ON MONOGENIC ORDERS

Attila Bérczes, Kálmán Győry, Jan-Hendrik Evertse

Number Theory and its applications
Debrecen, October 4–8, 2010

Conference dedicated to
Kálmán Győry, Attila Pethő, János Pintz, András Sárközy

INTRODUCTION (I)

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*.

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

INTRODUCTION (II)

Every order in a quadratic number field is monogenic.

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

THEOREM (Győry, 1976)
Let K be an algebraic number field, and O an order in K. Then it can be decided effectively if O is monogenic.
Moreover, in that case there are only finitely many equivalence classes of $\alpha \in O$ with

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

and a full system of representatives of those can be determined effectively.

k TIMES MONOGENEITY (I)

Let K be an algebraic number field, and O an order in K.

Definition. The order O is called precisely/at most/at least/... k times monogenic, if

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

has precisely/at most/at least/... k equivalence classes of solutions $\alpha \in O$.

Facts:

1) Every quadratic order is precisely one time monogenic.

2) Every cubic order is at most 10 times monogenic (Bennett, 2001).

3) The ring of integers of $\mathbb{Q}(e^{2\pi i/7} + e^{-2\pi i/7})$ is precisely 9 times monogenic (Baulin, 1960).

k TIMES MONOGENEITY (II)

THEOREM (Győry, Ev., 1985)
Let K be an algebraic number field of degree $r \geqslant 4$. Suppose that the normal closure of $K/\mathbb{Q}$ has degree g. Let O be an order in K. Then O is at most

$$\left(3 \times 7^{3g}\right)^{r-2}$$

times monogenic.

This can be improved to

$$2^{12r^2(r-2)}$$

(Győry, Ev. 2010).

ORDERS IN A FIXED NUMBER FIELD

We fix a number field K and consider varying orders in K.

Example. Assume that $[K : \mathbb{Q}] \geqslant 3$ 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 at least two times monogenic orders $\mathbb{Z}[\varepsilon] = \mathbb{Z}[\varepsilon^{-1}]$ in K.

THEOREM 1 (Bérczes, Győry, Ev., 2010)
Let K be an algebraic number field of degree $\geqslant 3$. Then there are only finitely many orders in K that are at least three times monogenic.

The proof is ineffective.

TWO TIMES MONOGENIC ORDERS

Let K be a number field of degree $r \geqslant 3$ and N the normal closure of K.

Denote by S_r the permutation group on r elements.

THEOREM 2 (Bérczes, Győry, Ev., 2010)
Assume that

$$\mathrm{Gal}(N/\mathbb{Q}) \cong S_r.$$

Then there are only finitely many orders in K that are at least two times monogenic and not of type A or type B.

ORDERS OF TYPE A OR TYPE B

An order O in K is of **type A** if there are $\alpha, \beta \in O$ such that $O = \mathbb{Z}[\alpha] = \mathbb{Z}[\beta]$, and

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

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

An order O in K is of **type B** if $[K : \mathbb{Q}] = 4$, and 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 such that $\mathrm{Gal}(N/\mathbb{Q}) \cong S_4$ and K has infinitely many orders of type B.

CONNECTION WITH UNIT EQUATIONS

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

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 $1 \leqslant i < j \leqslant r$,*

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

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

Notice that for $1 \leqslant i < j < k \leqslant r$,

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

This leads to equations of the type $ax + by = 1$ in $x, y \in \Gamma$, where Γ is a finitely generated multiplicative group.

UNIT EQUATIONS

Let F be a field of characteristic 0. Consider equations

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

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

Two pairs of coefficients (a, b), (a', b') are called equivalent if a/a', $b/b' \in \Gamma$.

Equations of type (2) have only finitely many solutions.

Equations of type (2) with equivalent pairs of coefficients have the same number of solutions.

THEOREM (Győry, Stewart, Tijdeman, Ev., 1988)
For all pairs (a, b) *outside a union of finitely many equivalence classes, Eq.* (2) *has at most* **two** *solutions.*

SKETCH OF PROOF OF THEOREM 1

Let $O = \mathbb{Z}[\alpha]$ be an at least three times monogenic order.

Consider the β with $\mathbb{Z}[\beta] = O$. Put $\varepsilon_{ij} := \frac{\beta^{(i)} - \beta^{(j)}}{\alpha^{(i)} - \alpha^{(j)}}$.

Then there are $1 \leqslant i < j < k \leqslant r$ such that

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

has at least three solutions $(\varepsilon_{ij}/\varepsilon_{ik}, \varepsilon_{jk}/\varepsilon_{ik})$.

The Theorem of GSTE + relations between the ε_{ij} imply that we have only finitely many possibilities for each $\frac{\alpha^{(i)} - \alpha^{(j)}}{\alpha^{(i)} - \alpha^{(k)}}$ $(1 \leqslant i < j < k \leqslant r)$.

This leads to only finitely many possibilities for $O = \mathbb{Z}[\alpha]$. $\square$

SKETCH OF PROOF OF THEOREM 2 (I)

Assume $[K:\mathbb{Q}] = r \geqslant 4$. Let $O = \mathbb{Z}[\alpha] = \mathbb{Z}[\beta]$ be an at least two times monogenic order. Put $\varepsilon_{ij} := \frac{\beta^{(i)}-\beta^{(j)}}{\alpha^{(i)}-\alpha^{(j)}}$. From

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

we infer

$$\frac{\alpha^{(i)}-\alpha^{(j)}}{\alpha^{(i)}-\alpha^{(k)}} = \frac{\varepsilon_{ik}/\varepsilon_{jk} - 1}{\varepsilon_{ij}/\varepsilon_{jk} - 1} \quad (1 \leqslant i < j < k \leqslant r)$$

and from that, for all $1 \leqslant i < j < k < l \leqslant r$,

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

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

SKETCH OF PROOF OF THEOREM 2 (II)

The tuple $(\varepsilon_{ik}/\varepsilon_{jk}, \ldots, \varepsilon_{il}/\varepsilon_{lj})$ is a solution to

$$\frac{(x_1 - 1)}{(y_1 - 1)} \cdot \frac{(x_2 - 1)}{(y_2 - 1)} \cdot \frac{(x_3 - 1)}{(y_3 - 1)} = 1 \tag{3}$$

in $x_1, \ldots, y_3 \in O_N^*$.

LEMMA. *Let F be a field of characteristic 0 and Γ a finitely generated subgroup of F^*. Then with at most finitely many exceptions, every solution $x_1, \ldots, y_3 \in \Gamma$ of (3) is of one of the following types:*

a) (x_1, x_2, x_3) *is a permutation of* $(y_1^{\pm 1}, y_2^{\pm 1}, y_3^{\pm 1})$ *(with any possible choice of the signs);*

b) *at least one of* $x_i x_j$, x_i/x_j, $y_i y_j$, y_i/y_j $(1 \leqslant i < j \leqslant 3)$ *is* ± 1 *or a cube root of unity.*

SKETCH OF PROOF OF THEOREM 2 (III)

Let F be a field of characteristic 0 and Γ a finitely generated subgroup of F^*.

Let $g \in F[X_1, \ldots, X_n]$ and consider the equation

$$(4) \qquad g(x_1, \ldots, x_n) = 0 \quad \text{in } x_1, \ldots, x_n \in \Gamma.$$

A solution $(x_1, \ldots, x_n)$ to (4) is called *degenerate* if there are integers $c_1, \ldots, c_n$ with $\gcd(c_1, \ldots, c_n) = 1$ such that

$$g(x_1 T^{c_1}, \ldots, x_n T^{c_n}) \equiv 0 \quad \text{identically in the variable } T,$$

and *non-degenerate* otherwise.

THEOREM (Laurent, 1984).
Eq. (4) *has only finitely many non-degenerate solutions.*

SKETCH OF PROOF OF THEOREM 2 (IV)

Let $O = \mathbb{Z}[\alpha] = \mathbb{Z}[\beta]$ be the at least two times monogenic order we started with, and put $\varepsilon_{ij} = \frac{\beta^{(i)} - \beta^{(j)}}{\alpha^{(i)} - \alpha^{(j)}}$ $(1 \leqslant i < j \leqslant r)$.

The Lemma, together with the assumption Gal$(N/\mathbb{Q}) \cong S_r$, leads to a list of conditions on $\varepsilon_{ij}/\varepsilon_{ik}$ $(1 \leqslant i < j < k \leqslant r)$.

Applying

$$\frac{\alpha^{(i)} - \alpha^{(j)}}{\alpha^{(i)} - \alpha^{(k)}} = \frac{\varepsilon_{ik}/\varepsilon_{jk} - 1}{\varepsilon_{ij}/\varepsilon_{jk} - 1} \quad (1 \leqslant i < j < k \leqslant r)$$

we infer that $\mathbb{Z}[\alpha]$ is either of type A or type B, or belongs to a finite set independent of α. $\square$

Open problem. What happens if we drop the assumption Gal$(N/\mathbb{Q}) \cong S_r$?