Statement of Research Interests

Jay Daigle

1 Introduction

My research focuses on number theory, and in particular on using algebraic tools. I currently have two research projects. One is studying the theory of non-unique factorization in numerical monoids, which is easily accessible to students with an undergraduate-level background and provides a foundation for an undergraduate research program. The other is using (ϕ, Γ)-modules to study the equivariant Tamagawa number conjecture, a deep conjecture tying together much of arithmetic geometry and algebraic number theory.

2 Numerical Monoids and Factorization

Questions of factorization, unique and not, are foundational to number theory. Though the integers famously and importantly have unique factorization, most number fields do not; this was first noticed by Kummer and raised in importance when Cauchy and Lamé simultaneously presented (incorrect) proofs of Fermat's Last Theorem that depended on unique factorization in certain number fields (see [ST15] 11.1 for more historical background here).

The factorization structure of number fields is quite difficult to understand. But monoids, which are effectively groups without inverses, can have a rich and accessible theory of factorization. In particular, it is easy to construct and understand monoids that do not have unique factorization, which makes them a fruitful field for research into various factorization constants.

In my research I have studied numerical monoids, which are additive submonoids of $\mathbb{N}$. In particular, we take a set of generators $S = \{n_1, \ldots, n_k\} \subset \mathbb{N}$ and let the set of integer linear combinations with non-negative coefficients $M = \{a_1 n_1 + \cdots + a_k n_k | a_i \in \mathbb{N}_{\geq 0}\}$ be our monoid. If $m \in M$ then a factorization of m is a k-tuple $(a_1, \ldots, a_k)$ such that $a_1 n_1 + \cdots + a_k n_k = m$.

If $k > 1$ then many elements will have more than one factorization; it is easy to see, for instance, that the element $n_1 n_2$ has $(n_2, 0)$ and $(0, n_1)$ as two distinct factorizations. A number of constants have been developed to quantify the factorization structure of such a monoid:

- If $\gcd(S) = 1$ then the set of all natural numbers not in M is finite. The largest element of this set is called the *Frobenius number* $F(M)$ of the monoid M.
- The *length* of a factorization $(a_1, \ldots, a_k)$ is the sum of of the coefficients $a_1 + \cdots + a_k$. For a fixed $m \in M$ we define the *set of lengths* $\mathcal{L}(m)$ to be the set of lengths of all possible factorizations of m.
- The *delta set* $\Delta(m)$ is the set of successive differences of the lengths: if $\mathcal{L}(m) = \{x_1, \ldots, x_r\}$ with $x_i < x_{i+1}$, then $\Delta(m) = \{x_{i+1} - x_i\}$. This measures the ways we can "trade out" some generators for others without affecting the actual monoid element.

  We define the delta set of the entire monoid $\Delta(M)$ to be the union of the delta sets of each element of M.

- The *catenary degree* $c(m)$ of an element $m \in M$ measures how easy it is to move from one factorization from m to another. In particular, $c(m) = N$ if N is the smallest integer such that, given any two factorizations of m, it is possible to move from one to the other switching out only N elements at a time.

  The catenary degree of a monoid is again the union of the catenary degrees of all the elements of the monoid: that is, $c(M) = \bigcup_{m \in M} c(m)$.

- The *omega primality* $\omega(m)$ measures how far an element is from being prime; by definition, m is prime precisely when $\omega(m) = 1$.

  In particular $\omega(m)$ is the smallest number r such that if m divides a sum of many elements, it must divide some subsum of at most r elements. This extends the definition of a prime number as a number that, whenever it divides a product, then it divides one of the factors.

Though much is known about each of these invariants (see [OP17] for a good survey), none of them is trivial to compute.

I plan to start an undergraduate-centric research program into understanding many of these invariants for different subclasses of numerical monoid. Recent work in this field has included [CCM$^+$17], [CGH$^+$17], [GS17], [OPTW16], and others. Our research would involve a combination of computer-aided search to understand the structure of chosen numerical monoids and generate conjectures, and then theoretical work to prove those conjectures.

In particular, recent work in [GGMFVT15] building on the original work of [CHK09] has made the computation of the delta sets of monoids computationally feasible, and [CCM$^+$14] has done the same for the catenary degree. These results enable computational work to generate many exciting new reults and conjectures.

I'm particularly interested in studying factorization in "non-uniquely generated" monoids—monoids where the generating set S has a proper subset that generates the same monoid. These are so far not widely studied, but have a factorization theory as interesting as the commonly studied minimally presented monoids. In [CDHK10] we studied some basic examples of non-minimally

3 The equivariant Tamagawa number conjecture

3.1 An overview of the Tamagawa number conjecture

The Tamagawa number conjecture of [BK90] is a deep conjecture about special values of L-functions, which relates to both the Birch and Swinnerton-Dyer conjecture and the Riemann zeta function (and in fact the Birch and Swinnerton-Dyer conjecture is a special case of the Tamagawa number conjecture). The conjecture also has close ties to the main conjecture of Iwasawa theory.

Given a "motive" M (which can be thought of as a smooth projective variety X over $\mathbb{Q}$ with some cohomological data attached), we can write an L-series

$$L(M, s) = \prod_p P_p(p^{-s})^{-1} \tag{1}$$

where $P_p(T) = \det(1 - Fr_p^{-1} \cdot T)$ (where Fr_p is the Frobenius operator on a certain space) is a polynomial, conjectured to lie in $\mathbb{Q}[T]$. This L-function is a complex series which is conjectured (and known in many cases) to converge for $\Re(s) \gg 0$. The Tamagawa number conjecture holds that $L(M,s)$ has a meromorphic continuation to the complex plane, and predicts the behavior at zero. That is, we can write a Laurent series centered at zero

$$L(M,s) = L^*(M)s^{r(M)} + \ldots$$

and the Tamagawa number conjecture predicts $L^*(M) \in \mathbb{R}$ and $r(M) \in \mathbb{Z}$.

If L is a number field and $M = h^0(L)(0)$, then $L(M,s)$ is the Dedekind zeta function

$$L(M,s) = \zeta_L(s) = \prod_{\mathfrak{p} \subset \mathcal{O}_K} (1 - N_{K/\mathbb{Q}}(P))^{-s}$$

Then the Tamagawa number conjecture is equivalent to the analytic class number formula: if $L \otimes_{\mathbb{Q}} \mathbb{R} \cong R^{r_1} \times \mathbb{C}^{r_2}$ then $r(M) = r_1 + r_2 - 1$ and $L^*(M) = -hR/w$ where R is the regulator of L, w the number of roots of unity in L, and h is the class number of $\mathcal{O}_L$.

If X is an abelian variety over a number field and $M = h^1(X)(1)$ then $L(M, s-1)$ is the classical Hasse-Weil L-function of the dual abelian variety and thus also of X. In particular, if X is an elliptic curve over $\mathbb{Q}$ then the Tamagawa number conjecture implies the Birch and Swinnerton-Dyer conjecture, which holds that $r(M)$ is the rank of the elliptic curve and $L^*(M)$ is given by various arithmetic data associated to X.

The conjecture of [BK90] was later refined by [FK06] and others to an equivariant statement, using algebraic K-theory, which can incorporate information from a $\mathbb{Q}$-algebra acting on M. We can investigate this equivariant conjecture "locally," on each of the P_p factors of the L-function.

We are far from being able to prove the equivariant Tamagawa number conjecture in full generality, but progress has been made on easier cases. The analytic class number formula has been known at least since Dirichlet, and the Birch and Swinnerton-Dyer conjecture is an area of active research with many partial results; in their original Tamagawa number conjecture paper, [BK90] show that the Tamagawa number conjecture, and thus the l-primary part of the Birch and Swinnerton-Dyer conjecture, holds for elliptic curves with CM. They also spend some time addressing a motive known as the Tate motive.

3.2 The equivariant Tamagawa number conjecture for the Tate motive

The Tate motive $\mathbb{Q}(r)$, is the formal inverse to the Lefschetz motive attached $\mathbb{P}^1$. It is associated to the classical Riemann zeta function, since its L-function over $\mathbb{Q}$ is $L(s, \mathbb{Q}(r)) = \zeta(s+r)$. It is difficult to define in generality, but the Tate motive over the field $\mathbb{Q}_p$ is simply $\mathbb{Q}_p$ acted on by the rth power of the cyclotomic character—that is, if $\chi^{\text{cyclo}} : \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \to \mathbb{Z}_p^\times$ is the cyclotomic character, then $\mathbb{Q}_p(r)$ has the action $\gamma \cdot x = \chi^{\text{cyclo}}(\gamma)^r \cdot x$.

The Tamagawa conjecture for the Tate motive over a finite extension $K/\mathbb{Q}_p$ can be stated:

Conjecture 3.1 (local Tamagawa number conjecture for Tate motives)**.** *There are elements $\epsilon(K/\mathbb{Q}_p, 1-r), [C_\beta] \in K_1(\overline{\mathbb{Q}_p}[\mathrm{Gal}(K/\mathbb{Q}_p)])$ such that if $\beta \in H^1(K, \mathbb{Z}_p(1-r))$ spans a free $\mathbb{Z}_p[\mathrm{Gal}(K/\mathbb{Q}_p)]$-submodule, then the element*

$$[(r-1)!] \cdot \epsilon(K/\mathbb{Q}_p, 1-r) \cdot [\mathrm{per}(\exp^*(\beta) \otimes 1)] \cdot [C_\beta] \cdot \left[\frac{1 - p^{r-1}\phi}{1 - p^{-r}\phi^{-1}}\right] \tag{2}$$

of $K_1(\mathbb{Q}_p^{ur}[\mathrm{Gal}(K/\mathbb{Q}_p)])$ lies in the image of $K_1(\mathbb{Z}_p^{ur}[\mathrm{Gal}(K/\mathbb{Q}_p)])$.

The case where $r \geq 2$ and K is an unramified extension of $\mathbb{Q}_p$ was proven in [BK90] modulo a power of 2 (and modulo an additional conjecture if r is odd). The proof has three ingredients. First, there is a reciprocity law involving the Bloch-Kato exponential, allowing explicit computations of the map $\exp : K \tilde{\to} H^1(K, \hat{\mathbb{Z}}(r)) \otimes \mathbb{Q}$. Second, there is the Coleman exact sequence

$$0 \to \mathbb{Z}_p(1) \to U' \to^{\phi} \mathcal{O}_K[\![\pi]\!]^{\psi=0} \to \mathbb{Z}_p(1) \to 0, \tag{3}$$

where U' is the pro-p part of $U = \varprojlim_n (\mathcal{O}_K[\zeta_{p^n}]^\times)$. Third, there is a basis for the space $\mathcal{O}_K[\![\pi]\!]^{\psi=0}$ over $\mathcal{O}[\![\mathrm{Gal}(K_\infty/K)]\!]$: specifically, $\mathcal{O}[\![\pi]\!]^{\psi}$ is a rank-1 $\mathcal{O}[\![\mathrm{Gal}(K_\infty/K)]\!]$-module (see [PR90]).

There are a few alternate proofs of the reciprocity law of [BK90] , but all of them depend on the exact sequence (3), and neither this exact sequence nor the reciprocity law have easy or obvious generalizations to the case where K is ramified over $\mathbb{Q}_p$.

3.3 Using (ϕ, Γ)-modules

In my thesis I constructed a new and more easily generalizable proof which uses neither the reciprocity law nor the Coleman exact sequence. Instead, I use a reciprocity law from [CC99] to translate conjecture 3.1 into a statement about the image of a certain (ϕ, Γ)-module under the dual map to the Perrin-Riou exponential:

Theorem 3.2 (Cherbonnier-Colmez IV.2.1)**.** *Let p be a prime and let $K/\mathbb{Q}_p$ be finite. Let $\mathrm{Exp}^*_{\mathbb{Q}_p} : H^1_{Iw}(K, \mathbb{Q}_p(1)) \tilde{\to} A_K^{\psi=1}(1)$ be the inverse of the Perrin-Riou exponential. Let T_m be defined for any $K(\zeta_{p^n})$ as $p^{m-n}\,\mathrm{Tr}_{K(\zeta_{p^n})/K(\zeta_{p^m})}$ and extend it linearly to $K[\![t]\!]$. Then*

1. *If n is large enough and $\mu \in H^1_{Iw}(K, \mathbb{Q}_p(1))$, then $T_m(\phi^{-n}(\mathrm{Exp}^*_{\mathbb{Q}_p}(\mu)))$ is an element of $K(\zeta_{p^m})((t))(1)$ independent of n.*
2. *If n is large enough and $\mu \in H^1_{Iw}(K, \mathbb{Q}_p(1))$, then*

$$(T_m \circ \phi^{-n}) \left(\mathrm{Exp}^*_{\mathbb{Q}_p}(\mu) \right) = \sum_{r \geq 0} \exp^*_{\mathbb{Q}_p(1-r)} pr_{m,r}(\mu) \otimes t^{r-1} \tag{4}$$

where $pr_{m,r}$ is the projection of the Iwasawa cohomology onto its mth component, with a twist by r.

This reciprocity law does not require that $K/\mathbb{Q}_p$ be unramified, but holds for arbitrary finite extensions of $\mathbb{Q}_p$. Since this relates Exp^* on $H^1_{Iw}(K, \mathbb{Q}_p(1))$ to $\exp^*$ on $H^1(K, \mathbb{Q}_p(1-r))$, I used it to prove:

Proposition 3.3.

1. *The ring $A_K^{\psi=1}(1)$ mentioned in Theorem 3.2 is a rank one $\Lambda_K = \mathbb{Z}_p[\mathrm{Gal}(K/\mathbb{Q}_p)] \otimes_{\mathbb{Z}_p} \Lambda$-module, where Λ is the Iwasawa algebra.*
2. *If α is spans a free Λ_K-submodule of $A_K^{\psi=1}(1)$, and for some $m \geq 0$ β spans a free $\mathbb{Z}_p[\mathrm{Gal}(K(\zeta_{p^m})/\mathbb{Q}_p)]$-submodule of $H^1(K(\zeta_{p^m}), \mathbb{Z}_p(1-r))$ as in theorem 3.2, then*

$$\exp^*(\beta) = \left(\frac{d^{r-1}}{dt^{r-1}} T_m \phi^{-n} \frac{\alpha}{(r-1)!} \right) \Big|_{t=0}. \tag{5}$$

Though this result is technical and uninteresting in itself, it turns out that if α is known, the quantity on the right-hand side of (5) is easy to calculate if you know α explicitly. A generalization by [PR90] of the Coleman exact sequence allows us to calculate α for $K/\mathbb{Q}_p$ unramified, and thus proves:

Theorem 3.4. *If $r \geq 2$, $p > 2$, and $K/\mathbb{Q}_p$ unramified, then the the local Tamagawa number conjecture holds for the Tate motive $\mathbb{Q}_p(r)$ over K and over $K(\zeta_p)$.*

This gives a new proof of the result of [BK90]. With Matthias Flach I have also proven Conjecture 3.1 in small twists of certain tamely ramified extensions $K/\mathbb{Q}_p$ (see [DF16]).

3.4 Research Goals

My most immediate research goal is to finish our extension of Theorem 3.4 to all tamely ramified finite extensions $K/\mathbb{Q}_p$. Perrin-Riou's generalization of the Coleman sequence does not allow us to compute an exact α, but a careful combinatorial argument on $A_K^{\psi=1} \mod p$ seems to show that the conjecture holds.

In the medium term, I would like to extend our results to $p = 2$; this is not in principle difficult, but requires dealing with some unpleasant details which are not present in the case where p is odd. I also plan to work on computing the $\epsilon(K(\zeta_{p^m})/\mathbb{Q}_p, 1 - r)$ factor for $m > 1$. This would allow us to prove conjecture 3.1 for cyclotomic extensions of unramified extensions of $\mathbb{Q}_p$, and possibly of tamely ramified extensions as well.

In the long term, I'd like to use these and similar techniques to study other motives and their L-functions as well. The reciprocity law of Theorem 3.2 applies to any Galois representation, not just $\mathbb{Q}_p(r)$, and thus can be used to study motives other than the Tate motive. The field of (ϕ, Γ)-modules is still developing and I hope to sharpen these tools, and apply them to reveal more about L-functions and the Tamagawa number conjecture.

References

[BK90] Spencer Bloch and Kazuya Kato, *L-functions and Tamagawa numbers of motives*, The Grothendieck Festschrift, Vol. I, Progr. Math., vol. 86, Birkhäuser Boston, Boston, MA, 1990, pp. 333–400. MR 1086888 (92g:11063)

[CC99] Frédéric Cherbonnier and Pierre Colmez, *Théorie d'Iwasawa des représentations p-adiques d'un corps local*, J. Amer. Math. Soc. **12** (1999), no. 1, 241–268. MR 1626273 (99g:11141)

[CCM+14] Scott T Chapman, Marly Corrales, Andrew Miller, Chris Miller, and Dhir Patel, *The catenary and tame degrees on a numerical monoid are eventually periodic*, Journal of the Australian Mathematical Society **97** (2014), no. 3, 289–300.

[CCM+17] ______, *The catenary degrees of elements in numerical monoids generated by arithmetic sequences*, Communications in Algebra (2017).

[CDHK10] S. T. Chapman, Jay Daigle, Rolf Hoyer, and Nathan Kaplan, *Delta sets of numerical monoids using nonminimal sets of generators*, Comm. Algebra **38** (2010), no. 7, 2622–2634. MR 2674690 (2011g:20099)

[CGH+17] Rebecca Conaway, Felix Gotti, Jesse Horton, Christopher O'Neill, Roberto Pelayo, Mesa Williams, and Brian Wissman, *Minimal presentations of shifted numerical monoids*, arXiv preprint arXiv:1701.08555 (2017).

[CHK09] Scott T Chapman, Rolf Hoyer, and Nathan Kaplan, *Delta sets of numerical monoids are eventually periodic*, Aequationes mathematicae **77** (2009), no. 3, 273–279.

[DF16] Jay Daigle and Matthias Flach, *On the local tamagawa number conjecture for tate motives over tamely ramified fields*, Algebra and Number Theory **10** (2016), no. 6, 1221–1275.

[FK06] Takako Fukaya and Kazuya Kato, *A formulation of conjectures on p-adic zeta functions in noncommutative Iwasawa theory*, Proceedings of the St. Petersburg Mathematical Society. Vol. XII, Amer. Math. Soc. Transl. Ser. 2, vol. 219, Amer. Math. Soc., Providence, RI, 2006, pp. 1–85. MR 2276851 (2007k:11200)

[GGMFVT15] JI García-García, MA Moreno-Frías, and A Vigneron-Tenorio, *Computation of delta sets of numerical monoids*, Monatshefte für Mathematik **178** (2015), no. 3, 457–472.

[GS17] Alfred Geroldinger and Wolfgang Schmid, *A realization theorem for sets of lengths in numerical monoids*, arXiv preprint arXiv:1710.04388 (2017).

[OP17] Christopher ONeill and Roberto Pelayo, *Factorization invariants in numerical monoids*, Algebraic and Geometric Methods in Discrete Mathematics **685** (2017), 231.

[OPTW16] Christopher ONeill, Vadim Ponomarenko, Reuben Tate, and Gautam Webb, *On the set of catenary degrees of finitely generated cancellative commutative monoids*, International Journal of Algebra and Computation **26** (2016), no. 03, 565–576.

[PR90] Bernadette Perrin-Riou, *Théorie d'Iwasawa p-adique locale et globale*, Invent. Math. **99** (1990), no. 2, 247–292. MR 1031902 (91b:11116)

[ST15] Ian Stewart and David Tall, *Algebraic number theory and fermat's last theorem*, CRC Press, 2015.