ON THE SMALLEST NUMBER OF TERMS OF VANISHING SUMS OF UNITS IN NUMBER FIELDS

CS. BERTÓK, K. GYŐRY, L. HAJDU, A. SCHINZEL

Abstract. Let K be a number field. In the terminology of Nagell a unit ε of K is called *exceptional* if $1-\varepsilon$ is also a unit. The existence of such a unit is equivalent to the fact that the unit equation $\varepsilon_1+\varepsilon_2+\varepsilon_3=0$ is solvable in units $\varepsilon_1,\varepsilon_2,\varepsilon_3$ of K. Numerous number fields have exceptional units. They have been investigated by many authors, and they have important applications.

In this paper we deal with a generalization of exceptional units. We are interested in the smallest integer k with $k\geq 3$, denoted by $\ell(K)$, such that the unit equation $\varepsilon_1+\dots+\varepsilon_k=0$ is solvable in units $\varepsilon_1,\dots,\varepsilon_k$ of K. If no such k exists, we set $\ell(K)=\infty$. Apart from trivial cases when $\ell(K)=\infty$, we give an explicit upper bound for $\ell(K)$. We obtain several results for $\ell(K)$ in number fields of degree at most 4, cyclotomic fields and general number fields of given degree. We prove various properties of $\ell(K)$, including its magnitude, parity as well as the cardinality of number fields K with given degree and given odd resp. even value $\ell(K)$.

Finally, as an application, we deal with certain arithmetic graphs, namely we consider the representability of cycles. We conclude the paper by listing some problems and open questions.

1. Introduction

Let K be a number field. We are interested in the smallest integer k having the following property:

$$\text{(1)} \qquad \text{there exist units } \varepsilon_1,\dots,\varepsilon_k\in K \text{ such that } \varepsilon_1+\dots+\varepsilon_k=0.$$

Observe that for any even integer $k=2t$, we have a trivial assertion given by $t\times 1+t\times(-1)=0$. So we shall use the following definitions.

Write $\ell_o(K)$ for the smallest odd $k\geq 3$ for which (1) is valid. Further, let $\ell_e(K)$ be the smallest even $k\geq 4$ for which (1) is valid, such that the sum appearing in (1) has no proper vanishing subsum. If no appropriate k

Date: October 9, 2018.

2010 *Mathematics Subject Classification.* 11R27, 11D85, 11D72.

Key words and phrases. Exceptional units, unit equations, arithmetic graphs.

Research supported in part by the Hungarian Academy of Sciences, the ÚNKP-17-3, New National Excellence Program of the Ministry of Human Capacities, the NKFIH grant K115479 and by the projects EFOP-3.6.1-16-2016-00022, EFOP-3.6.2-16-2017-00015 and EFOP-3.6.3-VEKOP-16-2017-00002, co-financed by the European Union and the European Social Fund.

exists at all, then we set $\ell_o(K) = \infty$ or $\ell_e(K) = \infty$, respectively. We put $\ell(K) = \min(\ell_o(K), \ell_e(K))$.

Before proceeding further, we make a trivial observation. First note that if $k = \ell_o(K)$, then the sum of units appearing in (1) has no proper vanishing subsum. Indeed, otherwise we would have a proper vanishing subsum with an odd number of terms, contradicting the minimality of $k = \ell_o(K)$.

The above notions can be generalized to orders of number fields. Let $\mathcal{O}$ be an order of a number field K. Then we can define $\ell_o(\mathcal{O}), \ell_e(\mathcal{O}), \ell(\mathcal{O})$ in the obvious way. Note that if $\mathcal{O}$ is the maximal order of K, then we clearly have $\ell_o(\mathcal{O}) = \ell_o(K)$, $\ell_e(\mathcal{O}) = \ell_e(K)$, $\ell(\mathcal{O}) = \ell(K)$.

In this paper we obtain several results concerning $\ell(K), \ell_o(K), \ell_e(K)$ and $\ell(\mathcal{O}), \ell_o(\mathcal{O}), \ell_e(\mathcal{O})$. We show among other things that $\ell(K)$ is finite for any number field K, apart from the cases where $K = \mathbb{Q}$ or K is an imaginary quadratic field. Further, we prove that for any integer $k \geq 3$ there exists an order of a real quadratic number field with $\ell(\mathcal{O}) = k$, and also a complex cubic number field K with $\ell(K) = k$ - in the latter case excluding values k of the form $k = 4t^4 - 4t + 2$. On the other hand, we show that for each k, there are only finitely many quadratic fields, complex cubic fields and (up to certain completely described exceptions) totally complex quartic fields with $\ell(K) \leq k$, and all these number fields can be effectively determined. Furthermore, it is shown that for any number field K different from $\mathbb{Q}$ and the imaginary quadratic fields we have $\ell_e(K) < \infty$. Finally, we prove that for $d \geq 3$ there are infinitely many number fields K of degree d with $\ell_e(K) = 4$, and for $d \geq 2$ there are infinitely many number fields K of degree d with $\ell_o(K) = \infty$.

We give some applications of our results to certain arithmetic graphs, more precisely to graphs having vertices from the set of integers of K, in which two vertices α, β are connected by an edge if and only if $\alpha - \beta$ is a unit in K. We mention that Győry has several results about and applications of such graphs (see e.g. [14] and the references given there), and recently Győry, Hajdu, Tijdeman [16, 17] and Ruzsa [28] made a systematic study of the representability of such graphs. Our results allow us to extend some results from the mentioned papers, concerning representations of cycles.

Clearly, the existence of units appearing in (1) means that the unit equation

$$\varepsilon_1 + \cdots + \varepsilon_k = 0 \tag{2}$$

has a solution in units $\varepsilon_1, \ldots, \varepsilon_k$ of K such that the left hand side has no proper vanishing subsum. For $k = 3$, the solvability of (2) is equivalent to the existence of a unit ε, called exceptional unit, see Nagell [26], such that $1 - \varepsilon$ is also a unit. Obviously, we have $\ell(K) = \ell_o(K) = 3$ if and only if K contains an exceptional unit. There is an extremely rich literature on unit equations of the form (2). For given $k \geq 3$, there are results stating the finiteness of the number of solutions up to a proportional factor. Further, there are explicit upper bounds for the number of solutions and, for $k = 3$, even for the size of the solutions. Moreover, for $k = 3$ and for some special number fields K, all the solutions have been determined. Many books and survey papers deal with these equations, their generalizations and various applications; see e.g. Lang [22], Győry [12, 13], Evertse [4], Mason [24], Shorey and Tijdeman [35], Evertse, Győry, Stewart and Tijdeman [7], Schmidt [34], Smart [39], Evertse and Győry [6] and the references given there.

We organize our paper as follows. First we present our main results, followed by their proofs. After that we give applications to arithmetic graphs. We conclude the paper with some open problems.

2. Main results

In this section we present our main results. We split them into two parts: first we provide statements concerning the parameters $\ell(K), \ell_o(K), \ell_e(K)$ and $\ell(\mathcal{O}), \ell_o(\mathcal{O}), \ell_e(\mathcal{O})$. Then we give results concerning so-called odd and even units, since they play an important role in our proofs.

2.1. Results concerning $\ell(K), \ell_o(K), \ell_e(K)$ and $\ell(\mathcal{O}), \ell_o(\mathcal{O}), \ell_e(\mathcal{O})$.

Our first theorem is a simple, but important statement.

Theorem 2.1. *For any number field K different from $\mathbb{Q}$ and the imaginary quadratic fields, $\ell(K)$ is finite. Further,*

$$\ell(K) \le 2(d+1)\exp\{cR_K\},$$

where

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

Here r, d and R_K denote the unit rank, the degree and the regulator of K, respectively.

We note that

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

where D_K denotes the discriminant of K, and $\log^*(x) = \max\{\log x, 1\}$. This is an improvement of an inequality of Landau [20]; see (59) in Győry and Yu [19].

Remark. Obviously, $\ell(K) = \infty$ for $K = \mathbb{Q}$ and the same is true for all imaginary quadratic fields (including the Gaussian field $\mathbb{Q}(i)$), except for $K = \mathbb{Q}(\sqrt{-3})$. In the latter case we have $\ell(K) = 3$.

We also mention that a statement similar to Theorem 2.1 could be formulated for orders $\mathcal{O}$ of number fields, as well.

Our next result shows that $\ell(\mathcal{O})$ can be an arbitrary integer $k \ge 3$.

Theorem 2.2. *For any $k \ge 3$ there exists an order $\mathcal{O}$ of some number field K with $\ell(\mathcal{O}) = k$. In fact, $\mathcal{O}$ can be chosen as an order of a real quadratic number field.*

Our next result shows that apart from the values k taken by a particular quartic polynomial, $\ell(K)$ can also be an arbitrary integer $k \geq 3$.

Theorem 2.3. *For any $k \geq 3$ which is not of the form $4t^4 - 4t + 2$ ($t \in \mathbb{Z} \setminus \{0, 1\}$) there exists a number field K with $\ell(K) = k$. In fact, one can choose K to be a complex cubic number field.*

We are sure that the above theorem is valid for all values of k. So we propose the following

Conjecture. For any $k \geq 3$ there exists a number field K with $\ell(K) = k$.

We provide some numerical results to support our conjecture.

Proposition 1. *Let $K_t = \mathbb{Q}(\alpha_t)$, where α_t is a root of the polynomial $x^3 + x^2 + (4t^4 - 4t - 1)x + 1$ for $t \in \{-20, \ldots, -1\} \cup \{2, \ldots, 20\}$. Then we have $\ell(K_t) = 4t^4 - 4t + 2$.*

Our next theorem shows that under some restrictions, for any k, there are only finitely many number fields K with $\ell(K) \leq k$. Clearly, some restriction is needed to obtain such a result: for example, if ε is a root of the polynomial $x^n + x + 1$ with $n \geq 2$, then for the number field $K = \mathbb{Q}(\varepsilon)$ we obviously have $\ell(K) = 3$. In what follows, we write ζ_n for a primitive root of unity of order n.

Theorem 2.4. *For any $k \geq 3$, there are only finitely many quadratic fields, complex cubic number fields and totally complex quartic number fields K with $\ell(K) \leq k$, in the latter case assuming that K does not have a real quadratic subfield and $\zeta_3 \notin K$, and all such fields can be effectively determined.*

Remark. There are infinitely many totally complex quartic fields K having a real quadratic subfield L. As for all such fields K we have $\ell(K) \leq \ell(L)$, the above statement is not valid for them. Similarly, there are infinitely many totally complex quartic fields K with $\zeta_3 \in K$, and hence with $\ell(K) = 3$. Thus they also have to be excluded from Theorem 2.4.

The value of $\ell_o(K)$ can be infinite in non-trivial cases (i.e. excluding $\mathbb{Q}$ and the imaginary quadratic fields) as well.

Theorem 2.5. *Let $d \geq 2$. There are infinitely many number fields K of degree d with $\ell_o(K) = \infty$.*

Our final result in this subsection shows that $\ell_e(K)$ can take its minimal value (that is 4) for infinitely many number fields, having any prescribed degree ≥ 3. Note that in view of Theorem 2.4, the case $d = 2$ has to be excluded, so our statement is best possible in this respect.

Theorem 2.6. *Let $d \geq 3$. There are infinitely many number fields K of degree d with $\ell_e(K) = 4$.*

2.2. **Results concerning odd and even units.**

In this subsection we investigate the existence of odd and even units in a number field K. This is an important question from our viewpoint: as we shall see soon, if K contains an odd unit then $\ell_o(K)$ is finite, and, similarly, if K contains an even unit then $\ell_e(K)$ is finite.

We need a little preparation. For any integer polynomial

$$g(x) = b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0$$

write

$$L(g) = |b_n| + |b_{n-1}| + \cdots + |b_1| + |b_0|$$

for the length of $g(x)$. The properties of lengths of polynomials have been studied by several authors; see e.g. [8, 31, 32] and the references given there.

We call an algebraic integer α even, if $L(f)$ is even, where $f(x)$ is the minimal monic polynomial of α (over $\mathbb{Q}$); otherwise α is odd. Observe that α is even if and only if $f(1)$ is even.

Let ε be a unit of K, different from the roots of unity, and let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be the minimal monic polynomial of ε. Observe that then the equation

$$\varepsilon^n + a_{n-1}\varepsilon^{n-1} + \cdots + a_1\varepsilon + a_0 = 0$$

shows that (1) is satisfied in K with $k = L(f)$ terms, and also that there cannot be proper vanishing subsums of the left hand side. In particular, we have that if ε is odd then $\ell_o(K) < \infty$, and if ε is even then $\ell_e(K) < \infty$. In what follows, this observation will be frequently used.

The next theorem shows that excluding the trivial cases, every number field contains a non-trivial even unit.

Theorem 2.7. *Every number field K different from $\mathbb{Q}$ and the imaginary quadratic fields, contains an even unit different from ± 1. In particular, we have $\ell_e(K) < \infty$.*

As it was mentioned in the Remark after Theorem 2.1, for $K = \mathbb{Q}$ and the imaginary quadratic fields with the exception of $\mathbb{Q}(\zeta_3)$, we have $\ell(K) = \infty$. Hence $\ell_e(K) = \infty$ is also valid for these fields. Further, it is easy to check that $\ell_e(\mathbb{Q}(\zeta_3)) = \infty$, too.

Theorems 2.5 and 2.7 imply that for $d \geq 3$ and for $d = 2$ with K quadratic real, $\ell_e(K) < \infty$ holds, and there are infinitely many number fields K of degree d with $\ell_o(K) = \infty$.

For $d \leq 4$, we have the following more explicit result.

Theorem 2.8. *Let K be a real quadratic, a complex cubic or a totally complex quartic field; in the latter case assume that K does not contain roots of unity different from ± 1. Suppose that K has a fundamental unit which is even. Then all units of K are even. In particular, in these cases we have $\ell_o(K) = \infty$.*

Our final result in this section shows that in general, cyclotomic fields contain odd units.

Theorem 2.9. *In every cyclotomic field $K = \mathbb{Q}(\zeta_n)$ except $n \mid 4$ there exists an odd unit. In particular, in these number fields we have $\ell_o(K) < \infty$ and $\ell_e(K) < \infty$.*

By our previous remarks, for $n = 1, 2, 4$ we have $\ell(K) = \infty$.

3. Lemmas, auxiliary results and proofs of our main results

We start with the proofs of our theorems concerning odd and even units. For this, we need several lemmas.

Lemma 3.1. *Let F be the minimal monic polynomial of a unit ε over $\mathbb{Q}$ and n a positive integer. Then ε^n is even if $\prod_{i=0}^{n-1} F(\zeta_n^i)$ is even, where ζ_n is a primitive root of unity of order n.*

Proof. Let G be the minimal monic polynomial of ε^n over $\mathbb{Q}$. Since $G(\varepsilon^n) = 0$, we have $F(x) \mid G(x^n)$. It follows that for every $i = 0, \dots, n-1$ we have $F(\zeta_n^i x) \mid G(x^n)$ whence $\prod_{i=0}^{n-1} F(\zeta_n^i x) \mid G(x^n)^n$. If the assumption of the lemma holds, then $G(1)$ is even, thus ε^n is even. □

Let ϕ be the canonical map of $\mathbb{Z}[x]$ onto $\mathbb{F}_2[x]$.

Lemma 3.2. *Let ε be a unit of a number field K and F its minimal polynomial over $\mathbb{Q}$. Then ε^{2^n-1} is even, if n is the degree of an irreducible factor over $\mathbb{F}_2$ of $\phi(F)$.*

Proof. By the theory of finite fields we have

$$x^{2^n} - x = \prod f(x),$$

where the product on the right hand side is taken over all distinct irreducible polynomials over $\mathbb{F}_2$ whose degree divides n. Hence, over $\mathbb{F}_2$ we have

$$\phi(\Phi_{2^n-1}(x)) = \prod f(x),$$

where Φ_m denotes the cyclotomic polynomial of order m, and the product on the right hand side is now taken over all distinct irreducible polynomials over $\mathbb{F}_2$ of degree n. By Dedekind's theorem on congruences we have

$$(2) = \prod (G_f(\zeta_{2^n-1}), 2) \quad \text{with } G_f \in \mathbb{Z}[x],\ \phi(G_f) = f,$$

where the product on the right hand side is taken as before, and the ideals are prime. Write $\mathcal{P}_{f,n} = (G_f(\zeta_{2^n-1}), 2)$. It follows that if $f \mid F$ over $\mathbb{F}_2$ with $\deg(f) = n$, then we have

$$\prod_{j=1}^{2^n-1} F(\zeta_{2^n-1}^j) \equiv N_{\mathbb{Q}(\zeta_{2^n-1})/\mathbb{Q}}(F(\zeta_{2^n-1})) \equiv 0 \pmod{N_{\mathbb{Q}(\zeta_{2^n-1})/\mathbb{Q}}(\mathcal{P}_{f,n})},$$

whence the congruence also holds modulo 2. This shows, by Lemma 3.1, that ε^{2^n-1} is even, and the statement follows. □

Proof of Theorem 2.7. The statement is an immediate consequence of Lemma 3.2. □

To prove Theorem 2.8, we need the following

Lemma 3.3. *Let K be a real quadratic, a complex cubic or a totally complex quartic field; in the latter case assume that K does not contain roots of unity different from ± 1. Let ε be a fundamental unit of K. Suppose that ε is even. Then if $\varepsilon_1 + \cdots + \varepsilon_k = 0$ holds for some units $\varepsilon_1, \dots, \varepsilon_k$ of K then k is even.*

Proof. Suppose to the contrary that with some odd k, we have an equality of the form $\varepsilon_1 + \cdots + \varepsilon_k = 0$. Let $f(x)$ be the minimal monic polynomial of ε over $\mathbb{Z}$. By multiplying the equation by an appropriate power of ε (in view of that the unit rank of K is one and K contains no roots of unity different from ± 1) we get an equation of the form $h(\varepsilon) = 0$, where $h \in \mathbb{Z}[x]$. Dividing h by an appropriate integer if necessary, we may further assume that it is primitive. Then, by the Gauss lemma we easily deduce that $h(x) = f(x)g(x)$ holds, where $g(x) \in \mathbb{Z}[x]$. However, since $L(h)$ is odd and $L(f)$ is even, it yields a contradiction. Hence the lemma follows. □

Proof of Theorem 2.8. The statement is an immediate consequence of Lemma 3.3. □

Since we find it of independent interest, now we show that a statement similar to Lemma 3.3 is true for totally real cubic fields (having already unit rank 2).

Proposition 2. *Let K be a totally real cubic field. Suppose that K has a system of fundamental units which are even. Then all units of K are even.*

Proof. Write ε, η for a system of fundamental units of K. Since ε is even, either $\varepsilon^3 + \varepsilon^2 + \varepsilon + 1 \equiv 0 \pmod 2$, or $\varepsilon^3 + 1 \equiv 0 \pmod 2$, and the same is valid with η in place of ε. If $\varepsilon^3 + 1 \equiv \eta^3 + 1 \pmod 2$ then all units of K are even. Indeed, if $\nu = \pm\varepsilon^m \eta^n$ $(m, n \in \mathbb{Z})$ would be an odd unit of K with minimal monic polynomial $x^3 + ax^2 + bx \pm 1$, then we would have

$$a + b \equiv 1 \pmod 2 \quad \text{and} \quad a(\varepsilon^m\eta^n)^2 + b(\varepsilon^m\eta^n) \equiv 0 \pmod 2,$$

which is impossible.

Thus without loss of generality we may assume that

$$\varepsilon^3 + \varepsilon^2 + \varepsilon + 1 \equiv 0 \pmod 2.$$

We have five cases, according to the splitting of the prime 2 (the principal ideal (2)) in K:

- $(2) = \mathcal{P}_1$, $\mathcal{P}_1$ is a prime ideal,
- $(2) = \mathcal{P}_1\mathcal{P}_2$, $\mathcal{P}_i$ is a prime ideal of degree i $(i = 1, 2)$,
- $(2) = \mathcal{P}_1\mathcal{P}_2\mathcal{P}_3$, the $\mathcal{P}_i$ are distinct prime ideals $(i = 1, 2, 3)$,
- $(2) = \mathcal{P}_1^2\mathcal{P}_2$, the $\mathcal{P}_i$ are distinct prime ideals $(i = 1, 2)$,
- $(2) = \mathcal{P}_1^3$, $\mathcal{P}_1$ is a prime ideal.

Observe that in all cases, by

$$\varepsilon^3 + \varepsilon^2 + \varepsilon + 1 \equiv (\varepsilon + 1)^3 \equiv 0 \pmod 2,$$

we obtain $\varepsilon \equiv 1 \pmod{\mathcal{P}_1}$. If we had also $\eta \equiv 1 \pmod{\mathcal{P}_1}$, then $\pm\varepsilon^m\eta^n \equiv 1 \pmod{\mathcal{P}_1}$ $(m, n \in \mathbb{Z})$ would follow, showing that

$$a + b \equiv 1 \pmod 2 \quad \text{and} \quad a(\varepsilon^m\eta^n)^2 + b(\varepsilon^m\eta^n) \equiv 0 \pmod{\mathcal{P}_1} \tag{3}$$

is impossible. It remains to check the case

$$\varepsilon \equiv 1 \pmod{\mathcal{P}_1} \quad \text{and} \quad \eta^3 \equiv 1 \pmod 2.$$

However, as one can easily check, (3) is also impossible in this case. Hence our statement follows. □

Proof of Theorem 2.9. If $n \neq 2^\alpha$, one can take $\varepsilon = \zeta_n$. Indeed, the minimal monic polynomial of ζ_n is $\Phi_n(x)$ and we have

$$\Phi_n(1) \equiv 1 \pmod 2.$$

If $n = 2^\alpha$ $(\alpha \geq 3)$, one can take

$$\varepsilon = 1 + \zeta_8 + \zeta_8^2 = \frac{\zeta_8^3 - 1}{\zeta_8 - 1}.$$

Indeed, the minimal monic polynomial of ε is $x^4 + 14x^3 + 5x^2 + 2x + 1$, and the theorem follows. □

Now we turn to the proofs of our theorems concerning $\ell(K), \ell_o(K), \ell_e(K)$. In fact, the proof of Theorem 2.1 is based upon a simple observation.

Proof of Theorem 2.1. Let ε be a unit of K, different from 1 and -1. Write $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$ for the minimal monic polynomial of ε. Then the equality $f(\varepsilon) = 0$ can be considered as an equation of the form (1), with $k := 1 + |a_{n-1}| + \cdots + |a_1| + |a_0|$ terms on the left hand side. Since $f(x)$ is the minimal monic polynomial of ε, it is obvious that this equation has no vanishing subsums. This proves that $\ell(K) \leq k$. Since $n \leq d$ and $k \leq (d+1)H(f)$, where $H(f)$ denotes the height (i.e. the maximum absolute value of the coefficients) of f, it suffices to to give an upper bound for the height of the minimal monic polynomial of an appropriate unit ε of K.

It follows from Proposition 4.3.9 in Evertse and Győry [6], an improvement of a classical result of Siegel [38], that there is a unit ε in K such that $h(\varepsilon) \leq cR_K$ with the constant specified in Theorem 2.1. Here $h(\varepsilon)$ denotes the absolute logarithmic height of ε. But by (1.9.3) of Evertse and Győry [6], the height of the minimal monic polynomial of ε is at most $2\exp\{h(\varepsilon)\}$, hence the claimed upper bound for $\ell(K)$ follows. □

To prove Theorem 2.2, we need two lemmas. The first one is due to Louboutin [23].

Lemma 3.4. *Let $\varepsilon > 1$ be a real quadratic unit. Then ε is the fundamental unit of the quadratic order $\mathbb{Z}[\varepsilon]$, with the sole exception of $\varepsilon = (3+\sqrt{5})/2$.*

Proof. The statement is an immediate consequence of Theorem 1 of [23]. □

The next lemma shows that in case of some quadratic and cubic polynomials $f(x) \in \mathbb{Z}[x]$ of special shape, $L(fg) \geq L(f)$ holds for all $g(x) \in \mathbb{Z}[x]$ which is not identically zero.

Lemma 3.5. *Let a be a positive integer, and $f(x)$ be one of the polynomials x^2-ax-1, x^3+ax+1, x^3+x^2+ax+1; in the latter case assume further that $a \geq 3$. Then for any $g(x) \in \mathbb{Z}[x]$ not identically zero, we have $L(fg) \geq L(f)$.*

Proof. Let a be a positive integer, and $g(x) = b_nx^n + \cdots + b_1x + b_0$ with $n \geq 0$ and $b_n, \ldots, b_0 \in \mathbb{Z}$, $b_n \neq 0$. Clearly, we may assume that $n \geq 1$, $b_n > 0$ and $b_0 \neq 0$, whence $L(g) \geq 2$. Further, we put $h(x) = f(x)g(x)$.

First let $f(x) = x^2 - ax - 1$. Then we have

$$h(x) = c_{n+2}x^{n+2} + \cdots + c_1x + c_0,$$

with

$$c_{n+2} = b_n,\ c_{n+1} = b_{n-1} - ab_n,\ c_1 = -ab_0 - b_1,\ c_0 = -b_0$$

and

$$c_i = b_{i-2} - ab_{i-1} - b_i\ (i = 2, \ldots, n).$$

Hence we get

$$L(h) = \sum_{i=0}^{n+2} |c_i| \geq |b_n| + |b_0| + aL(g) - \sum_{i=0}^{n-1} |b_i| - \sum_{i=1}^{n} |b_i| \geq (a-2)L(g) + 4.$$

As $L(g) \geq 2$ and $L(f) = a + 2$, this implies our claim for $a \geq 2$. If $a = 1$ then $L(f) = 3$, and we are done unless $L(h) = 2$, that is, $h(x) = x^{n+2} \pm 1$. However, then $f(x) \nmid h(x)$, which is a contradiction, proving our claim in this case.

Assume now that $f(x) = x^3 + ax + 1$. Then we have

$$h(x) = c_{n+3}x^{n+3} + \cdots + c_1x + c_0,$$

with

$$c_{n+3} = b_n, \quad c_{n+2} = b_{n-1}, \quad c_{n+1} = b_{n-2} + ab_n,$$
$$c_2 = ab_1 + b_2, \quad c_1 = ab_0 + b_1, \quad c_0 = b_0$$

and

$$c_i = b_{i-3} + ab_{i-1} + b_i\ (i = 3, \ldots, n).$$

Similarly to the case $f(x) = x^2 - ax - 1$, we get

$$L(h) \geq |b_n| + |b_{n-1}| + |b_0| + aL(g) - \sum_{i=0}^{n-2} |b_i| - \sum_{i=1}^{n} |b_i| \geq (a-2)L(g) + 4.$$

This gives that the statement is valid for $a \geq 2$. For $a = 1$, $L(h) < L(f)$ would imply $x^3 + x + 1 \mid x^{n+3} \pm 1$, which does not hold. Hence the lemma follows also in this case.

Finally, let $f(x) = x^3 + x^2 + ax + 1$. Then we can write

$$h(x) = c_{n+3}x^{n+3} + \cdots + c_1x + c_0,$$

with

$$c_{n+3} = b_n, \quad c_{n+2} = b_{n-1} + b_n, \quad c_{n+1} = b_{n-2} + b_{n-1} + ab_n,$$
$$c_2 = b_0 + ab_1 + b_2, \quad c_1 = ab_0 + b_1, \quad c_0 = b_0$$

and

$$c_i = b_{i-3} + b_{i-2} + ab_{i-1} + b_i \ (i = 3, \dots, n).$$

Similarly to the case $f(x) = x^2 - ax - 1$, we get

$$L(h) \geq |b_n| + |b_{n-1} + b_n| + |b_0| + aL(g) - \sum_{i=0}^{n-2} |b_i| - \sum_{i=0}^{n-1} |b_i| - \sum_{i=1}^{n} |b_i| \geq$$
$$\geq (a-3)L(g) + 6.$$

As $a \geq 3$, $L(f) = a + 3$ and $L(g) \geq 2$, this gives $L(h) \geq L(f)$, and the lemma follows. □

Proof of Theorem 2.2. Let $k \geq 3$. Let ε be a root of the polynomial $f(x) = x^2 - (k-2)x - 1$, and set $\mathcal{O} = \mathbb{Z}[\varepsilon]$. By Lemma 3.4 we know that ε is a fundamental unit of $\mathcal{O}$. Then, in the same way as in the proof of Lemma 3.3, we see that all vanishing sums of units in $K = \mathbb{Q}(\varepsilon)$ are obtained from the integer polynomial multiples $h(x)$ of $f(x)$. Now by Lemma 3.5 we get that for all such $h(x)$, $L(h) \geq L(f) = k$ holds. This implies the statement. □

To prove Theorem 2.3, we need a result concerning cubic factors of certain special trinomials. For theorems on the reducibility of general trinomials, see e.g. [29] and the corresponding chapter of [33].

Lemma 3.6. *Let m, A, E be integers with $m \geq 2$ and $E \in \{-1, 1\}$. Suppose that $x^{3m} + Ax^m + E$ has an irreducible cubic factor in $\mathbb{Z}[x]$. Then one of the following cases occurs:*

(i) *$m = 11$, $A = 67$ and $E = 1$, when $x^3 + x + 1$ is the only cubic factor,*
(ii) *$m = 4$, $A = 1040$ and $E = -1$,*
(iii) *$m = 2$, $E = -1$ and A is of the form $A = 4t^4 - 4t$ $(t \in \mathbb{Z} \setminus \{0, 1\})$.*

Proof. The statement is an immediate consequence of the Theorem in Tverberg [40]. Note that this result of Tverberg is an extension of the Theorem in Bremner [2], where only the case $E = 1$ was considered. It is easy to check (e.g. by Magma [1]) that the only cubic factor of the polynomial $x^{33} + 67x^{11} + 1$ is $x^3 + x + 1$. □

Now we can give the

Proof of Theorem 2.3. For given k not of the form $4t^4 - 4t + 2$, take $A = k - 2$ and consider the polynomial $f(x) = x^3 + Ax + 1$. As one can easily check, $f(x)$ (in view of $A \geq 1$) is irreducible over $\mathbb{Q}$, and has one real and two complex roots. Let ε be a root of $f(x)$, and put $K = \mathbb{Q}(\varepsilon)$. Write $\varepsilon = \pm\eta^m$ with some $m \geq 2$, where η is an appropriately chosen fundamental unit of K. Let $h(x)$ be the minimal monic polynomial of η. It is easy to see that $h(x)$ divides one of the polynomials $x^{3m} + Ax^m \pm 1$ in $\mathbb{Z}[x]$. Noting that as

$1040 = 4(-4)^4 - 4(-4)$ we have $A \neq 1040$, by Lemma 3.6 we obtain that if $A \neq 67$ then $m = 1$ holds.

We conclude that if A is not of the form $4t^4 - 4t$ ($t \in \mathbb{Z} \setminus \{0, 1\}$), then ε is a fundamental unit of K, unless $A = 67$. So in the cases where $A \neq 67$, just as before, we get that any vanishing sum of units in K comes from a multiple of $f(x)$. However, by Lemma 3.5 we obtain that the number of the terms in any such sum is at least $L(f) = A+2 = k$, and the theorem follows in these cases.

Hence we are left with $k-2 = A = 67$. In this case consider the polynomial $f(x) = x^3 + x^2 + 66x + 1$. A simple check by Magma [1] shows that this polynomial is irreducible, has one real and two complex roots. Further, taking a root ε of $f(x)$, ε is a fundamental unit of $K = \mathbb{Q}(\varepsilon)$. By Lemma 3.5 we get that for any $g \in \mathbb{Z}[x]$ which is not identically zero, we have $L(fg) \geq L(f) = 69$. This in the same way as before shows that $\ell(K) = 69$, and the theorem follows. □

Now we give the proof of Proposition 1.

Proof of Proposition 1. A simple calculation with Magma [1] shows that α_t is a fundamental unit of K_t for the values of t under consideration. Hence following the usual argument, the statement follows by Lemma 3.5. □

To prove Theorem 2.4 we need the following lemma, essentially due to Mignotte [25]. It provides a weaker, but much more general lower bound for $L(fg)$ than Lemma 3.5.

Lemma 3.7. *Let $f \in \mathbb{Z}[x]$ of degree $n \geq 0$. Then for any $g \in \mathbb{Z}[x]$ which is not identically zero, we have $L(fg) \geq 2^{-n} L(f)$.*

Proof. Write

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \quad \text{and} \quad f(x)g(x) = b_s x^s + \cdots + b_1 x + b_0.$$

Theorem 2 of [25] gives

$$|a_i| \leq \binom{n}{i} \sqrt{\sum_{j=0}^{s} b_j^2} \quad (i = 0, \ldots, n).$$

Thus

$$L(f) = |a_n| + \cdots + |a_0| \leq 2^n \sqrt{\sum_{j=0}^{s} b_j^2} \leq 2^n L(fg),$$

and the statement follows. □

The last assertion we need in the proof of Theorem 2.4 concerns lengths of polynomials $g(x)$ such that $L(fg)$ is "small" for a given $f(x)$.

Lemma 3.8. *Let $f(x) \in \mathbb{Z}[x]$ having no cyclotomic factors, and let $N \geq 1$. Then there exists an effectively computable constant $C(L(f), N)$ depending only on $L(f)$ and N such that for any $g(x) \in \mathbb{Z}[x]$ with $L(fg) \leq N$ we* *have* $L(g) \leq C(L(f), N)$*. Further, at least one such* g *satisfies* $\deg(g) \leq C(L(f), N)(\deg(f) + 1)$*.*

Proof. The first part of the statement is an immediate consequence of Theorem 1 in [8]. Note that in [8] in place of the length the authors work with another norm, however, it is easy to reformulate their result for $L(g)$. Further, $C(L(f), N)$ is not claimed to be effective in [8], but following the argument there, one can easily see that this constant is effectively computable, indeed. (See also Theorem 3 in [8], where in a special case a $C(L(f), N)$ is explicitly given.)

To prove the second statement concerning the degree of g, observe the following. Writing $n = \deg(f)$, $m = \deg(g)$ and $g(x) = \sum\limits_{i=0}^{m} b_i x^i$, if $n+1$ consecutive coefficients of g, say $b_i, \dots, b_{i+n}$ are all zero, then clearly $L(fg) = L(fg^*)$ with $g^*(x) = \sum\limits_{j=0}^{n+i-1} b_j x^j + \sum\limits_{j=n+i}^{m-1} b_{j+1} x^j$. This shows that if $L(fg) \leq N$ with $L(g) \leq C(L(f), N)$, then starting from g, we can construct a $g_0(x) \in \mathbb{Z}[x]$ such that $L(fg_0) \leq N$, $L(g_0) \leq C(L(f), N)$ and there are at most n consecutive zeros among the coefficients of g_0. Hence the statement follows. □

Proof of Theorem 2.4. Let $k \geq 3$ be fixed, and suppose that K is an algebraic number field as in the statement, with $\ell(K) \leq k$. Let ε be a fundamental unit of K, and write $f(x) = x^n + a_{n-1}x^{n-1} \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ for its minimal monic polynomial. Note that here $n \in \{2, 3, 4\}$ and $a_0 \in \{-1, 1\}$. Further, since by our assumption K has no real quadratic subfields and $\mathbb{Q}(\varepsilon)$ cannot be an imaginary quadratic field, we also have $K = \mathbb{Q}(\varepsilon)$.

Let $\varepsilon_1, \dots, \varepsilon_k$ be units in K with

$$\varepsilon_1 + \cdots + \varepsilon_k = 0. \tag{4}$$

Assume first that K does not contain roots of unity different from ±1. By the usual argument, since by our assumption K does not contain any roots of unity different from ±1, this gives $h(\varepsilon) = 0$ with $h \in \mathbb{Z}[x]$ such that $L(h) = k$. Hence for some $g \in \mathbb{Z}[x]$ not identically zero, we have $L(fg) = k$. This by Lemma 3.7 yields $L(f) \leq 16k$. So as $K = \mathbb{Q}(\varepsilon)$, there are only finitely many such K. Checking all the possibilities with $L(f) \leq 16k$, in view of Lemma 3.8 these number fields can be effectively determined.

Suppose next that K contains some root of unity different from ±1. Then K contains a primitive m-th root of unity η with some $m \geq 3$. As we have $\varphi(m) \leq 4$, we get that

$$m \in \{3, 4, 5, 6, 8, 10, 12\}.$$

If m is one of $3, 6, 12$, then $\zeta_3 \in K$, which is excluded. If m is 5 or 10, then K is defined by the polynomial $x^4 + x^3 + x^2 + x + 1$. However, then (as one can readily check e.g. by Magma [1]) K has $\mathbb{Q}(\sqrt{5})$ as a subfield, which is excluded again. If $m = 8$, then K is defined by $x^4 + 1$, and using again

Magma, we see that $\mathbb{Q}(\sqrt{2})$ is a subfield of K, which is also excluded. So we are left with the only possibility $m = 4$, and the roots of unity of K are precisely $\pm 1, \pm i$.

In this case, one can do the following.[1] First note that every polynomial $R(x) \in \mathbb{Q}(i)[x]$ can be written as $R(x) = P(x) + iQ(x)$ with $P, Q \in \mathbb{Q}[x]$. With this notation, put $\bar{R}(x) = P(x) - iQ(x)$ and $L^*(R) = L(P) + L(Q)$.

Let ε be a fundamental unit of K. Then $K = \mathbb{Q}(\varepsilon)$, and K is a quadratic extension of $\mathbb{Q}(i)$. As $\varepsilon \notin \mathbb{Q}(i)$, ε is a quadratic element over $\mathbb{Q}(i)$. Let $f^*(x)$ be the minimal polynomial of ε over $\mathbb{Q}(i)$. Then the minimal polynomial $f(x)$ of ε over $\mathbb{Q}$ is $f(x) = f^*(x)\bar{f}^*(x)$. From (4) we infer that

$$P(\varepsilon) + iQ(\varepsilon) = 0 \tag{5}$$

with some $P, Q \in \mathbb{Z}[x]$ and $L^*(P + iQ) = k$. Note that thus we have $L(P) + L(Q) = k$. Further, equation (5) implies that

$$P(x) + iQ(x) = f^*(x)g^*(x) \tag{6}$$

holds with some $g^*(x) \in \mathbb{Z}[i][x]$. Letting $g(x) = g^*(x)\bar{g}^*(x)$ (which is in $\mathbb{Z}[x]$) this implies

$$P(x)^2 + Q(x)^2 = f(x)g(x).$$

As by the well-known and trivial inequalities $L(P^2) \leq L(P)^2$ and $L(Q^2) \leq L(Q)^2$ we have

$$L(P^2 + Q^2) \leq k^2,$$

using Lemma 3.7 we get that $L(f) \leq 16k^2$.

Thus Lemma 3.8 implies that $L(g) < C_1(k)$, where $C_1(k), C_2(k), C_3(k)$ denote explicitly computable constants depending only on k.

The following observation will be of great help: for any $u, v, w \in \mathbb{Z}[i][x]$ and $A > 0$ we have

$$L^*(w(x)\cdot(u(x)+x^{A+\deg w+\deg u}v(x))) = L^*(w(x)\cdot(u(x)+x^{1+\deg w+\deg u}v(x))).$$

Thus for any $g^*(x)$ with $L^*(f^*g^*) \leq k$ there exists a $g_0^*(x) \in \mathbb{Z}[i][x]$ for which $L^*(f^*g_0^*) \leq k$, with $L^*(g_0^*) = L^*(g^*)$ and $\deg g_0^* < C_2(k)$. This follows by noting that the number of non-zero coefficients of g^* is bounded by $L^*(g^*)$, and further, by the above observation, (inductively) all the 'large gaps' among consecutive non-zero coefficients of $g^*(x)$ (in view of $\deg f^* = 2$) can be 'shortened' below an effectively computable bound. So we can restrict our attention to polynomials $g^*(x)$ with degree bounded in terms of k; in what follows, we assume that $\deg g^* < C_2(k)$.

The upper bounds established for $L(f)$ and $L(g)$ yield

$$\max\{L^*(f^*), L^*(g^*)\} < C_3(k).$$

This follows from the fact that for any $h(x) \in \mathbb{Z}[i][x]$, $L^*(h)$ can be explicitly bounded from above in terms of $L(h\bar{h})$ and $\deg h$ (see Theorem 2 of Mignotte [25]).

[1] Note that this paragraph is different (much shorter) in the published version of the paper. We find that it is worth to give more explanation at this point.

As clearly all such $f^*(x)$ and $g^*(x)$ can be explicitly listed, we can effectively check the finitely many candidate number fields $\mathbb{Q}(\varepsilon)$ defined by $f(x)$, whether (5) may hold for them (where $P(x)+iQ(x)$ is defined by (6)) or not. □

Proof of Theorem 2.5. For an integer A set

$$f_A(x) = x^d + 2A^2x + 2.$$

Then by Eisenstein's theorem $f_A(x)$ is irreducible over $\mathbb{Q}$. Let α be a zero of $f_A(x)$, and put $K_A = \mathbb{Q}(\alpha)$. Observe that $N_{K_A/\mathbb{Q}}(\alpha) = 2(-1)^d$. Hence every algebraic integer in K_A is congruent to one of $0,1$ modulo α. Consequently, any unit of K_A is congruent to 1 modulo α. This immediately shows that a sum of odd number of units cannot be zero; in other words, $\ell_o(K_A) = \infty$.

It remains to show that there are infinitely many number fields K_A of the above form. If there existed only finitely many number fields of the form K_A, then letting K be a number field containing all of them, we would obtain that, for every integer A, the polynomial $f_A(x)$ would have a zero in O_K, the ring of integers of K. However, it is easy to see that the algebraic curve

$$X^d + 2XY^2 + 2 = 0$$

is non-rational. Hence, by Siegel's theorem [37], the set of points $(x,y) \in O_K \times \mathbb{Z}$ on this curve is finite which yields a contradiction. □

Proof of Theorem 2.6. Let $a_1 = 0$, $a_2 = 2$ and $a_3, \dots, a_{d-1}$ be fixed integers with $2 < a_3 < \dots < a_{d-1}$. (When $d = 3$, we have only a_1 and a_2.) For any integer $N > a_{d-1}$, set

$$f_N(x) = x(x-2)(x-a_3)\dots(x-a_{d-1})(x-N) - 1.$$

Then $f_N(x)$ is irreducible (see Westlund [41] or Flügel [9], or for more general results e.g. Győry and Rimán [18] or Győry, Hajdu and Tijdeman [15] and the references there). Let ξ_N be a zero of $f_N(x)$, and $K_N = \mathbb{Q}(\xi_N)$. Observe that $-\xi_N$ and $\xi_N - 2$ are both (non-rational) units of K. Hence $(-\xi_N, \xi_N - 2, 1, 1)$ is a solution of the unit equation

$$\varepsilon_1 + \varepsilon_2 + \varepsilon_3 + \varepsilon_4 = 0 \tag{7}$$

in units $\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4$ of K_N such that $\varepsilon_3 = \varepsilon_4 = 1$, $\varepsilon_1, \varepsilon_2$ are not rational, and the left hand side of (7) has no vanishing subsum. This proves that $\ell_e(K) = 4$.

It remains to show that there are infinitely many distinct number fields K_N of the above type. Suppose, on the contrary, that there exist only finitely many distinct number fields K_N with the above properties. Then there are infinitely many number fields $K_{N'} = \mathbb{Q}(\xi_{N'})$ which coincide with $K_N = \mathbb{Q}(\xi_N)$ for a fixed ξ_N. Here $\xi_{N'}$ denotes a zero of $f_{N'}(x)$.

The tuple $(-\xi_{N'}, \xi_{N'} - 2, 1, 1)$ is also a solution of (7) for every N' under consideration. But the tuples $(-\xi_N, \xi_N - 2, 1, 1)$ and $(-\xi_{N'}, \xi_{N'} - 2, 1, 1)$

coincide only if $\xi_{N'} = \xi_N$, when $N' = N$. Consequently, equation (7) has infinitely many distinct solutions $(-\xi_{N'}, \xi_{N'} - 2, 1, 1)$ in K_N, which contradicts the finiteness results of Evertse [5] and van der Poorten and Schlickewei [27] on unit equations. □

Remark. In the above proofs of Theorem 2.5 and 2.6 we could also use Hilbert's Irreducibility Theorem (see e.g. [30] Theorem 46) to prove the irreducibility of $f_A(x)$ and $f_N(x)$. Further, the argument used in the second part of the proof of Theorem 2.5 could also be applied at the end of the proof of Theorem 2.6 as well.

4. An application to arithmetic graphs - representing cycles

Let K be an algebraic number field, and let $A = \{\alpha_1, \dots, \alpha_m\}$ be a finite ordered subset of O_K, the ring of integers of K. Denote by $\mathcal{G}(A)$ the graph with vertex set A whose edges are the pairs $[\alpha_i, \alpha_j]$ with

$$\alpha_i - \alpha_j \in O_K^*,$$

where O_K^* denotes the unit group of O_K. The ordered subsets of the form $A = \{\alpha_1, \dots, \alpha_m\}$ and $A' = \{\alpha'_1, \dots, \alpha'_m\}$ of O_K are called equivalent if $\alpha'_i = \varepsilon\alpha_i + \beta$ $(i = 1, \dots, m)$ with some $\varepsilon \in O_K^*$ and $\beta \in O_K$. Clearly, in this case the graphs $\mathcal{G}(A)$ and $\mathcal{G}(A')$ are isomorphic. The concept of $\mathcal{G}(A)$ was introduced in Győry [10, 11]. For given $m \geq 3$, there are infinitely many equivalence classes of ordered subsets A with $|A| = m$. Apart from finitely many equivalence classes, the structure of these arithmetic graphs have been described by Győry; see, say [14]. These graphs have many important applications to various and wide classes of Diophantine problems; see e.g. Győry [14], Evertse and Győry [6] and the references given there.

Győry, Hajdu and Tijdeman [16, 17] performed a systematic study of of the representability of arithmetic graphs over $\mathbb{Q}$ in the S-unit case, and over algebraic number fields, respectively. Among other things, they have generalized some results of Ruzsa [28].

Ruzsa [28] described the cycles[2] which are representable by arithmetic graphs over $\mathbb{Q}$, using S-units. In this case the set of vertices A is a subset of $\mathbb{Z}$, and $[a_i, a_j]$ with $a_i, a_j \in A$ is an edge if and only if all the prime divisors of $a_i - a_j$ belong to a fixed finite set of primes $S = \{p_1, \dots, p_s\}$. Ruzsa [28] gave a complete characterization of cycles in this case, by proving that if $2 \in S$ then $\mathcal{G}(A)$ contains cycles of every length ≥ 3, while if $2 \nmid S$ then $\mathcal{G}(A)$ contains cycles of every *odd* length ≥ 3, but none of even length. (See also [3] for certain related problems and results.)

Now connecting to the above mentioned result of Ruzsa [28], we completely characterize the possible lengths of cycles among the graphs $\mathcal{G}(A)$ over number fields K, where A is a finite subset of the ring of integers of K.

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

Theorem 4.1. *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 of every even length ≥ 4,*

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

Proof. If $\ell_o(K) = \infty$, then there is nothing to prove about odd cycles, so throughout the proof we shall assume that $\ell_o(K) < \infty$. (It will be clear from the proof that this assumption has no effect at all on the statement concerning even cycles.) Let $\varepsilon \in O_K^*$ such that neither of $1 \pm \varepsilon$ is a unit. The existence of such units follows from deep finiteness results of Siegel [36] and Lang [21] on unit equations. However, it can be seen also in many elementary ways. For example, take a prime ideal $\mathcal{P}$ in K lying above 2, and let η be any unit of infinite order. Then writing n for the order of η modulo $\mathcal{P}$, we have $1-\eta^n \in \mathcal{P}$ and by $1+\eta^n = 2-(1-\eta^n)$, also $1-\eta^n \in \mathcal{P}$. Hence taking $\varepsilon = \eta^n$, $1 \pm \varepsilon$ are not units.

Then as one can readily check, $A = \{0, 1, 1+\varepsilon, \varepsilon\}$ is a cycle of length 4. Observe that the existence of an odd cycle of length $< \ell_o(K)$ would contradict the minimality of $\ell_o(K)$. Let now $\varepsilon_1, \dots, \varepsilon_k \in O_K^*$ with $k = \ell_o(K)$ such that $\varepsilon_1 + \dots + \varepsilon_k = 0$, and let

$$\alpha_i = \varepsilon_1 + \dots + \varepsilon_i \quad (i = 1, \dots, k).$$

We claim that $\mathcal{G}(A)$ with $A = \{\alpha_1, \dots, \alpha_k\}$ is a cycle. For this, first observe that $\alpha_i \neq \alpha_j$ for $1 \leq i < j \leq k$. Indeed, otherwise we would have

$$\varepsilon_{i+1} + \dots + \varepsilon_j = 0,$$

and consequently

$$\varepsilon_1 + \dots + \varepsilon_i + \varepsilon_{j+1} + \dots + \varepsilon_k = 0.$$

However, as one of $j-i$, $i+k-j$ is odd, this would violate the minimality of $\ell_o(K)$. Then, also observe that $[\alpha_i, \alpha_j]$ with $1 \leq i < j \leq k$ is an edge in $\mathcal{G}(A)$ if and only if either $j-i=1$, or $(i,j) = (1,k)$. Indeed, assume to the contrary that $[\alpha_i, \alpha_j]$ is an edge with $1 \leq i$, $i+2 \leq j$ and $(i,j) \neq (1,k)$. Hence $\alpha_j - \alpha_i = \varepsilon_0 \in O_K^*$. Then $\alpha_j - \alpha_i - (\alpha_j - \alpha_i) = 0$ implies

$$\varepsilon_{i+1} + \dots + \varepsilon_j - \varepsilon_0 = 0,$$

whence also

$$\varepsilon_1 + \dots + \varepsilon_i + \varepsilon_{j+1} + \dots + \varepsilon_k + \varepsilon_0 = 0.$$

Similarly as above, we see that one of $j-i+1$ and $i+k-j+1$ is odd. Further, $2 \leq j-i \leq k-2$ shows that $\max\{j-i+1, i+k-j+1\} < k$. This violates the minimality of $\ell_o(K)$ once again. That is, $\mathcal{G}(A)$ is a cycle (of length $\ell_o(K)$), indeed.

Now we prove that if $\mathcal{G}(A)$ is a cycle of length $t \geq 3$, then there exists a cycle $\mathcal{G}(A')$ of length $t+2$. This clearly finishes the proof. To prove this assertion, we adopt the construction of Ruzsa from the proof of Theorem 3.1 in [28].

Suppose that

$$A = \{\alpha_1, \alpha_2, \ldots, \alpha_{t-1}, \alpha_t\}$$

is a subset of O_K such that $\mathcal{G}(A)$ is a cycle (of length t). Let $\varepsilon \in O_K^*$ be such that $\alpha_i + \varepsilon \neq \alpha_j$ and $\alpha_i + \varepsilon - \alpha_j \notin O_K^*$ $(i = 1, \ldots, t-1,\ j = 1, t-1, t$ with $i \neq j)$. By the already mentioned finiteness results of Siegel [36] and Lang [21] on unit equations, such an ε exists. (Note that this assertion could also be proved by simpler tools.) Put

$$A' = \{\alpha_1, \alpha_1 + \varepsilon, \alpha_2 + \varepsilon, \ldots, \alpha_{t-1} + \varepsilon, \alpha_{t-1}, \alpha_t\}.$$

Now by the choice of ε, using that $\mathcal{G}(A)$ is a cycle of length t, we easily see that $\mathcal{G}(A')$ is a cycle of length $t+2$. Hence the proof is complete. □

Remark. The cases where $K = \mathbb{Q}$ or K is an imaginary quadratic field, can be handled easily. The only cases that need some simple considerations are $K = \mathbb{Q}(i), \mathbb{Q}(\zeta_3)$.

As an immediate consequence of Theorems 2.3 and 4.1 we obtain

Corollary 4.1. *For every odd $t \geq 3$ there exists a number field K with the following properties: among the graphs $\mathcal{G}(A)$*

i) *there are cycles of every even length ≥ 4,*
ii) *there are cycles of every odd length $\geq t$, but there are no cycles of odd length $< t$.*

5. Problems and open questions

In this concluding section we list some problems and open questions, and we also give a remark about a possible continuation of our research.

Problems and open questions.

i) Prove that for all k of the form $k = 4t^4 - 4t + 2$ $(t \in \mathbb{Z} \setminus \{0, 1\})$ there exists a number field K with $\ell(K) = k$. (That is, prove the Conjecture after Theorem 2.3).
ii) 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 infinitely many number fields such that $\deg(K) = d$, $\ell_e(K) = a$ and $\ell_o(K) = b$?
iii) Can we say something about the distribution of $\ell(K) \pmod{n}$, where $n \geq 3$ is an integer?
iv) Are there infinitely many totally real quadratic, cubic (both totally real and complex) and totally complex quartic fields K, in the latter case assuming that K contains no nontrivial roots of unity, with a system of fundamental units, consisting of even units? (This question is related to Theorem 2.8 and Proposition 2.)

Remark. In a forthcoming paper, we plan to describe the properties of the set $\mathcal{L}(K)$ of those integers $k \geq 3$ for which the unit equation (2) is solvable in units $\varepsilon_1, \ldots, \varepsilon_k$ of K such that the left hand side of the above equation has no proper vanishing subsum. If $\ell(K) < \infty$ then $\ell(K)$ is the minimal element of $\mathcal{L}(K)$. It is clear that if K is different from $\mathbb{Q}$ and the imaginary quadratic fields, then the set $\mathcal{L}(K)$ contains arbitrarily large values k. Indeed, take an arbitrary unit ε in K, with minimal monic polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$. Observe that $f(\varepsilon) = 0$ can be considered as an equation of the form (2) with $k = k_\varepsilon = 1 + |a_{n-1}| + \cdots + |a_0|$ terms, clearly with no proper vanishing subsums. Since $k_\varepsilon < C$ can be valid only for finitely many ε for any constant C, but K contains infinitely many units, $|\mathcal{L}(K)| = \infty$ follows. We (at least some of us) intend to study $\mathcal{L}(K)$ further.

References

[1] W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997) 235–265.

[2] A. Bremner, *On trinomials of type $x^n + Ax^m + 1$*, Math. Scand. **49** (1981), 145–155.

[3] A. Ćustić, L. Hajdu, D. Kreso, R. Tijdeman, *On conjectures and problems of Ruzsa concerning difference graphs of S-units*, Acta Math. Hungar. **146** (2015), 391–404.

[4] J.-H. Evertse, *Upper bounds for the number of solutions of Diophantine equations*, PhD thesis, University of Leiden, Leiden.

[5] J.-H. Evertse, *On sums of S-units and linear recurrences*, Compos. Math. **53** (1984), 225–244.

[6] J.-H. Evertse, K. Győry, *Unit equations in Diophantine number theory*, Cambridge University Press, 2015.

[7] J.-H. Evertse, K. Győry, C. L. Stewart, R. Tijdeman, *S-unit equations and their applications*, In: A. Baker (ed.) New Advances in Transcendence Theory, New York: Cambridge University Press, 1988. pp. 110-174.

[8] M. Filaseta, I. Solan, *Norms of factors of polynomials*, Acta Arith. **82** (1997), 243–255.

[9] W. Flügel, *Solution to problem 226*, Archiv. der Math. und Physik **15** (1909), 271.

[10] K. Győry, *Sur l'irréducibilité d'une classe des polynômes, I*, Publ Math. Debrecen **18** (1971), 289–307.

[11] K. Győry, *Sur l'irréducibilité d'une classe des polynômes, II*, Publ Math. Debrecen **19** (1972), 293–326.

[12] K. Győry, *Résultats effectifs sur la représentation des entiers par des formes décomposables*, Queens Papers in Pure and Applied Math. (1980), No. 56.

[13] K. Győry, *Some recent applications of S-unit equations*, Astérisque **209** (1992), 17–38.

[14] K. Győry, *On certain arithmetic graphs and their applications to Diophantine problems*, Funct. Approx. **39** (2008), 289–314.

[15] K. Győry, L. Hajdu, R. Tijdeman, *Irreducibility criteria of Schur-type and Pólya-type*, Monatsh. Math., **163** (2011), 415–443.

[16] K. Győry, L. Hajdu, R. Tijdeman, *Representation of finite graphs as difference graphs of S-units, I*, J. Combinatorial Theory, Ser A, **127** (2014), 314–335.

[17] K. Győry, L. Hajdu, R. Tijdeman, *Representation of finite graphs as difference graphs of S-units, II*, Acta Math. Hung. **149** (2016), 423–447.

[18] K. Győry and J. Rimán, *On irreducibility criteria of Schur type (in Hungarian, English summary)*, Matematikai Lapok **24**, 1973 (1977), 225–253.

[19] K. Győry, K. Yu, *Bounds for the solutions of S-unit equations and decomposable form equations*, Acta Arith. **123**, (2006), 9–41.

[20] E. Landau, *Verallgemeinerung eines Pólyaschen Satzes auf algebraische Zahlkörper*, Nachr. Ges. Wiss. Göttingen 1918, 478–488.

[21] S. Lang, *Integral points on curves*, Inst. Nantes Études Sci. Publ. Math. **6** (1960), 27–43.

[22] S. Lang, *Diophantine geometry*, 1962, Wiley.

[23] S. R. Louboutin, *The fundamental unit of some quadratic, cubic or quartic orders*, J. Ramanujan Math. Soc. **23** (2008), 191–210.

[24] R. C. Mason, *Diophantine equations over function fields*, Cambridge University Press, 1984.

[25] M. Mignotte, *An inequality about factors of polynomials*, Math. Comp. **28** (1974), 1153–1157.

[26] T. Nagell, *Sur un type particulier d'unités algébriques*, Arkiv f. Matem. **8** (1970), 163–184.

[27] A. J. van der Poorten, H. P. Schlickewei, *The growth condition for recurrence sequences*, Macquarie University Math. Rep. 1982, 82-0041.

[28] I. Z. Ruzsa, *The difference graph of S-units*, Publ. Math. Debrecen **79** (2011), 675–685.

[29] A. Schinzel, *On reducible trinomials*, Dissertationes Mathematicae, 1993, pp. 83.

[30] A. Schinzel, *Polynomials with special regard to irreducibility*, Encyclopedia of Mathematics and its Applications, Cambridge University Press, 2000.

[31] A. Schinzel, *On the reduced length of a polynomial with real coefficients, I*, Funct. Approx. **35** (2006), 271–306.

[32] A. Schinzel, *On the reduced length of a polynomial with real coefficients, II*, Funct. Approx. **37** (2007), 445–459.

[33] A. Schinzel, *Selecta* (H. Iwaniec, W. Narkiewicz and J. Urbanowicz, eds.), EMS Publishing House, 2007.

[34] W. M. Schmidt, *Diophantine Approximations and Diophantine Equations*, Lecture Notes in Mathematics **1467** (1991), Springer-Verlag.

[35] T. Shorey, R. Tijdeman, *Exponential Diophantine equations*, Cambridge University Press, 1986, pp. 240.

[36] C. L. Siegel, *Approximation algebraischer Zahlen*, Math. Z. **10** (1921), 173–213.

[37] C. L. Siegel, *Über einige Anwendungen diophantischer Approximationen*, Abh. Preuss. Akad. Wissen. Phys.-Math. Klasse 1929, Nr. 1.

[38] C. L. Siegel, *Abschätung fon Einheiten*, Nachr. Göttingen 1969, 71–86.

[39] N. Smart, *The Algorithmic Resolution of Diophantine Equations*, 1998, Cambridge University Press.

[40] H. Tverberg, *On cubic factors of certain trinomials*, Math. Scand. **53** (1983), 178–184.

[41] J. Westlund, *On the irreducibility of certain polynomials*, Amer. Math. Monthly **16** (1909), 66–67.

Cs. Bertók
Faculty of Informatics
and the MTA-DE Research Group "Equations, Functions and Curves"
of the Hungarian Academy of Sciences and the University of Debrecen
University of Debrecen
H-4002 Debrecen, P.O. Box 400
Hungary
E-mail address: `bertok.csanad@inf.unideb.hu`

K. Győry, L. Hajdu
Institute of Mathematics
University of Debrecen
H-4002 Debrecen, P.O. Box 400
Hungary
E-mail address: `gyory@science.unideb.hu`
E-mail address: `hajdul@science.unideb.hu`

A. Schinzel
Institute of Mathematics
Polish Academy of Sciences
ul. Sniadeckich 8, 00-656, Warszawa
Poland
E-mail address: schinzel@impan.pl