RESEARCH STATEMENT

GREG KNAPP

1. Introduction

I am currently a number theorist who is also also interested in logic and computation. The major theme that runs throughout my research is the utility of complexity: by measuring the complexity of different mathematical objects (rational numbers, polynomials, proofs, etc.), we can find useful bounds on the number and types of solutions to classical problems.

My most recent work concerns bounding the number of solutions to certain Diophantine equations by relating those solutions to rational approximations of algebraic numbers. My results are both asymptotic (depending on certain parameters constraining the type of Diophantine equation under examination) and explicit (when those parameters are fixed, I find bounds on the implicit constants involved in the asymptotic estimates). My PhD dissertation will include these bounds along with auxiliary bounds about the distances between roots of polynomials with integer coefficients.

My master's thesis explored the provability of Minkowski's Linear Forms Theorem (a foundational theorem in the branch of number theory known as the geometry of numbers) in the system of first-order arithmetic known as Elementary Function Arithmetic (a set of axioms which is much weaker than the standard Zermelo-Fraenkel set theory axioms under which we typically work). I maintain active interest in this and similar projects, like decidability problems. For instance, is there an algorithm which, on input $f(x_1, \ldots, x_n) \in \mathbb{Q}[x_1, \ldots, x_n]$, decides whether or not $f(x_1, \ldots, x_n) \geqslant 0$ for all $x_1, \ldots, x_n \in \mathbb{Q}$?

In this statement, I will describe my current work on and my future plans for improving the bounds on the number of solutions to Thue's Inequality and I will follow that up with descriptions of my interests in other projects in number theory, logic, and analysis.

2. Thue's Inequality

2.1. **Current Work.** My thesis project concerns the following problem about solutions to a polynomial inequality. Let $F(x, y)$ be an irreducible *integral binary form* (meaning that $F(x, y)$ is a homogeneous polynomial in two variables and has integer coefficients) of degree $n \geqslant 3$. Let $h \in \mathbb{Z}_{>0}$. The main motivating question of my research is: how many solutions are there to the inequality

$$|F(x, y)| \leqslant h \tag{1}$$

for $x, y \in \mathbb{Z}$? It is not obvious that there are only finitely many, though Thue proved this in 1909 in [20], resulting in the inequality (1) being named *Thue's inequality.*

Mahler later (1933) gave upper bounds on the number of integer-pair solutions to (1) by considering the problem geometrically. He noted that by taking x and y to be real variables rather than integer variables, the inequality $|F(x, y)| \leqslant h$ corresponds to a region of the xy-plane, like in figure 1.

Mahler's insight was to use intuition from the geometry of numbers, which indicates that the number of integer-pair solutions to (1) should be approximately equal to the volume of the region bounded by the curve $|F(x, y)| = h$. A quick change of variables relates the volume of the region bounded by the curve $|F(x, y)| = h$ to the volume of the region bounded by the curve $|F(x, y)| = 1$ and in [11], Mahler gives an upper bound for the volume of the region bounded by $|F(x, y)| = 1$.

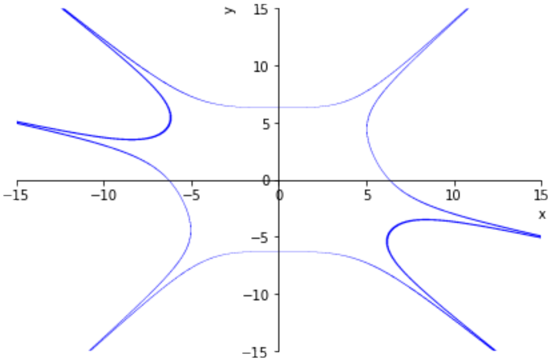

Figure 1. $|x^5 + 3x^4y - y^5| = 10000$

Consequently, when counting the number of solutions to (1), it typically suffices to count the number of integer pair solutions to

$$|F(x, y)| = 1. \tag{2}$$

In my thesis, I improve both asymptotic and explicit upper bounds on the number of solutions to (1) and (2) in particular contexts. Before stating these results, however, we need to take note of Siegel's observation in [17] that the number of nonzero summands in $F(x, y)$ should play an important role in the number of solutions to (1). Roughly speaking, this is because solutions (p, q) to (2) correspond to good rational approximations $\frac{p}{q}$ of roots of $f(Z) := F(Z, 1)$. Rational numbers cannot approximate the properly complex roots of $f(Z)$ very well, so the number of solutions to (2) should be controlled by the number of real roots of $f(Z)$, which is in turn controlled by the number of nonzero summands in $f(Z)$ (see Lemma 1 in [16]). To that end, suppose that $F(x, y)$ is the sum of $s + 1$ nonzero monomials.[1]

Note that the correspondence between solutions, (p, q), and rational numbers, $\frac{p}{q}$, is only one-to-one if $\gcd(p, q)$ is guaranteed to be 1. This is guaranteed for solutions to (2), but is not guaranteed for solutions to (1). To handle this situation, we say that a solution to (1) is *primitive* if $\gcd(p, q) = 1$ and we first count only primitive solutions to (1). We can than compute bounds on the total number of solutions from bounds on the number of primitive solutions using partial summation methods as in [12].

2.1.1. *Results.* My asymptotic result stems from an approach to this problem initiated by Mueller and Schmidt in the 1980s, the major ideas of which are contained in [12]. They classify each solution as being large, medium, or small, and they use different techniques to find upper bounds on the number of each different type of solution. Mueller and Schmidt find an excellent upper bound on the number of large solutions, but conjecture that their bounds for the number of medium and small solutions can be improved. My first result improves the bounds on the number of medium solutions to inequality (1).

Theorem 2.1 (K., 2021)**.** *Let $F(x, y)$ be an irreducible, integral binary form of degree $n \geqslant 3$. Suppose that $F(x, y)$ is the sum of exactly $s + 1$ nonzero monomials and that $n \geqslant 3s$. Let H denote the maximum of the absolute values of the coefficients of F. Let $N_M(F, h)$ denote the number of*

[1] The use of $s + 1$ rather than s to denote the number of nonzero summands is a standard convention, loosely because this use of s is properly analogous to the degree, n. A degree n polynomial can have at most $n + 1$ nonzero summands, so we use $s + 1$ to denote the number of nonzero summands. Moreover, by using s in this way, s must live in the interval $[1, n]$, whereas the number of nonzero summands must live in the less "natural" interval $[2, n + 1]$.

primitive, medium solutions to (1)*. Then*

$$N_M(F,h) \ll s\left(1+\log\left(s+\frac{\log h}{\max(1,\log H)}\right)\right).$$

This result is an improvement on Bengoechea's result in [4] (both in the sense that my definition of a "medium" solution is broader than that in [4] and in the sense that my upper bounds are smaller by a factor of s in some cases and $\log s$ in others) and the methods which lead to this result give a fundamentally different proof of the same bound on the number of medium solutions that can be found in a paper of Akhtari and Bengoechea [1].

My explicit result comes in a more specific context. In 2000 in [19], Thomas is able to show that when $F(x,y)$ is an irreducible, integral binary form of degree $n \geqslant 6$ which is a trinomial (fix $s=2$, meaning $F(x,y) = ax^n + bx^k y^{n-k} + cy^n$ for some $a,b,c,k,n \in \mathbb{Z}$ with $0<k<n$), then there are no more than $8w(n)+8$ integer pair solutions to (2) where $w(n)$ is piecewise defined by the following table:

n	6	7	8	9	10–11	12–16	17–37	$\geqslant 38$
$w(n)$	16	13	11	9	8	7	6	5

Note that solutions to (2) are automatically primitive, so there is no need to add that hypothesis. In my thesis, I use a mixture of theoretical techniques and Python code to show that $w(n)$ can be improved as follows:

Theorem 2.2 (K., [9])**.** *The function $w(n)$ in Thomas' result can be replaced by $z(n)$, defined with the following table.*

n	6	7	8	9	10–11	12–16	17–38	39–218	$\geqslant 219$
$z(n)$	15	12	11	9	8	7	6	5	4

It is worth noting that 4 is the best possible value that could be obtained for $z(n)$ using any approach analogous to Thomas', though it remains possible that $z(n)$ could be reduced to 4 for values of n less than 219.

2.1.2. *Methods.* Both of these theorems result from improvements I made to a counting technique based on what is called the gap principle. The gap principle is not a specific theorem, but rather the general notion that "large enough" solutions to (2) should be "exponentially far apart." This notion relies on the previously stated correspondence between primitive solutions to (2) and good rational approximations of $F(Z,1)$. A typical result looks roughly like this: if (p,q) is a primitive solution to (2), then there exists a root α of $f(Z) := F(Z,1)$ so that $\left|\frac{p}{q}-\alpha\right| < \frac{K}{q^r}$ (for some specific values of K and r which depend on F).

Now we can show that solutions which produce good rational approximations to the same root of $f(Z)$ must be far apart. Suppose that (p,q) and (p',q') are distinct solutions to (2) with $q' \geqslant q > 0$ and so that $\frac{p}{q}$ and $\frac{p'}{q'}$ are both close to the same root, α, of $f(Z)$ in the sense of the previous paragraph. Then by the fact that

$$\left|\frac{p}{q}-\alpha\right| < \frac{K}{q^r} \quad \text{and} \quad \left|\frac{p'}{q'}-\alpha\right| < \frac{K}{(q')^r},$$

the triangle inequality allows us to conclude that

$$\left|\frac{p}{q}-\frac{p'}{q'}\right| < \frac{2K}{q^r}.$$

A little bit of additional estimation shows that

$$\frac{1}{qq'} < \frac{2K}{q^r}$$

and rearranging this inequality yields $q' > \frac{q^{r-1}}{2K}$. This is the essence of the gap principle: by starting with only the assumptions that $q' \geqslant q$ and that $\frac{p}{q}$ and $\frac{p'}{q'}$ are good approximations of the same irrational number, one can find that there actually an exponential gap between q' and q.

This exponential gap can help quantify the maximum number of such q that can live between two fixed quantities. My results are largely a function of discovering sharp upper bounds for that maximum.

2.2. Future Work.

I have several ideas for future work that could be done on the topic of Thue inequalities. In order to find better bounds on the total number of solutions to (1), we must find better bounds on the number of small solutions to (1). This is an extremely broad goal, however. Concretely, there are a number of observations I have made in the literature that could lead to improvements in these bounds.

First, Akhtari and Bengoechea in [1] make major improvements to the bounds on the number of small solutions under the assumption that h is small relative to the discriminant of F. I would like to explore their techniques to see if their work can be modified to allow for improvements in general or in other settings (say, if h is small relative to the sizes of the coefficients of F to fit into a conjecture of Mueller and Schmidt in [12]).

In [19], Thomas uses a novel approach to counting solutions to (2) when F is a trinomial. Grundman and Wisniewski extend this approach to tetranomials in [6] and I would like to explore whether this approach can be further extended to arbitrary binary forms.

Moreover, I believe that both Thomas' ([19]) and Grundman and Wisniewski's ([6]) work can be improved by the following means. Both papers appeal to a result of Bombieri and Schmidt in [5] generalizing the Thue-Siegel method. Bombieri and Schmidt's result, however, is based off of a different approximation philosophy and a different approximation result than what is found in Thomas' or Grundman and Wisniewski's papers. By integrating Thomas' or Grundman and Wisniewski's approximation result into Bombieri and Schmidt's general method, I believe that both Thomas' and Grundman and Wisniewski's results could be further improved.

Finally, it is worth noting that foundational papers on Thue's Inequality did not have access to the hindsight that we now have. For instance, Bombieri and Schmidt's paper [5] on the Thue-Siegel method does not keep track of the number of nonzero coefficients of $F(x, y)$. It would be worthwhile to update Bombieri and Schmidt's results to account for this additional parameter.

3. Other Areas of Interest

3.1. The Weil Height.

Of additional interest to me is the theory of height functions. The Weil height on $\overline{\mathbb{Q}}$ can be generalized to a height function (which I will still call the Weil height) on $\mathbb{P}^m(\overline{\mathbb{Q}})$ which still enjoys the Northcott property. For any number field, K of degree n, one might consider the behavior of the Weil height on $\mathbb{Q}$-bases of K, thought of as points in $\mathbb{P}^{n-1}(K)$ by treating the basis $\alpha_1, \ldots, \alpha_n$ as the point $(\alpha_1 : \cdots : \alpha_n)$. Since the Weil height has the Northcott property, there exists a $\mathbb{Q}$-basis of K of minimal height. Let $B(K)$ denote the minimal height of any basis of K.[2]

Conjecturally, $B(K)$ is close to $|\Delta_K|^{1/2}$ (up to a constant factor depending on $n = [K : \mathbb{Q}]$), where Δ_K is the discriminant of K. In [18], Silverman shows that $B(K) \gg_n |\Delta_K|^{1/2}$. In [14], Roy and Thunder show that for any $\varepsilon > 0$, $B(K) \ll_{n,\varepsilon} R(K)^{1-\varepsilon}|\Delta_K|^{\frac{1}{2}+2\varepsilon}$ where $R(K)$ is the regulator of K. In the quadratic imaginary case, they actually construct such a basis. In [15], Ruppert shows (non-constructively) for quadratic K that $B(K) \ll |\Delta_K|^{1/2}$.

Computing $B(K)$ for different fields K is repetitive and tedious, so I expect that these computations could be carried out effectively with a computer. I would like to encode Roy and Thunder's construction for quadratic fields, constructively compute $B(K)$ for a large number of quadratic K, then see if this provides insight into finding a constructive proof of Ruppert's result.

[2] In this section, I am conflating the Weil height with an appropriate normalization of the Weil height for simplicity.

Moreover, I expect that this problem is easier when $\mathcal{O}_K$ is monogenic since $|\Delta_K|$ relates nicely to a power basis for K and the question of basis height can then be connected to the question of whether or not number fields have defining elements of small height. The monogeneity condition is more manageable when the defining polynomial of K has few coefficients (see [7] for instance) and so as a first step, it might be worth looking at $B(K)$ under the condition that K is defined by a binomial or trinomial and $\mathcal{O}_K$ is monogenic.

3.2. **Elementary Function Arithmetic.** Philosophically, the question of what makes a good proof has always intrigued mathematicians. A plausible (though not indisputable) answer to this question is that the best proof of a theorem is the simplest—the one that uses the fewest assumptions. This motivates the main question in the field of reverse mathematics: how many assumptions are needed to prove a given theorem? More precisely, given any theorem, can it be proven from a simple set of axioms? If so, how simple?

One such candidate for a simple axiom scheme is that of Peano Arithmetic. The axioms of Peano Arithmetic describe the arithmetic of the natural numbers: how to add, multiply, and exponentiate numbers, together with a scheme of induction which allows you to prove theorems from inductive techniques in addition to the deductive logical rules that are always available to mathematicians. Of more interest for technical reasons is the axiom scheme of Elementary Function Arithmetic (EFA), which has somewhat fewer axioms than Peano Arithmetic, but functions similarly.

Given that EFA appears to have much to say about the natural numbers and little to say about sets, it may be surprising to learn that much of modern mathematics can be derived from the axioms of EFA. One can work with much or all of finite dimensional linear algebra, the theory of finite groups, and even some analysis (see page 271 of [3]). Colin McLarty is working on number field theory in EFA and to that end, I tried to prove Minkowski's Linear Forms Theorem from the axioms of EFA for my master's thesis. I was able to show in [8] that conditional on my definition of the volume of a convex polytope being well-defined in EFA, Minkowski's Linear Forms Theorem follows from the axioms of EFA.

I am currently collaborating with a graduate student at Montana State University to show the well-definedness of volume. Future work for this project might include showing that a result of Raghavan in [13] follows from the axioms of EFA and that hence, the number field property of "having an embedding into $\mathbb{R}$" can be defined in EFA.

3.3. **Nonnegativity and Sums of Squares.** A final project of interest for me concerns the relationship between nonnegativity and sums of squares. Hilbert's 17th problem asks whether a polynomial $f(x_1, \ldots, x_n) \in \mathbb{R}[x_1, \ldots, x_n]$ which satisfies $f(x_1, \ldots, x_n) \geqslant 0$ for all $x_1, \ldots, x_n \in \mathbb{R}$ can be written as a sum of any number of squares. It turns out that not every nonnegative polynomial can be written as a sum of squares of other polynomials, but it is possible for every nonnegative polynomial to be expressed as a sum of squares of rational functions with coefficients in $\mathbb{R}$ (see [2]).

The condition that $f \in \mathbb{R}[x_1, \ldots, x_n]$ can be written as a sum of squares of rational functions is equivalent to the statement that there exist $g, f_1, \ldots, f_k \in \mathbb{R}[x_1, \ldots, x_n]$ so that

$$g^2 f = f_1^2 + \cdots + f_k^2.$$

Here, $g, f_1, \ldots, f_k$ serve as "certificates of nonnegativity" because their existence guarantees that f is nonnegative. In [10], Lombardi, Perrucci, and Roy show that not only do such g and f_i exist, but moreover, the degree of each g and f_i is bounded by

$$2^{2^{2^{\deg(f)^{4^n}}}}.$$

Lombardi, Perrucci, and Roy do not prove bounds on k nor on the sizes of the coefficients of g and f_i. I would like to explore their methods to see if I can find such bounds. If such bounds were obtained and if one could work over $\mathbb{Z}$ or $\mathbb{Q}$ rather than $\mathbb{R}$, we would have a naïve algorithm for checking whether a polynomial with integer coefficients is nonnegative: run through all of the combinations of polynomials $g, f_1, \dots, f_k$ with degrees and coefficients appropriately bounded (of which there are finitely many) and check to see whether or not $g^2 f = f_1^2 + \cdots + f_k^2$. If yes, we note that f is nonnegative. If no, then f is not nonnegative.

References

[1] Shabnam Akhtari and Paloma Bengoechea. Representation of integers by sparse binary forms. *Trans. Amer. Math. Soc.*, 374(3):1687–1709, dec 2020.

[2] Emil Artin. Über die Zerlegung definiter Funktionen in Quadrate. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 5(1):100–115, 1927.

[3] Jeremy Avigad. Number theory and elementary arithmetic. *Philosophia Mathematica. Philosophy of Mathematics, its Learning, and its Application. Series III*, 11(3):257–284, 2003.

[4] Paloma Bengoechea. Thue inequalities with few coefficients. *Int. Math. Res. Not.*, (2):1217–1244, 2022.

[5] Enrico Bombieri and Wolfgang M. Schmidt. On Thue's equation. *Invent. Math.*, 88(1):69–81, 1987.

[6] Helen G. Grundman and Daniel P. Wisniewski. Tetranomial Thue equations. *J. Number Theory*, 133(12):4140–4174, 2013.

[7] Ryan Ibarra, Henry Lembeck, Mohammad Ozaslan, Hanson Smith, and Katherine E. Stange. Monogenic fields arising from trinomials. *Involve*, 15(2):299–317, 2022.

[8] Greg Knapp. Minkowski's Linear Forms Theorem in Elementary Function Arithmetic. Master's thesis, Case Western Reserve University, 2017.

[9] Greg Knapp. The Number of Solutions to the Trinomial Thue Equation. *Functiones et Approximatio Commentarii Mathematici*, 2023.

[10] Henri Lombardi, Daniel Perrucci, and Marie-Françoise Roy. An elementary recursive bound for effective Positivstellensatz and Hilbert's 17th problem. *Memoirs of the American Mathematical Society*, 263(1277):v+125, 2020.

[11] Kurt Mahler. Zur Approximation algebraischer Zahlen. I - Über den größten Primteiler binärer Formen. *Math. Ann.*, 107(1):691–730, 1933.

[12] Julia Mueller and Wolfgang M. Schmidt. Thue's equation and a conjecture of Siegel. *Acta Math-djursholm*, 160(3-4):207–247, 1988.

[13] S. Raghavan. Bounds for minimal solutions of diophantine equations. *Nachr. Akad. Wiss. Gottingen Math-Phys. Kl.*, 2(9):109–114, 1975.

[14] Damien Roy and Jeffrey Lin Thunder. Bases of number fields with small height. *Rocky Mt. J. Math.*, 26(3):1089–1098, 1996.

[15] Wolfgang M. Ruppert. Small generators of number fields. *Manuscripta Math*, 96(1):17–22, 1998.

[16] Wolfgang M. Schmidt. Thue equations with few coefficients. *Trans. Amer. Math. Soc.*, 303(1):241–255, 1987.

[17] Carl L. Siegel. Über einige Anwendungen diophantischer Approximationen [reprint of Abhandlungen der Preußischen Akademie der Wissenschaften. Physikalisch-mathematische Klasse 1929, Nr. 1]. In *On some applications of Diophantine approximations*, volume 2 of *Quad./Monogr.*, pages 81–138. Ed. Norm., Pisa, 2014.

[18] Joseph H. Silverman. Lower bounds for height functions. *Duke Mathematical Journal*, 51(2):395–403, 1984.

[19] Emery Thomas. Counting solutions to trinomial Thue equations: a different approach. *Trans. Amer. Math. Soc.*, 352(8):3595–3622, 2000.

[20] Axel Thue. Über Annäherungswerte algebraischer Zahlen. *J. Reine Agnew. Math*, 135(135):284–305, 1909.