Thue Equations and Their Applications

Shabnam Akhtari

Pennsylvania State University

July 2025

Thue Equations

Let

$$F(x, y) = a_0 x^d + a_1 x^{d-1} y + \ldots + a_d y^d,$$

with $a_i \in \mathbb{Z}$, be a form of degree $d \geq 3$ which is irreducible over $\mathbb{Q}$.

Thue (1909)

The equation

$$F(x, y) = m$$

has only finitely many solutions in integers x and y, for any fixed integer m.

The Proof of Finiteness

$F(x, y) \in \mathbb{Z}[x, y]$. If $(x, y) \in \mathbb{Z}^2$ satisfies

$$\begin{aligned} F(x,y) &= a_0 x^d + a_1 x^{d-1} y + \ldots + a_d y^d \\ &= a_0 (x - \alpha_1 y) \ldots (x - \alpha_d y) \\ &= a_0 y^d \left(\frac{x}{y} - \alpha_1 \right) \ldots \left(\frac{x}{y} - \alpha_d \right) = m, \end{aligned}$$

then $\frac{x}{y}$ is a good **rational approximation** for one of the algebraic numbers α_i.

The Number of Solutions of Thue Equations

Evertse proved the first bound for the number of solutions that is independent of the coefficients of the form $F(x, y)$.

J. H. Evertse, Upper Bounds for the Numbers of Solutions of Diophantine Equations. Mathematical Centre Tracts, 168, Amsterdam, 1983.

The Number of Solutions of Thue Equations

Bombieri-Schmidt (1987)

The Tue equation $F(x, y) = m$ as at most

$$Cd^{1+\omega(m)}$$

primitive solutions.

The Size of Solutions of Thue Equations

Baker's method of linear forms in logarithms.

Solvability of Thue Equations

A positive proportion of Thue equations have no solutions.

Applications: Finiteness of Integral Points on Elliptic Curves.

Mordell was the first to prove the finiteness of the number of integral points on an elliptic curve, a theorem generalized by Siegel to all curves of genus $g \geq 1$.

Alpöge and Ho: *The second moment of the number of integral points on elliptic curves is bounded.*

Orders in Number Fields

K is a number field.

$\mathcal{O}$ is an order in K (a subring of $\mathcal{O}_K$ with quotient field K).

Monogenic Orders

The ring $\mathcal{O}$ is called monogenic if it is generated by one element as a $\mathbb{Z}$-algebra.

$\mathcal{O} = \mathbb{Z}[\alpha]$ for an element $\alpha \in K$.

The element α is called a monogenizer of $\mathcal{O}$.

Monogenization

For any $c \in \mathbb{Z}$,

$$\mathcal{O} = \mathbb{Z}[\alpha] = \mathbb{Z}[\pm\alpha + c].$$

We call α and $\pm\alpha + c$ equivalent.

A monogenization of $\mathcal{O}$ is an equivalence class of its monogenizers.

The Number of Monogenizations

K. Győry (1976)

An order $\mathcal{O}$ has at most finitely many monogenizations.

The Number of Monogenizations

Evertse and Győry (1985)

An order $\mathcal{O}$ in a number field K of degree n has at most $\left(3 \times 7^{2n!}\right)^{n-2}$ monogenizations.

The strategy is to reduce the problem to some Unit Form Equations.

The Number of Monogenizations

J.-H. Evertse (2011)

An order $\mathcal{O}$ in a number field K of degree n has at most $2^{4(n+5)(n-2)}$ monogenizations.

A. and Bhargava (2022)

An order $\mathcal{O}$ in a quartic number field K has at most 2760 monogenizations.

Orders in Quadratic Number Fields

Quadratic rings are parametrized by their discriminants D.

The unique (up to isomorphism) quadratic ring of discriminant D is

$$\mathbb{Z}\left[\frac{D+\sqrt{D}}{2}\right]$$

All quadratic rings are monogenic, and all have exactly one monogenization.

Monogenic Number Fields

We call a number field monogenic if its ring of integers (the maximal order) is monogenic.

In 1878 Dedekind gave the first example of a non-monogenic cubic field.

$$\mathbb{Q}[x]/(x^3 - x^2 - 2x - 8).$$

Non-Monogenic Number Fields

In the number field

$$\mathbb{Q}[x]/(x^3 - x^2 - 2x - 8).$$

2 splits completely.

Dedekind's result is a special case of the assertion that if 2 splits completely in a number field K of degree $n \geq 3$, then K cannot be monogenic.

Suppose $O_K = \mathbb{Z}[x]/(f(x))$ for a monic integral polynomial $f(x)$ of degree $n \geq 3$, then 2 factors in O_K as $f(x)$ factors (mod 2).

$f(x)$ cannot split completely (mod 2), as there are only two monic linear polynomials (mod 2).

Monogenic Number Fields

It is an open conjecture that a positive proportion of number fields of degree greater than 2 are not monogenic.

L. Alpöge, M. Bhargava, A. Shnidman (2020, 2021): A positive proportion of cubic and quartic number fields are not monogenic.

Diophantine Equations

Discriminant Form Equations

Let $\{1, \omega_2, \ldots, \omega_n\}$ be an integral basis for the number field K.

The discriminant form equation:

$$D_{K/\mathbb{Q}}(x_2\omega_2 + \ldots + x_n\omega_n) = D$$

in $x_2, \ldots, x_n$.

Discriminant of an Algebraic Number

The discriminant of an algebraic number is equal to the discriminant of its minimal polynomial over $\mathbb{Z}$.

The discriminant of the polynomial

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$$

is equal to

$$a_n^{2n-2} \prod_{i<j} (\alpha_i - \alpha_j)^2,$$

where α_i are the roots of the polynomial.

Index of an Algebraic Integer

We have

$$D(\alpha) = I^2(\alpha) D_K.$$

$I(\alpha)$ is the index of $\mathbb{Z}[\alpha]$ in the ring of integers of K.

For a given $\{1, \omega_2, \ldots, \omega_n\}$ integral basis for the number field K, we can write

$$D_{K/\mathbb{Q}}(x_2\omega_2 + \ldots + x_n\omega_n) = D_{K/\mathbb{Q}}(x_2, \ldots, x_n) = (I(x_2, \ldots, x_n))^2 D_K.$$

Index Form Equations

Let $\{1, \omega_2, \ldots, \omega_n\}$ be an integral basis for the number field K.

The index form equation:

$$I(x_2\omega_2 + \ldots + x_n\omega_n) = I(x_2, \ldots, x_n)$$

in $x_2, \ldots, x_n$.

The form $I(x_2\omega_2 + \ldots + x_n\omega_n)$ has degree $\binom{n}{2}$.

Index Forms in Cubic Number Fields

To find all algebraic integers in a given cubic number field with index m, we need to find the integer solutions of the cubic equation

$$I(x_2, x_3) = \pm m.$$

A Thue equation!!

Cubic Thue's Inequality

The number of solutions of $F(u, v) = m$ is expected to depend on m, in particular, the number of prime factors of m.

A. (2013)

$$|F(u, v)| \leq m$$

has at most $12 + B(\epsilon)$ primitive solutions in integers (u, v), provided that $m < D^{1/4-\epsilon}$.

The ring of integers in a cubic field of discriminant D can have at most $12 + B(\epsilon)$ monogenic subrings of index less than $D^{1/4-\epsilon}$.

Cubic Rings

Levi, Delone-Faddeev, Gan-Gross-Savin

The isomorphism classes of cubic rings are in natural $1-1$ correspondence with classes of binary cubic forms.

A. and Bhargava (2019)

A positive proportion of cubic Thue equations $F(x,y) = \pm 1$ have no solution.

The cubic forms are ordered by the size of their discriminant.

Many Cubic Rings Are Not Monegenic

Since the isomorphism classes of cubic rings are in natural $1-1$ correspondence with classes of binary cubic forms.

A. and Bhargava (2019)

A positive proportion of cubic rings are not monogenic.

Orders in Quartic Number Fields

$K = \mathbb{Q}(\alpha)$.

I_0 the index of the algebraic integer α.

Since $I(\alpha) = I_0$, for every algebraic integer $\beta \in K$, we have

$$I_0\beta \in \mathbb{Z}[\alpha].$$

Let

$$I_0\beta = a_\beta + x\alpha + y\alpha^2 + z\alpha^3,$$

with $a_\beta \in \mathbb{Z}$.

Index Forms in Quartic Number Fields

let $K = \mathbb{Q}(\alpha)$, and $\omega_1 = 1$, ω_2, ω_3 and ω_4 a fixed integral basis for K, with associated index form $I(x, y, z)$.

$$I_0 = I(\alpha).$$

Gaál, Pethő and Pohst (1996)

The triple $(x_1, y_1, z_1) \in \mathbb{Z}^3$ is a solution of $I(x, y, z) = m$ if and only if there is a solution $(u_1, v_1) \in \mathbb{Z}^2$ of a cubic Thue equation

$$F(u, v) = \pm I_0^5 m$$

such that (x_1, y_1, z_1) satisfies the system of ternary quadratic equations

$$Q_1(x, y, z) = u_1, \;\; Q_2(x, y, z) = v_1.$$

How?

$$K = \mathbb{Q}(\alpha),\ I(\alpha) = I_0.$$

We are looking for β with index m.

$$\beta' = I_0\beta \in \mathbb{Z}[\alpha].$$

$\alpha^{(i)}$ and $\beta'^{(i)}$ are algebraic conjugates of α and β' over $\mathbb{Q}$.

$$\prod_{(i,j,k,l)} \left(\frac{\beta'^{(i)} - \beta'^{(j)}}{\alpha^{(i)} - \alpha^{(j)}}\right)\left(\frac{\beta'^{(k)} - \beta'^{(l)}}{\alpha^{(k)} - \alpha^{(l)}}\right) = \pm\frac{I_0^6 m}{I_0} = \pm I_0^5 m,$$

where $(i,j,k,l) \in \{(1,2,3,4),(1,3,2,4),(1,4,2,3)\}$.

Ternary Quadratic Forms

For each (i, j, k, l),

$$\begin{aligned} & \left(\frac{\beta'^{(i)} - \beta'^{(j)}}{\alpha^{(i)} - \alpha^{(j)}} \right) \left(\frac{\beta'^{(k)} - \beta'^{(l)}}{\alpha^{(k)} - \alpha^{(l)}} \right) \\ = \quad & Q_1(x, y, z) - \alpha_{i,j,k,l} Q_2(x, y, z), \end{aligned}$$

where

$$\alpha_{i,j,k,l} = \alpha^{(i)}\alpha^{(j)} + \alpha^{(k)}\alpha^{(l)}.$$

Ternary Quadratic Forms

$K = \mathbb{Q}(\alpha)$ a quartic number field.

$f(X) = X^4 + a_1X^3 + a_2X^2 + a_3X + a_4$ the minimal polynomial of α.

$$
\begin{aligned}
&Q_1(x, y, z) = \\
&x^2 - a_1xy + a_2y^2 + (a_1^2 - 2a_2)xz + \\
&+(a_3 - a_1a_2)yz + (-a_1a_3 + a_2^2 + a_4)z^2,
\end{aligned}
$$

and

$$Q_2(x, y, z) = y^2 - xz - a_1yz + a_2z^2.$$

The Cubic Form

$$F(u,v) = u^3 - a_2u^2v + (a_1a_3 - 4a_4)uv^2 + (4a_2a_4 - a_3^2 - a_1^2a_4)v^3$$

Resolvent Cubic Form

Let

$$f(X) = X^4 + a_1X^3 + a_2X^2 + a_3X + a_4 \in \mathbb{Z}[X]$$

be the minimal polynomial of α.

$$F(u, v) = u^3 - a_2u^2v + (a_1a_3 - 4a_4)uv^2 + (4a_2a_4 - a_3^2 - a_1^2a_4)v^3$$

is the cubic resolvent of the polynomial $f(X)$.

The discriminant of $f(X)$ is equal to the discriminant of $F(u, 1) \in \mathbb{Z}[u]$.

Finding the Monogenizers

To find monogenizers of $\mathbb{Z}[\alpha]$, start with the power integral basis $\{1, \alpha, \alpha^2, \alpha^3\}$ and construct an index form, say $I(x, y, z)$.

A. (2021)

The triple $(x_1, y_1, z_1) \in \mathbb{Z}^3$ is a solution of $I(x, y, z) = \pm 1$ if and only if there is a solution $(u_1, v_1) \in \mathbb{Z}^2$ of the cubic Thue equation

$$F(u, v) = \pm 1$$

such that (x_1, y_1, z_1) satisfies

$$Q_1(x, y, z) = u_1, \;\; Q_2(x, y, z) = v_1.$$

Solutions of $F(u, v) = \pm 1$.

(u_1, v_1) satisfies the cubic Thue equation

$$F(u, v) = \pm 1$$

and (x_1, y_1, z_1) satisfies

$$Q_1(x, y, z) = u_1, \;\; Q_2(x, y, z) = v_1.$$

u_1, v_1 must be relatively prime.

The forms Q_1 and Q_2 are ternary quadratic and help us construct a quartic Thue equation!

Cubic and Quartic Thue Equations

M. Bennett

A cubic Thue equation $F(u, v) = 1$ has at most 10 solutions in integers u, v.

A. (2010)

A quartic Thue equation $F(u, v) = 1$ has at most 276 solutions in integers u, v.

An order $\mathcal{O}$ in a quartic number field K has at most 2760 monogenizations, because $2760 = 276 \times 10$.

Parametrization of Quartic Rings, A Different View

Bhargava in Higher Composition Laws III (2004)

There is a canonical bijection between the set of $\mathrm{GL}_3(\mathbb{Z}) \times \mathrm{Gl}_2(\mathbb{Z})$-orbits of the space of pairs of integral ternary quadratic forms and the set of isomorphism classes of pairs (Q, R), where Q is a quartic ring and R is a cubic resolvent ring of Q.

Wood in Quartic rings associated to binary quartic forms (2008)

There is a natural, discriminant-preserving bijection between the set of $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of binary quartic forms and the set of isomorphism classes of pairs (Q, C) where Q is a quartic ring and C is a monogenic cubic resolvent of Q (where isomorphisms are required to preserve the generator of C modulo $\mathbb{Z}$).

Multiply Monogenic Orders

An order is called m times monogenic if it has at least m monogenizations.

Bérczes, Evertse, Győry

Let K be a number field of degree at least 3. Then there are at most finitely many three times monogenic orders in K.

Classifying Multiply Monogenic Orders

An order $\mathcal{O}$ is called **Type I** if there are α and β in $\mathcal{O}$, and

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$$

such that

$$\mathcal{O} = \mathbb{Z}[\alpha] = \mathbb{Z}[\beta], \quad \text{and} \quad \beta = \frac{a\alpha + b}{c\alpha + d},$$

with $c \neq 0$.

Classifying Multiply Monogenic Orders

An order $\mathcal{O}$ is called **Type II** if there are α and β in $\mathcal{O}$ such that

$$\mathcal{O} = \mathbb{Z}[\alpha] = \mathbb{Z}[\beta]$$

and

$$\beta = a_0\alpha^2 + a_1\alpha + a_2, \quad \text{and} \quad \alpha = b_0\alpha^2 + b_1\alpha + b_2,$$

for some integers $a_0, a_1, a_2, b_0, b_1, b_2$.

What We Know

Bérczes, Evertse, Győry

Let K be a quartic number field, whose normal closure has Galois group S_4. Then apart from finitely many exceptions, every multiply monogenic order in K is two times monogenic of type I or II.

Type I Quartic Monogenic Orders

The monogenizers α and β have Type I relation if and only if they come from the same solution to the cubic equation $F(u, v) = \pm 1$.

In particular, this means that the two monogenizers α and β have Type I relation if and only if they correspond to the same monogenizer of the cubic resolvent ring of $\mathbb{Z}[\alpha]$.

Kappe and Warren (1989)

The Galois group of the normal closure of the quartic field K dictates the splitting behaviour of the cubic form $F(u, v)$ over $\mathbb{Q}$.

References

Papers

Bérczes, Evertse, Győry, Multiply Monogenic Orders, Ann. Sc. Norm. Super. Pisa Cl. Sci. (5) V ol. XII (2013)

Evertse, A survey on monogenic orders, *Publ. Math. Debrecen* 79 (3) (2011).

Books

J.-H. Evertse and K. Győry, Discriminant Equations in Diophantine Number Theory, Cambridge University Press, 2017.

I. Gaal, Diophantine Equations and Power Integral Bases, 2nd ed., Birkhäuser, 2019.

Thank You!