Integral polynomials of given discriminant and their applications

(brief survey + some new joint results with Bhargava, Evertse, Remete and Swaminathan)

K. Győry
University of Debrecen

CENT 2023, Sopron

August 28, 2023

Slides have been posted at

`https://math.unideb.hu/en/talks-kalman-gyory`

The **theory** *of polynomials with coefficients in* $\mathbb{Z}$ (*integral polynomials*) *and with given discriminant* have a great number of **applications**, among others to *Diophantine equations, Diophantine approximations* and *algebraic number theory*.

Comprehensive treatment of the theory and its applications can be found in the work

K. Győry, *Résultats effectifs sur la représentation des entiers par des forms décomposables*, Kingston, Canada, 1980; monic case,

and in the monograph

J. H. Evertse and K. Győry, *Discriminant equations in Diophantine number theory*, Cambridge, 2017.

In our paper M. Bhargava, J. H. Evertse, K. Győry, L. Remete and A. A. Swaminathan (BEGyRS, 2023), *Hermite equivalence of polynomials*, Acta Arith. 2023

we have *integrated* in the theory a long-forgotten *notion of equivalence* for integral polynomials of given discriminant, introduced by Hermite (1850's) and his corresponding *finiteness theorem*. We have *compared Hermite's theorem* with the *most significant results* of this area, obtained by Birch and Merriman (1972) and *independently*, in an *effective form* by Győry (1973), and later by Evertse and Győry (1991, 2017).

We *pointed out* that these results are *much more precise* than Hermite's theorem and require *deeper tools* to prove. In particular, we *corrected* a *faulty reference* to Hermite's result in Narkiewicz's excellent book

W. Narkiewicz, *The story of algebraic numbers in the first half of the 20th century*, Springer, 2018.

In our *talk*, we give a *brief overview* of the *most important results* of the *theory*, and following BEGyRS (2023), we *compare them with the* long-forgotten *theorem* of Hermite. Then, as *consequences* of the *theory, general effective finiteness theorems* will be presented among others for *monogenic number fields*. Further, *algorithmic/computational* results on *monogenity* will be discussed. Finally, some other *related* results will be stated and **open problems** will be proposed.

$\mathbb{Z}$-equivalence and $GL_2(\mathbb{Z})$-equivalence of integral polynomials

$GL_2(\mathbb{Z})$: multiplicative group of 2×2 integral matrices with determinant ± 1

- *Two monic polynomials* $f, f^* \in \mathbb{Z}[X]$ *are called* $\mathbb{Z}$-**equivalent** *if* $f^*(X) = f(X+a)$ *for some* $a \in \mathbb{Z}$;
- *Two polynomials* $f, f^* \in \mathbb{Z}[X]$ *of degree* $n \geq 2$ *are called* $GL_2(\mathbb{Z})$ -**equivalent** *if there is* $\left(\begin{smallmatrix} b & a \\ d & c \end{smallmatrix}\right) \in GL_2(\mathbb{Z})$ *such that*

$$f^*(X) = \pm(dX+c)^n f\left(\frac{bX+a}{dX+c}\right)$$

$\Longrightarrow$ in both cases, f, f^* *have the* same discriminant

$\mathbb{Z}$-*equivalence* is much *stronger*, $\mathbb{Z}$-equivalent monic polynomials in $\mathbb{Z}[X]$ are clearly $GL_2(\mathbb{Z})$-equivalent with $\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \in GL_2(\mathbb{Z})$

similar interpretation in terms of **binary forms**

Reduction theory of integral polynomials I, degree ≤ 3 case

For $f \in \mathbb{Z}[X], H(f)$ *height* of f, i.e. the maximum absolute value of its coefficients

Lagrange (1773): *For* **quadratic** $f \in \mathbb{Z}[X]$ *with discriminant* $D \neq 0$, *there exists* $f^* \in \mathbb{Z}[X]$ $GL_2(\mathbb{Z})$*-equivalent to* f *such that* $H(f^*) \leq c(D)$

$$\Longleftrightarrow$$

There are only finitely many $GL_2(\mathbb{Z})$*-equivalence classes of* **quadratic** *polynomials in* $\mathbb{Z}[X]$ *with given non-zero discriminant* + **effective** (in terms of binary forms)

Similar assertions for monic quadratic polynomials in $\mathbb{Z}[X]$ with $\mathbb{Z}$*-equivalence*

Gauss (1801): *more precise result*

Hermite (1851): *There are only finitely many $GL_2(\mathbb{Z})$-equivalence classes of* **cubic** *polynomials in $\mathbb{Z}[X]$ with given non-zero discriminant*

Delone (1930), Nagell (1930), independently: *Up to $\mathbb{Z}$-equivalence, there are only finitely many irreducible* **cubic** *monic polynomials in $\mathbb{Z}[X]$ with given non-zero discriminant* + **ineffective**

Very likely, Hermite *attempted* to extend his theorem to the case of **arbitrary degree**≥ 3, but without success. Instead, he proved the weaker Theorem A below.

Hermite equivalence of decomposable forms

Consider decomposable forms of degree $n \geq 2$ in n variables

$$F(\underline{X}) = c\prod_{i=1}^{n}(\alpha_{i,1}X_1 + \cdots + \alpha_{i,n}X_n) \in \mathbb{Z}[X_1, \ldots, X_n],$$

where $c \in \mathbb{Q}^\times$ and $\alpha_{i,j} \in \overline{\mathbb{Q}}$ for $i, j = 1, \ldots, n$. The discriminant of F is given by

$$D(F) := c^2(\det(\alpha_{i,j}))^2.$$

We have $D(F) \in \mathbb{Z}$.

*Two decomposable forms F, F^* as above are called $GL_n(\mathbb{Z})$-**equivalent** if*

$$F^*(\underline{X}) = \pm F(U\underline{X}) \text{ for some } U \in GL_n(\mathbb{Z})$$

(where $\underline{X} = (X_1, \dots, X_n)^T$ is a column vector)

Two $GL_n(\mathbb{Z})$-equivalent decomposable forms have the same discriminant.

Theorem (Hermite, 1850)

Let $n \geq 2, D \neq 0$. Then, the decomposable forms in $\mathbb{Z}[X_1, \dots, X_n]$ of degree n and discriminant D lie in finitely many $GL_n(\mathbb{Z})$-equivalence classes.

Hermite equivalence of polynomials and Hermite's finiteness theorem

Let $f(X) = c(X-\alpha_1)\cdots(X-\alpha_n) \in \mathbb{Z}[X]$ with $c \in \mathbb{Z}\setminus\{0\}$, $\alpha_1,\ldots,\alpha_n \in \overline{\mathbb{Q}}$. Then the discriminant of f : $D(f) = c^{2n-2}\prod_{1\le i<j\le n}(\alpha_i-\alpha_j)^2 \in \mathbb{Z}$.

To f we associate the *decomposable form*

$$[f](\underline{X}) := c^{n-1}\prod_{i=1}^{n}(X_1+\alpha_i X_2+\cdots+\alpha_i^{n-1}X_n) \in \mathbb{Z}[X_1,\ldots,X_n].$$

We have $D(f) = D([f])$ (Vandermonde).

Hermite (1857): *Two polynomials $f, f^* \in \mathbb{Z}[X]$ of degree n are called* **Hermite equivalent** *if the associated decomposable forms $[f]$ and $[f^*]$ are $GL_n(\mathbb{Z})$-equivalent, i.e.,*

$$[f^*](\underline{X}) = \pm[f](U\underline{X}) \text{ for some } U \in GL_n(\mathbb{Z}).$$

$\Longrightarrow$ *Hermite equivalent polynomials in $\mathbb{Z}[X]$ have the same* discriminant.

Hermite's theorem on decomposable forms and the above fact imply the following *finiteness theorem on polynomials:*

Theorem A (Hermite, 1857)

Let $n \geq 2, D \neq 0$. Then the polynomials $f \in \mathbb{Z}[X]$ of degree n and of discriminant D lie in finitely many Hermite equivalence classes.

$+$ **ineffective**

Comparison of Hermite equivalence with $GL_2(\mathbb{Z})$-equivalence and $\mathbb{Z}$-equivalence

Surprisingly, **Theorem A** of Hermite was not mentioned in the literature until Narkiewicz (2018) book quoted above, where $GL_2(\mathbb{Z})$-*equivalence*, resp. $\mathbb{Z}$-*equivalence* and *Hermite equivalence* were mixed up. In part, this fact motivated the paper BEGyRS (2023) to provide a thorough treatment of the notion of *Hermite equivalence*, and compare *Hermite equivalence* with $GL_2(\mathbb{Z})$-*equivalence* resp. $\mathbb{Z}$-*equivalence* of integral polynomials.

For polynomials of degree 2 and 3, *Hermite equivalence* and $GL_2(\mathbb{Z})$-*equivalence*, resp. $\mathbb{Z}$-*equivalence* **coincide**.

Theorem 1 (BEGyRS, 2023)

If $f, f^* \in \mathbb{Z}[X]$ are GL_2-equivalent, resp. $\mathbb{Z}$-equivalent, then they are Hermite equivalent.

Theorem 2 (BEGyRS, 2023)

For every $n \geq 4$ there are infinitely many pairs (f, f^*) of irreducible primitive polynomials in $\mathbb{Z}[X]$ with degree n such that f, f^* are Hermite equivalent but $GL_2(\mathbb{Z})$-inequivalent, resp. $\mathbb{Z}$-inequivalent in the monic case.

Corollary (BEGyRS, 2023)

$GL_2(\mathbb{Z})$-equivalence, resp. $\mathbb{Z}$-equivalence are stronger than Hermite equivalence.

Breakthroughs in the 1970's

Hermite *original objective* – proving that there are only finitely many $GL_2(\mathbb{Z})$-equivalence, resp. $\mathbb{Z}$-equivalence classes of integral polynomials of given degree and given non-zero discriminant – was finally achieved more than a century later by Birch and Merriman (1972) and *independently*,for monic polynomials, in a more prcise and **effective** form by Győry (1973).

Birch and Merriman proved the following result.

Theorem B (Birch and Merriman, 1972)

Let $n \geq 2, D \neq 0$. There are only finitely many $GL_2(\mathbb{Z})$-equivalence classes of polynomials in $\mathbb{Z}[X]$ with degree n and discriminant D.

Proof, partly based on the finiteness of the number of solutions of unit equations + some *ineffective* arguments $\Longrightarrow$ **ineffective**

For monic polynomials, the corresponding result with $\mathbb{Z}$-equivalence was proved independently by Győry.

Theorem C (Győry, 1973)

There are only finitely many $\mathbb{Z}$-equivalence classes of monic polynomials in $\mathbb{Z}[X]$ with given discriminant $D \neq 0$, and a full set of representatives of these classes can be, at least in principle, **effectively** *determined.*

Note that here the degree of the monic polynomials under consideration is not fixed.

Theorem C confirmed a conjecture of Nagell (1967,68) in an effective form. Further, it made effective and significantly *generalized* the theorems of Delone (1930) and Nagell (1930) obtained in the cubic case.

In the proof of Theorem C, first the degree of the polynomials in question is bounded. Then one reduces the problem to so-called *"connected" system of unit equations*, and finally Baker's method is applied to bound the heights of the units and thus of the representatives, see below.

Explicit versions of Theorems B and C

First **effective** version of Theorem B (Birch and Merriman): Evertse and Győry (1991) in a quantitative form. In 2017, improved and completely **explicit** version:

Theorem B' (Evertse and Győry (2017))

Let $f \in \mathbb{Z}[X]$ be a polynomial of degree $n \geq 2$ and discriminant $D \neq 0$. Then f is $GL_2(\mathbb{Z})$-equivalent to a polynomial $f^* \in \mathbb{Z}[X]$ for which

$$H(f^*) \leq \exp\{(4^2 n^3)^{25n^2} \cdot |D|^{5n-3}\}. \quad (1)$$

Further (Győry, 1974):

$$n \leq 3 + 2\log|D|/\log 3.$$

First quantitative version of Theorem C (Győry): Győry (1974). Improved version:

Theorem C' (Evertse and Győry, 2017)

Let $f \in \mathbb{Z}[X]$ be a monic polynomial of degree $n \geq 2$ and discriminant $D \neq 0$. Then f is $\mathbb{Z}$-equivalent to a polynomial $f^* \in \mathbb{Z}[X]$ for which

$$H(f^*) \leq \exp\{n^{20} 8^{n^2+19} (|D|(\log|D|)^n)^{n-1}\}. \tag{2}$$

Further (Győry, 1974):

$$n \leq 2 + 2\log|D|/\log 3.$$

Clearly, Theorem B and in particular B', and in the monic case Theorem C, C' are *much more precise* and *deeper* than Theorem A of Hermite.

The *exponential feature* of the *bounds* in (1) and (2) is a consequence of the use of *Baker's method*.

Method of proof of Theorems C and C'

General approach for *effective/algorithmic/computational* versions

Main steps of the proof of Theorem C:

1) The proof can be reduced to the case of irreducible polynomials. Then $f \in \mathbb{Z}[X]$ irreducible, monic with discriminant $D \neq 0$ and distinct zeros $\alpha_1, \dots, \alpha_n$. L splitting field of $f \Longrightarrow [L:\mathbb{Q}] \leq n!$.
2) $n \leq c_1(D)$, $|D_L| \leq c_2(D)$ *explicit*, elementary; fix n, L splitting field of f
3) $$\prod_{1\leq i<j\leq n} (\alpha_i - \alpha_j)^2 = D \Longrightarrow |N_{L/\mathbb{Q}}(\alpha_i - \alpha_j)| \leq c_3(D) \text{ explicit} \Longrightarrow \alpha_i - \alpha_j = \delta_{ij}\varepsilon_{ij},\ \varepsilon_{ij} \text{ unit, } H(\delta_{ij}) \leq c_4(D) \text{ explicit} \quad (3)$$
4) $$(\alpha_i - \alpha_j) + (\alpha_j - \alpha_k) + (\alpha_k - \alpha_i) = 0 \text{ for every } i, j\ k \quad (4)$$

   graph: *vertices* $\alpha_i - \alpha_j$, *edges* $[\alpha_i - \alpha_j, \alpha_j - \alpha_k]$, connected
5) (4) $\Longrightarrow$ "connected" system of unit equations

$$\delta_{ijk}\varepsilon_{ijk} + \tau_{ijk}\nu_{ijk} = 1, \quad (5)$$

δ_{ijk}, τ_{ijk} with explicitly bounded heights, $\varepsilon_{ijk}, \nu_{ijk}$ **unknown** *units* in L.

6) *Represent* ε_{ijk}
$$\varepsilon_{ijk} = \xi_{ijk}\rho_1^{a_{ijk,1}} \cdots \rho_r^{a_{ijk,r}}$$
and similarly ν_{ijk}, where ζ_{ijk} root of unity, $\rho_1, \ldots, \rho_r$ *fundamental system of units* with *effectively/explicitly bounded heights* in L with $r \leq n! - 1$ (Dirichlet theorem)

7) Applying *Baker's method* to (5) $\Longrightarrow$ *effective/explicit bounds for* $|a_{ijk,1}|, \ldots, |a_{ijk,r}|$.

Remark: in Gy (1974), this was the first application of Baker's method to *general unit equations* of the form (5) with explicit bound.

8) using the *connectedness* of unit equations involved $\Longrightarrow$ *effective/explicit* bound for the *height* of $\alpha_i - \alpha_j$ for every i, j;

9) *adding* the *differences* $\alpha_i - \alpha_j$ for $j = 1, \ldots, n$, using the fact that $\alpha_1 + \cdots + \alpha_n \in \mathbb{Z}$, putting $\alpha_1 + \cdots + \alpha_n = na + a'$ with $a, a' \in \mathbb{Z}$, $0 \leq a' < n$, and writing $\alpha_i^* := \alpha_i - a$ for $i = 1, \ldots, n$, for $f^*(X) := \prod_{i=1}^n (X - \alpha_i^*)$ we have $f^*(X) = f(X + a) \in \mathbb{Z}[X]$ with *effectively/explicitly bounded height.* □

Consequences and applications of the theory

I. Integral polynomials with given non-zero discriminant

Generalization of **Theorem B** (Birch and Merriman, 1972) and **Theorem B'** (Evertse and Gy, 1991, 2017) for polynomials over rings of S-integers of a number field.

Consequences/applications of **Theorem B'** (Evertse and Gy, 1991, 2017) to:

- Thue equations, Thue–Mahler equations (Stewart, Evertse and Gy, Evertse, Thunder, Akhtari);
- explicit upper bounds for the minimal non-zero values of binary forms at integral points (Evertse and Gy);
- GL_2-equivalence classes of algebraic numbers with given discriminant (Evertse and Gy);
- root separation of integral polynomials (Evertse);
- effective version of Shafarevich' conjecture/Faltings' theorem for hyperelliptic curves (von Känel);
- rational monogenizations of orders in a number field (Evertse)

II. Monic integral polynomials with given non-zero discriminant

K number field, $n = [K : \mathbb{Q}]$, *discriminant* D_K, *ring of integers* $\mathcal{O}_K$; for $\alpha \in \mathcal{O}_K$, $f_\alpha(X) \in \mathbb{Z}[X]$ *minimal* (monic) *polynomial of* $\alpha \Longrightarrow$

$$\begin{cases} D_{K/\mathbb{Q}}(\alpha) & := D(f_\alpha) \text{ discriminant of } \alpha, \\ I(\alpha) & := [\mathcal{O}_K : \mathbb{Z}[\alpha]] \text{ index of } \alpha; \text{ we have} \end{cases} \tag{6}$$

$$D_{K/\mathbb{Q}}(\alpha) = I^2(\alpha) \cdot D_K \tag{7}$$

Definition

- $\alpha, \alpha^* \in \mathcal{O}_K$ **equivalent** *if* $\alpha^* = \alpha + a$, $a \in \mathbb{Z} \Rightarrow D_{K/\mathbb{Q}}(\alpha) = D_{K/\mathbb{Q}}(\alpha^*)$, $I(\alpha) = I(\alpha^*)$
- K **monogenic** *if* $\mathcal{O}_K = \mathbb{Z}[\alpha]$ *for some* $\alpha \in \mathcal{O}_K \Leftrightarrow \{1, \alpha, \ldots, \alpha^{n-1}\}$ **power integral basis** *in* K
- K *is called* $k \geq 1$ **times monogenic** *if* $\mathcal{O}_K = \mathbb{Z}[\alpha_1] = \ldots = \mathbb{Z}[\alpha_k]$ *for some pairwise inequivalent* $\alpha_1, \ldots, \alpha_k \in \mathcal{O}_K$; k **multiplicity** of *monogenity*

Most important consequences of Theorem C (Győry, 1973): **effective finiteness theorems in** Gy (1973, 74, 76, 78a, 78b), i.e. in Part I-V of Gy (1973)

for algebraic integer α, $D(\alpha) := D_{K/\mathbb{Q}}(\alpha)$, where $K = \mathbb{Q}(\alpha)$

Corollary 1 of Theorem C

Up to equivalence, there are only finitely many algebraic integers with given non-zero discriminant + **effective** (Part I; apply Theorem C with $D(\alpha) = D(f_\alpha)$, f_α minimal (monic) polynomial of α)

in **given number field** K of degree n:

Corollary 2 of Theorem C

Up to equivalence, there are only finitely many $\alpha \in \mathcal{O}_K$ with given index I + **effective** and **quantitative** (Part III, apply Corollary 1 with $D_{K/\mathbb{Q}}(\alpha) = I^2 \cdot D_K$ for $\alpha \in \mathcal{O}_K$)

Corollary 3 of Theorem C

Up to equivalence, there only finitely many $\alpha \in \mathcal{O}_K$ *with* $\mathcal{O}_K = \mathbb{Z}[\alpha] \Leftrightarrow \{1, \alpha, \ldots, \alpha^{n-1}\}$ *power integral basis* + **effective** and **quantitative** (Part III, apply Corollary 2 with $I = 1$)

breakthrough $\Longrightarrow$ the **first general effective algorithm** for **deciding** the **monogenity** resp. **multiplicity of monogenity** of a **number field** and, up to equivalence, **determining all power integral bases** in K + **generalization** for the **relative case** (Part IV)

An important reformulation of Corollary 2 and 3 in terms of index form equations

Hensel (1894): *To every integral basis* $\{1, \omega_2, \dots, \omega_n\}$ *of* K *there corresponds a form* $I(X_2, \dots, X_n)$ *of degree* $n(n-1)/2$ *in* $n-1$ *variables with coefficients in* $\mathbb{Z}$ *such that for* $\alpha \in \mathcal{O}_K$,

$$I(\alpha) = |I(x_2, \dots, x_n)| \text{ if } \alpha = x_1 + x_2\omega_2 + \cdots + x_n\omega_n \text{ with } x_1, \dots, x_n \in \mathbb{Z} \quad (8)$$

$I(X_2, \dots, X_n)$ *is called an* **index form**, *and for given non-zero* $I \in \mathbb{Z}$

$$I(x_2, \dots, x_n) = \pm I \text{ in } x_2, \dots, x_n \in \mathbb{Z} \quad (9)$$

an **index form equation**.

In view of (8), Corollary 2 is **equivalent** to

Corollary 4 of Theorem C

For given $I \in \mathbb{Z} \setminus \{0\}$ *the index form equation* (9) *has only finitely many solutions, and they can be, at least in principle, effectively determined* (Part III).

In particular, **for** $I = 1$ we get the following *equivalent reformulation* of *Corollary 3*

Corollary 5 of Theorem C

The index form equation

$$I(x_2, \ldots, x_n) = \pm 1 \textit{ in } x_2, \ldots, x_n \in \mathbb{Z} \qquad (10)$$

has only finitely many solutions + **effective** and **quantitative** (Part III).

The best known bound for the solutions of (10):

$$\max_{2 \le i \le n} |x_i| < \exp\{10^{n^2} (|D_K| (\log |D_K|)^n)^{n-1}\}, \qquad (11)$$

see Evertse and Győry (2017).

Generalizations of Theorem C (Gy, 1973) **and its Corollaries 1–5**

- $\mathcal{O}_K$ *replaced by* **any order** $\mathcal{O}$ *in* K (Gy, Part III, IV);
- D *resp.* I *replaced by* $\mathbf{p_1^{z_1}} \cdots \mathbf{p_s^{z_s}}$, p_i *given primes*, $\mathbf{z_i} \geq \mathbf{0}$ *also* **unknowns** (Gy, Part V; Trelina);
- **discriminant form equations** (Gy, Part III, Gy–Papp, Gy, Evertse–Gy);
- **relative case,** S-**integers** (Gy, Part IV; Gy–Papp, Gy, Evertse–Gy);
- *more general* **decomposable form equations** (Gy–Papp, Gy, Evertse–Gy);
- **"inhomogeneous"** case (Gaál);
- *analogue results over* **function fields** (Gaál, Gy, Shlapentokh);
- **Recently**, étale algebras (Evertse–Gy);

  case of **finitely generated ground domains** (Evertse–Gy)

Further applications of Theorem C (Gy, 1973), **its Corollaries 1–5 and their generalizations**

- **Diophantine equations**; Thue, Mordell, elliptic, superelliptic, discriminant form, *of discriminant type* (in *alphabetical* order: Bérczes, Brindza, Evertse, Gy, Haristoy, Papp, Pink, Pintér, Trelina);
- **minimal index** in number fields (Gy);
- **irreducible polynomials** (Gy);
- **arithmetic properties** of **discriminants** and **indices** of elements of $\mathcal{O}_K$ (Gy);
- **canonical number systems** in number fields (Kovács, Pethő, and recently Evertse, Gy, Pethő, Thuswaldner);

⋮

Problem 1: *extend* the **effective theory** and **its consequences** above *to the case of* **finitely generated groundrings over** $\mathbb{Z}$

main difficulty: *Dirichlet unit theorem generalized for finitely generated domains over* $\mathbb{Z}$ *should be made* **effective**

For further **consequences, generalizations, applications** and **quantitative versions**, see the **books** with a *great number of references*:

- K. Győry, Résultats effectifs sur la représentation des entiers par des formes décomposables, Kingston, Canada, 1980.
- K. Győry, Discriminant form and index form equations, In: Algebraic Number Theory and Diophantine Analysis, de Gruyter, 2000. pp. 191–214.
- G. Wüstholz (ed.), A Panorama in Number Theory and The View from Baker's Garden, Cambridge, 2002.
- J.-H. Evertse and K. Győry, Unit Equations in Diophantine Number Theory, Cambridge, 2015.
- J.-H. Evertse and K. Győry, Discriminant Equations in Diophantine Number Theory, Cambridge, 2017.
- J.-H. Evertse and K. Győry, Effective Results and Methods for Diophantine Equations over Finitely Generated Domains, Cambridge, 2022.

Algorithmic resolution of index form equations, application to (multiply) monogenic number fields

K number field of *degree* $n \geq 3$, $\mathcal{O}_K$ ring of integers, $I(X_2, \ldots, X_n)$ an *index form* over K

$$I(x_2, \ldots, x_n) = \pm 1 \textit{ in } x_2, \ldots, x_n \in \mathbb{Z} \tag{10}$$

(11) **exponential** bound for $\max_i |x_i|$ *too large* for *practical* use

If $|D_K|$ is not too large, there are *methods* for *solving* (10) in *concrete* cases $\Leftrightarrow$ for *computing* all *generators* of *power integral bases* in K, *up to degree* $\mathbf{n \leq 6}$ **in general**, and for many special *higher degree fields up to about degree* 15 $\Rightarrow$ for *deciding how many times K is monogenic*. **Breakthrough in the 1990's, computational results** and **tables**, **practical algorithms**.

For $\mathbf{n = 3, 4}$, (10) $\Longrightarrow$ *Thue equations of degree* ≤ 4*, efficient algorithm;*

$\mathbf{n = 3}$, (10) $\Longrightarrow$ *cubic Thue quation* (Gaál, Schulte 1989);

$\mathbf{n = 4}$, (10) $\Longrightarrow$ *one cubic and some quartic Thue equations* (Gaál, Pethő, Pohst, 1991–96), many very interesting results

Refined version of the general approach combined with reduction and enumeration algorithms

In general, for $\mathbf{n \geq 5}$, a **refined version** of the **general approach** involving **unit equations** is needed. Since

$$(10) \iff D_{K/\mathbb{Q}}(\alpha) = D_K \iff D(f_\alpha) = D_K \text{ in } \alpha \in \mathcal{O}_K$$

with minimaly polynomial $f_\alpha \in \mathbb{Z}[X]$, in case of *concrete equations* (10), the **basic idea** of the **proof** of **Theorem C** must be *combined* with *further fundamental algorithms* and *refinements:*

Refined version of the general method: *reduction* to *unit equations* but in considerably smaller subfields in the normal closure L of K. Then the number r of unknown exponents a_{ijk} in the *unit equation* (5) with $\varepsilon_{ijk} = \xi_{ijk}\rho_1^{a_{ijk,1}} \cdots \rho_r^{a_{ijk,r}}$ is much smaller, $\leq n(n-1)/2 - 1$ instead of $r \leq n! - 1$; cf. Gy (1998, 2000), see also Gaál and Gy (1999), Evertse and Gy (2017). Then, in concrete cases *bound* the exponents $|a_{ijk}|$ by *Baker's method*.

The *bounds* in concrete cases are still *too large*. Hence **reduction algorithm** is needed, *reducing* the *Baker's bound* for $|a_{ijk}|$ in several steps if necessary by *refined versions* of the L^3-*algorithm*; cf. de Weger; Wildanger; Gaál and Pohst.

The *last step* is to apply **enumeration algorithm**, determining the **small** solutions *under the reduced bound*; cf. Wildanger; Gaál and Pohst; Bilu, Gaál and Gy.

Combining the *refined version* with *reduction* and *enumeration algorithms*, for $\mathbf{n} = \mathbf{5}, \mathbf{6}$ Gaál and Győry (1999), resp. Bilu, Gaál and Győry (2004) $\Longrightarrow$ *algorithms for determining all power integral bases* $\Longrightarrow$ checking the *monogenity* and the *multiplicity of the monogenity* of K.

The use of the *refined version* of the general approach is *particularly important* in the *enumeration algorithm*.

To perform computations, *algebraic number theory packages*, a *computer algebra system* and in some cases a *supercomputer* were needed.

Examples: Resolution of *index form equations* (10), in the most difficult case when $K=\mathbb{Q}(\alpha)$, degree n, *totally real*, with Galois group S_n, $f\in\mathbb{Z}[X]$ *minimal polynomial of* $\alpha \Longrightarrow$ *all power integral bases* $\Longrightarrow$ *multiplicity of the monogenity of* K:

$\mathbf{n=3}$, $f(X) = X^3 - X^2 - 2X + 1$, K 9 *times* monogenic (Gaál, Schulte, 1989);

$\mathbf{n=4}$, $f(X) = X^4 - 4X^2 - X + 1$, K 17 *times* monogenic (Gaál, Pethő, Pohst, 1990's);

$\mathbf{n=5}$, $f(X) = X^5 - 5X^3 + X^2 + 3X - 1$, K 39 *times* monogenic (Gaál, Gy, 1999); $\approx$ 8h

$\mathbf{n=6}$, $f(X) = X^6 - 5X^5 + 2X^4 + 18X^3 - 11X^2 - 19X + 1$, K, 45 *times* monogenic (Bilu, Gaál, Gy, 2004); hard computation

Books, research papers

There are extremely many *algorithmic results* and several important *algorithms* published in books and in a great number of research papers:

Books

- *B. M. M. de Weger*, Algorithms for Diophantine Equations, CW, Tract 45, Amsterdam, 1989.
- *N. P. Smart*, The Algorithmic Resolution of Diophantine Equations, Cambridge, 1988.
- *J.-H. Evertse and K. Győry*, Discriminant Equations in Diophantine Number Theory, Cambridge, 2017.
- *I. Gaál*, Diophantine Equations and Power Integral Bases, 2nd ed., Birkhäuser, 2019.

Research papers, a great number of authors, including: Ahmed, Arnóczki, Bilu, El Fadil, Gaál, Gassert, Guardia, Győry, Hamed, Husnine, Jadrijevič, Járási, Kashio, Kim, Lavallee, Montes, Motoda, Nakahara, Nar, Nyul, Olajos, Pethő, Pohst, Remete, Robertson, Schertz, Schulte, Shah, Smart, Smith, Spearman, Stange, Szabó, Tanoé, de Weger, Wildanger, Williams, Ziegler,. . .

Some other related results and open problems

Diophantine approach via unit equations

1) **Integral polynomials with given discriminant**

Further generalization: A integrally closed integral domain of characteristic 0 that is finitely generated over $\mathbb{Z}$ (and may contain *transcendental* elements), and G a finite extension of the quotient field of A. Then monic $f, f^* \in A[X]$ A-equivalent if $f^*(X) = f(X + a)$ with some $a \in A \Longrightarrow D(f^*) = D(f)$.

Theorem (Gy, 1982)

Up to A-equivalence, there are only finitely many monic $f(X)$ in $A[X]$ with a given non-zero discriminant having all their zeros in G + **effective** in Gy (1984) and Evertse and Gy (2017).

Problem 2. *Is this statement true without fixing the splitting field G?*

Problem 3. *Extend Theorem B to the finitely generated case* (at least in **ineffective** form)

2) **Index form equations, monogenity of number fields**

K number field of degree $\mathbf{n} \geq \mathbf{3}$, $I(X_2, \ldots, X_n)$ and associated *index form*

$$I(x_2, \ldots, x_n) = \pm 1 \text{ in } x_i \in \mathbb{Z} \Leftrightarrow \mathcal{O}_K = \mathbb{Z}[\alpha], \quad \alpha = x_1 + x_2\omega_2 + \cdots + x_n\omega_n \ \ (x_1 \in \mathbb{Z}) \tag{10}$$

Problem 4. *Improve the exponential upper bound* (11) *for the solutions. Does there exist polynomial bound for the solutions?*

For $\mathbf{3} \leq \mathbf{n} \leq \mathbf{6}$, there are *practical algorithms* for *solving* (10) in **any** *number field* of *degree n* with *not too large discriminant*.

Problem 5. *For given* $\mathbf{n} \geq \mathbf{7}$, *give such an algorithm*.

$M(n)$: for given $n \geq 3$, maximal *number of solutions* of equations (10); $M(3) \leq 10$ (Bennett), $M(4) \leq 2760$ (Bhargava), for $n \geq 5$ $M(n) \leq 2^{4(n+5)(n-2)}$ (Evertse); for $3 \leq n \leq 6$, $M(n) \geq n^2$, see above

Problem 6. (Gy, 2000). *Is* $M(n)$ *polynomial or exponential in terms of* n?

Extension of finiteness results on (10): *number field case*, Gy (1981), **effective**, *finitely generated case*, Gy (1982), **ineffective**

Problem 7. *Make* **effective** *this result in the finitely generated case*

Arithmetic characterization approach

Hasse's problem (1960's): *give an arithmetic characterization* of **monogenic** *number fields*

a very great number of *important results* for **deciding** the **monogenity** (or **non-monogenity**) of certain special classes of number fields, including *cyclotomic, abelian, cyclic, pure, composible* number fields, *various types of quartic, sextic* and *multiquadratic fields, relative extensions*, and *parametric families of number fields defined by binomial and trinomial irreducible polynomials*

various approaches...

Professors István Gaál and **László Remete** will speak about such results and methods

Problem 8. *Give an arithmetic characterization of* **multiply monogenic** *number fields*

Distribution of monogenic number fields

K number field of degree n

for $\mathbf{n = 1, 2}$, K monogenic;

for $\mathbf{n = 3}$, first example for *non-monogenic* number field: Dedekind (1878);

for fixed $\mathbf{n \geq 3}$, infinitely many *monogenic* and infinitely many *non-monogenic* number fields of degree n;

for $\mathbf{n = 3, 4, 6}$, tables of Gaál (2019): *frequency of monogenic number fields of degree n is decreasing in tendency as $|D_K|$ increases.*

$N_n(X)$: *number of isomorphism classes of monogenic number fields K of degree n with $|D_K| \leq X$ and with Galois group S_n.*

Theorem (Bhargava, Shankar and Wang, 2016, 202?):

$$N_n(X) \gg X^{1/2+1/(n-1)}.$$

Method of proof: arithmetic statistics

Problem 9. *Give an asymptotic formula for $N_n(X)$ as $X \longrightarrow \infty$.*

Canonical number systems in number fields

Kovács, Pethő, later Pethő, Thuswaldner, Evertse, Győry,. . .

Monogenic orders in number fields

Bérczes, Evertse, Győry, and recent generalization by Evertse

Further properties of Hermite equivalence

E.g. algebraic criterion for Hermite equivalence, BEGyRS

Thank you for your attention!