On monogenic orders

Jan-Hendrik Evertse
Universiteit Leiden

Joint work with Attila Bérczes, Kálmán Győry (Debrecen)

ERC Research Period on Diophantine Geometry,

Pisa, October 19, 2012

Introduction

Let K be an algebraic number field. Denote by O_K its ring of integers.

An *order* in K is a subring of O_K with quotient field K.

An order O in K of the form $\mathbb{Z}[\alpha]$ is called *monogenic*.

For a given order O we consider the "Diophantine equation"

$$\mathbb{Z}[\alpha] = O \quad \text{in } \alpha \in O. \tag{1}$$

The solutions of (1) can be divided into equivalence classes, where two solutions α, β are called equivalent if

$$\beta = \pm\alpha + a \text{ for some } a \in \mathbb{Z}.$$

Győry's theorem

Every order in a quadratic number field is monogenic.

In number fields of degree ≥ 3 there may be non-monogenic orders (Dedekind).

Theorem (Győry, 1976)

Let K be an algebraic number field, and O an order in K. Then there are only finitely many equivalence classes of $\alpha \in O$ with

$$\mathbb{Z}[\alpha] = O. \tag{1}$$

Moreover, there exists an algorithm which, for any explicitly given K, O, decides if O is monogenic and if so, determines a full system of representatives for the equivalence classes of α.

Proof.

Baker's Theorem on linear forms in logarithms. □

Multiply monogenic orders

Let K be an algebraic number field, and O an order in K.
We focus on the *number* of equivalence classes of solutions of $\mathbb{Z}[\alpha] = O$.

Definition

The order O is called k times monogenic, if

$$\mathbb{Z}[\alpha] = O \quad \text{in } \alpha \in O \tag{1}$$

has at least k equivalence classes of solutions, i.e., if there are $\alpha_1, \dots, \alpha_k$ with

$$\mathbb{Z}[\alpha_1] = \cdots = \mathbb{Z}[\alpha_k] = O, \quad \alpha_i \pm \alpha_j \notin \mathbb{Z} \text{ for } 1 \leq i \neq j \leq k.$$

The order O is called at most/precisely k times monogenic if (1) has at most/precisely k equivalence classes of solutions.

Multiply monogenic orders

Let K be an algebraic number field, and O an order in K.
We focus on the *number* of equivalence classes of solutions of $\mathbb{Z}[\alpha] = O$.

Definition

The order O is called k times monogenic, if

$$\mathbb{Z}[\alpha] = O \quad \text{in } \alpha \in O \tag{1}$$

has at least k equivalence classes of solutions, i.e., if there are $\alpha_1, \ldots, \alpha_k$ with

$$\mathbb{Z}[\alpha_1] = \cdots = \mathbb{Z}[\alpha_k] = O, \quad \alpha_i \pm \alpha_j \notin \mathbb{Z} \text{ for } 1 \leq i \neq j \leq k.$$

The order O is called at most/precisely k times monogenic if (1) has at most/precisely k equivalence classes of solutions.

Facts:

- Every order in a quadratic n.f. is precisely one time monogenic.
- Every order in a cubic n.f. is at most 10 times monogenic (Bennett, 2001).
- $\mathbb{Z}[e^{2\pi i/7} + e^{-2\pi i/7}]$ is precisely 9 times monogenic (Baulin, 1960).

Multiply monogenic orders of higher degree

Theorem (Győry, E., 1985)

Let K be an algebraic number field of degree $d \geq 4$. Then every order O in K is at most $c(d)$ times monogenic.

Győry, E. (1985): $c(d) = (3 \times 7^{4d!})^{d-2}$;
E. (2012): $c(d) = 2^{5d^2}$

Multiply monogenic orders of higher degree

Theorem (Győry, E., 1985)

Let K be an algebraic number field of degree $d \geq 4$. Then every order O in K is at most $c(d)$ times monogenic.

Győry, E. (1985): $c(d) = (3 \times 7^{4d!})^{d-2}$;
E. (2012): $c(d) = 2^{5d^2}$

Example (Miller-Sims, Robertson, 2005).
Let $p \geq 11$ be a prime and $\zeta_p = e^{2\pi i/p}$.
Then $O_p := \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$ is $\frac{5}{2}(p-1)$ times monogenic.

In fact, $\mathbb{Z}[\alpha] = O_p$ has the solutions

$$\alpha = \zeta_p^m + \zeta_p^{-m}, \quad \frac{1}{\zeta_p^m + \zeta_p^{-m} + a} \qquad (m = 1, \ldots, \tfrac{1}{2}(p-1),\ a = -1, 0, 1, 2).$$

These are pairwise inequivalent if $p \geq 11$.

Multiply monogenic orders in a given number field

Question

Can a number field have infinitely many k times monogenic orders for $k = 2, 3, \ldots$?

Multiply monogenic orders in a given number field

Question

Can a number field have infinitely many k times monogenic orders for $k = 2, 3, \ldots$?

Example.

Assume that $[K : \mathbb{Q}] \geq 3$ and that K is not a totally complex quadratic extension of a totally real field.

Then O_K has infinitely many units ε such that $K = \mathbb{Q}(\varepsilon)$.

These give rise to infinitely many two times monogenic orders $\mathbb{Z}[\varepsilon] = \mathbb{Z}[\varepsilon^{-1}]$ in K.

Multiply monogenic orders in a given number field

Question

Can a number field have infinitely many k times monogenic orders for $k = 2, 3, \ldots$?

Example.

Assume that $[K : \mathbb{Q}] \geq 3$ and that K is not a totally complex quadratic extension of a totally real field.

Then O_K has infinitely many units ε such that $K = \mathbb{Q}(\varepsilon)$.

These give rise to infinitely many two times monogenic orders $\mathbb{Z}[\varepsilon] = \mathbb{Z}[\varepsilon^{-1}]$ in K.

Theorem 1 (Bérczes, Győry, E., 2011)

Let K be an algebraic number field of degree ≥ 3. Then K has only finitely many three times monogenic orders.

The proof is ineffective.

Two times monogenic orders

A number field K may have infinitely many two times monogenic orders, e.g., $\mathbb{Z}[\varepsilon] = \mathbb{Z}[\varepsilon^{-1}]$, ε a unit.

There may be other infinite classes of two times monogenic orders, but these are all rather special.

Vague belief

Every number field K of degree ≥ 3 has finitely many infinite classes of 'special' two times monogenic orders, and only finitely many two times monogenic orders outside these classes.

We have proved a precise result of this type for a special class of number fields.

Orders of type I and II

Type I orders

Let K be an algebraic number field of degree ≥ 3. An order O in K is of **type I** if there are $\alpha, \beta \in O$ such that $O = \mathbb{Z}[\alpha] = \mathbb{Z}[\beta]$, and

$$\beta = \frac{a + b\alpha}{c + d\alpha} \text{ for some } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, \mathbb{Z}) \text{ with } d \neq 0.$$

If K is not a totally complex quadratic extension of a totally real field, it has infinitely many orders of type I.

Orders of type I and II

Type I orders

Let K be an algebraic number field of degree ≥ 3. An order O in K is of **type I** if there are $\alpha, \beta \in O$ such that $O = \mathbb{Z}[\alpha] = \mathbb{Z}[\beta]$, and

$$\beta = \frac{a + b\alpha}{c + d\alpha} \text{ for some } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, \mathbb{Z}) \text{ with } d \neq 0.$$

If K is not a totally complex quadratic extension of a totally real field, it has infinitely many orders of type I.

Type II orders

Let K be a quartic number field. An order O in K is of **type II** if there are $\alpha, \beta \in O$ such that $O = \mathbb{Z}[\alpha] = \mathbb{Z}[\beta]$, and

$$\beta = \pm\alpha^2 + a\alpha + b, \ \alpha = \pm\beta^2 + c\beta + d \text{ for some } a, b, c, d \in \mathbb{Z}.$$

There are infinitely many quartic fields K with infinitely many orders of type II.

The theorem for two times monogenic orders

Fact.
If K has degree 3 then every two times monogenic order of K is of type I.

We denote by S_d the permutation group on d elements.

Theorem 2 (Bérczes, Győry, E., 2011)

Let K be a number field of degree $d \geq 4$. Assume that the normal closure of K has Galois group $\cong S_d$.

(i) If $d = 4$ then K has only finitely many two times monogenic orders which are not of type I or II.

(ii) If $d \geq 5$ then K has only finitely many two times monogenic orders which are not of type I.

Connection with unit equations

Let K be an algebraic number field of degree $d \geq 3$, and N its normal closure. Denote the conjugates of $\alpha \in K$ in N by $\alpha^{(1)}, \ldots, \alpha^{(d)}$.

Lemma

Let α, β be elements of O_K such that $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta) = K$ and $\mathbb{Z}[\alpha] = \mathbb{Z}[\beta]$. Then for $1 \leq i < j \leq d$,

$$\varepsilon_{ij} := \frac{\beta^{(i)} - \beta^{(j)}}{\alpha^{(i)} - \alpha^{(j)}} \in O_N^*.$$

Proof.

$\beta = f(\alpha)$, $\alpha = g(\beta)$ for some $f, g \in \mathbb{Z}[X]$. □

Connection with unit equations

Let K be an algebraic number field of degree $d \geq 3$, and N its normal closure. Denote the conjugates of $\alpha \in K$ in N by $\alpha^{(1)}, \ldots, \alpha^{(d)}$.

Lemma

Let α, β be elements of O_K such that $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta) = K$ and $\mathbb{Z}[\alpha] = \mathbb{Z}[\beta]$. Then for $1 \leq i < j \leq d$,

$$\varepsilon_{ij} := \frac{\beta^{(i)} - \beta^{(j)}}{\alpha^{(i)} - \alpha^{(j)}} \in O_N^*.$$

Proof.

$\beta = f(\alpha)$, $\alpha = g(\beta)$ for some $f, g \in \mathbb{Z}[X]$. □

We have for all distinct $i, j, k \in \{1, \ldots, d\}$,

$$\frac{\alpha^{(i)} - \alpha^{(j)}}{\alpha^{(i)} - \alpha^{(k)}} \cdot \frac{\varepsilon_{ij}}{\varepsilon_{ik}} + \frac{\alpha^{(j)} - \alpha^{(k)}}{\alpha^{(i)} - \alpha^{(k)}} \cdot \frac{\varepsilon_{jk}}{\varepsilon_{ik}} = \frac{\beta^{(i)} - \beta^{(j)}}{\beta^{(i)} - \beta^{(k)}} + \frac{\beta^{(j)} - \beta^{(k)}}{\beta^{(i)} - \beta^{(k)}} = 1.$$

This leads to unit equations $ax + by = 1$ in $x, y \in O_N^*$.

Unit equations

Let F be a field of characteristic 0. We consider equations

$$(2) \qquad ax + by = 1 \text{ in } x, y \in \Gamma$$

where $a, b \in F^*$ and Γ is a finitely generated subgroup of F^*.

Such equations have only finitely many solutions (Siegel, Mahler, Lang, 1960).

Unit equations

Let F be a field of characteristic 0. We consider equations

$$ax + by = 1 \quad \text{in } x, y \in \Gamma \tag{2}$$

where $a, b \in F^*$ and Γ is a finitely generated subgroup of F^*.

Such equations have only finitely many solutions (Siegel, Mahler, Lang, 1960).

We call (a, b) *normalized* if $a + b = 1$.

If (2) has a solution $u, v \in \Gamma$, then $(a', b') = (au, bv)$ is normalized, and $a'x + b'y = 1$ in $x, y \in \Gamma$ has the same number of solutions as (2).

Theorem (Győry, Stewart, Tijdeman, E., 1988)

There are only finitely many normalized pairs $(a, b) \in F^* \times F^*$ such that eq. (2) *has more than two solutions.*

Sketch of the proof of Theorem 1

Let K be a number field of degree $d \geq 3$.
Let $O = \mathbb{Z}[\alpha] = \mathbb{Z}[\beta] = \mathbb{Z}[\gamma]$ with α, β, γ inequivalent. Put

$$\varepsilon_{ij} := \frac{\beta^{(i)} - \beta^{(j)}}{\alpha^{(i)} - \alpha^{(j)}}, \quad \eta_{ij} := \frac{\gamma^{(i)} - \gamma^{(j)}}{\alpha^{(i)} - \alpha^{(j)}} \quad (i, j, k \in \{1, \ldots, d\} \text{ distinct}).$$

Sketch of the proof of Theorem 1

Let K be a number field of degree $d \geq 3$.
Let $O = \mathbb{Z}[\alpha] = \mathbb{Z}[\beta] = \mathbb{Z}[\gamma]$ with α, β, γ inequivalent. Put

$$\varepsilon_{ij} := \frac{\beta^{(i)} - \beta^{(j)}}{\alpha^{(i)} - \alpha^{(j)}}, \ \ \eta_{ij} := \frac{\gamma^{(i)} - \gamma^{(j)}}{\alpha^{(i)} - \alpha^{(j)}} \ \ (i, j, k \in \{1, \ldots, d\} \text{ distinct}).$$

1) For each i, j, k, the equation

$$\frac{\alpha^{(i)} - \alpha^{(j)}}{\alpha^{(i)} - \alpha^{(k)}} \cdot x + \frac{\alpha^{(j)} - \alpha^{(k)}}{\alpha^{(i)} - \alpha^{(k)}} \cdot y = 1 \ \text{ in } x, y \in O_N^*$$

has solutions $(1, 1)$, $\left(\varepsilon_{ij}/\varepsilon_{ik}, \varepsilon_{jk}/\varepsilon_{ik}\right)$, $\left(\eta_{ij}/\eta_{ik}, \eta_{jk}/\eta_{ik}\right)$.

Sketch of the proof of Theorem 1

Let K be a number field of degree $d \geq 3$.
Let $O = \mathbb{Z}[\alpha] = \mathbb{Z}[\beta] = \mathbb{Z}[\gamma]$ with α, β, γ inequivalent. Put

$$\varepsilon_{ij} := \frac{\beta^{(i)} - \beta^{(j)}}{\alpha^{(i)} - \alpha^{(j)}}, \quad \eta_{ij} := \frac{\gamma^{(i)} - \gamma^{(j)}}{\alpha^{(i)} - \alpha^{(j)}} \quad (i, j, k \in \{1, \dots, d\} \text{ distinct}).$$

1) For each i, j, k, the equation

$$\frac{\alpha^{(i)} - \alpha^{(j)}}{\alpha^{(i)} - \alpha^{(k)}} \cdot x + \frac{\alpha^{(j)} - \alpha^{(k)}}{\alpha^{(i)} - \alpha^{(k)}} \cdot y = 1 \quad \text{in } x, y \in O_N^*$$

has solutions $(1, 1)$, $\big(\varepsilon_{ij}/\varepsilon_{ik}, \varepsilon_{jk}/\varepsilon_{ik}\big)$, $\big(\eta_{ij}/\eta_{ik}, \eta_{jk}/\eta_{ik}\big)$.

2) The Theorem of GSTE + combinatorics (to dispose of the problem that for some i, j, k two solutions may coincide) imply that there are only finitely many possible values for the quotients

$$\frac{\alpha^{(i)} - \alpha^{(j)}}{\alpha^{(i)} - \alpha^{(k)}} \quad \text{for all distinct } i, j, k \in \{1, \dots, d\}.$$

3) There are only finitely many orders $O = \mathbb{Z}[\alpha] = \mathbb{Z}[\beta] = \mathbb{Z}[\gamma]$ with prescribed values for these quotients. □

Sketch of the proof of Theorem 2 (I)

Assume $[K:\mathbb{Q}] = d \geq 4$. Let N be the normal closure of K.
By assumption $\mathrm{Gal}(N/\mathbb{Q}) \cong S_d$.

Let $O = \mathbb{Z}[\alpha] = \mathbb{Z}[\beta]$ with α, β inequivalent. Put $\varepsilon_{ij} := \frac{\beta^{(i)} - \beta^{(j)}}{\alpha^{(i)} - \alpha^{(j)}}$.
From

$$\frac{\alpha^{(i)} - \alpha^{(j)}}{\alpha^{(k)} - \alpha^{(j)}} \cdot \frac{\varepsilon_{ij}}{\varepsilon_{jk}} + \frac{\alpha^{(k)} - \alpha^{(i)}}{\alpha^{(k)} - \alpha^{(j)}} \cdot \frac{\varepsilon_{ik}}{\varepsilon_{jk}} = 1$$

we infer

$$\frac{\alpha^{(i)} - \alpha^{(j)}}{\alpha^{(i)} - \alpha^{(k)}} = \frac{\varepsilon_{ik}/\varepsilon_{jk} - 1}{\varepsilon_{ij}/\varepsilon_{jk} - 1} \quad (i, j, k \in \{1, \ldots, d\} \text{ distinct}).$$

Sketch of the proof of Theorem 2 (I)

Assume $[K:\mathbb{Q}] = d \geq 4$. Let N be the normal closure of K.
By assumption $\mathrm{Gal}(N/\mathbb{Q}) \cong S_d$.

Let $O = \mathbb{Z}[\alpha] = \mathbb{Z}[\beta]$ with α, β inequivalent. Put $\varepsilon_{ij} := \frac{\beta^{(i)}-\beta^{(j)}}{\alpha^{(i)}-\alpha^{(j)}}$.
From

$$\frac{\alpha^{(i)}-\alpha^{(j)}}{\alpha^{(k)}-\alpha^{(j)}} \cdot \frac{\varepsilon_{ij}}{\varepsilon_{jk}} + \frac{\alpha^{(k)}-\alpha^{(i)}}{\alpha^{(k)}-\alpha^{(j)}} \cdot \frac{\varepsilon_{ik}}{\varepsilon_{jk}} = 1$$

we infer

$$\frac{\alpha^{(i)}-\alpha^{(j)}}{\alpha^{(i)}-\alpha^{(k)}} = \frac{\varepsilon_{ik}/\varepsilon_{jk} - 1}{\varepsilon_{ij}/\varepsilon_{jk} - 1} \quad (i,j,k \in \{1,\ldots,d\} \text{ distinct}).$$

Hence for all distinct $i,j,k,l \in \{1,\ldots,d\}$,

$$\frac{(\varepsilon_{ik}/\varepsilon_{jk} - 1)}{(\varepsilon_{ij}/\varepsilon_{jk} - 1)} \cdot \frac{(\varepsilon_{il}/\varepsilon_{kl} - 1)}{(\varepsilon_{ik}/\varepsilon_{kl} - 1)} \cdot \frac{(\varepsilon_{ij}/\varepsilon_{lj} - 1)}{(\varepsilon_{il}/\varepsilon_{lj} - 1)}$$

$$= \frac{(\alpha^{(i)}-\alpha^{(j)})}{(\alpha^{(i)}-\alpha^{(k)})} \cdot \frac{(\alpha^{(i)}-\alpha^{(k)})}{(\alpha^{(i)}-\alpha^{(l)})} \cdot \frac{(\alpha^{(i)}-\alpha^{(l)})}{(\alpha^{(i)}-\alpha^{(j)})} = 1.$$

Sketch of the proof of Theorem 2 (II)

Let $O = \mathbb{Z}[\alpha] = \mathbb{Z}[\beta]$ with α, β inequivalent, and $\varepsilon_{ij} := \frac{\beta^{(i)} - \beta^{(j)}}{\alpha^{(i)} - \alpha^{(j)}}$. Then

$$\mathbf{u} := (\varepsilon_{ij} : 1 \leq i < j \leq d) \in X \cap \Gamma$$

where $\Gamma = (O_N^*)^{d(d-1)/2}$ and X is the algebraic subvariety of $\mathbb{G}_m^{d(d-1)/2}$ given by

$$\frac{(\varepsilon_{ik}/\varepsilon_{jk} - 1)}{(\varepsilon_{ij}/\varepsilon_{jk} - 1)} \cdot \frac{(\varepsilon_{il}/\varepsilon_{kl} - 1)}{(\varepsilon_{ik}/\varepsilon_{kl} - 1)} \cdot \frac{(\varepsilon_{ij}/\varepsilon_{lj} - 1)}{(\varepsilon_{il}/\varepsilon_{lj} - 1)} = 1 \;\; \forall i, j, k, l.$$

We apply:

Theorem (Laurent, 1984)

Let F be a field of characteristic 0, X an algebraic subvariety of $\mathbb{G}_m^R$ defined over F and Γ a finitely generated multiplicative subgroup of $\mathbb{G}_m^R(F) = (F^*)^R$.

Then $X \cap \Gamma$ is contained in a finite union $\mathbf{u}_1 H_1 \cup \cdots \cup \mathbf{u}_t H_t$ of cosets of algebraic subgroups of $\mathbb{G}_m^R$ with $\mathbf{u}_i H_i \subseteq X$ for $i = 1, \ldots, t$.

Sketch of the proof of Theorem 2 (III)

Let $O = \mathbb{Z}[\alpha] = \mathbb{Z}[\beta]$ and $\varepsilon_{ij} := \frac{\beta^{(i)} - \beta^{(j)}}{\alpha^{(i)} - \alpha^{(j)}}$ $(1 \leq i < j \leq d)$.

Lemma

There is a finite set $\mathcal{S}$ depending only on K such that at least one of the three following assertions is true:
(i) $\varepsilon_{ij}/\varepsilon_{ik} \in \mathcal{S}$ *for all distinct* $i, j, k \in \{1, \ldots, d\}$;
(ii) $\varepsilon_{ij}\varepsilon_{kl} = \varepsilon_{ik}\varepsilon_{jl}$ *for all distinct* $i, j, k, l \in \{1, \ldots, d\}$;
(iii) $d = 4$ *and* $\varepsilon_{12} = -\varepsilon_{34}$, $\varepsilon_{13} = -\varepsilon_{24}$, $\varepsilon_{14} = -\varepsilon_{23}$.

Proof.

1) Apply Laurent's Theorem.
2) Use the relations between the ε_{ij} following from our assumption $\mathrm{Gal}(N/\mathbb{Q}) \cong S_d$. □

Sketch of the proof of Theorem 2 (III)

Let $O = \mathbb{Z}[\alpha] = \mathbb{Z}[\beta]$ and $\varepsilon_{ij} := \frac{\beta^{(i)} - \beta^{(j)}}{\alpha^{(i)} - \alpha^{(j)}}$ $(1 \le i < j \le d)$.

Lemma

There is a finite set $\mathcal{S}$ depending only on K such that at least one of the three following assertions is true:
(i) $\varepsilon_{ij}/\varepsilon_{ik} \in \mathcal{S}$ for all distinct $i, j, k \in \{1, \ldots, d\}$;
(ii) $\varepsilon_{ij}\varepsilon_{kl} = \varepsilon_{ik}\varepsilon_{jl}$ for all distinct $i, j, k, l \in \{1, \ldots, d\}$;
(iii) $d = 4$ and $\varepsilon_{12} = -\varepsilon_{34}$, $\varepsilon_{13} = -\varepsilon_{24}$, $\varepsilon_{14} = -\varepsilon_{23}$.

Completion of the proof of Theorem 2.

(i) gives rise to only finitely many possibilities for O;
(ii) implies that $O = \mathbb{Z}[\alpha] = \mathbb{Z}[\beta]$ is of type I;
(iii) implies that O is of type II.

This proves Theorem 2. □

Extension to non-integers

Let K be a number field of degree d.

For α with $K = \mathbb{Q}(\alpha)$ define the $\mathbb{Z}$-module and order

$$M_\alpha := \Big\{ \sum_{i=0}^{d-1} x_i \alpha^i : x_i \in \mathbb{Z} \Big\}, \quad O_\alpha := \Big\{ \lambda \in K : \lambda M_\alpha \subseteq M_\alpha \Big\}.$$

If α is an algebraic integer, then $O_\alpha = \mathbb{Z}[\alpha]$.

We call $\alpha, \beta \in K$ $GL(2,\mathbb{Z})$-*equivalent* if

$$\beta = \frac{a + b\alpha}{c + d\alpha} \text{ for some } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2,\mathbb{Z}).$$

If $\alpha, \beta \in K$ are $GL(2,\mathbb{Z})$-equivalent then $O_\alpha = O_\beta$.

An open problem

Given an order O in a number field K, denote by $N(O)$ the number of $GL(2,\mathbb{Z})$-equivalence classes of α with

$$\mathbb{Q}(\alpha) = K, \quad O_\alpha = O.$$

Theorem

Let K be a number field of degree $d \geq 3$. Then for every order O in K we have
$N(O) = 1$ if $d = 3$ (Delone, Faddeev, 1940);
$N(O) \leq 2^{24d^3}$ if $d \geq 4$ (Bérczes, Győry, E., 2004).

Open problem.

Is there an absolute constant N $(= 2?)$ such that for every number field K of degree ≥ 4 we have $N(O) \leq N$ for all but finitely many orders O in K?

Thank you for your attention!