Email: eva.goedhart@williams.edu, Phone: (484) 868-6486
Website: www.evagoedhartphd.com
Skype: eva.goedhart
Pronouns: she, her, hers

Summary

My research program stems from solving *Diophantine equations*, polynomial equations with integer coefficients for which integral solutions are sought. Though simple to state, Diophantine equations often require tools from many different areas to solve, such as number theory, algebra, combinatorics, graph theory, and analysis. My work thus far includes factoradic happy numbers, families of Diophantine equations, Thue equations, b-invisible forests, connecting 2-adic valuations with trees, and privileged parking functions. These projects range from work with academic colleagues to undergraduate student research projects. With the versatility of the types of projects available, Diophantine equations are excellent for a capstone project but also an introduction to mathematical research.

1 Introduction

Consider an integral function $f : \mathbb{Z}^+ \times \mathbb{Z}^+ \times \mathbb{Z}^+ \to \mathbb{Z}$ given by $f(x, y, z) = 2^x + 3^y - 4^z$. If I am only interested in the integer solutions (x, y, z) to the equation $f(x, y, z) = 0$, then this is an example of a *Diophantine equation.*

The main goal in Diophantine equations is to find all possible integer solutions.

In the example, suppose that a solution $x, y, z \neq 0$ exists in integers. Then $2^x + 3^y = 4^z$. Now, the left hand side of the equation will always be odd while the right hand side is even, a contradiction. Therefore there are no integer solutions to $f(x, y, z) = 0$. Though this type of argument is a common technique used throughout Diophantine Analysis, the problems I work on require more complicated methods.

A focus of study for hundreds of years, *Diophantine Analysis*, the study of Diophantine equations and inequalities, remains a vibrant area of research. It has yielded a multitude of beautiful results and has wide ranging applications in other areas of mathematics, in cryptography, biology, and in physics. One of the most famous results is that of Fermat's Last Theorem, proven by Wiles and Taylor nearly 350 years after it was stated. The rich history of Diophantine equations and flexibility to other fields lends itself well to collaborations and can be appealing to mathematics majors, science majors, and some humanities majors.

I have published work on several families of Diophantine equations (see [7–9]). As an example, families of equations such as $X^2 + D = Y^N$, where D is a product of powers of a small number of primes have been studied for decades. Some of these families have no integer solutions.

Theorem 1 (G. and Grundman, [7]) *Let $N > 1$ be an integer. Then the equation*

$$NX^2 + 2^L 3^M = Y^N$$

has no solutions with L, M, X, $Y \in \mathbb{Z}^+$ and $\gcd(NX, Y) = 1$.

Another kind of integral function, the *happy function*, can be found in my most recent publication with Josh Carlson (Williams College), and Pamela Harris (Williams College) [3]. We describe an extension of the happy function, $S_{e,!} : \mathbb{Z}^+ \to \mathbb{Z}^+$ by $S_{e,!}(n)$ which is the sum of the e-powers of the digits of factorial representation of n. Then n is a *happy number* if the iterative process of repeatedly applying $S_{e,!}$ terminates in the number one. As an example, 2020 is a factoradic happy number since $S^5_{2,!}(2020) = 1$. There are infinitely many happy numbers. Here rather than finding and enumerating all of them, we prove the following result on the length of sequences of factoradic happy numbers.

Theorem 2 (Carlson, G., Harris, [3]) *For $e \in \{1, 2, 3, 4\}$ and for any e-power factoradic fixed point b of $S_{e,!}$, there exists arbitrarily long sequences of e-power factoradic b-happy numbers.*

2 Current Work in Diophantine Analysis

Each additional area of my research draws upon some aspect of Diophantine Analysis. My collaborators, faculty, graduate students, and undergraduates students, all bring valuable tools of their own to the projects that I pursue. In the sections below, I describe those projects.

2.1 Relative Thue Equations

Let $F(X, Y)$ be an irreducible homogeneous polynomial of degree $n \geq 3$ with integer coefficients and let m be a nonzero integer. Then the Diophantine equation

$$F(X, Y) = m$$

is called a *Thue equation*. In 1909, Axel Thue proved that Thue equations have only finitely many solutions over the integers [17]. Individual such Thue equations of small degree such as

$$X^3 - 3X^2Y - Y^3 = 1$$

can now be solved over the integers using algorithms that are implemented in various computer algebra programs. (See [18] for details.) In this case, the only integer solutions of the above equation are $(x, y) = (1, 0)$, $(0, -1)$, $(-1, 1)$, $(2, 1)$, $(-3, 2)$, and $(1, -3)$, as seen in [19].

Since 1990, starting with Thomas's result [16], several infinite families of Thue equations parametrized $t \in \mathbb{Z}$, which can not be solved by computer algebra system, have been completely solved over the integers Of particular interest to me, is the extension of Thomas's work on parametrized families of the simplest cubic, quartic, and sextic forms, given as

$F_t^3(X,Y)=X^3-(t-1)X^2Y-(t+2)XY^2-Y^3,$
$F_t^4(X,Y)=X^4-(t-1)X^3Y-6X^2Y^2+(t-1)XY^3+Y^4,$ and
$F_t^6(X,Y)=X^6-2(t-1)X^5Y-(5t+10)X^4Y^2-20X^3Y^3+5(t-1)X^2Y^4+(2t+4)XY^5+Y^6,$

where $t \notin \mathbb{Z}$ is an imaginary quadratic number. The solutions of the *relative Thue equation* $F_t^3(X,Y) = \mu$, where $X, Y \in \mathbb{Z}_{\mathbb{Q}(t)}$, and μ is a root of unity in $\mathbb{Z}_{\mathbb{Q}(t)}$ can be found in the work of Heuberger, Pethő, and R.F. Tichy [11], and Heuberger [12]. They separately used the hypergeometric method and Baker's method to solve that family of relative Thue equations.

Now, Daniel Wisniewski (DeSales University), postdoctoral student Bernadette Faye (University Gaston Berger of Saint Louis, Senegal), graduate student Benjamin Earp-Lynch (Carelton University, Canada) and I are adapting the hypergeometric method, Baker's method, Padé approximations, combining them with results more advanced computational work to complete the following project.

Theorem 3 (Earp-Lynch, Faye, G., Wisniewski) *Let t be an imaginary quadratic integer with $|t| \geq 163$. Then family of Thue equations*

$$F_t^{(4)}(X,Y) = X^4 - (t-1)X^3Y - 6X^2Y^2 + (t-1)XY^3 + Y^4 = \mu$$

for μ a root of unity in $\mathbb{Q}(t)$ has no solutions $(X,Y) \in \mathcal{O}^2_{\mathbb{Q}(t)}$ with $|Y| \geq 2$.

More recently Gaál, Jadrijević, and Remete [6] solved the above quartic and sextic families of Thue equations $F_t^k(X,Y) = \mu$ for $k = 4, 6$ over the imaginary quadratic number field with the parameter $t \in \mathbb{Z}$. However, since they restrict their attention to integer parameters, their methods are quite different than our own.

2.2 2-Adic Valuation of n in a Tree

Let $n = x^2 + 7$ be an integer. What is the minimal $x \in \mathbb{Z}^+$ so that the *2-adic valuation* of n, the exact number of 2's that divide $x^2 + 7$, is known to be $c \in \mathbb{Z}^+$ for some fixed c? This question can be formulated as a Diophantine equation.

Problem 1 *For a given $c \in \mathbb{Z}^+$, find a formula for the minimal integer solutions (x, y) of*

$$x^2 + 7 = 2^c y.$$

Maila Brucal-Hallare (Norfolk State University), Bianca Thompson (Westminster College), undergraduate student Ryan Riley (Williams College), and I use computational methods to devise a recursive algorithm in terms of c. This computational information can be

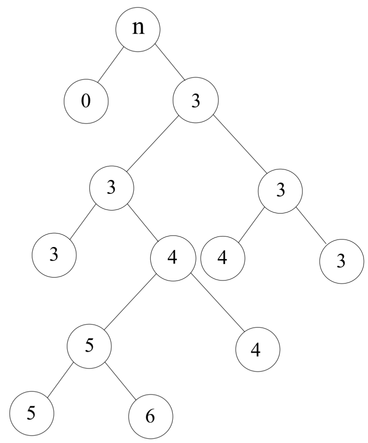

Figure 1: 2-adic valuation of n

viewed in an infinite binary tree. Note that this is an incomplete image. We would label each *level* or horizontal line of nodes in the tree, starting with level 0 at the top. Also, for levels beyond the third one, there will be exactly four nodes at every level (not pictured in Figure 1). Aside from the topmost node, which is the root of the tree, the labels on the nodes correspond to the value of c for the leaves of the tree. The other nodes are labeled with a lower bound on c. We can determine x, and subsequently y, from this tree from labeling the branches in each level.

Using *defective Lucas pairs*, a Diophantine equation technique, we next aim to find a closed formula for solutions (x, y). A pair of algebraic integers is called a Lucas pair if their quotient is not a root of unity and their product and sum are nonzero coprime integers. The Lucas pair is called t-defective, for $t \in \mathbb{Z}^+$, if the pair has a certain property depending on the divisors of a number constructed from the Lucas pair. For almost all $t \in \mathbb{Z}^+$, the t-defective Lucas pairs have been enumerated [2]. Comparing a t-defective Lucas pair for some t, constructed from a hypothetical solution, to the list of known defective Lucas pairs can lead to finding all solutions to the Diophantine equation above.

2.3 From b-Visible to Visible

Imagine that you were standing at the edge of a forest in which the trees were all planted only on vertices of the integer lattice. Marking the southwestern most corner of the forest as the origin, where you are standing, all the trees fall on points of the form (r, s) where r, $s \in \mathbb{Z}^+$. Looking at the forest, you notice that some trees are visible and some are hidden from view. This line of sight can be modeled by a linear function through the origin, the solid line on Figure 2. If our sight was mapped in curves instead, as in the dotted line in Figure 2, which trees in the lattice would now be visible and invisible? To answer this question Goins, Harris, Kubik, and Mbirika [10] define line of sight along curves of the form ax^b for $b \in \mathbb{Z}^+$ fixed. Then integer lattice point (r, s) is called *b-visible* from the origin if it

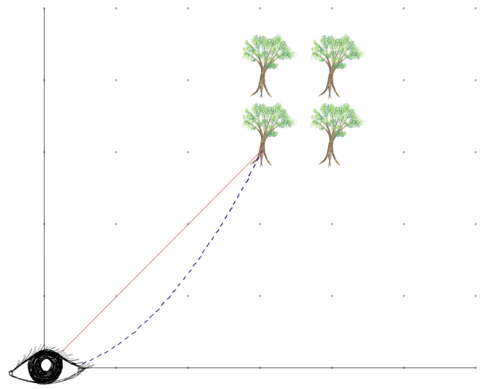

Figure 2: b-visibility of a 2×2 forest

lies on some curve of the form ax^b, for some $a \in \mathbb{Q}$ and if there are no other integer lattice points blocking the view of that point. Points are *b-invisible* if they are not b-visible. We ask the natural question to follow this.

Problem 2 *Given a specific sized rectangular forest, how close to the origin can we find a b-invisible forest of that size?*

For linear visibility, $b = 1$, the minimum distance has been bounded by Laishram and Luca [13]. With my Williams College colleagues Josh Carlson, Pamela Harris, Haydee Lindo, and graduate student Santiago Estupiñan Salmanca (Universidad de los Andes, Colombia), I am generalizing this to b-invisible rectangles using an integral function to characterize a relationship between b-visible and 1-visible points. For $b \in \mathbb{Z}^+$, define a function $f_b : \mathbb{Z}^+ \times \mathbb{Z}^+ \to \mathbb{Z}^+ \times \mathcal{Y}$, where $\mathcal{Y} = \{y \in \mathbb{Z}^+ : y \text{ is square-free}\}$, by

$$f_b(r,s) = (r, \prod_{\substack{p \text{ prime} \\ p^b | s}} p).$$

The point (r, s) is b-visible if and only if $f_b(r, s)$ is 1-visible. If $(x, y) \in \mathbb{Z}^+ \times \mathcal{Y}$, then the preimage $f_b^{-1}(x, y) = \{(x, ay^b) \in \mathbb{Z}^+ \times \mathbb{Z}^+ : a \text{ is } b\text{-power free}\}$. Together, we are examining the preimage of 1-visible points to find ways to use the known bounds on 1-invisible rectangles to bound the b-invisible rectangles.

2.4 Privileged Parking Functions

Introduced to me by Pamela Harris, as part of the AIM UP REU program, undergraduate students Saisha Goboodun (Williams College), Sasha Ruth Sepulveda (University of Arizona), Jingyi Wu (Mount Holyoke College), and I consider a generalization of parking functions called *privileged parking function.* Though at different institutions, we will continue this work during the upcoming semester.

Generally, a parking function is a sequence of parking spot preferences for a list of cars to park along a one way street. *Privileged parking functions* allow for the cars to back up a specific amount to find a parking spot depending on their order in line. Figure 3 created by Jingyi Wu describes the choices that each car has as they are looking for a parking spot. Specifically, the i-th car in a line of $n \in \mathbb{Z}^+$ cars to park along the street can back up at

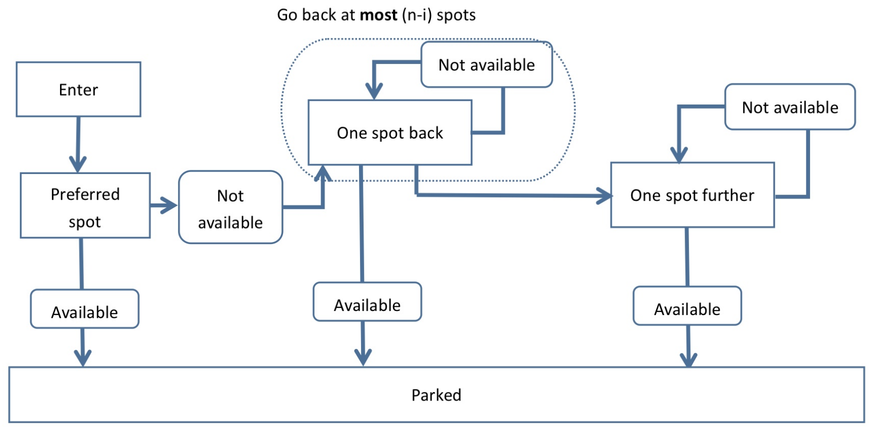

Figure 3: Privileged Parking Function Flow Chart

most $n - i$ spots for $1 \leq i \leq n$.

There are several ways to define generalizations that allow backing up, see [4] for examples. We explore the relationship between privileged parking functions and other types of generalizations of parking functions in order to determine the exact number of privileged parking functions for a given $n \in \mathbb{Z}^+$.

Problem 3 *Find a closed formula for the number of privileged parking functions.*

We have begun by programming python to find all privileged parking functions for small values of n. The sequences of number of privileged parking functions for a given n is not a known sequence in OEIS. The techniques from Diophantine analysis, creating integral functions, lend themselves well to working on this combinatorial problem of counting different ways that we can parking n cars.

3 Future Opportunities for Students

There are many places to include undergraduate, graduate students, and faculty in my research program depending on their mathematical background. With today's technologies all of these collaborators may be at different institutions around the world. Below are projects that I plan to pursue.

3.1 Relative Thue Inequalities and Continued Fractions

One natural way to continue from Thue equations is to replace the equality with an inequality. For example, Lettl, Pethő, and Voutier [14] solve the families $F_t^k(X,Y) \leq p(t)$ over the integers, where $p(t)$ is an integral polynomial of $t \in \mathbb{Z}$, and $k = 3, 4, 6$ as in Section 2.1. What if we consider relative Thue inequalities?

Project 1 *For an imaginary quadratic integer t, find all solutions $(x, y) \in \mathbb{Z}^2_{\mathbb{Q}(t)}$ to the relative Thue inequality $|F_t^4(X,Y)| \leq 6|t| - 7$.*

This project will require implementing continued fractions on non-Euclidean imaginary quadratic fields. This area of research is still quite new and is Daniel E. Martin's most recent work [15]. Undergraduate student Jason Meintjes (Williams College) and I have been studying Martin's work. By explicitly computing of the constants demonstrated to exist in Martin's work, we will be able to solve the above Thue inequality by synthesizing and extending with other known methods.

3.2 SAGE Programming in Cryptography

Amy Feaver (The King's University, Canada) and I led a cryptography project [1] with undergraduate students to create an interactive sage wiki page to allow users to explore and program with different cryptosystems. The goals of the project are to create a platform for students to learn some basic cryptography, to develop SAGE programming skills, as well as to provide another resource for professors teaching cryptography in upcoming semesters.

Project 2 *Create more interactions for modern cryptosystems and refine the code used for the classical cryptosystems.*

This project allows students to learn basic concepts of programming in SAGE while also learning the basics of cryptography with the addition of creating a public facing product.

3.3 Extensions of Diophantine Equations

Lastly, I list a few Diophantine equations projects that are specifically designed for undergraduate students.

Project 3 *Suppose k, n, x, $y \in \mathbb{Z}^+$ such that $n > 1$ and*

$$nx^2 + 3^{2k} = y^n$$

with $\gcd(nx, y) = 1$. If $n \equiv 7 \pmod 8$, prove that y is odd. Given that $nu^2 + v^2 = y^s$ and $x\sqrt{-n} + 3^k = \pm(u\sqrt{-n} + v)^t$ such that $n = st$, $t > 1$, and $\gcd(u, v) = 1$, prove that $3|u$ or $3|v$. Given $\gamma = 3^k + u\sqrt{-n}$ and $\delta = -3^k + u\sqrt{-n}$, prove that (γ, δ) is a t-defective Lehmer pair. Prove that $t \neq 5$.

Project 4 *Suppose x, y, $z \in \mathbb{Z}^+$ such that*

$$(x^5-2)(y^5-2)=(z^5-2)^2.$$

Given that $\alpha = \sqrt[5]{1/(x^5-1)}$ and $\beta = y/z^2$, can you prove that β is a convergent of the continued fraction expansion of α. Given that $\beta = p_J/q_J$ and given an upper bound for z, derive an upper bound for q_J. Further, given an upper bound for z, derive a lower bound for the partial quotients of α. Use a computer to calculate the first ten partial quotients, a_j of α. Compute q_j of α for $1 \leq j \leq 10$.

I look forward to sharing the richness and depth of Diophantine analysis with students and exploring other opportunities for research based on student interest.

References

[1] S. Arpin, C. Camacho-Navarro, H.P. Chaos, A. Feaver, E. Goedhart, S. Lapan, R.L. Miller, A. Newton, and N. Sahajpal."Sage Interactions - Cryptography", `https://wiki.sagemath.org/interact/cryptography`.

[2] Y. Bilu, G. Hanrot, and P.M. Voutier, "Existence of primitive divisors of Lucas and Lehmer numbers, with appendix by M. Mignotte", *J. Reine Angew. Math.* **539** (2001) 75–122.

[3] J. Carson, E. Goedhart, and P. Harris,"Sequences of consecutive factoradic happy", *Rocky Mountain J. of Math.* **50** (2020) no. 4, 1241–1252.

[4] A. Christensen, P.E. Harris, Z. Jones, M. Loving, A. Ramos Rodríguez, J. Rennie, G. Rojas Kirby, "A generalization of parking functions with backward movement", *The Electronic Journal of Combinatorics*, **27** no. 1 (2020), P1.33. https://doi.org/10.37236/8948

[5] B. Faye, E. Goedhart, B. Earp-Lynch, and D. Wisniewski, "The complete solution to a quartic family of Thue equations over imaginary quadratic number fields", in preparation.

[6] I. Gaál, B. Jadrijević, and L. Remete. "Simplest quartic and simplest sextic Thue equations over imaginary quadratic fields", *J. Number Theory* (2018), 1–17.

[7] E. Goedhart and H.G. Grundman, "On the Diophantine equation $NX^2+2^L3^M=Y^N$", *J. Number Theory* **141** (2014), 214–224.

[8] E. Goedhart and H.G. Grundman, "Diophantine approximation and the equation $(a^2cx^k-1)(b^2cy^k-1)=(abcz^k-1)^2$", *J. Number Theory*, **154** (2015), 74–81.

[9] E. Goedhart and H.G. Grundman, "On the Diophantine equation $X^{2N}+2^{2\alpha}5^{2\beta}Y^{2\gamma}=Z^5$", *Period. Math. Hung.* **75** (2017), no. 2, 196–200.

[10] E.H. Goins, P.E. Harris, B. Kubik, and A. Mbirika, "Lattice Point Visibility on Generalized Lines of Sight", *The American Mathematical Monthly*, **125** no. 7, (2018), 593–601. DOI: 10.1080/00029890.2018.1465760

[11] C. Heuberger, A. Pethő, and R.F. Tichy, "Thomas' family of Thue equations over imaginary quadratic fields", *J. Symbolic Comput.* **34** (2002), no. 5, 437–449.

[12] C. Heuberger, "All solutions to Thomas' family of Thue equations over imaginary quadratic number fields", *J. Symbolic Comput.* **41** (2006), no. 9, 980–998.

[13] S. Laishram and F. Luca, "Rectangles of nonvisible lattice points", *J. Integer Sequences***18** (2015), Article no. 15.10.8.

[14] G. Lettl, A. Pethő, and P.M. Voutier, "Simple families of Thue inequalities", *Trans. Amer. Math. Soc.* **351** (1999), no. 5, 1871–1894.

[15] D.E. Martin, "Continued fractions in non-Euclidean imaginary quadratic fields," *arXiv.org*, preprint arXiv:1908.00121, (2019).

[16] E. Thomas, "Complete solutions to a family of cubic Diophantine equations", *J. Number Theory* **34** (1990), no. 2, 235–250.

[17] A. Thue, "Uber Annäherungswerte algebraischer Zahlen", *J. Reine Angew. Math.* **135** (1909), 284–305.

[18] N. Tzanakis and B.M.M. de Weger, "On the practical solution of the Thue equation", *J. Number Theory* **31** (1989), 99–132.

[19] N. Tzanakis, "The Diophantine equation $x^3 - 3xy^2 - y^3 = 1$ and related equations", *J. Number Theory*, **18** (1984), 192–205.

[20] V. Zeigler, "On a family of cubics over imaginary quadratic fields", *Period. Hung. Math.* **51** (2005), no. 2, 109–130.