Index Form Equations in Quartic Number Fields

Shabnam Akhtari

March 10, 2023

Discriminant Form Equations

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

The discriminant form equation:

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

in $x_2, \dots, x_n$.

Evertse and Győry's Book: Discriminant Equations in Diophantine Number Theory.

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

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

Index Forms

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

The index form:

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

in $x_2, \ldots, x_n$.

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

Index Form Equations

Upper bounds for the number of solutions of index form equations are obtained by Evertse, Győry, Bérczes, ...

Index Forms in Cubic Number Fields

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

Index of a Quartic Algebraic Integer

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

I_0 the index of the algebraic integer α.

Since $I(\alpha) = I_0$, for every algebraic integer β, 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

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

$\omega_1 = 1$, ω_2, ω_3 and ω_4 a fixed integral basis for K.

$$\mathfrak{l}_1 := \mathfrak{l}_1(x, y, z) = x\omega_2 + y\omega_3 + z\omega_4.$$

$\mathfrak{l}_i$ denotes the algebraic conjugates of $\mathfrak{l}_1$ for $i = 1, 2, 3, 4$.

$$D_{K/\mathbb{Q}}(x\omega_2 + y\omega_3 + z\omega_4) = \prod_{1\le i<j\le 4} \left(\mathfrak{l}_i(x,y,z) - \mathfrak{l}_j(x,y,z)\right)^2 .$$

$$D_{K/\mathbb{Q}}(x\omega_2 + y\omega_3 + z\omega_4) = \left(I(x,y,z)\right)^2 D,$$

where D is the discriminant of the number field K.

$I(x,y,z) \in \mathbb{Z}[x,y,z]$ is a form of degree 6.

For any algebraic integer $\beta = a + x\omega_2 + y\omega_3 + z\omega_4$, with $a, x, y, z \in \mathbb{Z}$, the index $I(\beta)$ is equal to $|I(x,y,z)|$, where $I(\beta)$ is the module index of $\mathbb{Z}[\beta]$ in O_K.

How to Solve an Index Form Equation?

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

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

$$\mathfrak{l}_1 := \mathfrak{l}_1(x, y, z) = x\omega_2 + y\omega_3 + z\omega_4.$$

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

We denote by $\alpha^{(i)}$ and $\beta'^{(i)}$ the corresponding algebraic conjugates of α and β' over $\mathbb{Q}$, for $i = 1, 2, 3, 4$.

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

Finding Monogenizers of $\mathbb{Z}[\alpha]$

$$\prod_{(i,j,k,l)} \left(\frac{\beta^{(i)} - \beta^{(j)}}{\alpha^{(i)} - \alpha^{(j)}} \right) \left(\frac{\beta^{(k)} - \beta^{(l)}}{\alpha^{(k)} - \alpha^{(l)}} \right) = \pm 1$$

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

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

A Binary Cubic Form

$$\prod_{(i,j,k,l)} \left(\frac{\beta'^{(i)} - \beta'^{(j)}}{\alpha^{(i)} - \alpha^{(j)}}\right)\left(\frac{\beta'^{(k)} - \beta'^{(l)}}{\alpha^{(k)} - \alpha^{(l)}}\right)$$

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

$$Q_2(X, Y, Z) = y^2 - xz - a_1yz + a_2z^2.$$

How to Solve an Index Form Equation?

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

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

$$\mathfrak{l}_1 := \mathfrak{l}_1(x, y, z) = x\omega_2 + y\omega_3 + z\omega_4.$$

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

We denote by $\alpha^{(i)}$ and $\beta'^{(i)}$ the corresponding algebraic conjugates of α and β' over $\mathbb{Q}$, for $i = 1, 2, 3, 4$.

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

Index Forms in Quartic Number Fields

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

$\omega_1 = 1$, 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 $(x, y, z) \in \mathbb{Z}^3$ is a solution of $I(x, y, z) = m$ if and only if there is a solution $(u, v) \in \mathbb{Z}^2$ of the cubic Thue equation

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

such that (x, y, z) satisfies

$$Q_1(x, y, z) = u, \;\; Q_2(x, y, z) = v.$$

A Monogenic Order

K is a number field.

$\mathcal{O}$ is an order in K.

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 $\mathcal{O}$.

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.

The Number of Monogenizations

K. Győry (1976)

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

The Number of Monogenizations

J.-H. Evertse and K. Győry, On unit equations and decomposable form equations (1985).

Evertse and Győry

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 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)

A quartic order $\mathcal{O}$ has at most 2760 monogenizations.

Finding the Monogenizers of $\mathbb{Z}[\alpha]$

$$\prod_{(i,j,k,l)} \left(\frac{\beta^{(i)} - \beta^{(j)}}{\alpha^{(i)} - \alpha^{(j)}}\right) \left(\frac{\beta^{(k)} - \beta^{(l)}}{\alpha^{(k)} - \alpha^{(l)}}\right) = \pm 1.$$

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

with

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

Finding the Monogenizers of $\mathbb{Z}[\alpha]$

$$\prod_{(i,j,k,l)} \left(\frac{\beta^{(i)} - \beta^{(j)}}{\alpha^{(i)} - \alpha^{(j)}}\right) \left(\frac{\beta^{(k)} - \beta^{(l)}}{\alpha^{(k)} - \alpha^{(l)}}\right) = \pm 1.$$

$$\prod \left(Q_1(x, y, z) - \alpha_{i,j,k,l} Q_2(x, y, z)\right) = \pm 1.$$

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

$$F(u, v) = u^3 - a_2 u^2 v + (a_1 a_3 - 4a_4) u v^2 + (4a_2 a_4 - a_3^2 - a_1^2 a_4) v^3$$

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 $F(u,1) \in \mathbb{Z}[u]$.

Constructing Quartic Thue Equations

$$F(u,v) = u^3 - a_2u^2v + (a_1a_3 - 4a_4)uv^2 + (4a_2a_4 - a_3^2 - a_1^2a_4)v^3 = \pm 1$$

$$Q_1(x,y,z) = 1.$$

$$Q_2(x,y,z) = y^2 - xz - a_1yz + a_2z^2 = 0.$$

$$X(p,q) = p^2 - a_1pq + a_2q^2,\ Y(p,q) = pq,\ Z(p,q) = q^2.$$

$$Q_1(X(p,q), Y(p,q), Z(p,q)) = 1.$$

A quartic Thue equation!

Constructing Quartic Thue Equations for Non-trivial (u, v)

$$Q_1(x, y, z) = u_0,$$

$$Q_2(x, y, z) = v_0.$$

Find $s, t \in \mathbb{Z}$ such that

$$su_0 + tv_0 = 1.$$

Bhargava's Method

Manjul Bhargava, On the number of monogenizations of a quartic order, Publicationes Mathematicae (2022).

M. Wood, Quartic rings associated to binary quartic forms (2008): Natural bijection between classes of integral binary quartic forms and isomorphism classes of triples $(Q; R; \beta)$ where Q is a quartic ring, R is a monogenic cubic resolvent ring of Q, and β is a monogenizer of R up to equivalence.

Bhargava's Parametrization of Quartic Rings:
Canonical bijection between 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.

Index Form Equations

$$I(x, y, z) = \pm m$$

How many solutions?

We can give an upper bound for the number of integer solutions.

Index Form Equations

$$I(x, y, z) = \pm m$$

Index Form Equations

$$I(x, y, z) = \pm m$$

If there is an algebraic integer α in the quartic number field K with index m, then we can consider a cubic Thue equation:

$$F(u, v) = \pm m^6.$$

The cubic form F is the cubic resolvent of the minimal polynomial of α.

Solutions of Cubic Thue Equations

In order to find primitive solutions of the cubic equation

$$F(u, v) = \pm m^6.$$

we may reduce this equation modulo each prime divisor of m to obtain a family of cubic Thue equations of the shape

$$G(u, v) = \pm 1.$$

How many equations $G(u, v) = \pm 1$ can we possibly produce?

Primitive Solutions of Cubic Thue Equations

How many equations

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

do we have?

Quadratic Ternary Systems and Quartic Thue Equations

Each solution (u_0, v_0) of

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

gives a system of quadratic ternary equations

$$Q'_1(x, y, z) = u_0, \; Q'_2(x, y, z) = v_0.$$

This system gives a quartic Thue equation

$$Q(\mathfrak{p}, \mathfrak{q}) = 1.$$

Bhargava's Parametrization of Quartic Rings

Let $\left(\mathrm{Sym}^2\mathbb{Z}^3 \otimes \mathbb{Z}^2\right)^*$ denote the space of pairs of ternary quadratic forms having integer coefficients.

There is a canonical bijection between the set of $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{GL}_3(\mathbb{Z})$-orbits on the space $\left(\mathrm{Sym}^2\mathbb{Z}^3 \otimes \mathbb{Z}^2\right)^*$ of pairs of integral ternary quadratic forms and the set of isomorphism classes of pairs $(\mathfrak{Q}, \mathfrak{R})$, where $\mathfrak{Q}$ is a quartic ring and $\mathfrak{R}$ is a cubic resolvent ring of $\mathfrak{Q}$.

Non-primitive Solutions of Cubic Thue Equations

Non-primitive solutions of

$$F(u,v) = \pm m^6.$$

How many equations

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

do we have?

Questions?