ESSENTIAL
NUMBER THEORY

Quartic index form equations and monogenizations of quartic orders

Shabnam Akhtari

2022

vol. 1 no. 1

msp

msp

Essential Number Theory
Vol. 1, No. 1, 2022
https://doi.org/10.2140/ent.2022.1.57

Quartic index form equations and monogenizations of quartic orders

Shabnam Akhtari

Some upper bounds for the number of monogenizations of quartic orders are established by considering certain classical Diophantine equations, namely index form equations in quartic number fields, and cubic and quartic Thue equations.

1. Introduction

Let K be an algebraic number field and O_K its ring of integers. Let O be an order in K (a subring of O_K with quotient field K). We call the ring O *monogenic* if it is generated by one element as a $\mathbb{Z}$-algebra, i.e., $O = \mathbb{Z}[\alpha]$ for some $\alpha \in O$; the element α is called a *monogenizer* of O. If α is a monogenizer of O, than so is $\pm\alpha + c$ for any $c \in \mathbb{Z}$. We call two monogenizers α and α' of O *equivalent* if $\alpha' = \pm\alpha + c$ for some $c \in \mathbb{Z}$. Then by a *monogenization* of O, we mean an equivalence class of monogenizers of O. By fundamental work of Győry [1976], we know that any order in an algebraic number field can have at most finitely many monogenizations and that effectively computable upper bounds on the number of these monogenizations can be determined. It is a difficult computational problem to find or even count the monogenizations of a given order (many computational examples, interesting special cases and efficient algorithms in low degree number fields may be found in [Gaál 2019]).

We are interested in counting the number of monogenizations of a given order. An overview of various results on estimates for the number of monogenizations of orders in number fields is given in [Evertse 2011]. There are further extensions and generalizations of such results in [Evertse and Győry 2017] (in particular, see the relevant results in Section 9.1).

Monogenicity of algebraic number rings has a long history. It is an interesting problem to decide whether a given number field K is monogenic, that is, whether its ring of integers O_K, which is the maximal order in K, is monogenic. It is well known that quadratic number fields are monogenic. Dedekind [1878] gave the first example of a nonmonogenic cubic field. It is an open conjecture that most of

MSC2020: 11D25, 11D45, 11R04, 11R16.
Keywords: monogenizations of a quartic order, index form equations, Thue equations.

number fields of degree greater than 2 are not monogenic. For recent progress in this direction in the cases of cubic and quartic number fields, we refer the reader to the work of Alpöge, Bhargava, and Shnidman [Alpöge et al. 2021a; 2021b].

In this article we focus on the problem of counting the number of monogenizations of a quartic order. Evertse and Győry [1985] proved explicit upper bounds for the number of monogenizations of an order in a number field K. These bounds depend only on the degree of K. The best known result for $n \geq 4$ is due to Evertse [2011], who proved in that an order O in a number field K of degree n can have at most $2^{4(n+5)(n-2)}$ monogenizations. In the case $n = 4$, Evertse's result shows that an order in a quartic field can have at most 2^{72} monogenizations. Recently, Bhargava [2022] gave an improved bound in, showing that an order in a quartic number field can have at most 2760 monogenizations (and even fewer when the discriminant of the order is large enough). We give another proof for Theorem 1.1 of [Bhargava 2022].

Theorem 1.1. *Let O be an order in a quartic number field. The number of monogenizations of O is at most* 2760. *If the absolute value of the discriminant of O is sufficiently large, the number of monogenizations of O is at most* 182. *Moreover, if the discriminant of O is negative and has sufficiently large absolute value, the number of monogenizations of O is at most* 70.

In the above theorem the assumptions about the size of the discriminant are the result of such assumptions to overcome certain technical difficulties in some approximation methods used to prove Propositions 2.3, 2.5, and 2.6. These restrictions can be expressed explicitly. For instance, assuming the absolute value of the discriminant is at least 10^{500} will suffice; see [Akhtari 2009; 2012], where such explicit values are established but no effort has been made to optimize them. It is known that there are only finitely many quartic number fields with the absolute value of their discriminants bounded by a constant; see [Birch and Merriman 1972; Evertse and Győry 1991]. By the identity in (2), which relates the discriminant of an order to that of the underlying number field, Theorem 1.1 implies that with at most finitely many exceptions, a quartic order with positive discriminant can have at most 182 monogenizations and a quartic order with negative discriminant can have at most 70 monogenizations.

Our approach involves refining and modifying an algorithmic method developed by Gaál, Pethő and Pohst [Gaál et al. 1996] to solve an index form equation $I(X, Y, Z) = \pm 1$ in a quartic number field. Using this method, we will be able to associate explicit polynomials and binary and ternary forms to a monogenic order and a fixed monogenizer of that, and eventually reduce our problem to the resolution of a number of Thue equations of degree 3 and 4. The proof in [Bhargava 2022] uses a more abstract viewpoint by utilizing two ways of parametrizing quartic rings, one established by Bhargava [2004] and another one established by Wood [2012].

2. Preliminaries: discriminants, Thue equations, discriminant and index form equations

2A. ***Discriminants.*** We recall the definitions of discriminants of orders, polynomials, algebraic numbers, and binary forms which will be frequently used throughout this manuscript. We will also refer to the discriminant of number fields. The discriminant of a number field K is the discriminant of its maximal order, the ring of integers O_K. For $K = \mathbb{Q}(\alpha)$, the discriminant of K can be expressed in terms of the discriminant of the algebraic number α and its index in $\mathbb{Q}(\alpha)$. The index of an algebraic integer and the discriminant of orders are defined in Section 2B.

Let $\boldsymbol{P}(T) \in \mathbb{Z}[T]$ be a polynomial of degree n and leading coefficient $a \in \mathbb{Z}$. The discriminant $\mathrm{Disc}(\boldsymbol{P})$ of $\boldsymbol{P}(T)$ is

$$\mathrm{Disc}(\boldsymbol{P}) = a^{2n-2} \prod_{i<j} (\gamma_i - \gamma_j)^2,$$

where $\gamma_1, \ldots, \gamma_n \in \mathbb{C}$ are the roots of $\boldsymbol{P}(T)$.

The discriminant of an algebraic number is defined as the discriminant of its minimal polynomial.

Let $F(U, V) \in \mathbb{Z}[U, V]$ be a binary form of degree n that factors over $\mathbb{C}$ as

$$\prod_{i=1}^{n} (\alpha_i U - \beta_i V).$$

The discriminant $D(F)$ of F is given by

$$D(F) = \prod_{i<j} (\alpha_i \beta_j - \alpha_j \beta_i)^2. \tag{1}$$

We note that the discriminant of the polynomial $F(U, 1) \in \mathbb{Z}[U]$ is equal to the discriminant of the binary form $F(U, V) \in \mathbb{Z}[U, V]$.

2B. ***Discriminant and index form equations.*** Let K be an algebraic number field of degree n. Let $\alpha_1, \ldots, \alpha_n$ a linearly independent set of n elements of K. Let $\sigma_1, \ldots, \sigma_n : K \to \mathbb{C}$ be all the embeddings of K into $\mathbb{C}$. The discriminant of $(\alpha_1, \ldots, \alpha_n)$ is defined as the square of the determinant of an $n \times n$ matrix:

$$D_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) := (\det(\sigma_i(\alpha_j)))^2,$$

where $i, j \in \{1, \ldots, n\}$.

If $\{\beta_1, \ldots, \beta_n\}$ forms a basis for O_K, then the discriminant of K is

$$D_K = D_{K/\mathbb{Q}}(\beta_1, \ldots, \beta_n).$$

Let $\gamma_1, \gamma_2, \ldots, \gamma_n$ be an integral basis for an order O in a number field K of degree n (we note that by definition an order is a full-rank $\mathbb{Z}$-module in O_K). The

discriminant of O is defined as $D_{K/\mathbb{Q}}(\gamma_1, \ldots, \gamma_n)$ and is independent of the choice of the integral basis $\gamma_1, \gamma_2, \ldots, \gamma_n$; see [Koch 1997], or any introductory text in algebraic number theory.

The following basic well-known lemmas are due to Hensel [1908].

Lemma 2.1. *Let $\alpha_1, \ldots, \alpha_n \in O_K$ be linearly independent over $\mathbb{Q}$ and set*

$$O = \mathbb{Z}[\alpha_1, \ldots, \alpha_n].$$

then

$$D_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) = J^2 D_K, \tag{2}$$

where O_K^+ and O^+ are the additive groups of the modules O_K and O, respectively, and $J = (O_K^+ : O^+)$ is the module index.

For every $\gamma \in K$, we denote the algebraic conjugates of γ by $\gamma^{(i)}$ $(1 \le i \le n)$. Let $\{1, \omega_2, \ldots, \omega_n\}$ be an integral basis of K. Let

$$\boldsymbol{X} = (X_1, \ldots, X_n),$$

and

$$L(\boldsymbol{X}) = X_1 + \omega_2 X_2 + \cdots + \omega_n X_n, \tag{3}$$

with algebraic conjugates

$$L^{(i)}(\boldsymbol{X}) = X_1 + \omega_2^{(i)} X_2 + \cdots + \omega_n^{(i)} X_n,$$

$(1 \le i \le n)$. Kronecker and Hensel called the form $L(\boldsymbol{X})$ the *Fundamentalform* and

$$D_{K/\mathbb{Q}}(L(\boldsymbol{X})) = \prod_{1 \le i < j \le n} (L^{(i)}(\boldsymbol{X}) - L^{(j)}(\boldsymbol{X}))^2 \tag{4}$$

the *Fundamentaldiskriminante*.

Lemma 2.2. *We have*

$$D_{K/\mathbb{Q}}(L(\boldsymbol{X})) = (I(X_1, \ldots, X_n))^2 D_K,$$

where D_K is the discriminant of the field K, the linear form $L(\boldsymbol{X})$ and its discriminant are defined in (3) *and* (4)*, and $I(X_1, \ldots, X_n)$ is a homogeneous form in $n-1$ variables of degree $n(n-1)/2$ with integer coefficients.*

The form $I(X_1, \ldots, X_n)$ in the statement of Lemma 2.2 is called the index form corresponding to the integral basis $\{1, \omega_2, \ldots, \omega_n\}$. An important property of the index form is that for any algebraic integer

$$\alpha = x_1 + x_2\omega_2 + \cdots + x_n\omega_n,$$

with $K = \mathbb{Q}(\alpha)$, by Lemma 2.2 we have

$$I(\alpha) = |I(x_2, \ldots, x_n)|,$$

where $I(\alpha)$ is the index of the module $\mathbb{Z}[\alpha]$ in O_K. The index form is independent of the variable X_1, for if $\beta = \alpha + a$, where $a \in \mathbb{Z}$, then $I(\alpha) = I(\beta)$.

We remark that in a cubic number field an index form equation is in fact a cubic Thue equation (see Section 2C for the definition)

$$I(X_2, X_3) = \pm m,$$

where $m \in \mathbb{Z}$. In [Akhtari 2020] we have discussed some results about cubic Thue equations and their consequences in resolving index form equations and counting the number of monogenizations of a cubic ring.

2C. ***Upper bounds on the number of solutions of cubic and quartic Thue equations.*** Let $F(U, V) \in \mathbb{Z}[U, V]$ be a binary form of degree at least 3. If $F(U, V)$ is irreducible over $\mathbb{Q}$, for any integer m, it is shown in [Thue 1909] that the equation

$$F(U, V) = m$$

has at most finitely many solutions in integers U, V. These equations are called *Thue equations*. We will summarize some useful results on the number of integer solutions of binary cubic and quartic Thue equations. In Propositions 2.3–2.6, two pairs of solutions (u, v), $(-u, -v) \in \mathbb{Z}^2$ are considered as one solution.

The following is the combination of main results due to Bennett [2001] and Okazaki [2002]; see also [Akhtari 2009].

Proposition 2.3. *A cubic Thue equation $F(U, V) = \pm 1$ has at most 10 integer solutions. If the absolute value of the discriminant of $F(U, V)$ is sufficiently large then $F(U, V) = \pm 1$ has at most 7 integer solutions.*

The following result was established independently by Delone [1930] and Nagell [1928].

Proposition 2.4. *Let $F(U, V) \in \mathbb{Z}[U, V]$ be a cubic binary form with negative discriminant. The Thue equation $F(U, V) = \pm 1$ has at most 5 integers solutions.*

The following is Theorem A.1 of [Bhargava 2022], where results from [Akhtari 2015; 2012; Bennet and Rechnitzer $\geq$ 2022] are combined to obtain upper bounds for the number of integral solutions to quartic Thue equations.

Proposition 2.5. *A quartic Thue equation $F(U, V) = \pm 1$ has at most 276 integer solutions. If the absolute value of the discriminant of $F(U, V)$ is sufficiently large then the quartic Thue equation $F(U, V) = \pm 1$ has at most 26 integer solutions.*

The following is part of the main theorem in [Akhtari 2012].

Proposition 2.6. *Let $F(U, V) \in \mathbb{Z}[U, V]$ be a quartic binary form with negative discriminant. If the absolute value of the discriminant of $F(U, V)$ is sufficiently large, the Thue equation $F(U, V) = \pm 1$ has at most 14 integer solutions.*

2D. ***Matrix actions on binary forms.*** We summarize some trivial facts about matrix actions on binary forms that are well known to those in the field. Let $F(U, V) \in \mathbb{Z}[U, V]$ and $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ be a 2×2 matrix with integer entries. We define the binary form

$$F_A(U, V) \in \mathbb{Z}[U, V]$$

by

$$F_A(U, V) = F(aU + bV, cU + dV).$$

Via the definition (1), we observe that for any 2×2 matrix A with integer entries

$$D(F_A) = (\det A)^{n(n-1)} D(F). \tag{5}$$

We say that two integral binary forms F and G are *equivalent* if $G = \pm F_A$ for some $A \in \mathrm{GL}_2(\mathbb{Z})$. This is in fact an equivalence relationship. Moreover, the discriminants of two equivalent forms are equal.

For $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$, and any $(u, v) \in \mathbb{Z}^2$, we clearly have

$$A^{-1} = \pm \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

and

$$F_A(du - bv, -cu + av) = \pm F(u, v).$$

Therefore, there is a one-to-one correspondence between the possible solutions of the Thue equation $F(U, V) = \pm 1$ and those of the Thue equation $F_A(U, V) = \pm 1$.

3. Index form equations in quartic number fields

Let ξ be a quartic algebraic integer with the minimal polynomial

$$\boldsymbol{P}(T) = T^4 + a_1 T^3 + a_2 T^2 + a_3 T + a_4 \in \mathbb{Z}[T]. \tag{6}$$

Let $K = \mathbb{Q}(\xi)$. Suppose that $\omega_1 = 1$, ω_2, ω_3 and ω_4 form an integral basis for the quartic number field K. We write σ_1, σ_2, σ_3 and σ_4 for the distinct embeddings of K into $\mathbb{C}$. For $i = 1, 2, 3, 4$, we define the linear forms

$$l_i(X, Y, Z) = X\omega_2^{(i)} + Y\omega_3^{(i)} + Z\omega_4^{(i)},$$

where $\omega_j^{(i)} = \sigma_i(\omega_j)$.

The *discriminant form* corresponding to the integral basis $\{1, \omega_2, \omega_3, \omega_4\}$ is defined by

$$D_{K/\mathbb{Q}}(X\omega_2 + Y\omega_3 + Z\omega_4) = \prod_{1 \le i < j \le 4} (l_i(X, Y, Z) - l_j(X, Y, Z))^2.$$

We have

$$D_{K/\mathbb{Q}}(X\omega_2 + Y\omega_3 + Z\omega_4) = (I(X, Y, Z))^2 D_K, \tag{7}$$

where D_K is the discriminant of the number field K and $I(X, Y, Z) \in \mathbb{Z}[X, Y, Z]$ is the *index form* corresponding to the fixed integral basis $\{1, \omega_2, \omega_3, \omega_4\}$. The integral ternary form $I(X, Y, Z)$ has degree 6. For any algebraic integer $\alpha = a + x\omega_2 + y\omega_3 + z\omega_4$, with $a, x, y, z \in \mathbb{Z}$, the index $I(\alpha)$ is equal to $|I(x, y, z)|$, where $I(\alpha)$ is the module index of $\mathbb{Z}[\alpha]$ in O_K, the ring of integers of K. In this section we consider the *index form equation*

$$I(X, Y, Z) = \pm m \tag{8}$$

where $m \in \mathbb{Z}$.

We follow a simple and efficient algorithm given by Gaál, Pethő and Pohst [1996], where they reduce the problem of solving an index form equation in a quartic number field to the problem of finding all solutions $(u_i, v_i) \in \mathbb{Z}^2$ of a cubic Thue equation $F(U, V) = \pm h$, with $h \in \mathbb{Z}$, and the resolution of corresponding systems of quadratic equations $\boldsymbol{Q}_1(X, Y, Z) = u_i$, $\boldsymbol{Q}_2(X, Y, Z) = v_i$, where $F(U, V) \in \mathbb{Z}[U, V]$ is a cubic form, and $\boldsymbol{Q}_1(X, Y, Z)$ and $\boldsymbol{Q}_2(X, Y, Z)$ are integral ternary quadratic forms. We state this reduction more precisely in Proposition 3.1.

We denote by I_0 the index of the algebraic integer ξ. Then

$$I_0 = I(\xi) = |I(x_0, y_0, z_0)|,$$

where $\xi = a_\xi + x_0\omega_2 + y_0\omega_3 + z_0\omega_4$, and $a_\xi, x_0, y_0, z_0 \in \mathbb{Z}$. Once again we remark that the algebraic integers ξ and $\xi - a_\xi$ have the same index in O_K. Since I_0 is the index of $\mathbb{Z}[\xi]$ in O_K, for every algebraic integer $\alpha \in O_K$, we have

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

Assume that $(x_1, y_1, z_1) \in \mathbb{Z}^3$ satisfies (8). Let

$$\alpha = x_1\omega_2 + y_1\omega_3 + z_1\omega_4, \tag{9}$$

and

$$\alpha' = I_0\alpha = a'_\alpha + x'_1\xi + y'_1\xi^2 + z'_1\xi^3 \in \mathbb{Z}[\xi]. \tag{10}$$

We have

$$I(\alpha') = I(x'\xi + y'\xi^2 + z'\xi^3) = \pm I_0^6 m. \tag{11}$$

We denote by $\xi^{(i)}$ and $\alpha'^{(i)}$ the algebraic conjugates of ξ and α', for $i = 1, 2, 3, 4$. Dividing both sides of the (11) by $I(\xi) = I_0$, we obtain

$$\prod_{(i,j,k,l)} \left(\frac{\alpha'^{(i)} - \alpha'^{(j)}}{\xi^{(i)} - \xi^{(j)}}\right)\left(\frac{\alpha'^{(k)} - \alpha'^{(l)}}{\xi^{(k)} - \xi^{(l)}}\right) = \pm\frac{I_0^6 m}{I_0} = \pm I_0^5 m, \tag{12}$$

where the above product is taken for $(i, j, k, l) = (1, 2, 3, 4), (1, 3, 2, 4), (1, 4, 2, 3)$. For each (i, j, k, l), via (10), we have

$$\left(\frac{\alpha'^{(i)} - \alpha'^{(j)}}{\xi^{(i)} - \xi^{(j)}}\right)\left(\frac{\alpha'^{(k)} - \alpha'^{(l)}}{\xi^{(k)} - \xi^{(l)}}\right) = \boldsymbol{Q}_1(x_1', y_1', z_1') - \xi_{i,j,k,l}\,\boldsymbol{Q}_2(x_1', y_1', z_1'), \tag{13}$$

where

$$\xi_{i,j,k,l} = \xi^{(i)}\xi^{(j)} + \xi^{(k)}\xi^{(l)},$$

$$\boldsymbol{Q}_1(X, Y, Z) = X^2 - a_1XY + a_2Y^2 + (a_1^2 - 2a_2)XZ + (a_3 - a_1a_2)YZ + (-a_1a_3 + a_2^2 + a_4)Z^2, \tag{14}$$

and

$$\boldsymbol{Q}_2(X, Y, Z) = Y^2 - XZ - a_1YZ + a_2Z^2. \tag{15}$$

The coefficients of the quadratic forms $\boldsymbol{Q}_1(X, Y, Z)$ and $\boldsymbol{Q}_2(X, Y, Z)$ are expressed in terms of the coefficients of $\boldsymbol{P}(T)$, the minimal polynomial of ξ given in (6). For each $(i, j, k, l) = (1, 2, 3, 4), (1, 3, 2, 4), (1, 4, 2, 3)$, we define the linear form

$$\mathcal{P}(i, j, k, l) = \mathcal{P}(i, j, k, l)(U, V) = U - \xi_{1,2,3,4}V.$$

Taking $U = \boldsymbol{Q}_1(X, Y, Z)$ and $V = \boldsymbol{Q}_2(X, Y, Z)$, by (12) and (13), we obtain

$$\prod_{(i,j,k,l)} \mathcal{P}(i, j, k, l) = (U - \xi_{1,2,3,4}V)(U - \xi_{1,3,2,4}V)(U - \xi_{1,4,2,3}V) = \pm I_0^5 m, \tag{16}$$

where the product is taken over $(i, j, k, l) = (1, 2, 3, 4), (1, 3, 2, 4), (1, 4, 2, 3)$.

The left-hand side of (16) is a cubic binary form in U and V whose coefficients are symmetric polynomials of $\xi^{(1)}, \xi^{(2)}, \xi^{(3)}, \xi^{(4)}$. Simple and routine calculations show that this integral cubic binary form is

$$\begin{aligned}\prod_{(i,j,k,l)} \mathcal{P}(i, j, k, l)(U, V) &= F(U, V)\\ &= U^3 - a_2U^2V + (a_1a_3 - 4a_4)UV^2 + (4a_2a_4 - a_3^2 - a_1^2a_4)V^3.\end{aligned} \tag{17}$$

The cubic polynomial

$$F(T, 1) = T^3 - a_2T^2 + (a_1a_3 - 4a_4)T + (4a_2a_4 - a_3^2 - a_1^2a_4)$$

is called the *cubic resolvent polynomial* of $\boldsymbol{P}(T)$, the minimal polynomial of ξ. The discriminant of $\boldsymbol{P}(T) \in \mathbb{Z}[T]$ is equal to the discriminant of $F(T, 1) \in \mathbb{Z}[T]$ and therefore to the discriminant of $F(U, V) \in \mathbb{Z}[U, V]$. Since the discriminant of the minimal polynomial $\boldsymbol{P}(T)$ is not zero, we conclude that $F(U, V)$ will factor into three pairwise nonproportional linear factors over $\mathbb{C}$. This, together with (16), implies that the three cubic algebraic integers $\xi_{1,2,3,4}$, $\xi_{1,3,2,4}$, and $\xi_{1,4,2,3}$ are distinct algebraic conjugates over $\mathbb{Q}$. The above argument can be found in [Gaál 2019] and [Gaál et al. 1996], and implies the following.

Proposition 3.1. *Let ξ be a quartic algebraic integer and*

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

Assume that $I(X, Y, Z) \in \mathbb{Z}[X, Y, Z]$ is an index form in the quartic number field $\mathbb{Q}(\xi)$. The triple $(x, y, z) \in \mathbb{Z}^3$ is a solution of the index form equation

$$I(X, Y, Z) = \pm m,$$

with $m \in \mathbb{Z}$, if and only if there exists a solution $(u, v) \in \mathbb{Z}^2$ of the cubic Thue equation

$$F(U, V) = \pm I_0^5 m \tag{18}$$

such that (x, y, z) satisfies the system of quadratic ternary equations

$$\boldsymbol{Q}_1(X, Y, Z) = u, \quad \boldsymbol{Q}_2(X, Y, Z) = v, \tag{19}$$

where $F(U, V)$ is an integral cubic binary form and $\boldsymbol{Q}_1(X, Y, Z)$ and $\boldsymbol{Q}_2(X, Y, Z)$ are integral quadratic ternary forms, respectively defined in (17), (14) *and* (15) *with coefficients expressed in terms of the coefficients of the minimal polynomial of the fixed generator ξ.*

Proposition 3.1 provides a general algorithm to find algebraic integers with index m in the quartic number field K by fixing any algebraic integer ξ that generates K. So in general the quantities I_0 and m need not to be related. Using an argument of Mordell [1969], in [Gaál et al. 1996] it is shown that all solutions of an index form equation in a quartic number field can be found through solving finitely many cubic and quartic Thue equations; see Theorems 1 and 2, as well as equations (8), (9) and (10) of [loc. cit.]. In Section 4 we will modify the argument in [loc. cit.] and apply our modification to an index form equation of the shape $I(X, Y, Z) = \pm 1$ connected to the quartic ring generated by an algebraic integer ξ. This will enable us to count these Thue equations more efficiently. Moreover, it turns out that in this case the right-hand sides of our Thue equations are ± 1, and therefore we may apply absolute upper bounds for the number of integer solutions recorded in Section 2C. This way we can provide an absolute upper bound for the number of solutions of

the index form equation that we study. These solutions will correspond to different monogenizations of the quartic order $\mathbb{Z}[\xi]$.

We end this section by recording another important relation between the ternary quadratic forms $\boldsymbol{Q}_1$ and $\boldsymbol{Q}_2$, defined in (14) and (15), and the integer values represented by the cubic form $F(U, V)$. For $(u_0, v_0) \in \mathbb{Z}^2$, we define

$$\boldsymbol{Q}(X, Y, Z) = u_0 \boldsymbol{Q}_2(X, Y, Z) - v_0 \boldsymbol{Q}_1(X, Y, Z). \tag{20}$$

Let $M_{\boldsymbol{Q}}$ be the 3×3 symmetric Gram matrix of the quadratic form $\boldsymbol{Q}(X, Y, Z)$. We have

$$4|\mathrm{Det}(M_{\boldsymbol{Q}})| = |F(u_0, v_0)|, \tag{21}$$

where $F(U, V)$ is defined in (17). The identity (21) can be verified easily and is established as an implication of Lemma 1 of [Gaál et al. 1996]. Its proof can also be found in Lemma 6.1.1 of [Gaál 2019]. The identity (21) is not used in our proofs, but it is crucial in confirming that the ternary quadratic forms $\boldsymbol{Q}_1$ and $\boldsymbol{Q}_2$ form a pair that parametrizes a quartic ring in the sense of Bhargava [2004]. Such a parametrization is used in Bhargava's proof of Theorem 1.1 [Bhargava 2022]. Another ingredient in [Bhargava 2022] is a beautiful parametrization due to Wood [2012] for quartic rings. We do not use any of these two parametrizations. However, in light of identities (20) and (21), one could view our discussion in the following section as an explicit way of expressing polynomials and binary forms that are appearing (implicitly) in Bhargava's and Wood's methods of parametrization.

4. Proof of Theorem 1.1

When treating a general index form equation in a quartic number field, one needs to consider the identity (10) in order to have integer values for x_1', y_1' and z_1'. In Theorem 1.1 we are interested in finding other possible monogenizers for a monogenized ring $\mathbb{Z}[\xi]$. Therefore, we are looking for algebraic integers $\alpha \in \mathbb{Z}[\xi]$ that satisfy the index form (8). In this case, under the assumption $\alpha \in \mathbb{Z}[\xi]$, we may express (10) as

$$\alpha = a_\alpha + x\xi + y\xi^2 + z\xi^3, \tag{22}$$

with $x, y, z \in \mathbb{Z}$. This will simplify some of the equations introduced in Section 3. Another simple observation is that if $\mathbb{Z}[\xi] = \mathbb{Z}[\alpha]$, then the algebraic integers α and ξ have the same index in the ring of integers of the underlying number field $\mathbb{Q}(\alpha) = \mathbb{Q}(\xi)$, and therefore in the index form (11) and (12), we may take $I_0 = m$.

Let K be a quartic number field and ξ an algebraic integer in K of index $I_0 = m$. We are interested in finding other monogenizers of $\mathbb{Z}[\xi]$. After replacing (10) by

(22), for $\alpha \in \mathbb{Z}[\xi]$ the identity (12) becomes

$$\prod_{(i,j,k,l)} \left(\frac{\alpha^{(i)} - \alpha^{(j)}}{\xi^{(i)} - \xi^{(j)}}\right)\left(\frac{\alpha^{(k)} - \alpha^{(l)}}{\xi^{(k)} - \xi^{(l)}}\right) = \pm 1. \tag{23}$$

Therefore, in Proposition 3.1, we may consider the cubic Thue equation

$$F(U, V) = \pm 1. \tag{24}$$

In fact, we obtain the following modification of Proposition 3.1.

Lemma 4.1. *The algebraic integer $x\xi + y\xi^2 + z\xi^3$, with $x, y, z \in \mathbb{Z}$ is a monogenizer of $\mathbb{Z}[\xi]$ if and only if there is a solution $(u, v) \in \mathbb{Z}^2$ of the cubic Thue equation*

$$F(U, V) = \pm 1 \tag{25}$$

such that (x, y, z) satisfies the system of quadratic ternary equations

$$\boldsymbol{Q}_1(X, Y, Z) = u, \quad \boldsymbol{Q}_2(X, Y, Z) = v. \tag{26}$$

4A. *The trivial solution of $F(U, V) = 1$.* First we notice that $F(U, V)$ is monic and therefore $(u, v) = (1, 0)$ satisfies the equation $F(U, V) = \pm 1$. This corresponds to the system of equations

$$\begin{aligned} \boldsymbol{Q}_1(X, Y, Z) &= 1 \\ \boldsymbol{Q}_2(X, Y, Z) &= 0, \end{aligned} \tag{27}$$

where the ternary quadratic forms $\boldsymbol{Q}_1$ and $\boldsymbol{Q}_2$ are defined in (14) and (15).

A special solution to the system of equations (27) is $(x, y, z) = (1, 0, 0)$ as ξ is trivially a monogenizer of $\mathbb{Z}[\xi]$; see (10).

Assume $x, y, z \in \mathbb{Z}$ satisfy (27). Then

$$\boldsymbol{Q}_2(x, y, z) = y^2 - xz - a_1yz + a_2z^2 = 0. \tag{28}$$

If $z = 0$ then $y = 0$. Since x, y, z also satisfy $\boldsymbol{Q}_1(X, Y, Z) = 1$, we conclude that $x = 1$.

Now assume that $z \neq 0$. From (28), we conclude that $z \mid y^2$. Let $q = \gcd(z, y)$, $y = qy'$ and $z = qz'$, with $\gcd(y', z') = 1$. We may rewrite (28) as

$$\boldsymbol{Q}_2(x, y, z) = y'^2q^2 - xz'q - a_1y'z'q^2 + a_2z'^2q^2 = 0$$

to conclude that $q \mid xz'$ and $z' \mid q$. Since (x, y, z) satisfies the system (27), in particular $\boldsymbol{Q}_1(x, y, z) = 1$, we have $\gcd(q, x) = 1$ and therefore $q \mid z'$. So we have $z' = \pm q$ and $q^2 = \pm z$. Since (x, y, z) and $(-x, -y, -z)$ give the same monogenization, we may assume $z \geq 0$ and $q^2 = z$. Now we can express x, y and z in terms of two integers q and p as follows:

$$x = p^2 - a_1pq + a_2q^2, \quad y = pq, \quad z = q^2. \tag{29}$$

The parametrization (29) can be done for any $(x, y, z) \neq (1, 0, 0)$ that satisfies (28). Substituting the parametrized values for variables X, Y and Z in (14), we may express the ternary quadratic form $\boldsymbol{Q}_1(X, Y, Z)$ as a quartic binary form in variables P, Q, where

$$X(P, Q) = P^2 - a_1 PQ + a_2 Q^2, \quad Y(P, Q) = PQ, \quad Z(P, Q) = Q^2. \tag{30}$$

We note that each $X(P, Q)$, $Y(P, Q)$ and $Z(P, Q)$ is a binary quadratic form in variables P and Q. The parametrization (29) was considered for $z \neq 0$, however the trivial (and special) solution $(x, y, z) = (1, 0, 0)$ also corresponds to a solution of the quartic Thue equation

$$\boldsymbol{Q}_1(X(P, Q), Y(P, Q), Z(P, Q)) = 1,$$

namely $(p, q) = (1, 0)$.

Let us define the quartic binary form

$$\mathcal{Q}_{(1,0)}(P, Q) = \mathcal{Q}(P, Q) = \boldsymbol{Q}_1(X(P, Q), Y(P, Q), Z(P, Q)). \tag{31}$$

We have shown that the number of solutions $(X, Y, Z) \in \mathbb{Z}^3$ of the system of ternary equations (27) is equal to the number of integer solutions (p, q) of the quartic Thue equation

$$\mathcal{Q}(P, Q) = 1.$$

Via (27), we may substitute the parameter X by $(Y^2 - a_1 YZ + a_2 Z^2)/Z^2$ in $\boldsymbol{Q}_1(X, Y, Z)$ to get

$$\boldsymbol{Q}_1(X, Y, Z) = Z^4 \boldsymbol{P}\big(\tfrac{Y}{Z} - a_1\big),$$

where $\boldsymbol{P}(T)$ is the minimal polynomial of ξ defined in (6). In other words,

$$\mathcal{Q}(P, Q) = Q^4 \boldsymbol{P}\big(\tfrac{P}{Q} - a_1\big).$$

Since $a_1 \in \mathbb{Z}$, we conclude that the discriminant of the quartic form $\mathcal{Q}(P, Q)$ is equal to the discriminant of ξ, and therefore, to the discriminant of the cubic form $F(U, V)$.

We also note that $\mathcal{Q}(P, Q)$ is a monic binary form, i.e., the coefficient of the term P^4 equals 1. This confirms the existence of the trivial solution $(p, q) = (1, 0)$ of the Thue equation $\mathcal{Q}(P, Q) = 1$.

We conclude that the trivial solution $(1, 0)$ of the cubic Thue equation $F(U, V) = 1$ corresponds to a quartic Thue equation, namely $\mathcal{Q}_{(1,0)}(P, Q) = 1$, defined in (31). Moreover, by (29), each pair of solution $(p, q) \in \mathbb{Z}^2$ corresponds to the monogenizer

$$X(p, q)\xi + Y(p, q)\xi^2 + Z(p, q)\xi^3$$

of the order $\mathbb{Z}[\xi]$. Clearly, the monogenizer ξ is produced by the solution $(p, q) = (1, 0)$ of the quartic Thue equation.

4B. ***Nontrivial solutions of*** $F(U, V) = 1$**.** For nontrivial solutions of the Thue equation (24), in [Gaál et al. 1996] the system of ternary quadratic equations (32) is reduced to a quartic Thue equation with a parametrization similar to (30); see equations (8) and (10) of [Gaál et al. 1996]. We simplify such a parametrization with help of a $\mathrm{GL}_2(\mathbb{Z})$ matrix that maps any given primitive solution of a Thue equation to the trivial solution $(1, 0)$ of an equivalent Thue equation. More precisely, assume that $(u_0, v_0) \in \mathbb{Z}^2$, with $(u_0, v_0) \neq (1, 0)$, satisfies (24). We have $\gcd(u_0, v_0) = 1$ and therefore we may choose fixed $s, t \in \mathbb{Z}$ so that

$$su_0 + tv_0 = 1.$$

Consequently, if $(x, y, z) \in \mathbb{Z}^3$ satisfies the system of equations in (19) with $(u, v) = (u_0, v_0)$, then (x, y, z) will satisfy

$$\begin{aligned} \mathbf{Q}'_1(X, Y, Z) &= s\,\boldsymbol{Q}_1(X, Y, Z) + t\,\boldsymbol{Q}_2(X, Y, Z) = 1 \\ \mathbf{Q}'_2(X, Y, Z) &= v_0\,\boldsymbol{Q}_1 - u_0\,\boldsymbol{Q}_2 = 0. \end{aligned} \tag{32}$$

The next step is to express this system as an equation of a quartic binary form to 1, via the parametrization (30).

Let $A = \left(\begin{smallmatrix} s & t \\ -v_0 & u_0 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$. Clearly we have

$$A\begin{pmatrix} u_0 \\ v_0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

The matrix $A^{-1} \in \mathrm{GL}_2(\mathbb{Z})$ acts on the binary cubic form $F(U, V)$ to produce the equivalent binary form $F_{A^{-1}}(U, V)$. The solution (u_0, v_0) of $F(U, V) = 1$ corresponds to the solution $(1, 0)$ of the cubic equation $F_{A^{-1}}(U, V) = 1$.

Since $(1, 0)$ satisfies the equation $F_{A^{-1}}(U, V) = 1$, the cubic binary form $F_{A^{-1}}(U, V)$ is monic. Similar to (31), and via parametrization (30), we obtain the binary quartic form

$$\mathcal{Q}_{(u_0, v_0)}(P, Q) = \mathbf{Q}'_1(X(P, Q), Y(P, Q), Z(P, Q)), \tag{33}$$

with $\mathbf{Q}'_1$ defined in (32). Therefore, in order to solve the system of ternary equations (32) one can solve the quartic Thue equation

$$\mathcal{Q}_{(u_0, v_0)}(P, Q) = 1 \tag{34}$$

in integers P, Q.

4C. ***Conclusion.*** Let ξ be an algebraic integer of degree 4 with the minimal polynomial given in (6). In order to count the number of monogenizations of $\mathbb{Z}[\xi]$, we defined the integral cubic form $F(u, v)$ in (17), and the integral quadratic forms $\boldsymbol{Q}_1(X, Y, Z)$ and $\boldsymbol{Q}_2(X, Y, Z)$ in (14) and (15), respectively. The coefficients of

these forms are all expressed in terms of the coefficients of the minimal polynomial of ξ. We showed that the following three numbers are equal:

(1) The number of solutions to the cubic Thue equation $F(U, V) = \pm 1$ in (24).

(2) The number of systems of ternary quadratic equations (32).

(3) The number of quartic Thue equations (34).

We have also shown that for any fixed solution $(u, v) \in \mathbb{Z}^2$ of the cubic Thue equation $F(U, V) = \pm 1$ in (24), each solution (p, q) of the corresponding quartic Thue equation (34) provides a monogenizer $X(p, q)\xi + Y(p, q)\xi^2 + Z(p, q)\xi^3$, with the integral binary quadratic forms $X(P, Q)$, $Y(P, Q)$ and $Z(P, Q)$ defined in (30).

Therefore, the number of monogenizations of $\mathbb{Z}[\xi]$ is bounded by an upper bound for the number of integer solutions to cubic Thue equations multiplied by an upper bound for the number of integer solutions to quartic Thue equations. Proposition 2.3 provides upper bounds for the number of solutions of cubic Thue equations and Proposition 2.5 provides upper bounds for the number of solutions of quartic Thue equations.

Acknowledgements

I am grateful to the anonymous referee for many helpful comments and suggestions, which improved an earlier version of this article significantly.

I thank *Professor Manjul Bhargava* for inspiring and insightful conversations about the general topic of this article. I thank *Professor Kálmán Győry* for encouragement, sharing his beautiful work, and comments on an earlier version of this article.

During the completion of this project I visited the department of mathematics at Cornell University and was supported by the Ruth I. Michler Memorial Prize. I am grateful to *Professor Michler's family* and AWM for creating this invaluable opportunity and to the Cornell math department for their hospitality. In particular, I thank *Professor Ravi Ramakrishna* for warmly welcoming me and making me feel at home in Ithaca.

This research has been supported in part by *the Simons Foundation Collaboration Grants*, Award Number 635880, and by *the National Science Foundation* Award DMS-2001281.

References

[Akhtari 2009] S. Akhtari, "Cubic Thue equations", *Publ. Math. Debrecen* **75**:3-4 (2009), 459–483. MR Zbl

[Akhtari 2012] S. Akhtari, "Upper bounds for the number of solutions to quartic Thue equations", *Int. J. Number Theory* **8**:2 (2012), 335–360. MR Zbl

[Akhtari 2015] S. Akhtari, "Representation of small integers by binary forms", *Q. J. Math.* **66**:4 (2015), 1009–1054. MR Zbl

[Akhtari 2020] S. Akhtari, "Counting monogenic cubic orders", pp. 13–24 in *Combinatorial and additive number theory, III*, edited by M. B. Nathanson, Springer Proc. Math. Stat. **297**, Springer, 2020. MR Zbl

[Alpöge et al. 2021a] L. Alpöge, M. Bhargava, and A. Shnidman, "A positive proportion of cubic fields are not monogenic yet have no local obstruction to being so", preprint, 2021. arXiv 2011.01186

[Alpöge et al. 2021b] L. Alpöge, M. Bhargava, and A. Shnidman, "A positive proportion of quartic fields are not monogenic yet have no local obstruction to being so", preprint, 2021. arXiv 2107.05514

[Bennet and Rechnitzer $\geq$ 2022] M. Bennet and A. Rechnitzer, "Tabulating binary quartic forms over $\mathbb{Z}$ by discriminant", in preparation.

[Bennett 2001] M. A. Bennett, "On the representation of unity by binary cubic forms", *Trans. Amer. Math. Soc.* **353**:4 (2001), 1507–1534. MR Zbl

[Bhargava 2004] M. Bhargava, "Higher composition laws, III: The parametrization of quartic rings", *Ann. of Math.* (2) **159**:3 (2004), 1329–1360. MR Zbl

[Bhargava 2022] M. Bhargava, "On the number of monogenizations of a quartic order", *Publ. Math. Debrecen* **100**:3-4 (2022), 513–531. MR Zbl

[Birch and Merriman 1972] B. J. Birch and J. R. Merriman, "Finiteness theorems for binary forms with given discriminant", *Proc. London Math. Soc.* (3) **24** (1972), 385–394. MR Zbl

[Dedekind 1878] R. Dedekind, "Ueber den Zusammenhang zwischen der Theorie der ideale und der Theorie der höheren Congruenzen", *Abhandlungen der Königlichen Gesellschaft der Wissenschaften in Göttingen* **23** (1878), 3–38.

[Delaunay 1930] B. Delaunay, "Über die Darstellung der Zahlen durch die binären kubischen Formen von negativer Diskriminante", *Math. Z.* **31**:1 (1930), 1–26. MR Zbl

[Evertse 2011] J.-H. Evertse, "A survey on monogenic orders", *Publ. Math. Debrecen* **79**:3-4 (2011), 411–422. MR Zbl

[Evertse and Győry 1985] J.-H. Evertse and K. Győry, "On unit equations and decomposable form equations", *J. Reine Angew. Math.* **358** (1985), 6–19. MR Zbl

[Evertse and Győry 1991] J.-H. Evertse and K. Győry, "Effective finiteness results for binary forms with given discriminant", *Compositio Math.* **79**:2 (1991), 169–204. MR Zbl

[Evertse and Győry 2017] J.-H. Evertse and K. Győry, *Discriminant equations in Diophantine number theory*, New Mathematical Monographs **32**, Cambridge University Press, 2017. MR Zbl

[Gaál 2019] I. Gaál, *Diophantine equations and power integral bases*, Birkhäuser, Boston, 2019. MR

[Gaál et al. 1996] I. Gaál, A. Pethő, and M. Pohst, "Simultaneous representation of integers by a pair of ternary quadratic forms—with an application to index form equations in quartic number fields", *J. Number Theory* **57**:1 (1996), 90–104. MR Zbl

[Győry 1976] K. Győry, "Sur les polynômes à coefficients entiers et de discriminant donné, III", *Publ. Math. Debrecen* **23**:1-2 (1976), 141–165. MR Zbl

[Hensel 1908] K. Hensel, "Theorie der algebraischen Zahlen, Band 1", 1908. Zbl

[Koch 1997] H. Koch, *Algebraic number theory*, Springer, 1997. MR Zbl

[Mordell 1969] L. J. Mordell, *Diophantine equations*, Pure and Applied Mathematics **30**, Academic Press, London, 1969. MR Zbl

[Nagell 1928] T. Nagell, "Darstellung ganzer Zahlen durch binäre kubische Formen mit negativer Diskriminante", *Math. Z.* **28**:1 (1928), 10–29. MR Zbl

[Okazaki 2002] R. Okazaki, "Geometry of a cubic Thue equation", *Publ. Math. Debrecen* **61**:3-4 (2002), 267–314. MR Zbl

[Thue 1909] A. Thue, "Über Annäherungswerte algebraischer Zahlen", *J. Reine Angew. Math.* **135** (1909), 284–305. MR Zbl

[Wood 2012] M. M. Wood, "Quartic rings associated to binary quartic forms", *Int. Math. Res. Not.* **2012**:6 (2012), 1300–1320. MR Zbl

Received 18 Mar 2022. Revised 22 Jun 2022.

SHABNAM AKHTARI:

akhtari@uoregon.edu
Department of Mathematics, University of Oregon, Eugene, OR, United States

ESSENTIAL NUMBER THEORY

msp.org/ent

See inside back cover or msp.org/ent for submission instructions.

Essential Number Theory (ISSN 2834-4634 electronic, 2834-4626 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online.

ENT peer review and production are managed by EditFlow® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

https://msp.org/

ESSENTIAL NUMBER THEORY

2022 vol. 1 no. 1

The cubic case of Vinogradov's mean value theorem 1
D. R. HEATH-BROWN

Exceptional zeros, sieve parity, Goldbach 13
JOHN B. FRIEDLANDER and HENRYK IWANIEC

A note on Tate's conjectures for abelian varieties 41
CHAO LI and WEI ZHANG

A Diophantine problem about Kummer surfaces 51
WILLIAM DUKE

Quartic index form equations and monogenizations of quartic orders 57
SHABNAM AKHTARI

Modularity lifting theorems 73
TOBY GEE