Research Statement
Eva G. Goedhart

My research is in Algebraic Number Theory, more specifically in Diophantine Analysis, the study of Diophantine equations and inequalities. A Diophantine equation is an equation with integer (or rational) coefficients that is to be solved in integers (or rational numbers). A focus of study for hundreds of years, Diophantine Analysis 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, and in the natural sciences.

In my dissertation, I prove that the equations in some specific families of Diophantine equations have no positive integer solutions. In general, I accomplish this by assuming a hypothetical solution exists and then applying various techniques to reach a contradiction. As a straightforward example, suppose that \( a, b, c \) are positive integers such that \( 2^a + 3^b = 4^c \). Since \( 2^a \) is even and \( 3^b \) is odd, the left side of the equation is odd while the right side is even, a contradiction. Therefore the equation \( 2^x + 3^y = 4^z \) has no solutions in positive integers. Though this type of argument is a common technique used throughout Diophantine Analysis, typical problems require much more complicated methods.

Below, I present the three main theorems from my dissertation [8] (see also [9–11]), and two problems that I am currently working on. For each, I give some context and briefly describe the primary method that I use in the proof. In the next section, I state one of the results on bounding linear recurrences from my Master’s research [4–6]. Finally, I describe my plans for future work including some projects appropriate for undergraduate research.

Dissertation Research

Equations of the form \((x^k - 1)(y^k - 1) = (z^k - 1)\) and \((x^k - 1)(y^k - 1) = (z^k - 1)^2\) with \( k \geq 4 \), have no solutions [2]. In the theorem below, I prove that equations in a generalization of the second family have no solutions.

**Theorem 1** Let \( a, b, c, k \in \mathbb{Z}^+ \) with \( k \geq 7 \). The equation

\[
(a^2cx^k - 1)(b^2cy^k - 1) = (abcz^k - 1)^2
\]

has no solutions in integers \( x, y, z > 1 \) with \( a^2x^k \neq b^2y^k \).

I prove Theorem 1 using Diophantine approximation, the study of how closely an irrational number \( \alpha \) can be approximated by a rational number \( \beta \). There are numerous results providing lower bounds of \( |\alpha - \beta| \) in terms of the denominator of \( \beta \). One way to apply this method is to construct an \( \alpha \) and \( \beta \) from a given hypothetical solution such that \( |\alpha - \beta| \) is small. For example, in the proof of Theorem 1, I use
\( \alpha = \sqrt[3]{a^2c/(a^2cx^k - 1)} \) and \( \beta = y/z^2 \). Applying known bounds on \( |\alpha - \beta| \) for particular types of \( \alpha \) can often result in a contradiction to most of the cases, usually leaving a finite number of possible values of \( \alpha \) and \( \beta \). For these, if the difference \( |\alpha - \beta| \) is small enough then \( \beta \) must be a convergent of the continued fraction expansion of \( \alpha \). Then computations and standard properties of continued fractions may lead to a contradiction.

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. More recently, there has been interest in the related family of equations, \( NX^2 + 2^K = Y^N \), showing that under certain conditions there are no solutions [13,17].

**Theorem 2** 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 \( \gcd(NX,Y) = 1 \).

I use defective Lehmer pairs in proving Theorem 2. A pair of algebraic integers is called a Lehmer pair if their quotient is not a root of unity and their product and square of their sum are nonzero coprime rational integers. The Lehmer 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 Lehmer pair. For almost all \( t \in \mathbb{Z}^+ \), the \( t \)-defective Lehmer pairs have been enumerated [1]. Comparing a \( t \)-defective Lehmer pair for some \( t \), constructed from a hypothetical solution, to the list of known defective Lehmer pairs can lead to a contradiction.

The Tijdeman-Zagier conjecture states that \( x^p + y^q = z^r \) has no solutions in positive integers when \( p, q, r > 2 \) and \( \gcd(x,y,z) = 1 \). For \( N = 2, 3, \) and \( 5 \) the family \( X^{2N} + Y^2 = Z^5 \) has no solutions [3,7,16]. I extend this work to all \( N > 1 \) when \( Y \) is a product of powers of 2, 5, and an arbitrary prime \( p \).

**Theorem 3** Let \( p \) be an odd prime, \( \alpha \geq 1 \), and \( \beta, \gamma \geq 0 \) be integers. The equation

\[ X^{2N} + 2^{2\alpha} 5^{2\beta} p^{2\gamma} = Z^5 \]

has no solutions with \( X, Z, N \in \mathbb{Z}^+ \), \( N > 1 \), and \( \gcd(X,Z) = 1 \).

The proof of Theorem 3, relies on the modular approach, a method that evolved from the proof of Fermat’s Last Theorem. In particular, working with a fixed hypothetical solution, there exists an elliptic curve \( E \) (often called a Frey curve), whose coefficients depend only on the given solution. If \( E \) exists, then through rather deep results on Galois representation theory, \( E \) must arise from a newform, \( f \) of level \( N_n \) where \( N_n \) divides the conductor of \( E \). The newform, \( f \), captures valuable information about the solution that can be used to achieve a contradiction.
CURRENT RESEARCH

As a continuation of Theorem 3, Helen G. Grundman and I are extending the result to include any even number $Y$ rather than an even number with at most one prime divisor other than 5, as currently stated.

Another line of research stemming from the Tijdeman-Zagier conjecture concerns families of equations in which the base numbers are related to each other. For example, $(am - 1)^x + m^y = (am + 1)^z$ has no solutions for $x > 2$ and $a$ odd [14]. When $a$ is even, the equation below can be reformulated so that I can consider the following problem.

**Problem 1** Let $a, k \in \mathbb{Z}^+$ with $a > 1$ odd. For what values of $k$ does the equation

$$(2^k am - 1)^x + m^y = (2^k am + 1)^z$$

have no solutions $m, x, y, z \in \mathbb{Z}^+$ with $x > 2$.

I have begun work on Problem 1 and a variant there of, utilizing *linear forms in logarithms*. A linear form in logarithms is a linear combination of logarithmic terms, $b_1 \log \alpha_1 + \ldots + b_n \log \alpha_n$ where $\alpha_i$ are algebraic numbers and $b_i$ are integers. From a hypothetical solution to a Diophantine equation one constructs a linear form in logarithms that can be bounded above and below in such a way as to produce bounds on the values of the variables. Various methods, including continued fractions, can be used on the remaining cases.

MASTER’S RESEARCH

The Fibonacci sequence is a very basic example of a sequence generated by a *second-order linear recurrence* or *difference equation*. In my Master’s thesis, I studied both second-order recurrences and third-order difference equations. For each type of recurrence, I find explicit and often sharp upper bounds for the sequences. For example, below is the statement of a result giving an explicit bound on a second-order linear recurrence.

**Theorem 4** For $k > 1$, define the sequence $\{b_k\}$ with initial values $b_0 = 0$, $b_1 = -1$, and coefficients $\alpha_k, \beta_k \in [0, A]$ by the recurrence

$$b_k + \alpha_k b_{k-1} + \beta_k b_{k-2} = 0.$$  

For a given $n \geq 76$, write $n - 1 = 15q + r$ with $q, r \in \mathbb{Z}$ such that $0 \leq r \leq 14$. If $\frac{2}{3} < A < \frac{3}{4}$, then $|b_n| \leq U_n$ where

$$U_n = \begin{cases} 2^{-4r+10\lfloor \frac{A}{2} \rfloor + 10q + 3q-7\lfloor \frac{A}{4} \rfloor - 7} A^{9q + r - \lfloor \frac{A}{4} \rfloor - 1}, & \text{if } r \equiv 2 \pmod{5}, \\ 2^{2r-5\lfloor \frac{A}{2} \rfloor} 3^{3q-r+3\lfloor \frac{A}{4} \rfloor} A^{9q + r - \lfloor \frac{A}{4} \rfloor}, & \text{otherwise.} \end{cases}$$

3
Future Research

Below, I describe my plans for further extending my dissertation work along with some new directions that I will investigate.

I will examine the generalization of Theorem 1 in which \( x, y, z \) are allowed to be negative with absolute value greater than one. I have confidence that the same methods will apply, though the proof will require more careful estimates. If, on the other hand, \(|x| = 1\), then the basic structure of the equation is changed. I believe some progress can still be made, using the modular approach.

Also for Theorem 1, I hope to prove that there are no solutions when \( 4 \leq k \leq 6 \). I think that the proof of Theorem 1 will easily adapt to the case \( k = 6 \), but I expect that the other cases will require additional methods.

Theorem 3 is a special case of the family \( C^2X^{2N} + 2^{2a_5}5^{2\gamma}p^{2\gamma} = Z^5 \) with \( C \in \mathbb{Z} \). I have noticed that for some values of \( C \) modifying the proof of Theorem 3 is quite straightforward. I hope to blend Lehmer number techniques with the modular approach in order to deal with other values of \( C \).

New directions for my research include exploring different families of equations and new methods. For example, the family of equations \( 1^k + 2^k + \ldots + x^k = y^n \) has been studied for over a century. It has been solved for \( 1 \leq k < 170 \) for \( n \) even [15], using local methods, the modular approach, linear forms in logarithms, elliptic curves, computer calculations, and previously known results. I will examine variations of this family using similar techniques.

In another direction, I am interested in proving that certain equations have infinitely many solutions. For example, for \( n \in \mathbb{Z}^+ \), the equations \( x^4 \pm ny^3 = z^2 \), have infinitely many coprime solutions [12].

Lastly, I list a few possible projects that are accessible to undergraduate students.

**Student Project 1** 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 \((\gamma, \delta)\) is a \( t \)-defective Lehmer pair. Prove that \( t \neq 5 \).

**Student Project 2** Suppose \( \ell > 1, m, n, x, y \in \mathbb{Z}^+ \) such that \( n > 1 \) and \( nx^2 + 2^{2\ell+1}5^{2m} = y^n \) with \( \gcd(nx, y) = 1 \). In which number field can you factor the left hand side? Prove those factors are relatively prime using the norms of their sum and product. Given that \( 2^\ell 5^m \sqrt{2} + x\sqrt{-n} = (u\sqrt{2} + v\sqrt{-n})^t \) with \( t|2n \), prove that \( u|2^\ell 5^m \) and \( \gcd(v, 10) = 1 \). If \( \gamma = 2^\ell 5^m \sqrt{2} + v\sqrt{-n} \), then what must \( \delta \) be in order for \((\gamma, \delta)\) to be a Lehmer pair?

**Student Project 3** 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 \( \beta \) is a convergent
of the continued fraction expansion of $\alpha$. 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 $\alpha$. Use a computer to calculate the first ten partial quotients, $a_j$ of $\alpha$. Compute $q_j$ of $\alpha$ for $1 \leq j \leq 10$.

References


