On the smallest number of terms of vanishing sums of units in number fields

(joint work with Cs. Bertók, L. Hajdu and A. Schinzel)

K. Győry
(Debrecen)

September, 2018

I. Unit equations in general

II. Exceptional units

III. A generalization of exceptional units

IV. Application to arithmetic graphs

I. Unit equations in general

K number field, $\mathcal{O}_K$ ring of integers, $\mathcal{O}_K^*$ unit group

Unit equation: for fixed $\alpha_1, \alpha_2 \in K \setminus \{0\}$

$$\alpha_1\varepsilon_1 + \alpha_2\varepsilon_2 = 1 \quad \text{in } \varepsilon_1, \varepsilon_2 \in \mathcal{O}_K^* \tag{1}$$

Results:

(1) *has finitely many solutions* $\begin{cases} \text{Siegel (1921), implicit} \\ \text{Lang (1960), in more general form} \end{cases}$

effective finiteness: Győry (1972–) (Baker's method),...

bound for # (number of solutions): Evertse (1984),...
independent of α_1, α_2

I. Unit equations in general

Generalizations:

S-unit equations
- finiteness: Mahler (1933), Parry (1950)
- effective finiteness: Győry (1979),...
- bound for #: Evertse (1984),...

finitely generated case
$\mathcal{O}_K \to A$, $\mathcal{O}_K^* \to A^*$
A finitely generated over $\mathbb{Z}$
- finiteness: Lang (1960)
- effective finiteness: Evertse–Győry (2013)
- bound for #: Beukers–Schlickewei (1996)

multivariate unit equations:

for fixed $\alpha_1, \ldots, \alpha_m \in K \setminus \{0\}$

$$\alpha_1\varepsilon_1 + \cdots + \alpha_m\varepsilon_m = 1 \quad \text{in } \varepsilon_1, \ldots, \varepsilon_m \in \mathcal{O}_K^* \tag{2}$$

solution $\varepsilon_1, \ldots, \varepsilon_m$ *degenerate* if in (2) there is a vanishing subsum

$\Rightarrow$ infinitely many sols if $\mathcal{O}_K^*$ is infinite

I. Unit equations in general

finiteness of #' (number of non-degenerate sols): van der Poorten–Schlickewei (1982), Evertse (1984) (Subspace Theorem)

bound for #': Schlickewei (1990), Evertse, Schlickewei, Schmidt (2002), Amoroso, Viada (2011) (Quantitative Subspace Theorem)

Open problem: effective finiteness for the non-degenerate solutions

- extremely rich **literature**
- great number of various **applications**

J.-H. Evertse–K. Győry, *Unit Equations in Diophantine Number Theory*, Cambridge University Press, 2015

II. Exceptional units

Nagell (1970): ε *exceptional unit* in K if $1-\varepsilon$ is also a unit

existence of such $\varepsilon \iff \varepsilon_1+\varepsilon_2+\varepsilon_3=0$ solvable in $\varepsilon_i \in \mathcal{O}_K^*$

For any $d \geq 2$ there is a number field of degree d, e.g. $K=\mathbb{Q}(\varepsilon)$ with ε a root of x^d+x+1 which has exceptional unit

Nagell (1964–70): all exceptional units in number fields K of unit rank 1 $(\mathrm{rank}\ \mathcal{O}_K^*=1)$ and in number fields of unit rank 2

$m \not\equiv 2 \pmod 4$, K_m m-th cyclotomic field, K_m^+ its maximal real subfield

Wildanger (2000): all exceptional units in K_m resp. K_m^+ for $m \leq 23$ (Baker's method + reduction algorithms)

Example: in K_{19}^+ 28398 exceptional units

II. Exceptional units

Several applications, one of them due to Lenstra (1977):

if $\mathcal{O}_K$ contains a "large" subset $\{\varepsilon_1, \dots, \varepsilon_n\}$ such that $\varepsilon_i - \varepsilon_j$ is a unit for each i, j then K (i.e. $\mathcal{O}_K$) is Euclidean

Using this, Lentsra, Mestre, Leutbecher–Martinet, Leutbecher–Niklash, Huriet obtained several hundreds of new examples for Euclidean number fields K

III. A generalization of exceptional units

K number field, $\mathcal{O}_K$, $\mathcal{O}_K^*$ as above

Def: $L(K)$ *smallest integer* m *with* $m \geq 3$ *such that the unit equation*

$$\varepsilon_1 + \cdots + \varepsilon_m = 0 \quad \text{is solvable in } \varepsilon_1, \ldots, \varepsilon_m \in \mathcal{O}_K^* \tag{3}$$

with no vanishing subsum on the left hand side.

If $\exists$ exceptional unit then $L(K) = 3$

If no such m exists, set $L(K) = \infty$

Examples: For $K = \mathbb{Q}$ and imaginary quadratic fields K $L(K) = \infty$, except for $K = \mathbb{Q}(\sqrt{-3})$ when $L(K) = 3$

III. A generalization of exceptional units

Results

Theorem 1. *For any number field K different from $\mathbb{Q}$ and the imaginary quadratic fields $L(K)$ is finite. Further,*

$$L(K) \leq 2(d+1)\exp\{cR_K\},$$

where r, d, R_K unit rank, degree and regulator of K and

$$c = \begin{cases} 1/d, & \textit{if } r = 1, \\ 29e\sqrt{r-1} \cdot r!(\log d), & \textit{if } r \geq 2. \end{cases}$$

We note that

$$R_K \leq |D_K|^{1/2}(\log^* |D_K|)^{d-1},$$

D_K *discriminant* of K, $\log^* x = \max(\log x, 1)$

III. A generalization of exceptional units

Similar statement for orders[1] $\mathcal{O}$ of number fields, where $L(\mathcal{O})$ can be defined as for number fields.

Theorem 2. *For any integer $m \geq 3$ there exists an order $\mathcal{O}$ of some number field K with $L(\mathcal{O}) = m$.*

In fact, $\mathcal{O}$ can be chosen as an order of a real quadratic number field.

Apart from some values of m, $L(K)$ can also be an arbitrary integer $m \geq 3$.

Theorem 3. *For any integer $m \geq 3$ which is* **not** *of the form $4t^4 - 4t + 2$ $(t \in \mathbb{Z} \setminus \{0, 1\})$ there exists a number field K with $L(K) = m$.*

One can choose K to be a complex cubic number field.

Conjecture. *For any integer $m \geq 3$ there exists a number field K with $L(K) = m$.*

[1] A subring $\mathcal{O}$ of $\mathcal{O}_K$ is called an *order* in K if $\mathcal{O}$ contains d linearly independent elements of K with $d = [K : \mathbb{Q}]$

III. A generalization of exceptional units

Write ξ_n for a primitive root of unity of order n.

Theorem 4. *For any integer $m \geq 3$, there are only finitely many quadratic fields, complex cubic fields and totally complex quartic fields K with $L(K) \leq m$, in the latter case assuming that K does not have a real quadratic subfield and $\xi_3 \notin K$, and all such fields can be effectively determined.*

There are infinitely many exceptional quartic fields with the properties mentioned.

III. A generalization of exceptional units

Write $L_o(K)$ for the *smallest odd* $m \geq 3$ for which

$$\varepsilon_1 + \cdots + \varepsilon_m = 0 \quad \text{solvable in } \varepsilon_1, \ldots, \varepsilon_m \in \mathcal{O}_K^*. \tag{3}$$

Further, let $L_e(K)$ be the *smallest even* $m \geq 4$ for which (3) is valid such that in (3) there is no proper vanishing subsum. If no appropriate m exists at all, set $L_o(K) = \infty$ or $L_e(K) = \infty$, resp. We have

$$L(K) = \min(L_o(K), L_e(K)).$$

Obviously, if $m = L_o(K)$ then in (3) there is no proper vanishing subsum.

Theorem 5. *Let $d \geq 2$. There are infinitely many number fields K of degree d with $L_o(K) = \infty$.*

III. A generalization of exceptional units

For $L_e(K)$ we have

Theorem 6. *Let $d \geq 3$. There are infinitely many number fields K of degree d with $L_e(K) = 4$.*

$\Longrightarrow$ for these number fields K, $L_e(K)$ can take its minimal value 4.

For the cyclotomic fields $K = \mathbb{Q}(\xi_n)$ with $n = 1, 2, 4$
$\Longrightarrow L(K) = \infty$. Except these fields, we have

Theorem 7. *In every cyclotomic field $K = \mathbb{Q}(\xi_n)$, except $n \mid 4$, $L_o(K) < \infty$ and $L_e(K) < \infty$ hold.*

IV. Application to arithmetic graphs

K number field, $A = \{\alpha_1, \dots, \alpha_m\}$ *finite ordered subset of* $\mathcal{O}_K$, $\mathcal{G}(A)$ the *graph* with *vertex set* A whose *edges* $[\alpha_i, \alpha_j]$ with

$$\alpha_i - \alpha_j \in \mathcal{O}_K^*;$$

Győry (1971, 1972). The ordered subsets $A = \{\alpha_1, \dots, \alpha_m\}$, $A' = \{\alpha_1', \dots, \alpha_m'\}$ of $\mathcal{O}_K$ *equivalent* if

$$\alpha_i' = \varepsilon\alpha_i + \beta \quad \text{with some } \varepsilon \in \mathcal{O}_K^*, \ \ \beta \in \mathcal{O}_K, \ \ i = 1, \dots, m.$$

$\Longrightarrow \mathcal{G}(A), \mathcal{G}(A')$ *isomorphic*.

In this terminology, Lenstra (1977) above mentioned theorem says: *if there is a "large" complete graph* $\mathcal{G}(A)$ *with* $A \subset \mathcal{O}_K \Rightarrow \mathcal{O}_K$ *is Euclidean*

IV. Application to arithmetic graphs

For given $m \geq 3$ there are *infinitely many* equivalence classes of ordered subsets A of $\mathcal{O}_K$ with $|A| = m$. Apart from finitely many equivalence classes, the *structure* of these graphs have been described by Győry (1980) $\Longrightarrow$ many important applications to wide classes of diophantine problems.

Theorem 8. *Let K be an algebraic number field different from $\mathbb{Q}$ and the imaginary quadratic fields. Then among the graphs $\mathcal{G}(A)$*

(i) *there are cycles*[2] *of every even length ≥ 4,*

(ii) *there are cycles of every odd length $\geq L_o(K)$, but there are no cycles of odd length $< L_o(K)$.*

---

[2] $A = \{\alpha_1, \ldots, \alpha_m\}$ forms a cycle if α_i and α_j are connected with an edge if and only if either $\{i, j\} = \{1, m\}$ or $|i - j| = 1$.

IV. Application to arithmetic graphs

This is a complete characterization of the possible lengths of cycles among the graphs $\mathcal{G}(A)$. It is closely related to some results of Ruzsa (2011) and Győry, Hajdu, Tijdeman (2014, 2016) on graphs $\mathcal{G}(A)$.

In our **proofs**, some diophantine and algebraic number–theoretic results and methods are combined.

Open question

Is it true that for any d with $d \geq 2$ and $a \in \mathbb{Z}_{\geq 4}$ even, $b \in \mathbb{Z}_{\geq 3} \cup \{\infty\}$ odd, there exist infintely many number fields K such that $\deg(K) = d$, $L_e(K) = a$ and $L_o(K) = b$?

Cs. Bertók, K. Győry, L. Hajdu, A. Schinzel, *On the smallest number of terms of vanishing sums of units in number fields*, J. Number Theory **192** (2018), 328–347.