serve this article as a culinary guide to differentiating and integrating functions of more than one variable – using differential forms which are the basis for de Rham Cohomology.

Sphere-of-Influence Graphs
With Talitha Washington. Wolfram Demonstrations Project (February 4, 2010).
[**?**], `http://demonstrations.wolfram.com/SphereOfInfluenceGraphs/`

Let S be a set of vertices chosen from a grid. Given a vertex V in S, let $N(V)$ be the closest neighbor to V in S and draw a circle with center V and radius $\big|V - N(V)\big|$. Draw an edge between two vertices U and V if their circles intersect. In other words, connect U and V if $|U - V| \leq \big|V - N(V)\big| + \big|U - N(U)\big|$. This gives the sphere-of-influence graph for the given set of vertices.

Palindromes in Different Bases: A Conjecture of J. Ernest Wilkins
INTEGERS: The Electronic Journal of Combinatorial Number Theory, Vol. 9 (2009), pgs. 725-734.
[18], `http://www.integers-ejcnt.org/vol9.html`

We show that there exist exactly 203 positive integers N such that for some integer $d \geq 2$ this number is a d-digit palindrome base 10 as well as a d-digit palindrome for some base b different from 10. To be more precise, such N range from 22 to 998683178136263187138689 9.

On the Diophantine Equation $\mathbf{x^2 + 2^\alpha 5^\beta 13^\gamma = y^n}$
With Florian Luca and Alain Togbe. Algorithmic Number Theory Seminar (ANTS-VIII); LCNS 5011 (2008), pgs. 430-442.
[32]

In this note, we find all the solutions of the Diophantine equation $x^2 + 2^\alpha\, 5^\beta 13^\gamma = y^n$ in nonnegative integers $x, y, \alpha, \beta, \gamma, n \geq 3$ with x and y coprime.

Pythagorean Quadruplets
With Alain Togbe. International Journal of Pure and Applied Mathematics, Vol. 35 (2007), no. 3, pgs 363 - 372.
[33], `http://ijpam.eu/contents/2007-35-3/10/10.pdf`

We consider the multiplicative properties of integer quadruplets (a, b, c, d) satisfying $a^2 + b^2 + c^2 = d^2$ as a generalization of Pythagorean Triplets. In the process we present a group structure on the rational points on the unit sphere minus the poles and discuss a factorization result.

Heron Triangles via Elliptic Curves
With D. Maddox. Rocky Mountain Journal of Mathematics, Vol. 36; (2005), no. 5, pgs. 1511 - 1526.
[43], `http://projecteuclid.org/euclid.rmjm/1181069379`

Given a positive integer n, one may ask if there is a right triangle with rational sides having area n. Such integers are called congruent numbers, and are closely related to elliptic curves in the form $y^2 = x^3 - n^2\, x$. In this paper, we generalize this idea and show that there is a correspondence between positive integers n associated with arbitrary triangles with rational sides having area n and the family of elliptic curves $y^2 = x\,(x - n\,\tau)\left(x + n\,\tau^{-1}\right)$ for nonzero rational τ.

Icosahedral $\mathbb{Q}$-Curve Extensions
Mathematical Research Letters, 10 (2003), no. 2-3, pgs. 205-217.
[25], http://www.mrlonline.org/mrl/2003-010-002/2003-010-002-008.pdf

We consider elliptic curves defined over $\mathbb{Q}(\sqrt{5})$ which are either 2- or 3-isogenous to their Galois conjugate and which have an absolutely irreducible mod 5 representation. Using Klein's classical formulas which associate an icosahedral Galois extension $K/\mathbb{Q}$ with the 5-torsion of an elliptic curve, we prove that there is an association of such extensions generated by quintics $x^5 + A\,x^2 + B\,x + C$ satisfying $A\,B = 0$ with the aforementioned elliptic curves.

A Ternary Algebra with Applications to Binary Quadratic Forms
Council for African-American Researchers in the Mathematical Sciences, Vol. IV; Contemp. Math. 284 (2001), pgs. 7 - 12.
[24], http://arxiv.org/abs/0912.0060v1

We discuss multiplicative properties of the binary quadratic form $a\,x^2 + b\,x\,y + c\,y^2$ by considering a ring of matrices which is closed under a triple product. We prove that the ring forms a ternary algebra in the sense of Hestenes, and then derive both multiplicative formulas for a large class of binary quadratic forms and a type of multiplication for points on a conic section which generalizes the algebra of rational points on the unit circle.

Artin's Conjecture and Elliptic Curves
Council for African-American Researchers in the Mathematical Sciences, Vol. III; Contemp. Math. 275 (2001), pgs. 39 - 51.
[23], http://arxiv.org/abs/0912.0058v1

Artin conjectured that certain Galois representations should give rise to entire L-series. We give some history on the conjecture and motivation of why it should be true by discussing the one-dimensional case. The first known example to verify the conjecture in the icosahedral case did not surface until Buhler's work in 1977. We explain how this icosahedral representation is attached to a modular elliptic curve isogenous to its Galois conjugates, and then explain how it is associated to a cusp form of weight 5 with level prime to 5.

On the Distribution of Fractional Parts
With M. Currie. Council for African-American Researchers in the Mathematical Sciences, Vol. III; Contemp. Math. 275 (2001), pgs. 13 - 31.
[12]

Let $[\cdot]$ denote the greatest integer function. Then

$$\lim_{n\to\infty} \sum_{k=1}^{n} \left(\frac{n}{k} - \left[\frac{n}{k} \right] \right) \frac{1}{n} = 1 - \gamma,$$

where $\gamma = 0.57721566\ldots$ is the Euler-Mascheroni constant. We generalize to results for the greatest multiple of $\frac{1}{m}$ and nearest multiple of $\frac{1}{m}$. In addition, we examine the limiting distribution of the fractional parts, establishing along the way connections with Stirling's approximation as well as the gamma and digamma functions. A measure μ associated with the distribution satisfies

$$\left[\mu \left[0, \mu \left[1 - \frac{1}{m}, 1 \right] \right] \right]_m = \frac{1}{m}\,,$$

where $[x]_m$ denotes the greatest multiple of $\frac{1}{m}$ in x.

Publications in Press

On the Number of Ways to Climb a Staircase
With Talitha Washington. Ars Combinatoria. Accepted July 24, 2009.
[34], `http://arxiv.org/abs/0909.5459`

> Let $\mathcal{S}$ be a subset of the positive integers and M be a positive integer. Mohammad Azarian, inspired by work of Tony Colledge, considered the number of ways to climb a staircase containing n stairs using "step-sizes" $s \in \mathcal{S}$ and multiplicities at most M. In this exposition, we find a solution via generating functions, i.e., an expression that counts the number of partitions of $n = \sum_{s \in \mathcal{S}} m_s\, s$ satisfying $0 \leq m_s \leq M$. We use this to answer a series of questions posed by Azarian and we conclude by posing an open problem.

Publications Submitted

Riordan Matrix Representations of Euler's Constant γ and Euler's Number e
with Asamoah Nkwanta. Submitted August 19, 2011.
[**?**],

> We show that the Euler-Mascheroni constant γ and Euler's number e can both be represented as a product of a Riordan matrix and certain row and column vectors.

The Area of the Surface Generated by Revolving a Graph About Any Line
with Talitha Washington. Submitted August 2, 2011.
[**?**], `http://arxiv.org/abs/1108.2624`

> We discuss a general formula for the area of the surface that is generated by a graph $[t_0, t_1] \to \mathbb{R}^2$ sending $t \mapsto \big(x(t),\, y(t)\big)$ revolved around a general line $L:\, A\,x + B\,y = C$. As a corollary, we obtain a formula for the area of the surface formed by revolving $y = f(x)$ around the line $y = m\,x + k$.

Points on Hyperbolas at Rational Distance
with Kevin Mugo. Submitted June 1, 2011.
[**?**], `http://arxiv.org/abs/1108.0690`

> Richard Guy asked for the largest set of points which can be placed in the plane so that their pairwise distances are rational numbers. In this article, we consider such a set of rational points restricted to a given hyperbola.
>
> To be precise, for rational numbers a, b, c, and d such that the quantity $D = \big(a\,d - b\,c\big)/\big(2\,a^2\big)$ is defined and nonzero, we consider rational distance sets on the conic section $a\,x\,y + b\,x + c\,y + d = 0$. We show that, if the elliptic curve $Y^2 = X^3 - D^2\,X$ has infinitely many rational points, then there are infinitely many sets consisting of four rational points on the hyperbola such that their pairwise distances are rational numbers. We also show that any rational distance set of three such points can always be extended to a rational distance set of four such points.

Which Ellipses Go Through Four Points?
Submitted April 7, 2011.
[**?**], `http://demonstrations.wolfram.com/WhichEllipsesGoThroughFourPoints/`

> Three points in the plane uniquely determine a circle, while five points uniquely determine a conic section. But what about four points? This demonstration shows that there are

often infinitely many ellipses that go through four given points in the plane. You can drag the four points as well as rotate the ellipse through any angle you wish.

Branch Decomposition Heuristics for Linear Matroids
with Jing Ma, Susan Margulies, and Illya V. Hicks. Submitted March 1, 2011.
[**?**]

This paper presents two new heuristics which utilize classification and max-flow algorithms respectively to derive near-optimal branch decompositions for linear matroids. In the literature, there are already excellent heuristics for graphs, however, no practical branch decomposition methods for general linear matroids have been addressed yet. Introducing a "measure" which compares the "similarity" of elements of a linear matroid, this work reforms the linear matroid into a similarity graph. Then, the classification method and the max-flow method, both based on the similarity graph, are utilized on the similarity graph to derive separations for a near-optimal branch decomposition. Computational results using the classification method and the max-flow method on linear matroid instances are shown respectively.

Explicit Descent via 4-Isogeny on an Elliptic Curve
New York Journal of Mathematics. Conditionally Accepted December 5, 2008.
[26], `http://arxiv.org/abs/math/0411215`

We work out the complete descent via 4-isogeny for a family of rational elliptic curves with a rational point of order 4; such a family is of the form $y^2 + x\,y + a\,y = x^3 + a\,x^2$ where $\sqrt{-a} \in \mathbb{Q}^\times$. In the process we (1) exhibit the 4-isogeny and the isogenous curve, (2) explicitly present the principal homogeneous spaces, and (3) discuss examples by computing the rank.

Extending the Serre-Faltings Method for $\mathbb{Q}$-Curves
Transactions of the American Mathematical Society. Conditionally accepted December 5, 2008.
[17]

We consider a method for calculating modular forms associated to elliptic curves with a rational point of order $\ell = 2, 3$. We discuss a variant of the Serre-Faltings method which considers the symmetric square representations. As an application, we show that certain $\mathbb{Q}$-curves with reducible mod 3 representations are modular.

Publications in Progress

Heptaoctahedral Galois Representations
In preparation.
[28]

We discuss Artin's Conjecture for 3-dimensional complex representations.

On the Modularity of Wildly Ramified Galois Representations, I and II
In preparation.
[27], `http://arxiv.org/abs/math/0411214`

We show that an infinite family of odd complex 2-dimensional Galois representations ramified at 5 having nonsolvable projective image are modular, thereby verifying Artin's conjecture for a new case of examples. Such a family contains the original example studied

by Buhler. In the process, we prove that an infinite family of residually modular Galois representations are modular by studying Λ-adic Hecke algebras.

Rational Distance Sets on Conic Sections
In preparation.
[**?**]

Richard Guy asked for the largest set of points which can be placed in the plane so that their pairwise distances are rational numbers. In this article, we consider such a set of rational points restricted to a given conic section.

There exist infinitely many rational Diophantine 6-tuples – almost
In preparation.
[20]

A set $\{m_1, m_2, \ldots, m_n\}$ of rational numbers is said to be a rational Diophantine n-tuple if $m_i\, m_j + 1$ is a perfect square for $i \neq j$. In the late 1700's, Euler showed that there exist infinitely many rational Diophantine 5-tuples. It is not known whether there exist infinitely many (nontrivial) rational Diophantine 6-tuples, although Gibbs found seven examples in 1999. In this exposition, we use properties of the elliptic curve $E_k : y^2 = (1-x^2)\,(1-k^2\,x^2)$ to explain how to find an infinite family of nontrivial 6-tuples. We are motivated by Dujella's results from 2001 using properties of elliptic curves. In the process, we find families of elliptic curves having large rank for the torsion subgroup $Z_2 \times Z_4$.

Why should I care about elliptic curves?
In preparation.
[21]

An elliptic curve E possessing a rational point is an arithmetic-algebraic object: It is simultaneously a nonsingular projective curve with an affine equation $y^2 = x^3 + A\,x + B$, which allows one to perform arithmetic on its points; and a finitely generated abelian group $E(\mathbb{Q}) \simeq E(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r$, which allows one to apply results from abstract algebra. In this talk, we discuss some basic properties of elliptic curves, and give applications along the way. This is a summary of the talk given as the David Blackwell Lecture at the MAA MathFest on August 7, 2009.

Heron Triangles, Diophantine Problems and Elliptic Curves
with Garikai Campbell. In preparation.
[8]

For all nonzero rational t, $E_t : v^2 = u^3 + (t^2+2)\,u^2 + u$ is an elliptic curve defined over $\mathbb{Q}$. By analyzing this family of curves, we are able to describe connections between the problem of finding Heron triangles with a given area possessing at least one side of a particular length, finding points in the plane at rational distance, and finding Diophantine quadruples and quintuples. We are then, quite naturally, led to study the relationship between these problems and elliptic curves defined over $\mathbb{Q}$ with rational torsion subgroup equal to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. Consequently, we find a new elliptic curve with this torsion having rank 3 (tying the record for the largest known rank of an elliptic curve of this kind). Assuming the Parity Conjecture, we also find several others with rank 1 or 3 and a few more having rank 2 or 4. We also find an infinite family of elliptic curves defined over $\mathbb{Q}$ with rational torsion subgroup equal to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ and rank at least 1 (again tying the record).

Counting Mod ℓ Solutions via Modular Forms
With L. Kilford. In preparation.
[30]

In 2006, Norm Hurt observed that a text by Moreno and Wagstaff contains the following gem: "Let $P(x)$ be an irreducible cubic with Galois group $G \simeq S_3$, and choose an irreducible continuous representation $\rho_P : G \to GL_2(\mathbb{C})$. Then for a prime ℓ which does not divide the discriminant of $P(x)$, the integer, $N_\ell(P) = \#\left\{x \in \mathbb{F}_\ell \,\middle|\, P(x) \equiv 0 \pmod{\ell}\right\} = 1 + \operatorname{tr}\rho(\mathrm{Frob}_\ell)$ where Frob_ℓ is the Frobenius element." In 2008, Hurt found similar results concerning the polynomials $x^3 - x - 1$ as studied by Wilton in 1929, $x^4 - 2\,x^3 + 2\,x^2 - 2\,x + 3$ as studied by Crispo in 1997, and $x^4 - x - 1$ as studied by Serre in 2003.

In this paper, we show that these results are part of a larger theory which focuses on the decomposition of the standard representation $\pi_P : G \to GL(V)$ of the roots of the polynomial. Using the full power of Serre's conjecture, we show how to express the L-series $L(P,s) = \prod_\ell \det\left[1 - \left(\pi_P\big|_{V^{I_\ell}}\right)(\mathrm{Frob}_\ell)\cdot\ell^{-s}\right]^{-1}$ as a product of L-series associated to modular forms.

Lutz-Nagell Theorem
With Yu Tsumura. In preparation.
[**?**]

This Wolfram Demonstrations Project allows one to determine the set of integral points on a given elliptic curve.

Books and Monographs

Council for African American Researchers in the Mathematical Sciences, Vol. V
Editor with Don King, Gaston N'Guérékata, and Alfred Noël. Council for African American Researchers in the Mathematical Sciences, Vol. V; Contemp. Math. 467 (2008), 152 pgs.
[31]

Ordinary Differential Equations
With Talitha Washington. In progress.
[35]

This textbook will cover the theory of ordinary differential equations by focusing on applications to various branches of science, including applied mathematics, biology, chemistry, and physics. It is meant to be used for advanced undergraduates or as a reference manual for graduate students. (The first 60 pages concerning first order differential equations has been completed. The authors have discussed publication deals with two book companies.)

Ordinary Differential Equations: Worked Examples with Solutions
With Talitha Washington. In progress.
[36]

This textbook is meant to be a companion to "Ordinary Differential Equations." Each of the exercises in the aforementioned book will contain a detailed solution. (Some 100 pages have been completed in this solution manual; the exercises concerning first order differential equations have already been written up.)

$y^2 = (1 - x^2)(1 - k^2x^2)$
In progress.
[29]

> This textbook will be an undergraduate monograph to walk the reader through the theory of elliptic curves from the historical motivation via elliptic integrals to the current research regarding finding curves of large rank. These lectures were written by the author during his years as a seminar director at the Summer Undergraduate Mathematical Sciences Research Institute (SUMSRI) at Miami University of Ohio. (The 200-page text has been written. It must be shortened in order to read more like a textbook rather than like lecture notes.)

Selmer Groups and Galois Representations
In progress.
[**?**]

> This textbook will be an research monograph on computing the Mordell-Weil groups of elliptic curves. The text will begin with basic principles, such as the Krull Topology on profinite groups and cohomology of abelian modules over such groups. The text is based on a graduate-level course given at Purdue University.

Future Research Overview

Introduction. There has been much interest in computing the Mordell-Weil groups of elliptic curves defined over the rational numbers. In 1963 and 1965, Bryan Birch and Peter Swinnerton-Dyer [4], [5] made extensive computations on the ranks of elliptic curves defined over the rational numbers, leading to surprising conjectures about the relationship with certain complex functions arising from Galois representations (namely the L-series) and certain groups arising from Galois cohomology (namely the Shafarevich-Tate group). In 1997, with the advent of stronger computing power and more efficient algorithms, John Cremona [10] extended these computations. In 2007, William Stein and Mark Watkins [3] created a database with the most extensive information to date. The computational aspects of arithmetic algebraic geometry have expanded from simply computing special values of L-series to understanding how the ranks of elliptic curves are distributed.

Many of these computations involve families of quadratic twists of elliptic curves. While this method helps to keep control over how fast the conductor grows, it does not keep track of how the torsion subgroup changes. Andrej Dujella [14] has kept a record of the largest known ranks parsed by torsion subgroups. However, there is no extensive data at present on how the ranks of elliptic curves are distributed according to their torsion. It is widely believed that the ranks of elliptic curves are not universally bounded. It is also widely believed that the ranks take on the values 0 and 1 with near 100% probability – but when separated according to torsion subgroup, almost nothing is known.

My future work seeks to gain a better understanding of the ranks of those elliptic curves having as much torsion as possible. I have classified [29] the family of elliptic curves with torsion subgroup $Z_2 \times Z_8$, and have worked for many years perfecting methods of computing the ranks of such curves using properties of their torsion. Many of the current methods in the literature to compute the rank employ a descent via 2-isogeny. Only recently have researchers been considering modifications by using 4-covering maps. I plan to implement these ideas, using newly discovered formulas [38] discovered during summer research with undergraduates, and possibly extend descent arguments using 8-covering maps. My ideas are different from those in the literature because I have discovered explicit formulas for the homogeneous spaces as quadric intersections.

Specific Goals. As mentioned above, I have shown [29] that each elliptic curve E defined over $\mathbb{Q}$ with torsion subgroup $E(\mathbb{Q})_{\text{tors}} \simeq Z_2 \times Z_8$ is birationally equivalent to the quartic curve

$$E_t: \quad y^2 = \left(1 - x^2\right)\left(1 - k^2\, x^2\right) \quad \text{where} \qquad k = \frac{t^4 - 6\,t^2 + 1}{\left(t^2 + 1\right)^2}$$

for some rational number t different from -1, 0, and 1. Consider an m-isogeny $\phi : E \to E'$ defined over $\mathbb{Q}$, and let $\hat{\phi} : E' \to E$ be its dual. Upon choosing embeddings $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$ for every place ℓ of $\mathbb{Q}$, Galois cohomology implies that we have the following short exact sequences:

$$\begin{array}{ccccccc}
\{\mathcal{O}\} & \longrightarrow & \dfrac{E'(\mathbb{Q})}{\phi\big(E(\mathbb{Q})\big)} & \xrightarrow{\delta_\phi} & H^1\big(\mathbb{Q},\, E[\phi]\big) & \longrightarrow & H^1\big(\mathbb{Q},\, E(\overline{\mathbb{Q}})\big) \\
 & & \big\downarrow & & \big\downarrow & & \big\downarrow \\
 & & \{\mathcal{O}\} & \longrightarrow & \displaystyle\prod_\ell H^1\big(\mathbb{Q}_\ell,\, E(\overline{\mathbb{Q}}_\ell)\big) & \xrightarrow{\sim} & \displaystyle\prod_\ell H^1\big(\mathbb{Q}_\ell,\, E(\overline{\mathbb{Q}}_\ell)\big)
\end{array}$$

for some connecting homomorphism δ_ϕ. The cohomology group $H^1\big(\mathbb{Q},\, E[\phi]\big)$ can be understood via Kummer Theory, but the Weil-Châtalet group $WC(E/\mathbb{Q}) = H^1\big(\mathbb{Q},\, E(\overline{\mathbb{Q}})\big)$ is much more mysterious. Instead, we consider the kernels of the vertical arrows to define ϕ-Selmer group $\text{Sel}^{(\phi)}(E/\mathbb{Q}) \subseteq H^1\big(\mathbb{Q},\, E[\phi]\big)$ and Shafarevich-Tate group $Ш(E/\mathbb{Q}) \subseteq WC(E/\mathbb{Q})$, respectively. This gives the following diagram:

$$\begin{array}{ccccccccc}
\dfrac{E'[\hat{\phi}]}{\phi\big(E[m]\big)} & \longrightarrow & \dfrac{E'(\mathbb{Q})}{\phi\big(E(\mathbb{Q})\big)} & \xrightarrow{\hat{\phi}} & \dfrac{E(\mathbb{Q})}{m\,E(\mathbb{Q})} & \longrightarrow & \dfrac{E(\mathbb{Q})}{\hat{\phi}\big(E'(\mathbb{Q})\big)} & \longrightarrow & \{\mathcal{O}\} \\
\simeq\big\downarrow & & \delta_\phi\big\downarrow & & \big\downarrow & & \delta_{\hat{\phi}}\big\downarrow & & \big\downarrow \\
\dfrac{E'[\hat{\phi}]}{\phi\big(E[m]\big)} & \longrightarrow & \text{Sel}^{(\phi)}(E/\mathbb{Q}) & \longrightarrow & \text{Sel}^{(m)}(E/\mathbb{Q}) & \xrightarrow{\phi} & \text{Sel}^{(\hat{\phi})}(E'/\mathbb{Q}) & \longrightarrow & \text{coker}\,\phi \\
\big\downarrow & & \big\downarrow & & \big\downarrow & & \big\downarrow & & \simeq\big\downarrow \\
\{1\} & \longrightarrow & Ш(E/\mathbb{Q})[\phi] & \longrightarrow & Ш(E/\mathbb{Q})[m] & \xrightarrow{\phi} & Ш(E'/\mathbb{Q})[\hat{\phi}] & \longrightarrow & \text{coker}\,\phi
\end{array}$$

In particular, when $m = 2$ and $E = E_t$, there are nonnegative integers r and s such that we have the orders $|E(\mathbb{Q})/2\,E(\mathbb{Q})| = 2^{r+2}$, $|\text{Sel}^{(2)}(E/\mathbb{Q})| = 2^{s+2}$, and $|Ш(E/\mathbb{Q})[2]| = 2^{s-r}$. My work seeks to gather information about the Mordell-Weil rank $r = r(t)$ and 2-Selmer rank $s = s(t)$ by resolving three separate tasks.

> **Search for Examples:** Are there infinitely many elliptic curves E defined over $\mathbb{Q}$ having torsion subgroup $Z_2 \times Z_8$ and Mordell-Weil rank $r \geq 2$? What about Mordell-Weil rank $r \geq 3$? Does there exist *even one* elliptic curve E defined over $\mathbb{Q}$ having torsion subgroup $Z_2 \times Z_8$ and Mordell-Weil rank $r \geq 4$?

In 2003, I (along with Garikai Campbell) [8] constructed an infinite family of curves E_t with Mordell-Weil rank $r \geq 1$. The idea was choose the parameter $t = (u+v-3)/(2\,u)$ corresponding to points on the elliptic curve $\mathcal{S}: v^2 = u^3 - u^2 - 9\,u + 9$. Since $\mathcal{S}$ has infinitely many rational points, there are infinitely many elliptic curves E_t with positive rank. I would like to generalize this to find an infinite family with Mordell-Weil rank $r \geq 2$.

For a given bound T, there are approximately $T^2/8$ curves E_t for $t = a/b$, where a and b are relatively prime integers satisfying $0 < (1 + \sqrt{2})\,a < b \leq T$. Currently, the largest known rank is $r = 3$, corresponding to twenty-seven examples in the range with $T = 1109$. In 2006, I directed five undergraduates on a project to find elliptic curves E_t with Mordell-Weil rank $r \geq 4$. Terris Brooks, Elizabeth Fowler, Katherine Hastings, Danielle Hiance, and Matthew Zimmerman [6] considered

the 503923 elliptic curves E_t corresponding to the bound $T = 2000$. They were searching for curves having rank $r \geq 4$ – but unfortunately did not find any. They parallelized their search by computing the Mordell-Weil ranks on dozens of nodes at the high-powered computing cluster at Miami University of Ohio. The searching process needs to be refined in order to do a better job at determining the Mordell-Weil rank precisely.

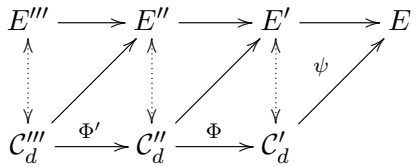
In 2007, I directed four undergraduates on a project to find elliptic curves E_t with Mordell-Weil rank $r \geq 3$. Jessica Flores, Kimberly Jones, Anne Rollick, and James Weigandt [16] considered the 3148208 elliptic curves E_t corresponding to the bound $T = 5000$. They discovered three curves of rank $r = 3$ not before found in the literature. As with the 2006 group, they parallelized their search on the high-powered computing cluster at Miami University of Ohio.

> **Parallelize Current Algorithms:** Improve `mwrank`'s algorithm to determine the image $\phi\left[\mathrm{Sel}^{(2)}(E/\mathbb{Q})\right] \subseteq \mathrm{Sel}^{(\hat{\phi})}(E'/\mathbb{Q})$. Implement an algorithm, optimized for distributed computing clusters, which will parallelize determination of $E(\mathbb{Q})/2\,E(\mathbb{Q})$ and $\mathrm{Sel}^{(2)}(E/\mathbb{Q})$.

A 2-isogeny $\phi : E \to E'$ sends $\mathrm{Sel}^{(2)}(E/\mathbb{Q}) \to \mathrm{Sel}^{(\hat{\phi})}(E'/\mathbb{Q})$. Hence one must determine the cokernel of ϕ in order to determine both the Mordell-Weil rank r and the 2-Selmer rank s. John Cremona's `mwrank` [11] is designed to compute the image of $\mathrm{Sel}^{(2)}(E/\mathbb{Q})$, but I have determined a flaw in this part of the code. I have spoken with Cremona on several occasions to verify that such a flaw does indeed exist. Since `mwrank` is now open source code bundled with William Stein's `SAGE` [47], I plan to fix this flaw.

I have spent the last several years [6], [16], [38] working on parallelizing `mwrank` for a high-powered computing cluster. In 2007, I worked with a team of four undergraduates to compute the 2-Selmer ranks of some 3148208 elliptic curves, distributed over 128 processors on the clusters at Miami University of Ohio. In 2008, I worked with Shweta Gupte, a master's student at Purdue University majoring in mathematics and computer science, and Jamie Weigandt, a doctoral student at Purdue University majoring in mathematics, to implement a similar idea on the clusters at Purdue.

> **Implement Descents via 4- and 8-Isogenies:** Determine the homogeneous spaces $\mathcal{C}_d$, $\mathcal{C}_d{}''$, $\mathcal{C}_d'''$ and exhibit maps $\Phi : \mathcal{C}_d'' \to \mathcal{C}_d'$, $\Phi' : C_d''' \to C_d''$ which make the following diagram commute:



In order to find rational points on E, one usually looks for rational points on the homogeneous space $\mathcal{C}_d$. As $\psi : \mathcal{C}_d' \to E$ is a 2-covering map, the corresponding compositions $\psi \circ \Phi : \mathcal{C}_d'' \to E$ and $\psi \circ (\Phi \circ \Phi') : \mathcal{C}_d''' \to E$ are 4- and 8-covering maps, respectively.

In 1996, J. R. Merriman, Samir Siksek, and Nigel Smart [44] outlined a method of how to use such a diagram in order to effectively compute the rank of an elliptic curve. In 2003, Tom Womack [50] described this process in more detail, and ultimately implemented code in `MAGMA` [9]. These papers emphasize the problem of determining equations for the principal homogeneous space using a quadric intersection, which they subsequently express as a pair of 4×4 matrices – assuming that the torsion subgroup is "small." In 2004, I [26] considered the problem of how to compute $\mathcal{C}_d''$ directly using the explicit 4-isogeny. In 2008, following a conversation with John Cremona, I determined [29] the explicit pair of 4×4 matrices arising from homogeneous spaces for those elliptic curves with "large" torsion subgroup.

In 2008, I directed six undergraduates in an attempt to implement these ideas. Samuel Ivy, Brett Jefferson, Michele Josey, Cheryl Outing, Clifford Taylor, and Staci White [38] studied the curve E_t for $t = 9/296$. They reduced the problem of determining the Mordell-Weil rank $r = r(t)$ to finding a rational point on at least one of the following homogeneous spaces:

$$\mathcal{C}'_{37}: \; w^2 = 2172344348297474273125\, z^4 + 58712815268370607681\, z^2 + 21779862847488;$$

$$\mathcal{C}''_{37}: \; w^2 = 218847037473549497379 7\, z^4 + 60017913360731350081\, z^2 + 23515280943436800.$$

The students attempted to use `MAGMA`'s command `PointsQI()` as well as Michael Stoll's `ratpoints` on various high-powered computing clusters, but failed to find any rational points. Even when points are found, one still needs to determine maps $\psi \circ \Phi : \mathcal{C}''_{37} \to \mathcal{C}'_{37} \to E_t$ in order to determine rational points on the elliptic curve.

In 2005, Sebastian Stamminger [46] considered the task of determining the rank of an elliptic curve using an 8-isogeny. Unfortunately, he assumed that the torsion subgroup of such curves is "small;" that is, he worked with curves not having a point of order 8. Still, this algorithm has been implemented in `MAGMA` [9]. I believe it is possible to determine a descent via 8-isogeny by computing the homogeneous space $\mathcal{C}'''_d$ as well as the corresponding map $\psi \circ (\Phi \circ \Phi') : \mathcal{C}'''_d \to E_t$ of degree 8.

Senior People Familiar with My Work

Nigel Boston	University of Wisconsin at Madison	`boston@math.wisc.edu`
Dan Bump	Stanford University	`bump@math.stanford.edu`
Kevin Buzzard	Imperial College	`buzzard@imperial.ac.uk`
Jordan Ellenberg	University of Wisconsin at Madison	`ellenber@math.wisc.edu`
Matthias Flach	California Institute of Technology	`flach@its.caltech.edu`
Barry Mazur	Harvard University	`mazur@math.harvard.edu`
Ken Ono	Emory University	`ono@mathcs.emory.edu`
Dinakar Ramakrishnan	California Institute of Technology	`dinakar@caltech.edu`
Chris Skinner	Princeton University	`cmcls@math.princeton.edu`
William Stein	University of Washington	`wstein@gmail.com`
Richard Taylor	Harvard University	`rtaylor@math.harvard.edu`

References

[1] Emil Artin. *The Collected Papers of Emil Artin*. 1965. Edited by Serge Lang and John T. Tate.

[2] Avner Ash and Pham Huu Tiep. Modular Representations of $GL(3, \mathbb{F}_p)$, Symmetric Squares, and mod-p Cohomology of $GL(3, \mathbb{Z})$. *J. Algebra*, 222(2):376–399, 1999.

[3] Baur Bektemirov, Barry Mazur, William A. Stein, and Mark Watkins. Average Ranks of Elliptic Curves: Tension between Data and Conjecture. *Bull. Amer. Math. Soc. (N.S.)*, 44(2):233–254 (electronic), 2007.

[4] B. J. Birch and H. P. F. Swinnerton-Dyer. Notes on Elliptic Curves. i. *J. Reine Angew. Math.*, 212:7–25, 1963.

[5] B. J. Birch and H. P. F. Swinnerton-Dyer. Notes on Elliptic Curves. ii. *J. Reine Angew. Math.*, 218:79–108, 1965.

[6] Terris D. Brooks, Elizabeth A. Fowler, Katherine C. Hastings, Danielle L. Hiance, and Matthew A. Zimmerman. Elliptic Curves with Torsion Subgroup $Z_2 \times Z_8$: Does a Rank 4 Curve Exist? *SUMSRI Journal*, 2006.

[7] Kevin Buzzard, Mark Dickinson, Nicholas I. Shepherd-Barron, and Richard Lawrence Taylor. On Icosahedral Artin Representations. *Duke Math. J.*, 109(2):283–318, 2001.

[8] Garikai Campbell and Edray Herber Goins. Heron Triangles, Diophantine Problems, and Elliptic Curves. Submitted.

[9] John Cannon and Catherine Playoust. MAGMA: A New Computer Algebra System. *Euromath Bull.*, 2(1):113–144, 1996.

[10] John Cremona. *Algorithms for Modular Elliptic Curves*. 1997.

[11] John Cremona. mwrank and Related Programs for Elliptic Curves over $\mathbb{Q}$. `http://www.warwick.ac.uk/staff/J.E.Cremona/mwrank/index.html`.

[12] Melvin Robert Currie and Edray Herber Goins. The Fractional Parts of $\frac{n}{k}$. *Contemporary Mathematics*, volume 275, pages 13–31. 2001.

[13] P. G. Lejeune Dirichlet. *Vorlesungen über Zahlentheorie*. 1968.

[14] Andrej Dujella. High Rank Elliptic Curves with Prescribed Torsion. `http://www.math.hr/ duje/tors/tors.html`.

[15] D. W. Erbach, J. Fisher, and John McKay. Polynomials with PSL(2, 7) as Galois Group. *J. Number Theory*, 11(1):69–75, 1979.

[16] Jessica Flores, Kimberly Jones, Anne Rollick, and Jamie Weigandt. A Statistical Analysis of 2-Selmer Groups for Elliptic Curves with Torsion Subgroup $Z_2 \times Z_8$. *SUMSRI Journal*, 2007.

[17] Edray Herber Goins. Extending the Serre-Faltings Method for $\mathbb{Q}$-Curves. *Trans. Amer. Math. Soc.*, Accepted.

[18] Edray Herber Goins. Palindromes in Different Bases: A Conjecture of J. Ernest Wilkins. Submitted.

[19] Edray Herber Goins. Semi-Magic Squares and Elliptic Curves. Submitted.

[20] Edray Herber Goins. There Exist Infinitely Many Rational Diophantine 6-tuples – Almost. In preparation.

[21] Edray Herber Goins. Why Should I Care About Elliptic Curves? In preparation.

[22] Edray Herber Goins. *Elliptic Curves and Icosahedral Galois Representations*. PhD thesis, 1999.

[23] Edray Herber Goins. Artin's conjecture and elliptic curves. *Contemporary Mathematics*, volume 275, pages 39–51. 2001.

[24] Edray Herber Goins. A Ternary Algebra with Applications to Binary Quadratic Forms. Contemporary Mathematics, volume 284, pages 7–12. 2001.

[25] Edray Herber Goins. Icosahedral $\mathbb{Q}$-curve extensions. *Math. Res. Lett.*, 10(2-3):205–217, 2003.

[26] Edray Herber Goins. Explicit Descent via 4-Isogeny on an Elliptic Curve. Submitted.

[27] Edray Herber Goins. On the Modularity of Wildly Ramified Galois Representations. Preprint.

[28] Edray Herber Goins. Heptaoctahedral Galois Representations. In preparation.

[29] Edray Herber Goins. $y^2 = (1 - x^2)(1 - k^2x^2)$. In preparation.

[30] Edray Herber Goins and Lloyd James Peter Kilford. Counting mod ℓ Solutions via Modular Forms. In preparation.

[31] Edray Herber Goins, Donald R King, Gaston M NGuérékata, and Alfred G. Noël. Council for African American Researchers in the Mathematical Sciences. vol. V. *Contemporary Mathematics*, volume 467:x+152, 2008.

[32] Edray Herber Goins, Florian Luca, and Alain Togbe. On the Diophantine Equation $x^2 + 2^\alpha 5^\beta 13^\gamma = y^n$. *Algorithmic Number Theory*, pages 430 – 442.

[33] Edray Herber Goins and Alain Togbe. Pythagorean Quadruples. *Int. J. Pure Appl. Math.*, 35(3):363–372, 2007.

[34] Edray Herber Goins and Talitha M. Washington. On the Number of Ways to Climb a Staircase. *Ars Combinatoria*, To appear.

[35] Edray Herber Goins and Talitha M. Washington. Ordinary Differential Equations. In preparation.

[36] Edray Herber Goins and Talitha M. Washington. Ordinary Differential Equations: Worked Examples with Solutions. In preparation.

[37] Edray Herber Goins and Talitha M. Washington. A Tasty Combination: Multivariable Calculus and Differential Forms. Preprint.

[38] Samuel Ivy, Brett Jefferson, Michele Josey, Cheryl Outing, Clifford Taylor, and Staci White. 4-Covering Maps on Elliptic Curves with Torsion Subgroup $Z_2 \times Z_8$. *SUMSRI Journal*, 2008.

[39] Chandrashekhar Khare and Jean-Pierre Wintenberger. On Serre's Reciprocity Conjecture for 2-Dimensional mod p Representations of the Galois Group of $\mathbb{Q}$. *arXiv*, Dec 2004.

[40] Felix Klein. *Gesammelte mathematische Abhandlungen*. 1973.

[41] Felix Klein and George Gavin Morrice. Lectures on the Icosahedron and the Solution of Equations of the Fifth Degree. *Dover Publications*, pages xvi+289, 1956.

[42] Robert P Langlands. *Base change for $GL(2)$*. 1980.

[43] Davin Maddox and Edray Herber Goins. Heron Triangles via Elliptic Curves. *Rocky Mountain J. Math.*, 36(5):1511–1526, 2006.

[44] J R Merriman, Samir Siksek, and Nigel P. Smart. Explicit 4-Descents on an Elliptic Curve. *Acta Math.*, 77(4):385–404, 1996.

[45] Jean-Pierre Serre. Sur les Représentations Modulaires de Degré 2 de Gal(Q/$\mathbf{Q}$). *Duke Math. J.*, 54(1):179–230, 1987.

[46] Sebastian Karl Michael Stamminger. *Explicit 8-Descent on Elliptic Curves*. PhD thesis, 2005.

[47] William A Stein. *SAGE: Open Source Mathematical Software (Version 3.1.2)*, 2008. `http://www.sagemath.org`.

[48] Jerrold Tunnell. Artin's Conjecture for Representations of Octahedral Type. *Bull. Amer. Math. Soc. (N.S.)*, 5(2):173–175, 1981.

[49] Andrew Wiles. Modular Elliptic Curves and Fermat's Last Theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.

[50] Tom Womack. *Explicit Descent on Elliptic Curves*. PhD thesis, 2003.