Reduction theory of integral polynomials with given discriminant, various applications, among others to monogenic number fields

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

K. Győry
University of Debrecen

Online Research Seminar *"Number Theory"*

24 November, 2023

Plan of the talk

I. Reduction of integral polynomials of degree ≤ 3 with given discriminant mod $GL_2(\mathbb{Z})$**-equivalence, resp.** $\mathbb{Z}$**-equivalence**

Theorems of Lagrange (1773) and Hermite (1851) in the quadratic and cubic cases

II. Hermite's attempt (1857) for extending the previous reduction results to the general case

III. Reduction theory of integral polynomials with given discriminant: the general case

General reduction Theorems for every degree $n \geq 3$, obtained by Birch and Merriman (1972) and independently, for monic polynomials and in effective form by Győry (1973).

IV. Consequences of Theorem of Győry (1973) for monogenic number fields

General effective finiteness theorems for monogenity and power integral bases of number fields.

V. Generalizations and further consequences/applications of Theorems of Birch and Merriman (1972), Győry (1973) and their explicit versions due to Győry (1974) and Evertse and Győry (1991,2017).

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

In number fields K of degree $n \leq 6$ and with not too large discriminant $|D_K|$, deciding the monogenity and computing all generators of power integral bases.

VII. Some other related results and open problems

I. Reduction of integral polynomials of degree ≤ 3 with given discriminant mod $GL_2(\mathbb{Z})$-equivalence, resp. $\mathbb{Z}$-equivalence

$\mathbb{Z}$-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**

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

Reduction theory was initiated by Lagrange in terms of integral binary forms. He proved the following theorem in terms of binary forms. We present here an equivalent formulation for integral polynomials.

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* $H(f^*) \leq c(D)$ *with some effectively computable constant* $c(D)$.

Equivalently

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

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**

Problem: *extend these results to the case of degree ≥ 3 resp. ≥ 4.*

II. Hermite's attempt (1857) for extending the previous reduction results to the general case

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

Hermite attempted to extend his theorem (1851) on cubic polynomials to the case of arbitrary degree $n \geq 4$, but *without success*. Instead, he proved a theorem with a *weaker equivalence*, see **Theorem A** below.

*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 $\underline{X} = (X_1, \ldots, X_n)^T$ 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 $\mathbb{Z}[X_1, \ldots, X_n]$ 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 : $D(f) = c^{2n-2} \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 \in \mathbb{Z}$.

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

In BEGyRS (2023), we have *integrated* Hermite's long-forgotten notion of equivalence and his finiteness theorem, corrected a faulty reference to Hermite's result in Narkiewicz book "The story of algebraic numbers in the first half of the 20th century", Springer, 2018, and compared Hermite's theorem with the *most significant results* of this area; see the next section.

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**.

In our paper BEGyRS (2023) we proved the following.

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.

This means that Hermite's **Theorem A** is much weaker than the *most significant results* of this area, presented below. In a subsequent talk, L. Remete will speak in detail about the proofs of Theorems 1 and 2.

III. Reduction theory of integral polynomials with given discriminant: the general case

Significant breakthrough in the 1970's

In BEGyRS (2023), we write: "Hermite's *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 precise and **effective** form by Győry (1973)."

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 (1973) in an **effective** form.

Theorem C (Győry, 1973)

Let $f \in \mathbb{Z}[X]$ be a monic polynomial of degree $n \geq 3$ with discriminant $D \neq 0$. There is an $f^* \in \mathbb{Z}[X]$, $\mathbb{Z}$-equivalent to f, such that $H(f^*) \leq c_1(n, D)$ and $n \leq c_2(D)$, where c_1, c_2 are **effectively** *computable positive numbers depending only on n, D, resp. on D.*

Apart from the **ineffectivity** of Theorem B, Theorems B and C are **generalizations** for $n \geq 3$ of the theorems of Lagrange (1773), case $n = 2$, and Hermite (1851), case $n = 3$.

Corollary (Győry, 1973)

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

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

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

Further (Győry, 1974):

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

First explicit version of Theorem C: 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, Theorems B, B', and in the monic case Theorems 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*. It is likely that the bounds in (1) and (2) can be replaced by some polynomial expressions in terms of $|D|$; cf. Conjecture 15.1 and Theorem 15.1.1 in Evertse and Győry, Discriminant Equations in Diophantine Number Theory, Cambridge, 2017.

Method of proof of Theorems C and C'

General approach for *effective/algorithmic/computational* versions

Main steps of the proof of Theorem C:

1) $n \leq c_1(D)$, *explicit*, elementary; fix n.
2) 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 $\alpha_1, \ldots, \alpha_n$. L splitting field of $f \Longrightarrow [L : \mathbb{Q}] \leq n!$, $|D_L| \leq c_2(D)$, *explicit*.
3) $$\prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 = D \Longrightarrow |N_{L/\mathbb{Q}}(\alpha_i - \alpha_j)| \leq c_3(D) \textit{ explicit} \\ \Longrightarrow \alpha_i - \alpha_j = \delta_{ij}\varepsilon_{ij},\ \varepsilon_{ij} \textit{ unit, } H(\delta_{ij}) \leq c_4(D) \textit{ explicit} \tag{3}$$
4) $$(\alpha_i - \alpha_j) + (\alpha_j - \alpha_k) + (\alpha_k - \alpha_i) = 0 \text{ for every } i,\ j\ k \tag{4}$$
   graph: *vertices* $\alpha_i - \alpha_j$, *edges* $[\alpha_i - \alpha_j, \alpha_j - \alpha_k]$, connected
5) (4) $\Longrightarrow$ "connected" system of unit equations
   $$\delta_{ijk}\varepsilon_{ijk} + \tau_{ijk}\nu_{ijk} = 1, \tag{5}$$
   δ_{ijk}, τ_{ijk} with explicitly bounded heights, $\varepsilon_{ijk}, \nu_{ijk}$ **unknown** *units* in L.

Effective/explicit bound for the solutions

6) *Represent* ε_{ijk}
$$\varepsilon_{ijk} = \zeta_{ijk}\rho_1^{a_{ijk,1}} \cdots \rho_r^{a_{ijk,r}}$$
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.* $\square$

IV. Consequences of Theorem of Győry (1973) for monogenic number fields

Important breakthrough; *general effective finiteness theorems* for monogenity and power integral bases of number fields.

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 $\alpha \Longrightarrow$*

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

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

Definition

- $\alpha, \alpha^* \in \mathcal{O}_K$ **equivalent** *if* $\alpha^* = \pm\alpha + a$, $a \in \mathbb{Z} \Rightarrow D_{K/\mathbb{Q}}(\alpha) = D_{K/\mathbb{Q}}(\alpha^*)$, $I(\alpha) = I(\alpha^*)$
- 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* $\mathcal{O}_K = \mathbb{Z}[\alpha] \Leftrightarrow \{1, \alpha, \dots, \alpha^{n-1}\}$ *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 + **generalizations** for **orders** (Part III) and for the **relative case** (Part IV); see below.

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

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

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

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

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

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

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

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

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

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

see Evertse and Győry (2017).

Extension to the relative case: *the ground field is a number field L with ring of integers $\mathcal{O}_L$.*

Two monic polynomials $f, f^* \in \mathcal{O}_L[X]$ are called *$\mathcal{O}_L$-equivalent* if $f^*(X) = f(X + a)$ for some $a \in \mathcal{O}_L$. Then $D(f^*) = D(f)$.

Győry (1978a): extension of Theorem C (Gy, 1973) to monic polynomials of given degree over $\mathcal{O}_L$; Part IV of Gy (1973).

Theorem D (Gy, 1978a)

Let $n \geq 3$ be an integer and $\delta \in \mathcal{O}_L \setminus \{0\}$. There are only finitely many $\mathcal{O}_L$-equivalence classes of monic polynomials $f \in \mathcal{O}_L[X]$ with degree n and discriminant δ, and a full set of representatives can be, at least in principle, effectively determined.

Problem 1: *In contrast with Theorem C, is it necessary to assume in Theorem D that the degree of the polynomials is fixed?*

Theorem D has similar **consequences** in the relative case as Theorem C (Gy, 1973) over $\mathbb{Q}$.

A finite relative extension K/L is called monogenic if $\mathcal{O}_K = \mathcal{O}_L[\alpha]$ for some $\alpha \in \mathcal{O}_K$. Then, if $n = [K\ \ L]$, $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a relative power integral basis of K over L. We say that $\alpha, \alpha^* \in \mathcal{O}_K$ are $\mathcal{O}_L$-equivalent if $\alpha^* = a + \varepsilon\alpha$ for some $a \in \mathcal{O}_L$ and unit ε in L. If α is a generator of $\mathcal{O}_K$ over $\mathcal{O}_L$ then so is every α^* $\mathcal{O}_L$-equivalent to α.

Corollary to Theorem D (Gy, 1978a)

There are only finitely many $\mathcal{O}_L$-equivalence classes of $\alpha \in \mathcal{O}_K$ with $\mathcal{O}_K = \mathcal{O}_L[\alpha]$, and a full set of representatives of such α can be, at least in principle, effectively determined.

This makes it possible, at least in principle to decide whether K is monogenic over L or not, and to determine all relative power integral bases of K over L.

Theorem D and its Corollary are proved in Győry (1978a) in a quantitative form.

Remark: we note that Theorem C, D and the above Corollary are quoted and treated in the monograph Evertse and Győry (2017).

V. Generalizations and further consequences/applications of Theorems of Birch and Merriman (1972), Győry (1973) and Evertse and Győry (1991,2017)

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)

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); see below.
- 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);
- *analogous results over* **function fields** (Gaál, Gy, Shlapentokh);
- **Recently**, <u>étale algebras</u> (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);

$\vdots$

Problem 2: *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**

VI. 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, practical algorithms, computational results** and **tables**.

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 $\mathbf{n} \geq \mathbf{5}$, 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 minimal 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 some reduction and enumeration algorithms.

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 $\varepsilon_{ijk} = \zeta_{ijk}\rho_1^{a_{ijk,1}} \cdots \rho_r^{a_{ijk,r}}$ 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 $\mathbf{n = 5, 6}$ 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 <u>most difficult case</u> 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

For $\mathbf{n \geq 7}$, the above algorithms **do not work** in general. Then the number of fundamental units, $\varrho_1, \ldots, \varrho_r$ involved can be too large to use the enumeration algorithm. Hence, for $n \geq 7$, further improvements would be needed.

VII. Some other related results and open problems

1. Monic polynomials with given discriminant over finitely generated domains

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

2. Index form equations, bounds for the solutions and for the number of solutions

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

3. Arithmetic characterization of monogenic and multiply monogenic number fields

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, composite* 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

- Infinite parametric families of fields, use of the index form approach;
- ideal theoretic approach, Dedekind's criterion;
- Montes algorithm, Newton polygons;
- Ore theorem;
- Gröbner bases approach;
- reduction to binomial Thue equations;
- irreducible monic polynomials with square-free discriminant;
- non-squarefree discriminant approach;

$\vdots$

Remark: in many cases the monogenity can be, but its multiplicity cannot be determined by the method used.

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

Books, research papers

Books: Hensel (1908), Hasse (1963), Narkiewicz (1990), Evertse and Győry (2017), Gaál (2019) with many references.

Research papers, a great number of *authors*, including:

Ahmad, Archinard, Arnóczki, Bell, Bérczes, Bilu, Bozlee, Brenner, Brunotte, Cougnard, Delone, Dummit, Evertse, El Fadil, Faddeev, Gaál, Gassert, Gras, Guardia, Győry, Hameed, Hasse, Huard, Husnine, Jadrijevic, Jakhar, Járási, Jones, Katayama, Khan, Khanduja, Kim, Kisilevsky, Kovács, Lavallee, Liang, Merriman, Montes, Motoda, Nakahara, Nart, Nguyen, Nyul, Park, Pethő, Pohst, Ranieri, Remete, Robertson, Russel, Sangwan, Sekigawa, Shah, Simon, Smart, Smith, Spearman, Stange, Sultan, Tanoé, Thérond, Uehara, Wildanger, Williams, Yakkou, Ziegler,...

4. Distribution of monogenic number fields

K number field of degree n

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

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

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

for $\mathbf{n} = \mathbf{3}, \mathbf{4}, \mathbf{6}$, 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 $|D_K| \leq X$.*

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

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

Bhargava and Yang (2022) guess that for some $c_n > 0$, $N_n(X)/X^{(n+1)/(2n-2)} \to c_n$ as $X \to \infty$.

5. Monogenic orders in number fields

K number field of degree ≥ 3, $\mathcal{O}$ and order of K (i.e., a subring of K that as a $\mathbb{Z}$-module is free of rank $[K : \mathbb{Q}]$). $\mathcal{O}$ is called monogenic if $\mathcal{O} = \mathbb{Z}[\alpha]$ with some $\alpha \in \mathcal{O}$, and three times monogenic if $\mathcal{O} = \mathbb{Z}[\alpha_1] = \mathbb{Z}[\alpha_2] = \mathbb{Z}[\alpha_3]$ with *pairwise $\mathbb{Z}$-inequivalent* $\alpha_1, \alpha_2, \alpha_3 \in \mathcal{O}$.

Bérczes, Evertse and Győry (2013) proved that *there are at most finitely many three times monogenic orders in K. Evertse will present in his lecture a more general result of this type for so-called rationally monogenic orders.*

6. Canonical number systems in orders of a number field

As above, K number field of degree ≥ 3, $\mathcal{O}$ an order in K; $\alpha \in \mathcal{O}$, $\alpha \neq 0$ is called a **basis** of a **canonical number system** (or **CNS basis**) for $\mathcal{O}$ if every non-zero element of $\mathcal{O}$ can be represented in the form

$$a_0 + a_1\alpha + \cdots + a_m\alpha^m$$

with $m \geq 0$, $a_i \in \{0, 1, \ldots |N_{K/\mathbb{Q}}(\alpha)| - 1\}$ for $i = 0, \ldots, m$ and $a_m \neq 0$.

CNS is a *natural* **generalization** of *radix representations* of rational integers to algebraic integers.

$\mathcal{O}$ is called a **CNS order** if there exists a CNS in $\mathcal{O}$. CNS orders have been intensively investigated, see e.g. the survey papers Brunotte, Huszti, Pethő (2006) and Evertse, Győry, Pethő and Thuswaldner (2019).

Kovács (1981) proved that $\mathcal{O}$ *is a CNS order* $\Longleftrightarrow$ $\mathcal{O}$ *is monogenic*. If α is a *CNS basis* in $\mathcal{O} \Rightarrow \mathcal{O} = \mathbb{Z}[\alpha]$. *Conversely, if* $\mathcal{O} = \mathbb{Z}[\alpha]$ *then there are infinitely many* α' $\mathbb{Z}$-equivalent *to* α *such that* α' *is a* CNS *basis for* $\mathcal{O}$. For a *characterization* of CNS bases in $\mathcal{O}$, see Kovács and Pethő (1991).

Consequence of **generalization for orders** (Gy, 1976) of **Corollary 3** to **Theorem C** (Gy, 1973). *Up to* $\mathbb{Z}$*-equivalence, there are only finitely many canonical number systems in* $\mathcal{O}$*, and all of them can be effectively determined.*

Thank you for your attention!