The Thue Equation

Research Immersion Lab Report

James Stearn

November 14, 2023

A Thue equation is a Diophantine equation $F(x, y) = m$, where $F(x, y) \in \mathbb{Z}[x, y]$ and $m \in \mathbb{Z}$. By a result of Thue, it is known that the number of solutions to any such equation is finite. We outline important results and the historical development of various methods for efficient resolution of the Thue equation. We also highlight the computational challenges associated with current methods for solving Thue equations. This research is motivated by the appearance of Thue equations in calculations of norms of prime ideals, an important element in the General Number Field Sieve, which is asymptotically the most efficient known factoring algorithm.

1 Introduction

A Thue equation is an irreducible bivariate homogeneous polynomial of the form:

$$a_0x^d + a_1x^{d-1}y + a_2x^{d-2}y^2 \dots a_dy^d = m \tag{1}$$

with coefficients $a_i, m \in \mathbb{Z}$, solutions $(x, y) \in \mathbb{Z}^2$ and degree $d \geq 3$.

In 1909, Axel Thue [Thu09] showed that his eponymous equation has only finitely many solutions.

Example 1. Let $F(x, y) = x^3 - 6x^2y - 4xy^2 + 5y^3$.
The Thue equation $F(x, y) = 1$ has only the following solutions: $(-2, -3), (1, 0), (13, 2)$.

Thue's result improved upon a previous elementary result of Liouville [Lio44]. Liouville's result was used to show that certain *well-approximable* numbers, the so-called Liouville numbers, cannot be algebraic, thereby establishing the existence of transcendental numbers.

Theorem 1 (Liouville, 1844)**.** *Let $\theta \in \mathbb{R}$ be an irrational algebraic number of degree d. Then there exists a non-zero constant C such that for all $\frac{p}{q} \in \mathbb{Q}$:*

$$\left|\theta - \tfrac{p}{q}\right| \geq \tfrac{C}{q^d}$$

Rational approximation of algebraics and resolution of the Thue equation (along with other types of Diophantine equation) are intimately linked, due to the following lemma:

Lemma 2. *Let $F(x, y) = m$ be a Thue equation of degree d. Let θ be an irrational algebraic number such that $F(\theta) = 0$. For an approximation $\frac{p}{q} \in \mathbb{Q}$ to θ, let the quality of the approximation μ be defined by:*

$$\left|\theta - \tfrac{p}{q}\right| = \tfrac{1}{q^\mu}$$
$$i.e.\ \mu = \log_q\left(\tfrac{1}{\left|\theta - \frac{p}{q}\right|}\right).$$

If $|F'(\theta)| > 1$, for a solution $(x, y) \in \mathbb{Z}^2$ to $F(x, y) = m$, the quality of approximation μ must be greater than d.

Proof. Let $|F'(\theta)| > 1$. For a solution $(x, y) \in \mathbb{Z}^2$, we have:

$$\frac{1}{F'(\theta)} = y^d \left(\frac{x}{y} - \theta\right) \tag{2}$$

$$\frac{1}{F'(\theta)} = y^d \cdot \frac{1}{y^\mu} \tag{3}$$

$$d - \mu = \log_y \left(\frac{1}{F'(\theta)}\right) \tag{4}$$

As $y \to \infty$, for constant c, $\log_y(c) \to 0$ which gives:

$$d - \mu \to 0 \implies \lim_{y\to\infty} \mu = d$$

So for a pair (x, y) to be a solution, the quality of the approximation must be $\mu > d$:

$$\left|\frac{x}{y} - \theta\right| < \frac{1}{y^d} \tag{5}$$

□

In order to find these exceptional approximations, we turn to the theory of continued fractions:

Lemma 3. [TdW89] *Let $F(x, y) = m$ be a Thue equation of degree d. Let $g(x) = F(x, 1)$ and $\theta^{(1)}, \ldots, \theta^{(s)}$ be the s real roots of $g(x) = 0$. If (x, y) is a solution to $F(x, y) = m$ and:*

$$y > \lceil (4 \cdot \frac{2^{d-1} \cdot |m|}{\min\limits_{1\le i\le s} |g'(\theta^{(i)})|})^{1/(d-2)} \rceil \tag{6}$$

then $\frac{x}{y}$ is a convergent from the continued fraction expansion of one of $\theta^{(1)}, \ldots, \theta^{(s)}$.

Proof. Let $C = \frac{2^{d-1}\cdot|m|}{\min\limits_{1\le i\le s} |g'(\theta^{(i)})|}$. Let y be as in Inequality 6, then:

$$\begin{aligned} \left|\theta^{(i)} - \frac{x}{y}\right| &\le C \cdot |y|^{-d} \\ &\le \frac{1}{4} \cdot y_1^{d-2} \cdot |y|^{-d} \\ &< \frac{1}{2} \cdot \frac{1}{|y|^2} \end{aligned} \tag{7}$$

So $\frac{x}{y}$ is a convergent to $\theta^{(i)}$ by the following classical lemma [HW79]:

Lemma 4. *If $\left|\theta - \frac{x}{y}\right| < \frac{1}{2y^2}$, then $\frac{x}{y}$ is a convergent to θ.*

□

Example 2. Let $F(x, y) = x^3 + 6x^2y - xy^2 - 9y^3$.
Then the Thue equation $F(x, y) = 1$ has only the solutions: $(1, 0)$, $(25, 21)$.

Obtaining the three real roots of $F(x, 1)$:

$$\theta_1 = -5.91162784275\ldots, \theta_2 = -1.27884219059\ldots, \theta_3 = 1.19047003335\ldots$$

We see that $\frac{25}{21} = 1.\overline{190476}$ is a very good rational approximation for θ_3, with approximation quality greater than 3:

$$\left|\theta_3 - \tfrac{25}{21}\right| \approx \tfrac{1}{21^{3.94\ldots}}$$

So we have $\mu \approx 3.94081528217\ldots$.

By Lemma 3, we can therefore group the solutions (x, y) into two classes:

- **'Small' solutions** - y is less than the bound in Inequality 6. As the bound is usually quite small in practice, we can find these solutions efficiently using either exhaustive search or a lattice reduction method based on an argument of Thunder [Thu15].
- **'Medium' solutions** - y is greater than the bound in Inequality 6 and so $\frac{x}{y}$ is a convergent to a real root of $F(x, 1)$. We find these solutions by checking the convergents of the continued fraction expansion.

The problem of solving Thue equations may therefore be reduced to the problem of finding an upper bound on y and checking all convergents up to this bound. Unfortunately, the structure of Thue's proof, and later improvements due to Siegel [Sie29] and Roth [Rot55], is intrinsically ineffective. As such, although the proof ensures that the number of solutions is finite, it does not allow us to directly calculate an upper bound on y and find all solutions for a given form.

The ineffectiveness of Thue's method was theoretically resolved by Alan Baker's work [Bak68] on linear forms in logarithms of algebraic numbers. Baker's theorem provides an explicitly computable lower bound for the value of such forms, which then allows one to derive an upper bound on y. Such an approach was used by Tzanakis and de Weger to solve Thue equations, as outlined in §5. In practice however, the bounds given by Baker's method are generally very large and do not allow for efficient enumeration of solutions. We are therefore currently restricted to solving completely only Thue equations of relatively low degree or with small discriminant.

2 Motivation

Our principal motivation in researching efficient resolution of the Thue equation lies in its relation to the Number Field Sieve factoring algorithm. This algorithm consists of 4 separate stages:

1. Polynomial selection
2. Relation collection (sieving)
3. Relation filtering
4. Linear algebra

Although it is highly parellelisable, relation collecting is by far the most computationally intensive stage of the algorithm. The present approach to relation collection involves evaluating $F(a, b)$ over fixed intervals of a and b and checking each evaluation for smoothness by a systematic process in which the value is sieved over a large set of primes. We test (a, b) pairs in the bivariate polynomial selected in Stage 1 for smoothness below some chosen prime bound. We seek prime ideals $\langle a + b\theta \rangle$ with smooth norm. The link to the Thue equation lies in the definition of the norm:

$$N(a + b\theta) = (-b)^d f(\frac{a}{b}) \tag{8}$$

with f a univariate polynomial of degree d.

Expanding the right hand side of Equation 8, we see that the norm is a bivariate homogenous polynomial, irreducible due to the restrictions placed on the polynomial in Stage 1; that is, Equation 8 is a Thue equation of degree d.

Figure 1 shows the values of $\log |F(a, b)|$ for $F = 4x^5 + 17x^4 - 18x^3 - 58x^2 + 6x + 1$ as a heat graph [Tho22], with blue and green shades representing smaller values of $\log |F(a, b)|$. As F has 5 real roots, we see that the graph has 5 *'valleys'* in which the norm is lower than in the surrounding areas. These valleys occur around (a, b) points that are good rational approximations to the real roots of F.

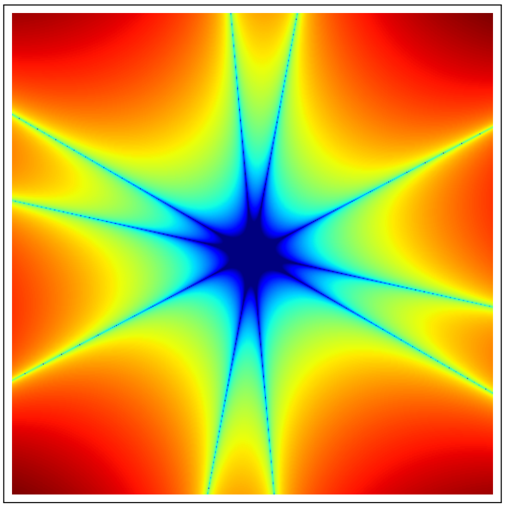

Figure 1: Plot of $\log|F(a,b)|$ for $F = 4x^5 + 17x^4 - 18x^3 - 58x^2 + 6x + 1$.

An (a, b) pair with small norm is more likely to be smooth due to the distribution of smooth numbers:

Theorem 5 (Canfield, Pomerance & Erdös, 1983)**.** [CEP83] *Let* $\psi(x, y) = \#\{1 \leq n \leq x : n \text{ is } y\text{-smooth}\}$.
Then:

$$\psi(x, x^{1/u}) = xu^{-u+o(u)} \tag{9}$$

uniformly as $u \to \infty$ *and* $u < (1 - \epsilon) \ln x / \ln \ln x$.

We are therefore interested in developing relation collection methods that search only within regions of small norm that are more likely to be smooth; that is, sieving only those (a, b) pairs that are good rational approximations to real roots of F. Although the vast majority of usable relations come from the dark blue central area of the graph (in which both a and b are relatively small, with correspondingly small norm for $\langle a + b\theta \rangle$), the valleys still contribute a significant percentage of the total relations used in Stages 3 and 4 of the algorithm, as shown in the graph below:

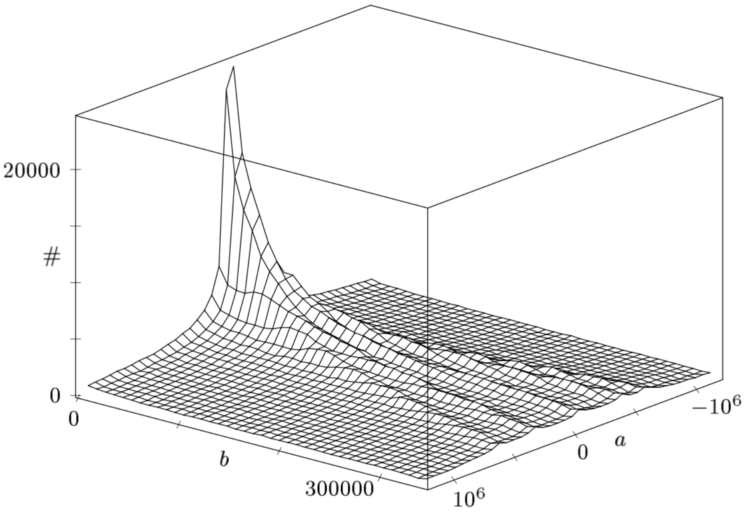

Figure 2: Relation yield for $x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$.

Figure 2 [EH96] shows the number of relations obtained via sieving $F = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$. Note that the majority of relations are obtained around small values of a and b, with five ridges along larger (a, b) values corresponding to the five real roots of F.

3 Thue's proof

We now outline the structure of Thue's proof to illustrate its ineffective nature. The refinements of Thue's result due to Siegel and Roth employ a similar argument and thereby inherit the ineffective property. In order to show that the number of solutions to any Thue equation is finite, Thue considered the number of very good approximations to θ, proving the following result:

Theorem 6 (Thue, 1909)**.** *(Thue's Approximation Theorem) Let θ be an irrational algebraic number of degree $d \geq 3$. Fix $\varepsilon > 0$, then there are only finitely many 'excellent' approximations $\frac{p}{q} \in \mathbb{Q}$ satisfying the inequality:*

$$\left|\theta - \frac{p}{q}\right| \leq \frac{1}{q^{1+\frac{d}{2}+\varepsilon}} \tag{10}$$

Finiteness of the number of solutions to the Thue equation clearly follows.

Sketch proof. To prove Theorem 6 and its refinements, the argument consists of four main steps. To begin, we assume that we have at least two *'excellent'* approximations (as defined in the statement of Theorem 6) and from there derive a contradiction. Of course, two such good approximations may not exist, in which case their number is clearly finite.

Let the two approximations be $\frac{p}{q}$ and $\frac{r}{s}$. The first step is to use the first excellent approximation $\frac{p}{q}$ to construct auxiliary polynomials $F_n(X,Y) = P_n(X) - YQ_n(X)$, for $n \in \mathbb{Z}, P_n(X), Q_n(X) \in \mathbb{Z}[X,Y]$. By construction F_n has bounded coefficients and $P_n(X) - \theta Q_n(X)$ vanishes to a high order at $X = \theta$, i.e. the point (θ, θ).

To obtain a contradiction, we now derive upper and lower bounds on $\left|F_n(\frac{p}{q}, \frac{r}{s})\right|$. Essentially, these bounds can be used to show that if $(\frac{p}{q}, \frac{r}{s})$ is very close to (θ, θ), then $F_n(\frac{p}{q}, \frac{r}{s})$ would vanish too much.

For the upper bound on $\left|F_n(\frac{p}{q}, \frac{r}{s})\right|$, we see that it is small as F_n has bounded coefficients and both $\frac{p}{q}$ and $\frac{r}{s}$ are excellent approximations to θ. The derivation of an explicit upper bound is the most technical part of the proof, involving analysis of the linear system generated by considering the $2n + 2$ coefficients of P_n and Q_n, and the linear constraints imposed by the fact that F_n has high-order zeros. §2.3 of Zannier's lecture notes [Zan15] provides full details.

The lower bound on $\left|F_n(\frac{p}{q}, \frac{r}{s})\right|$ is straight-forward. As $P_n(X), Q_n(X) \in \mathbb{Z}[X,Y]$, we have that $F_n(\frac{p}{q}, \frac{r}{s}) \in \mathbb{Q}$, with its denominator dividing $q^n s$. Then $F_n(\frac{p}{q}, \frac{r}{s}) \geq \frac{1}{q^n s}$, *provided* $F_n(\frac{p}{q}, \frac{r}{s}) \neq 0$. Given two excellent approximations of large enough height, these two bounds yield a contradiction.

The final step in the argument is to ensure that $F_n(\frac{p}{q}, \frac{r}{s}) \neq 0$ holds. This step is also quite intricate, involving analysis of the derivatives of F_n to generate an upper bound on the multiplicity of $F_n(\frac{p}{q}, \frac{r}{s})$ (i.e. we show that $D^i F(\frac{p}{q}, \frac{r}{s}) \neq 0$ for a small enough i.)

□

4 Bounding the number of solutions

There is a large body of work on bounding the number of solutions to Thue equations of a given form. In particular, we consider the number of *primitive* solutions, where x and y are coprime. Such work originates with investigations of Siegel and Mahler. Siegel [Sie29] established that there exists an explicit upper bound on the number of solutions to $F(x,y) = m$. In 1933, Mahler [Mah33] proved an upper bound for a closely related type of equation:

Theorem 7 (Mahler, 1933)**.** *Let $p_1^{z_1}, \dots, p_s^{z_s}$ be distinct primes and let $F(x,y)$ be a* ***Thue-Mahler*** *equation of degree $d \geq 3$, with solutions $(x,y) \in \mathbb{Z}^2$ and $z_1, \dots, z_s \in \mathbb{N}$:*

$$F(x,y) = p_1^{z_1} p_2^{z_2} \dots p_s^{z_s} \tag{11}$$

Then the number of primitive solutions (x,y) is less than C^{1+s}, where C is a constant depending only on F.

This bound was subsequently improved by Davenport and Roth [DR55], who gave an explicit bound depending on the degree and coefficients of the form:

Theorem 8 (Davenport & Roth, 1955)**.** *Let F be a Thue equation of degree $d \geq 3$:*

$$a_0x^d + a_1x^{d-1}y + a_2x^{d-2}y^2 \dots a_dy^d = m$$

Let $A = \max |a_i|$. Then the number of primitive solutions (x,y) is less than:

$$(4A)^{2n^2}|m|^3 + e^{(643d^2)} \tag{12}$$

In 1983, Evertse [Eve83] resolved Siegel's long-standing conjecture that the upper bound did not depend on the coefficients of F with the following result:

Theorem 9 (Evertse, 1983)**.** *Let F be a Thue equation of degree $d \geq 3$. Let $\omega(m)$ denote the number of distinct prime divisors of m. The number of primitive solutions (x,y) to $F(x,y) = m$ is bounded by:*

$$2 \cdot 7^{d^3(2\omega(m)+3)} \tag{13}$$

So, the upper bound depends only on the degree of the form and the number of prime divisors of m. The next improvement on this bound is due to Bombieri and Schmidt [BS87]:

Theorem 10 (Bombieri & Schmidt, 1987)**.** *Let F and $\omega(x)$ be as in Theorem 9. There exist absolute constants c_1, c_2 such that the number of primitive solutions (x,y) to $F(x,y) = m$ is less than:*

$$c_1d^{1+\omega(m)} \tag{14}$$

Further, for $d > c_2$, the number of solutions is less than:

$$215d^{1+\omega(m)} \tag{15}$$

The most recent general improvements on the bound are due to Stewart [Ste91] and Thunder.

Theorem 11 (Stewart, 1991)**.** *Let F and $\omega(x)$ be as in Theorem 9 and assume that the discriminant $D(F)$ is non-zero. Let $\varepsilon > 0$. Let n be a divisor of m such that $(n, D(F)) = 1$ and $n^{1+\varepsilon} \geq \frac{m^{(2/d)+\varepsilon}}{|D(F)|^{1/d(d-1)}}$ Then the number of primitive solutions (x,y) is bounded by:*

$$\left(5600d + \frac{1400}{\varepsilon}\right) d^{\omega(n)} \tag{16}$$

Thus, depending on the prime factorisation of m, Stewart's bound can be much stronger than the bound of Bombieri & Schmidt. Similarly, Thunder's results [Thu15] improve upon Stewart's bounds, dependent on the prime factorisation of a factor n of m. In the following theorem, the upper bound applies to the number of primitive solutions to the closely related **Thue inequality**:

$$|F(x,y)| \leq m \tag{17}$$

Theorem 12 (Thunder, 2015)**.** *For a form $F(x,y)$, consider its factorisation into linear forms over some splitting field: $F(x,y) = \prod_{i=1}^{d} L_i(x,y)$.*
For $F(x,y)$ and place v, let $c_F(v)$ be the number of linear factors L_i defined over $\mathbb{Q}_v$.
For $m \in \mathbb{Z}$, let $c_F(m) = \prod_{\substack{p|m \\ p \text{ prime}}} c_F(p)$.
Let F be a Thue equation of degree $d \geq 3$ with $D(F) \neq 0$ and content 1. Let n be a divisor of m such that $n = \frac{Am^{(2/d)}}{|D(F)|^{1/d(d-1)}}$ for some $A \geq 1$. Then the number of primitive solutions to Inequality 17 is less than:

$$2500d\left(59 + \frac{\log(2 + \log m/(1 + \log A))}{\log(d-1)}\right) c_F(n) \tag{18}$$

$c_F(n)$ will always be less than or equal to $d^{\omega(n)}$, but in the case where $c_F(n)$ is significantly smaller, we achieve a much sharper bound on the number of solutions. These general results have been supplemented with a large number of results on Thue equations of a specific form. A comprehensive survey of results on families of Thue equations of type $F_a(x,y) = \pm 1$, parameterised by a, is given by Heuberger [Heu04], and a more recent general survey by Waldschmidt [Wal20]. The majority of these fully resolved families focus on the cubic and quartic cases, although work by Bilu and Hanrot [BH96] focuses on solving Thue equations of high degree.

We now refer to some of the notable results of Heuberger's survey, the majority of which are obtained using variations on the method of linear forms in logarithms:

Theorem 13 (Mignotte, 2000)**.** [MT00] *Let $F(x,y) = x^3 - ax^2y - (a+1)xy^2 - y^3$. Let $a \geq 3$. For $F(x,y) = 1$, the only solutions are the trivial solutions:*

$$(1,0),(0,-1),(1,-1),(-a-1,1),(1,-a)$$

Theorem 14 (Wakabayashi, 2003)**.** [Wak03] *Let $F(x,y) = x^3 - a^2xy^2 + y^3$. If $a \geq 1.35 \cdot 10^{14}$, then $F(x,y) = 1$ has the five solutions:*

$$(0,1),(1,0),(1,a^2),(a,1),(-a,1)$$

Theorem 15 (Mignotte, Pethö & Roth, 1996)**.** [MPR96] *Let $F(x,y) = x^4 - ax^3y - x^2y^2 + axy^3 + y^4$. For $a \geq 3$ and $a \neq 4$, the only solutions to $F(x,y) = 1$ are:*

$$\pm\{(0,1),(1,0),(1,1),(1,-1),(a,1),(1,-a)\}$$

If there exists $c, \lambda = \theta(c,\lambda)$ such that $\left|\theta - \frac{p}{q}\right| > \frac{1}{cq^\lambda}$ with c effective, then c is an *effective irrationality measure* for θ. In these theorems, the general approach is to use results on linear forms in logarithms to obtain an effective irrationality measure that is less than the degree of F, thereby deriving an effective upper bound on the quality of approximations, and thus, the number of solutions.

While Baker's method allows for the resolution of large families of Thue equations, Thue himself used the distinct method of Padé approximation to consider solutions to the equation $(a+1)x^n - ay^n = 1$:

Theorem 16 (Thue, 1909)**.** *Let $F(x,y) = (a+1)x^n - ay^n$ and $a \gg d \geq 3$. Then $F(x,y) = 1$ has only the solution $(1,1)$.*

Although the method of Padé approximation gives smaller bounds than those obtained by Baker's method, it is only applicable to certain forms and therefore does not allow for general solution of the Thue equation.

A third method, of Bombieri, was used to obtain effective irrationality measures for numbers of the form $\sqrt[d]{\frac{a}{b}}$. Baker had previously given an effective irrationality measure for $\sqrt[3]{2}$, improved by Chudnovsky [Chu83] to, for $p, q \geq 1$:

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| > q^{-2.4297\ldots} \tag{19}$$

Bombieri's method is similar to Thue's original method, but removes the restriction that q must be large in an approximation $\frac{p}{q}$ to θ. Thue's argument derives a contradiction from the existence of two exceptional approximations, but his definition of an exceptional approximation is exceedingly restrictive. By circumventing this restriction, Bombieri is able to show that there can be at most one exceptional approximation, and to find this approximation explicitly for a range of numbers of the form $\sqrt[d]{\frac{a}{b}}$. The prinicipal result is given in a paper of Bombieri and Mueller [BM83]:

Theorem 17 (Bombieri & Mueller, 1983)**.** *Let $d \geq 3, (a,b) = 1, \delta = \frac{\log|a-b|}{\log b}$ and $\theta \in \mathbb{Q}(\sqrt[d]{\frac{a}{b}})$ be of degree d over $\mathbb{Q}$. Let $\mu(\theta)$ be an effective irrationality measure for θ.*
If $\delta < 1 - \frac{2}{d}$, then:

$$\mu(\theta) \leq \frac{2}{1-\delta} + 6\left(\frac{d^5 \log d}{\log b}\right)^{\frac{1}{3}} \tag{20}$$

So for large values of b and reasonable values of d, Theorem 17 gives an irrationality measure that allows us to completely resolve the corresponding Thue equation.

5 Efficient resolution of Thue equations

5.1 Linear forms in logarithms of algebraic numbers

In 1989, Tzanakis and de Weger [TdW89] published an algorithm for the effective resolution of any Thue equation, followed in 1991 by a p-adic variant for the solution of Thue-Mahler equations ([TdW91],[TdW92]).

The method of Tzanakis and de Weger generates a very large upper bound on y using updated results on linear forms in logarithms, descending from Baker's result. The size of this upper bound makes exhaustive checking of all convergents below the bound computationally infeasible. This very large bound is then iteratively reduced using the LLL lattice reduction algorithm to a reasonable size and convergents below this bound may then be checked. This algorithm is implemented in a number of computer algebra packages, including PariGP and Magma.

Using their method, Tzanakis and de Weger solved completely the following Thue equations:

$$x^4 - 4x^3y - 12x^2y^2 + 4y^4 = 1 \tag{21}$$

$$x^4 - 12x^2y^2 - 8xy^3 + 4y^4 = 1 \tag{22}$$

These equations are resolved using knowledge of a system of fundamental units of $\mathcal{O}_k$ of the associated number field $\mathbb{Q}(\theta)$, with θ a root of $F(x, 1)$. The system of fundamental units is obtained by a result of Billevič on units in cubic and quartic fields. For equations of higer degree, we therefore need other approaches in order to apply the method of Tzanakis and de Weger.

Whilst this method theoretically allows for the resolution of any Thue equation, in practice it is limited by the fact that the reduction algorithm requires knowledge of the unit group of the associated number field $\mathbb{Q}(\theta)$. If the discriminant of F or its degree is large, it becomes computationally infeasible to calculate the unit group and the method fails. Our goal is therefore to obtain upper bounds on y without requiring computation of the unit group of $\mathbb{Q}(\theta)$.

There has been some work on equations of higher degree, generally based on adaptations of the methods of Tzanakis and de Weger. Voutier [Vou95] employed the method to solve Thue equations of up to degree 14, although the structure of the Thue equations in question meant that the required algebraic number theoretic data was easily computable.

Bilu and Hanrot [BH96] also did further work on Thue equations of high degree, using a modified version of Tzanakis and de Weger's method to solve the equations $2x^{19} + y^{19} = \pm 1, \pm 2$ and a more complex equation of degree 33. Again, this was possible due to the fact that a system of fundamental units was easily computable for the associated number fields and the method does not generalise to arbitrary Thue equations of high degree. The particular improvement of their method on the method of [TdW89] is to replace application of the LLL algorithm to an inequality in a large number of variables with a simpler process based on continued fractions, applied to an inequality in only two variables.

Hanrot [Han00] took this idea further, modifying the method to solve equations without knowledge of the full unit group. In this paper, Hanrot solves a Thue equation of degree 41 with knowledge only of a subgroup of finite index of the unit group. However, Hanrot's result relies explicitly on the fact that the associated number field is a subfield of a cyclotomic field, allowing for trivial computation of a subgroup of the unit group. Thus it seems that the forms that can be resolved using this method are limited.

Smart [Sma96] provides a complexity analysis of the method of Tzanakis and de Weger. This analysis is given in terms of m and the coefficients of F, under the assumption that $F(x, 1)$ is monic. As discussed, the method of Tzanakis and de Weger requires computation of a system of fundamental units of $\mathcal{O}_k$; conjectured subexponential algorithms of Buchmann [Buc88] or Pohst and Zassenhaus [PZ97] may be used to do this.

Let $L(f) = \sum_{n}^{i=1} |a_i|$. Then, for computation of the solution set of the Thue equation using Tzanakis and de Weger's method, we have:

Lemma 18. [Sma96] *The complexity of finding the small solutions is* $O(|m|^{1/d-2})$.
The complexity of finding the medium solutions is $O\left((R_K^2 + (1 + R_K)(\log|m| + \log L(F)))^3\right)$, *with* R_K *the regulator of the field* K.

5.2 The modular approach

Kim takes a completely different approach to solving Thue equations (to be specific, the method applies to Thue-Mahler equations). A comparison of this method with that of Tzanakis and de Weger is found in §7 of [Kim17]. The approach is to generate a bound on $Y(\mathbb{Z}_S)$, where Y is an affine variety defined by the complement of zeros of $F(x, y)$ in a projective line, and $\mathbb{Z}_S$ the ring of S-integers of the primes in Equation 11. This upper bound is determined by associating each solution $t \in Y(\mathbb{Z}_S)$ with an elliptic curve X_t, then constructing a map:

$$\begin{aligned} \kappa : Y(\mathbb{Z}_S) &\to \{\text{Elliptic curves over } \mathbb{Q}\} \\ t &\mapsto X_t \end{aligned} \tag{23}$$

We can thereby study t by considering properties of X_t. The bottleneck of this method lies in requiring data on elliptic curves of a given conductor, which are then tested. Determining all possible suitable elliptic curves is a computationally hard task; if the conductor is not within the bounds for curves included in the *L-functions and Modular Forms Database* (LMFDB)[1], the computation is not trivial. However, if the associated elliptic curves are of a conductor within the database, solving the associated Thue-Mahler equation is highly efficient compared to the method of Tzanakis and de Weger. More recently, von Känel and Matschke [vKM23] have also used this modular approach to solve a variety of Diophantine equations, including Thue-Mahler equations.

[1] http://www.lmfdb.org/

References

[Bak68] Alan Baker. Linear forms in the logarithms of algebraic numbers (IV). *Mathematika*, 15(2):204–216, 1968. Publisher: London Mathematical Society.

[BH96] Yuri Bilu and Guillaume Hanrot. Solving Thue equations of high degree. *Journal of Number Theory*, 60(2):373–392, 1996. Publisher: Elsevier.

[BM83] Enrico Bombieri and Julia Mueller. On effective measures of irrationality for $\sqrt[3]{2}$ and related numbers. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 1983(342):173–196, July 1983.

[BS87] Enrico Bombieri and Wolfgang M. Schmidt. On Thue's equation. *Inventiones Mathematicae*, 88(1):69–81, 1987.

[Buc88] Johannes Buchmann. A subexponential algorithm for the determination of class groups and regulators of algebraic number fields. *Séminaire de théorie des nombres, Paris*, 1989(1990):27–41, 1988. Publisher: Citeseer.

[CEP83] E. Rodney Canfield, Paul Erdös, and Carl Pomerance. On a problem of Oppenheim concerning "factorisatio numerorum". *Journal of Number Theory*, 17(1):1–28, 1983. Publisher: Elsevier.

[Chu83] Gregory Volfovich Chudnovsky. On the method of Thue-Siegel: Dedicated to the memory of Carl Ludwig Siegel. *Annals of Mathematics*, pages 325–382, 1983. Publisher: JSTOR.

[DR55] Harold Davenport and Klaus F. Roth. Rational approximations to algebraic numbers. *Mathematika*, 2(2):160–167, 1955. Publisher: London Mathematical Society.

[EH96] Marije Elkenbracht-Huizing. An Implementation of the Number Field Sieve. *Experimental Mathematics*, 5(3):231–253, January 1996.

[Eve83] Jan-Hendrik Evertse. *Upper bounds for the numbers of solutions of Diophantine equations.* PhD thesis, 1983. Publisher: Centrum Voor Wiskunde en Informatica.

[Han00] Guillaume Hanrot. Solving Thue equations without the full unit group. *Mathematics of Computation*, 69(229):395–405, 2000.

[Heu04] Clemens Heuberger. Parametrized Thue Equations: A Survey. *Proceedings of the RIMS symposium "Analytic Number Theory and Surrounding Area"*, 1511:82–91, 2004.

[HW79] Godfrey Harold Hardy and Edward Maitland Wright. *An introduction to the Theory of Numbers.* Oxford University Press, 1979.

[Kim17] Dohyeong Kim. A modular approach to cubic Thue-Mahler equations. *Mathematics of Computation*, 86(305):1435–1471, 2017.

[Lio44] Joseph Liouville. Sur des classes très-étendues de quantités dont la valeur n'est ni algébrique ni même réductible à des irrationnelles algébriques. *CR Acad. Sci. Paris*, 18:883–885, 1844.

[Mah33] Kurt Mahler. *Zur approximation algebraischer zahlen.* Almqvist & Wiksell, 1933.

[MPR96] Maurice Mignotte, Attila Pethö, and Ralf Roth. Complete solutions of a family of quartic thue and index form equations. *Mathematics of computation*, 65(213):341–354, 1996.

[MT00] Maurice Mignotte and Nikos Tzanakis. Petho's cubics. *Publ. Math. Debrecen*, 56(3-4):481–505, 2000.

[PZ97] Michael Pohst and Hans Zassenhaus. *Algorithmic algebraic number theory*, volume 30. Cambridge University Press, 1997.

[Rot55] Klaus Friedrich Roth. Rational approximations to algebraic numbers. *Mathematika*, 2(1):1–20, 1955. Publisher: London Mathematical Society.

[Sie29] Carl L. Siegel. Über einige Anwendungen diophantischer Approximationen: Abhandlungen der Preußischen Akademie der Wissenschaften. Physikalisch-mathematische Klasse 1929, Nr. 1. In *On Some Applications of Diophantine Approximations*, pages 81–138. Scuola Normale Superiore, Pisa, 1929.

[Sma96] Nigel Smart. How difficult is it to solve a Thue equation? In Gerhard Goos, Juris Hartmanis, Jan Leeuwen, and Henri Cohen, editors, *Algorithmic Number Theory*, volume 1122, pages 363–373. Springer Berlin Heidelberg, Berlin, Heidelberg, 1996. Series Title: Lecture Notes in Computer Science.

[Ste91] Cameron Leigh Stewart. On the number of solutions of polynomial congruences and Thue equations. *Journal of the American Mathematical Society*, 4(4):793–835, 1991.

[TdW89] Nikos Tzanakis and Benjamin MM de Weger. On the practical solution of the Thue equation. *Journal of Number Theory*, 31(2):99–132, 1989. Publisher: Elsevier.

[TdW91] Nikos Tzanakis and Benjamin MM de Weger. Solving a specific Thue-Mahler equation. *Mathematics of Computation*, 57(196):799–815, 1991.

[TdW92] Nikos Tzanakis and Benjamin MM de Weger. How to explicitly solve a Thue-Mahler equation. *Compositio Mathematica*, 84(3):223–288, 1992.

[Tho22] Emmanuel Thomé. Number Field Sieve course notes, 2022.

[Thu09] Axel Thue. Über Annäherungswerte algebraischer Zahlen. *crll*, 1909(135):284–305, 1909.

[Thu15] Jeffrey Lin Thunder. Thue equations and lattices. *Illinois Journal of Mathematics*, 59(4):999–1023, 2015. Publisher: Duke University Press.

[vKM23] Rafael von Känel and Benjamin Matschke. *Solving S -Unit, Mordell, Thue, Thue–Mahler and Generalized Ramanujan–Nagell Equations via the Shimura–Taniyama Conjecture*, volume 286. American Mathematical Society, 2023.

[Vou95] Paul M. Voutier. Primitive divisors of Lucas and Lehmer sequences. *Mathematics of Computation*, 64(210):869–888, 1995.

[Wak03] Isao Wakabayashi. On a family of cubic Thue equations with 5 solutions. *Acta Arithmetica*, 109:285–298, 2003. Publisher: Instytut Matematyczny Polskiej Akademii Nauk.

[Wal20] Michel Waldschmidt. Thue Diophantine Equations: A Survey. In *Class Groups of Number Fields and Related Topics*, pages 25–41. Springer Singapore, Singapore, 2020.

[Zan15] Umberto Zannier. *Lecture notes on Diophantine analysis*, volume 8. Springer, 2015.