ON THE REPRESENTATION OF INTEGERS
AS LINEAR COMBINATIONS OF CONSECUTIVE VALUES
OF A POLYNOMIAL

JACQUES BOULANGER AND JEAN-LUC CHABERT

ABSTRACT. Let K be a cyclotomic field with ring of integers $\mathcal{O}_K$ and let f be a polynomial whose values on $\mathbb{Z}$ belong to $\mathcal{O}_K$. If the ideal of $\mathcal{O}_K$ generated by the values of f on $\mathbb{Z}$ is $\mathcal{O}_K$ itself, then every algebraic integer N of K may be written in the following form:

$$N = \sum_{k=1}^{l} \varepsilon_k f(k)$$

for some integer l, where the ε_k's are roots of unity of K. Moreover, there are two effective constants A and B such that the least integer l (for a fixed N) is less than $A\,\widetilde{N} + B$, where

$$\widetilde{N} = \max_{\sigma \in Gal(K/\mathbb{Q})} |\sigma(N)|.$$

1. INTRODUCTION

The Waring/Hilbert theorem says that, for each natural integer d, there exists an integer $g(d)$ such that every natural integer N may be written as the sum of $g(d)$ dth powers [8, Theorem 11.11].

Waring's problem for polynomials states that, for each integer-valued polynomial f with positive leading coefficient, if the greatest common divisor of the values of f is 1, then there is an integer $g(f)$ such that every sufficiently large integer N can be written as the sum of at most $g(f)$ values of f [8, Theorem 11.9].

One may change the problem:
— on the one hand, by strengthening the conclusion: we only consider sums either of consecutive dth powers or of consecutive values of f (see [5, §6]),
— on the other hand, by forgetting the common bound $g(d)$ or $g(f)$ and by introducing coefficients different from 1.

For instance, if the coefficients are 0 and 1, then we consider 'lacunary sums' of consecutive dth powers or of consecutive values, that is, sums of distinct powers or sums of values on distinct elements. With respect to this case, we have

Proposition 1.1 ([6, Theorem 1]). *Let f be an integer-valued polynomial with positive leading coefficient such that the greatest common divisor of the values of f*

---

is 1. *Then, every sufficiently large integer* N *can be written in the following way*:

$$N = \sum_{j=1}^{l} \varepsilon_j f(j), \quad \text{where } l \in \mathbb{N}^* \text{ and } \varepsilon_j = 0, 1 \ (j = 1, \ldots, l).$$

See also [4] when f has integral coefficients.

If the coefficients are $+1$ or -1, that is, if we consider 'signed sums' either of consecutive dth powers or of consecutive values, we have

Proposition 1.2 ([2, Theorem 1]). *Let d be a natural integer. Every natural integer N may be written in the following way*:

$$N = \sum_{j=1}^{l} \varepsilon_j j^d, \quad \text{where } l \in \mathbb{N}^* \text{ and } \varepsilon_j = \pm 1 \ (j = 1, \ldots, l).$$

According to [2], R.W. Prielipp proved this result for $d = 2$ in 1987 while, according to [3], Erdös would have proved this particular case in 1937 when he was sixteen. Seemingly independently, Proposition 1.2 was extended to integer-valued polynomials by Yu [10] and Bodini, Duchet and Lefranc [3, Théorème 2.1]:

Proposition 1.3. *Let f be an integer-valued polynomial such that the greatest common divisor of its values is* 1. *Then, every integer N may be written in the following way*:

$$N = \sum_{j=1}^{l} \varepsilon_j f(j), \quad \text{where } l \in \mathbb{N}^* \text{ and } \varepsilon_j = \pm 1 \ (j = 1, \ldots, l).$$

The aim of this paper is to extend this last result to integers of number fields by considering coefficients ε_j that are roots of unity. We are going to show that the previous proposition extends nearly word for word to cyclotomic fields (Theorem 5.3). To do so, we use techniques from [3] that seem simpler than Yu's. Doing this, we will correct a gap in the proof given by [3]. We also obtain an effective upper bound for the least integer l for which N has such a representation (Theorem 6.1).

2. HYPOTHESES AND NOTATION

Let K be a number field. Denote by $\mathcal{O}_K$ the ring of integers of K and by μ_K the group of roots of unity of K. We consider the polynomial ring

$$\text{Int}(\mathbb{Z}, \mathcal{O}_K) = \{g \in K[X] \mid g(\mathbb{Z}) \subseteq \mathcal{O}_K\}.$$

Let f be a fixed polynomial in $\text{Int}(\mathbb{Z}, \mathcal{O}_K)$. Denote by d the degree of f.

We are interested in the subset $\mathcal{R} = \mathcal{R}_K(f)$ of $\mathcal{O}_K$ formed by the integers $N \in \mathcal{O}_K$ that may be represented in the following form:

$$N = \sum_{j=1}^{l} \varepsilon_j f(j) \quad (l \in \mathbb{N}^*, \ \varepsilon_j \in \mu_K),$$

where l depends on N.

We denote by $\lambda(N) = \lambda_K(f, N)$ the smallest integer l such that N has such a representation.

Examples. (1) $\lambda_{\mathbb{Q}}(X^2, 0) = 8$, $\lambda_{\mathbb{Q}}(X^2, 2) = 4$, $\lambda_{\mathbb{Q}}(X^2, 3) = 2$.

(2) For each $k \in \mathbb{N}^*$, $\mathcal{R}_{\mathbb{Q}}(X^k) = \mathbb{Z}$.

(3) If $d \neq -1, -3$, then $\mathcal{R}_{\mathbb{Q}(\sqrt{d})}(X^k) = \mathbb{Z}$ because $\mu_{\mathbb{Q}(\sqrt{d})} = \{\pm 1\}$.

We are going to prove that, when K is a cyclotomic field, $\mathcal{R}_K(f) = \mathcal{O}_K$ if and only if the values of f on $\mathbb{Z}$ generate the ideal $\mathcal{O}_K$. When $K = \mathbb{Q}$, we obtain the previous result of Yu and Bodini, Duchet and Lefranc.

Of course, we have the following containment:

$$\mathcal{R}_K(f) \subseteq \mathbb{Z}[\mu_K] \cdot f(\mathbb{Z}),$$

where $\mathbb{Z}[\mu_K] \cdot f(\mathbb{Z})$ denotes the $\mathbb{Z}[\mu_K]$-module generated by the values of f on $\mathbb{Z}$. We are going to study some properties of stability of $\mathcal{R}$. For instance,

$$\forall\, \varepsilon \in \mu_K,\ \varepsilon \mathcal{R} = \mathcal{R}.$$

In the next section we introduce some tools taken from [3].

3. Operators on $\mathrm{Int}(\mathbb{Z}, \mathcal{O}_K)$

We begin with some easy properties concerning the elements of $\mathrm{Int}(\mathbb{Z}, \mathcal{O}_K)$.

Proposition 3.1. *Let g be a polynomial of $\mathrm{Int}(\mathbb{Z}, \mathcal{O}_K)$ and let e be its degree.*

(1) *There exists a unique sequence $b_0, b_1, \ldots, b_e$ of elements of $\mathcal{O}_K$ such that*

$$g(X) = \sum_{i=0}^{e} b_i \binom{X}{i}, \quad where \ \binom{X}{i} = \frac{X(X-1)\cdots(X-i+1)}{i!}.$$

In particular, $e! g(X) \in \mathcal{O}_K[X]$.

(2) *The following subsets of $\mathcal{O}_K$ generate the same $\mathbb{Z}$-module:*

$$\{g(k) \mid k \in \mathbb{Z}\}\,,\ \{g(0), g(1), \ldots, g(e)\}\,,\ \{b_0, b_1, \ldots, b_e\}.$$

We denote this $\mathbb{Z}$-module by $\mathbb{Z} \cdot g(\mathbb{Z})$. In particular, these three subsets generate the same $\mathbb{Z}[\mu_K]$-module.

Proof. (1) Obviously, one may write

$$g(X) = \sum_{i=0}^{e} b_i \binom{X}{i}, \quad \text{where } b_i \in K.$$

These b_i's are unique. Replacing X successively by $0, 1, \ldots, e$ leads to a triangular linear system in the b_i's whose matrix is unimodular with coefficients in $\mathbb{Z}$:

$$\begin{pmatrix} g(0) \\ g(1) \\ g(2) \\ \cdots \\ g(e) \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 0 & \cdots & 0 \\ 1 & 2 & 1 & \ldots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & \binom{e}{1} & \binom{e}{2} & \cdots & \binom{e}{e} \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ \cdots \\ b_e \end{pmatrix}.$$

Consequently, the b_i's are in $\mathcal{O}_K$.

(2) Obviously, we have the following inclusion of $\mathbb{Z}$-modules:

$$(g(0), g(1), \ldots, g(e)) \subseteq (g(k) \mid k \in \mathbb{Z}) \subseteq (b_0, b_1, \ldots, b_e).$$

Moreover, it follows from the previous linear system that we have

$$(b_0, b_1, \ldots, b_e) \subseteq (g(0), g(1), \ldots, g(e)). \qquad \square$$

Notation (following [3]). Let $A = (\varepsilon_1, \ldots, \varepsilon_l)$ be a sequence of elements of μ_K. Denote by $l(A) = l$ its length. For each $g \in \mathrm{Int}(\mathbb{Z}, \mathcal{O}_K)$ we define the action of A on g by

$$A[g] = \sum_{k=1}^{l} \varepsilon_k g(X + k).$$

The following map is clearly $\mathcal{O}_K$-linear:

$$A : g \in \mathrm{Int}(\mathbb{Z}, \mathcal{O}_K) \mapsto A[g] \in \mathrm{Int}(\mathbb{Z}, \mathcal{O}_K).$$

This symbolism is useful here because we have the equivalence

$$N = \sum_{k=1}^{l} \varepsilon_k f(k) \Leftrightarrow N = A[f](0).$$

Then

$$\lambda(N) = \min\{l(A) \mid A[f](0) = N\}.$$

We are going to use the following notation:

For $A = (\alpha_1, \ldots, \alpha_l) \in \mu_K^l$, $B = (\beta_1, \ldots, \beta_t) \in \mu_K^t$ and $\varepsilon \in \mu_K$, we let

$$\varepsilon A = (\varepsilon \alpha_1, \ldots, \varepsilon \alpha_l),$$

$$\overline{A} = -A = (-\alpha_1, \ldots, -\alpha_l),$$

$$A \times B = (\alpha_1, \ldots, \alpha_l, \beta_1, \ldots, \beta_t).$$

Then, one has

$$(\varepsilon A)[g] = \varepsilon\, A[g], \qquad \overline{A}[g] = -A[g]$$

and

$$(A \times B)[g](X) = \sum_{k=1}^{l(A)} \alpha_k g(X + k) + \sum_{h=1}^{l(B)} \beta_h f(X + l(A) + h).$$

Then we have the following obvious lemma.

Lemma 3.2. *For each $A \in \mu_K^l$ and each $g \in \mathrm{Int}(\mathbb{Z}, \mathcal{O}_K)$,*

$$(A \times \overline{A})[g](X) = A[g](X) - A[g](X + l).$$

If the leading term of $A[g]$ is aX^e, then the leading term of the polynomial $(A \times \overline{A})[g]$ is $-ael X^{e-1}$. In particular, $\deg(A \times \overline{A})[g] = \deg A[g] - 1$.

Definition 3.3. We define inductively the operators D_m ($m \in \mathbb{N}$) by

$$D_0 = (1) \quad \text{and} \quad D_{m+1} = D_m \times \overline{D_m}.$$

For instance, $D_1 = (1, -1), D_2 = (1, -1, -1, 1), \ldots$ Replacing 1 by 0 and -1 by 1, we get the Thue-Morse sequence (see [9, Sequence A010060]).

Clearly, $l(D_m) = 2^m$, and hence

$$D_{m+1}[g](X) = D_m[g](X) - D_m[g](X + 2^m).$$

If $m > \deg(g)$, then $D_m[g] = 0$.

In particular, for the fixed polynomial f of degree d introduced in Section 2:

— $D_{d+1}[f] = 0$, $0 \in \mathcal{R}_K(f)$ and $\lambda(0) \leq 2^{d+1}$.

— $D_d[f]$ is a constant that we denote by $C_K(f)$ or C. More precisely:

Lemma 3.4. *Let a_d be the leading coefficient of f. Then,*

$$D_d[f] = (-1)^d (d!) 2^{\frac{d(d-1)}{2}} a_d = C_K(f) = C \in \mathcal{O}_K.$$

Proof. By linearity,

$$D_d[f] = D_d[f - a_d X^d] + D_d[a_d X^d] = D_d[a_d X^d] = a_d D_d[X^d].$$

It follows from Lemma 3.2 that

$$D_d[X^d] = (-1)^d \times d \times (d-1) \times \cdots \times 2 \times 1 \times 2^{d-1} \times \cdots \times 2^2 \times 2 = (-1)^d \times d! \times 2^{\frac{d(d-1)}{2}}.$$

Finally, it follows from Proposition 3.1 that $d!a_k \in \mathcal{O}_K$, and hence $C_K(f) \in \mathcal{O}_K$. One could also say that, in fact,

$$C(f) \in \mathbb{Z}[\mu_K] \cdot f(\mathbb{Z}) \subseteq \mathcal{O}_K.$$

$\square$

4. STABILITY PROPERTIES OF $\mathcal{R}$

Proposition 4.1. *For $C = D_d[f]$, one has*

$$\mathcal{R} + C \cdot \mathbb{Z}[\mu_K] \subseteq \mathcal{R}.$$

Proof. Let $N \in \mathcal{R}$ and let $A = (\alpha_1, \ldots, \alpha_l) \in \mu_K^l$ be such that

$$N = A[f](0).$$

Then, for every $\varepsilon \in \mu_K$, one has

$$(A \times \varepsilon D_d)[f](X) = A[f](X) + \varepsilon D_d[f](X + l),$$

and hence

$$A[f](0) + \varepsilon D_d[f](l) = N + \varepsilon D_d[f] = N + \varepsilon C \in \mathcal{R}.$$

$\square$

The next result is an extension of [3, Lemme 2.2], where $K = \mathbb{Q}$ and $\varepsilon + \varepsilon' = \pm 2$.

Proposition 4.2. *Let $N \in \mathcal{R}$, $\varepsilon, \varepsilon' \in \mu_K$, and $k > \lambda(N)$. Then*

$$N + (\varepsilon + \varepsilon')f(k) \in \mathcal{R}.$$

Proof. Let $A = (\alpha_1, \ldots, \alpha_l)$ be such that $N = A[f](0)$ and $l = l(A) = \lambda(N)$. Let $m \in \mathbb{N}$ be such that $m > d$ and $2^m \geq k - l$. Then $m \geq d + 1$ implies that

$$(A \times \varepsilon D_m)[f](0) = (A \times \varepsilon \overline{D_m})[f](0) = N.$$

Moreover, $2^m \geq k - l$ implies that $-\varepsilon$ is the k-th term of one of the sequences $A \times \varepsilon D_m$ or $A \times \varepsilon \overline{D_m}$. If we replace this $-\varepsilon$ by ε', we obtain a sequence B such that

$$B[f](0) = N + (\varepsilon + \varepsilon')f(k).$$

$\square$

Bodini, Duchet and Lefranc forgot this condition $k > \lambda(N)$ in their proof of [3, Lemme 2.2]. Now we shall see how we may avoid the hypothesis $k > \lambda(N)$.

Proposition 4.3. *For all $N \in \mathcal{R}$, for all $\varepsilon, \varepsilon' \in \mu_K$, and for all $k \in \mathbb{Z}$, one has*

$$N + (\varepsilon + \varepsilon')f(k) \in \mathcal{R} + C\mathcal{O}_K.$$

Proof. Let $c \in \mathbb{N}$ be such that $C = D_d[f]$ divides c in $\mathcal{O}_K$. Since $d!a_d \in \mathcal{O}_K$, we may choose
$$c = 2^{\frac{d(d-1)}{2}} |N_{K/\mathbb{Q}}(d!a_d)|.$$
Then for k and $s \in \mathbb{Z}$, one has
$$f(k + d!cs) - f(k) \in c\mathcal{O}_K \subseteq C\mathcal{O}_K,$$
because $d!f \in \mathcal{O}_K[X]$.

Now, let $N \in \mathcal{R}$, let $\varepsilon, \varepsilon' \in \mu_K$ and let $k \in \mathbb{Z}$. Let $A = (\alpha_1, \ldots, \alpha_l)$ be such that $N = A[f](0)$. Let $s \in \mathbb{N}$ be such that $k' = k + d!cs > l(A) = l$. Then it follows from Proposition 4.2 that
$$N + (\varepsilon + \varepsilon')f(k') \in \mathcal{R}.$$
Moreover, one has
$$(f(k) - f(k')) \in C\mathcal{O}_K,$$
and hence
$$N + (\varepsilon + \varepsilon')f(k) \in \mathcal{R} + C\mathcal{O}_K.$$
$\square$

Note that in Proposition 4.3 we no longer have the condition $k > \lambda(N)$ of Proposition 4.2, but we no longer have the inclusion in $\mathcal{R}$. In order to be able to use the inclusion
$$\mathcal{R} + C\mathbb{Z}[\mu_K] \subseteq \mathcal{R},$$
of Proposition 4.1, we shall assume that
$$\mathbb{Z}[\mu_K] = \mathcal{O}_K.$$
This last equality is obviously equivalent to: K being a cyclotomic field. This will be our hypothesis.

5. Cyclotomic fields

From now on, we assume that K is a cyclotomic field, that is, $\mathcal{O}_K = \mathbb{Z}[\mu_K]$ (including the case $K = \mathbb{Q}$).

Lemma 5.1. *Assume* $\mathcal{O}_K = \mathbb{Z}[\mu_K]$. *Then, for all* $\varepsilon, \varepsilon' \in \mu_K$ *and for all* $x \in \mathbb{Z}[\mu_K] \cdot f(\mathbb{Z})$, *one has*
$$\mathcal{R} + (\varepsilon + \varepsilon')x \subseteq \mathcal{R}.$$

Proof. This lemma extends [3, Lemme 2.3], where $K = \mathbb{Q}$ and $\varepsilon + \varepsilon' = \pm 2$. It follows from Proposition 4.1 that
$$\mathcal{R} + C\mathcal{O}_K \subseteq \mathcal{R}$$
and, from Lemma 4.3, that for all $\varepsilon, \varepsilon' \in \mu_K$ and for all $k \in \mathbb{Z}$
$$(*) \qquad\qquad \mathcal{R} + (\varepsilon + \varepsilon')f(k) \subseteq \mathcal{R}.$$
Let $x \in \mathbb{Z}[\mu_K] \cdot f(\mathbb{Z})$. Proposition 3.1 shows that
$$x = \sum_{k=0}^{d} u_k f(k), \quad \text{where} \quad u_k \in \mathbb{Z}[\mu_K].$$
Writing
$$u_k = \sum_i m_{i,k}\varepsilon_{i,k}, \quad \text{where} \quad m_{i,k} \in \mathbb{N} \text{ and } \varepsilon_{i,k} \in \mu_K,$$

we have

$$(\varepsilon + \varepsilon')x = \sum_{i,k} m_{i,k}(\varepsilon\varepsilon_{i,k} + \varepsilon'\varepsilon_{i,k})f(k).$$

Using the containment (*), we see that

$$\mathcal{R} + (\varepsilon + \varepsilon')x \subseteq \mathcal{R}.$$

$\square$

Remark 5.2. The previous lemma doesn't say that

$$\mathcal{R} + \mathbb{Z}[\mu_K] \cdot f(\mathbb{Z}) \subseteq \mathcal{R}.$$

It essentially says that

$$\mathcal{R} + \sum_i m_i \varepsilon_i f(k) \subseteq \mathcal{R} \quad (k \in \mathbb{Z},\ m_i \in \mathbb{Z},\ \varepsilon_i \in \mu_K)$$

when $\sum_i m_i$ is even (see Proposition 4.2). We are going to show how this condition may be dropped in the cyclotomic case.

Theorem 5.3. *Let K be a cyclotomic field. Denote by $\mathcal{O}_K$ the ring of integers of K and by μ_K the group of roots of unity of K. Let f be a polynomial of $K[X]$ with degree d such that $f(\mathbb{Z}) \subseteq \mathcal{O}_K$. Let*

$$\mathcal{R} = \mathcal{R}_K(f) = \left\{ N \in \mathcal{O}_K \mid N = \sum_{j=1}^{l} \varepsilon_j f(j) \text{ with } \varepsilon_j \in \mu_K \right\}.$$

Then:

(1) *$\mathcal{R}$ is equal to the ideal of $\mathcal{O}_K$ generated by the values of f on $\mathbb{Z}$.*
(2) *$\mathcal{R} = \mathcal{O}_K$ if and only if the ideal generated by the set $\{f(0), f(1), \ldots, f(d)\}$ is the ring $\mathcal{O}_K$.*

Proof. Denote by $(f(\mathbb{Z}))$ the ideal of $\mathcal{O}_K$ generated by the values of f on $\mathbb{Z}$ (here $(f(\mathbb{Z})) = \mathbb{Z}[\mu_K] \cdot f(\mathbb{Z})$). Let $K = \mathbb{Q}(\zeta)$, where ζ is a primitive m-th root of unity.

(1) Obviously, $\mathcal{R} \subseteq (f(\mathbb{Z}))$. Conversely, if m is odd, then

$$1 = -(\zeta + \zeta^2 + \cdots + \zeta^{m-1}),$$

and it follows from Lemma 5.1 that $\mathcal{R} + (f(\mathbb{Z})) \subseteq \mathcal{R}$. In particular, $(f(\mathbb{Z})) \subseteq \mathcal{R}$ since $0 \in \mathcal{R}$, and hence $\mathcal{R} = (f(\mathbb{Z}))$.

If m is divisible by an odd number $m' > 1$, then, considering $\xi = \zeta^{m/m'}$, we have

$$1 = -(\xi + \xi^2 + \cdots + \xi^{m'-1}),$$

and we may also conclude.

There remains the case when m is a power of 2. First recall, from Lemma 5.1, that

$$\mathcal{R} + (1 - \zeta)(f(\mathbb{Z})) \subseteq \mathcal{R} \quad \text{and} \quad (1 - \zeta)(f(\mathbb{Z})) \subseteq \mathcal{R}.$$

One knows that

$$N_{K/\mathbb{Q}}(1 - \zeta) = 2.$$

Consequently, the element $1 - \zeta$ is not invertible in $\mathcal{O}_K$, and hence

$$(1 - \zeta)(f(\mathbb{Z})) \neq (f(\mathbb{Z})).$$

Moreover,

$$\operatorname{Card}\left((f(\mathbb{Z}))/(1 - \zeta)(f(\mathbb{Z}))\right) = N(1 - \zeta) = 2$$

implies that $(f(\mathbb{Z}))$ contains exactly two classes modulo $(1 - \zeta)(f(\mathbb{Z}))$.

Since $(1 - \zeta)(f(\mathbb{Z})) \neq (f(\mathbb{Z}))$, there is a smallest integer $j \geq 1$ such that $f(j) \notin (1 - \zeta)(f(\mathbb{Z}))$. Let $N_* = f(1) + f(2) + \cdots + f(j)$. Then, $N_* \in \mathcal{R}$ and $N_* \notin (1 - \zeta)(f(\mathbb{Z}))$. Thus, $\mathcal{R}$ contains two distinct classes modulo $(1 - \zeta)(f(\mathbb{Z}))$, and hence is equal to $(f(\mathbb{Z}))$.

(2) The second assertion results from the first one and from Proposition 3.1. $\square$

When $K = \mathbb{Q}$, the original result of Yu [10, Theorem] seems to be stronger, but Theorem 5.3 may be easily written in a more general form:

Corollary 5.4. *With the hypotheses and notation of Theorem 5.3, assume that $(f(\mathbb{Z})) = \mathcal{O}_K$. Then, for every fixed integer m, each element N of $\mathcal{O}_K$ may be written in the following way:*

$$N = \sum_{k=m+1}^{m+l} \varepsilon_k f(k), \quad \text{where} \quad \varepsilon_k \in \mu_K, \text{ and } l \in \mathbb{N}$$

(l depends on K, f, N and m).

Proof. Let $g(X) = f(X + m)$. Then $(g(\mathbb{Z})) = (f(\mathbb{Z})) = \mathcal{O}_K$, and it follows from Theorem 5.3 that there exist $l \in \mathbb{N}$ and $\varepsilon_k \in \mu_K$ $(k = 1, \ldots, l)$ such that

$$N = \sum_{k=1}^{l} \varepsilon_k g(k) = \sum_{k=1}^{l} \varepsilon_k f(k + m) = \sum_{k=m+1}^{m+l} \varepsilon_k f(k).$$

$\square$

6. An upper bound for $\lambda(N)$

In [2, §4], Bleicher shows that $\lambda(N)$, the least integer l such that

$$N = \sum_{k=1}^{l} \pm k^d \quad (N \in \mathbb{N}),$$

is less than

$$A \, N^{\frac{1}{d+1}} + B$$

for some constants A and B only depending on the exponent d. On the other hand, in a concluding remark, Yu [10] says that it seems more difficult to estimate this minimal value $\lambda(N)$ in the case of integer-valued polynomials. Nevertheless, we are going to give an upper bound for $\lambda(N)$ even in the general case of cyclotomic fields and for integer-valued polynomials.

Theorem 6.1. *Let $K = \mathbb{Q}(\zeta)$ be a cyclotomic field, where ζ is a primitive m-th root of unity (m is odd or divisible by 4). Let*

$$f(X) = \sum_{i=0}^{d} a_i X^i \in K[X] \quad \text{with } a_d \neq 0 \text{, and then } \deg(f) = d.$$

Assume that the values of f on $\mathbb{Z}$ belong to the ring of integers $\mathcal{O}_K$ and that the ideal generated by these values is $\mathcal{O}_K$ itself. For each $N \in \mathcal{O}_K$, denote by $\lambda(N)$ the least integer l such that

$$N = \sum_{k=1}^{l} \varepsilon_k f(k), \quad where \quad \varepsilon_k \in \mu_K \ (k = 1, \ldots, l).$$

Then there are two effective constants $A = A_K(f)$ and $B = B_K(f)$, only depending on K and f, such that

$$\lambda(N) \leq A \, \widetilde{N} + B,$$

where, for each $x \in K$,

$$\widetilde{x} = \max_{\sigma \in Gal(K/\mathbb{Q})} |\sigma(x)|.$$

More precisely, we may choose

$$A = \frac{2^{\frac{d(3-d)}{2}}}{d!} \, \varphi(m)^2 \, \alpha \, \beta \, \gamma$$

and

$$B = A \, \nu(\mathcal{N}) + \Lambda(\mathcal{N}),$$

where φ denotes Euler's function and Φ_m the m-th cyclotomic polynomial,

$$\alpha = \widetilde{\frac{1}{a_d}}, \quad \Phi_m(X) = \sum_{j=0}^{\varphi(m)} \beta_j X^j, \quad \beta = \sum_{j=0}^{\varphi(m)-1} |\beta_j|, \quad \gamma = \widetilde{\frac{1}{\Phi_m'(\zeta)}},$$

$\mathcal{N}$ denotes a subset of $\mathcal{O}_K$ containing at least one representative of the classes of $\mathcal{O}_K$ modulo C, with

$$C = C_K(f) = (-1)^d \, d! \, 2^{\frac{d(d-1)}{2}} a_d,$$

and where the constants

$$\nu(\mathcal{N}) = \max \{\widetilde{N} \mid N \in \mathcal{N}\}$$

and

$$\Lambda(\mathcal{N}) = \max \{\lambda(N) \mid N \in \mathcal{N}\}$$

are bounded in Propositions 6.5 and 7.1 below.

We begin with two technical lemmas.

Lemma 6.2. *Let N and N_0 in $\mathcal{O}_K$ be such that*

$$N = N_0 + \left(\sum_{i=1}^{s} n_i \varepsilon_i\right) C \quad with \ n_i \in \mathbb{Z}, \, \varepsilon_i \in \mu_K.$$

Then,

$$\lambda(N) \leq \lambda(N_0) + \left(\sum_{i=1}^{s} |n_i|\right) 2^d.$$

Proof. The case when $N = N_0 + \varepsilon C$ is a straightforward consequence of Proposition 4.1. We obtain the general case by iteration. $\square$

Lemma 6.3. *There is a constant $E = E_K$, only depending on K, such that, for every*

$$x = \sum_{0 \leq i < \varphi(m)} x_i\, \zeta^i \in \mathcal{O}_K \quad (x_i \in \mathbb{Z}),$$

one has

$$|x_i| \leq E\, \widetilde{x} \quad (0 \leq i < \varphi(m)).$$

One may choose

$$E = E_K = \varphi(m)\, \beta\, \gamma.$$

Proof. Denote by $\kappa_0, \kappa_1, \ldots, \kappa_{\varphi(m)-1}$ the dual basis of the basis $1, \zeta, \ldots, \zeta^{\varphi(m)-1}$ of K over $\mathbb{Q}$ with respect to the trace. Then, for $0 \leq i < \varphi(m)$, one has

$$x_i = tr_{K/\mathbb{Q}}(x\kappa_i) = \sum_{\sigma \in G} \sigma(x)\sigma(\kappa_i),$$

where $G = Gal(K/\mathbb{Q})$. Thus,

$$|x_i| \leq \widetilde{x} \sum_{\sigma \in G} |\sigma(\kappa_i)|.$$

It suffices to choose a constant E that is greater than

$$\max_{0 \leq i < \varphi(m)} \left(\sum_{\sigma \in G} |\sigma(\kappa_i)| \right).$$

One knows that the κ_i's are characterized by

$$\sum_{0 \leq i < \varphi(m)} \kappa_i X^i = \prod_{k \neq 1,\, (k,m)=1} \frac{X - \zeta^k}{\zeta - \zeta^k}$$

(see for instance [7, Proposition B03]). Since

$$\prod_{k \neq 1,\, (k,m)=1} (\zeta - \zeta^k) = \Phi'_m(\zeta),$$

one has

$$\Phi'_m(\zeta) \times \sum_i \kappa_i X^i = \frac{\Phi_m(X)}{X - \zeta} = -\zeta^{-1}\, \Phi_m(X) \left(\sum_{k \geq 0} \zeta^{-k} X^k \right),$$

and hence

$$|\Phi'_m(\zeta)|\, |\kappa_i| = \left| \sum_{j=0}^{i} \beta_j \zeta^{i-j} \right|, \quad \text{where}\ \ \Phi_m(X) = \sum_{j=0}^{\varphi(m)} \beta_j X^j.$$

Consequently, for every $\sigma \in G$ and every $i \in \{0, 1, \ldots, \varphi(m) - 1\}$,

$$|\Phi'_m(\sigma(\zeta))|\, |\sigma(\kappa_i)| \leq \sum_{j=0}^{i} |\beta_j|,$$

and hence

$$|\sigma(\kappa_i)| \leq \beta\, \frac{1}{\min_\sigma |\sigma(\Phi'_m(\zeta))|}, \quad \text{where}\ \ \beta = \sum_{j=0}^{\varphi(m)-1} |\beta_j|.$$

Let

$$\gamma = \frac{1}{\min_\sigma |\sigma(\Phi'_m(\zeta))|} = \max_\sigma \frac{1}{|\sigma(\Phi'_m(\zeta))|} = \widetilde{\frac{1}{\Phi'_m(\zeta)}}.$$

Finally,

$$\max_{0 \le i < \varphi(m)} \left(\sum_{\sigma \in G} |\sigma(\kappa_i)| \right) \le \varphi(m)\,\beta\,\gamma.$$

$\square$

Remarks 6.4. (1) Clearly,

$$1 + \beta = \sum_{j=0}^{\varphi(m)} |\beta_j| \le 2^{\varphi(m)}.$$

Recall also Bateman's results on the coefficients of cyclotomic polynomials [1]:

$$1 + \beta \le m^{\frac{d(m)}{2}},$$

where $d(m)$ denotes the number of divisors of m.

(2) Note also the following obvious inequality:

$$\gamma = \widetilde{\frac{1}{\Phi'_m(\zeta)}} \le \left(2 \sin \frac{\pi}{m} \right)^{1 - \varphi(m)}.$$

(3) When $m = 2^n$, one has $\Phi_{2^n}(X) = X^{2^{n-1}} + 1$ and $\Phi'_{2^n}(\zeta) = -\frac{1}{\zeta}\, 2^{n-1}$. Then $\beta = 1$ and $\gamma = 2^{1-n}$, so that $E = \varphi(2^n)\,\beta\,\gamma = 1$.

Proof of Theorem 6.1. Let $\mathcal{N}$ be a finite subset of $\mathcal{O}_K$ such that $\mathcal{N}$ contains at least one representative of the classes of $\mathcal{O}_K$ modulo C. Then, for every fixed element N in $\mathcal{O}_K$, there is at least one element N_0 in $\mathcal{N}$ and an element x in $\mathcal{O}_K$ such that

$$N - N_0 = Cx.$$

For each $\sigma \in G = Gal(K/\mathbb{Q})$,

$$|\sigma(x)| \le \frac{|\sigma(N)| + |\sigma(N_0)|}{|\sigma(C)|},$$

and hence

$$\tilde{x} \le (\widetilde{N} + \widetilde{N_0})\,\widetilde{\frac{1}{C}}.$$

Since $\mathcal{O}_K = \mathbb{Z}[\zeta]$, the element x may be written in the following way:

$$x = \sum_{0 \le i < \varphi(m)} x_i\,\zeta^i \quad \text{with} \quad x_i \in \mathbb{Z},$$

and Lemma 6.2 shows that

$$\lambda(N) \le \lambda(N_0) + 2^d \sum_{0 \le i < \varphi(m)} |x_i|.$$

On the other hand, it follows from Lemma 6.3 that

$$|x_i| \le E\,(\widetilde{N} + \widetilde{N_0})\,\widetilde{\frac{1}{C}}.$$

Consequently,

$$\lambda(N) \le \lambda(N_0) + 2^d\,\varphi(m)\,E\,(\widetilde{N} + \widetilde{N_0})\,\widetilde{\frac{1}{C}}.$$

Replacing $\widetilde{\frac{1}{C}}$ by $2^{\frac{d(1-d)}{2}}\frac{}{d!}\,\alpha$ and E by $\varphi(m)\,\beta\,\gamma$, we obtain

$$\lambda(N) \le \lambda(N_0) + A(\widetilde{N} + \widetilde{N}_0)$$

with

$$A = \frac{2^{\frac{d(3-d)}{2}}}{d!}\,\varphi(m)^2\,\alpha\,\beta\,\gamma.$$

Finally,

$$\lambda(N) \le \Lambda(\mathcal{N}) + A\,(\widetilde{N} + \nu(\mathcal{N})),$$

where

$$\nu(\mathcal{N}) = \max\,\{\widetilde{N}_0 \mid N_0 \in \mathcal{N}\}$$

and

$$\Lambda(\mathcal{N}) = \max\,\{\lambda(N_0) \mid N_0 \in \mathcal{N}\}.$$

We then may choose

$$B = A\,\nu(\mathcal{N})\; +\; \Lambda(\mathcal{N}).$$

The constant A is well defined. To prove the effectiveness of B, we have to give upper bounds for $\nu(\mathcal{N})$ and $\Lambda(\mathcal{N})$ for some choice of $\mathcal{N}$. This is done in Propositions 6.5 and 7.1 below. $\qquad\square$

A choice for $\mathcal{N}$. Let

$$c = c_K(f) = 2^{\frac{d(d-1)}{2}}\,(d!)^{\varphi(m)}\,|N_{K/\mathbb{Q}}(a_d)|.$$

Note that $c \in \mathbb{N}$ and C divides c in $\mathcal{O}_K$. Then let

$$\mathcal{N} = \left\{ N = \sum_{0 \le i < \varphi(m)} n_i\zeta^i \mid n_i \in \mathbb{Z},\; -\frac{c}{2} < n_i \le \frac{c}{2} \right\}.$$

For every $N = \sum_i n_i\,\zeta^i \in \mathcal{O}_K$ and for $0 \le i < \varphi(m)$, let $n_i^0 \in \mathbb{Z}$ be such that $n_i \equiv n_i^0 \pmod{c}$ and $-\frac{c}{2} < n_i^0 \le \frac{c}{2}$. Then $N_0 = \sum_i n_i^0\zeta^i \in \mathcal{N}$, and c divides $N - N_0$; a fortiori C divides $N - N_0$.

Proposition 6.5. *With the previous choice for* $\mathcal{N}$, *one has*

$$\nu(\mathcal{N}) = \max\,\{\widetilde{N} \mid N \in \mathcal{N}\} \le (d!)^{\varphi(m)}\,2^{\frac{d(d-1)}{2}-1}\,\varphi(m)\,|N_{K/\mathbb{Q}}(a_d)|.$$

Proof. Of course, for every $N_0 = \sum_i n_i^0\zeta^i \in \mathcal{N}$, one has

$$\widetilde{N}_0 \le \sum_i |n_i^0| \le \frac{c}{2}\,\varphi(m),$$

since every $\sigma(N_0)$ is of the form

$$\sum_i n_i^0\,\sigma(\zeta)^i = \sum_i n_i^0\zeta^{ik},$$

where k is prime to m. Let

$$\nu_K(f) = \frac{c}{2}\,\varphi(m) = (d!)^{\varphi(m)}\,2^{\frac{d(d-1)}{2}-1}\,\varphi(m)\,|N_{K/\mathbb{Q}}(a_d)|.$$

Then, for each $N_0 \in \mathcal{N}$, $\widetilde{N}_0 \le \nu_K(f)$. $\qquad\square$

Remarks 6.6. (1) Note that, with this choice for $\mathcal{N}$ and this bound for $\nu(\mathcal{N})$, one has

$$B = 2^{d-1} \, (d!)^{\varphi(m)-1} \, \varphi(m)^3 \, \alpha \, \beta \, \gamma \, |N_{K/\mathbb{Q}}(a_d)| \, + \, \Lambda(\mathcal{N}).$$

(2) In the case when $a_d \in \mathbb{Q}$, one has $\alpha = \frac{1}{|a_d|}$ and one may choose

$$c = 2^{\frac{d(d-1)}{2}} \, d! \, a_d.$$

Consequently,

$$B = 2^{d-1} \, \varphi(m)^3 \, \beta \, \gamma \, + \, \Lambda(\mathcal{N}).$$

(3) If $K = \mathbb{Q}$, then $m = \beta = \gamma = \varphi(m) = 1$,

$$A = \frac{2^{\frac{d(3-d)}{2}}}{d! \, a_d} \quad \text{and} \quad B = 2^{d-1} + \Lambda(\mathcal{N}).$$

It remains to give an effective bound for $\Lambda(\mathcal{N})$. This is done in Proposition 7.1 in the next section.

7. AN UPPER BOUND FOR $\Lambda(\mathcal{N})$

Notation 7.0. Recall that

$$\Lambda(\mathcal{N}) = \max \, \{\lambda(N) \mid N \in \mathcal{N}\},$$

where

$$\mathcal{N} = \left\{ N = \sum_{0 \leq i < \varphi(m)} n_i \zeta^i \mid n_i \in \mathbb{Z}, \ -\frac{c}{2} < n_i \leq \frac{c}{2} \right\}$$

and

$$c = c_K(f) = (d!)^{\varphi(m)} \, 2^{\frac{d(d-1)}{2}} \, |N_{K/\mathbb{Q}}(a_k)|.$$

Let $v_0, \ldots, v_d \in \mathcal{O}_K$ be such that

$$\sum_{k=0}^{d} v_k f(k) = 1$$

(it follows from Proposition 3.1 that $f(0), \ldots, f(d)$ generate the ideal $\mathcal{O}_K$), and let

$$V = V_K(f) = \max \, \{\widetilde{v}_k \mid 0 \leq k \leq d\}.$$

Denote by $\widetilde{f}$ the polynomial

$$\widetilde{f}(X) = \sum_{i=0}^{d} \widetilde{a}_i X^i$$

and let

$$F = \sum_{k=1}^{d+1} \widetilde{f}(k).$$

If m is not a power of 2, we denote by m' the least odd divisor ≥ 3 of m, we let

$$\delta(m) = \frac{m' - 1}{2},$$

and we put

$$\omega(m) = \left[(d+1) \, \varphi(m)^3 \, \delta(m) \, \beta \, \gamma \, V \, \frac{c}{2} \right].$$

If $m = 2^n$, we let

$$\delta(1) = \frac{1}{2}, \quad \delta(m) = \frac{1}{2 \sin \frac{\pi}{m}} \;\; \text{for } m \geq 4,$$

and

$$\omega(2^n) = \left[(d+1) \, 2^{n-1} \, \delta(2^n) \, V \; \left(2^{n-2}c + F \right) \right].$$

Proposition 7.1. *With the hypotheses of Theorem 5.3 and Notation 7.0, one has*

$$\Lambda(\mathcal{N}) \leq \lambda_{\omega(m)},$$

where $\lambda_{\omega(m)}$ is defined by

$$\lambda_0 = 2^{d+1} \quad and \quad \lambda_{k+1} = h(\lambda_k),$$

h denoting the polynomial

$$h(X) = 2 \, d! \, c \; + \; X \; + \; G \, \widetilde{f}(X + d!c)$$

with

$$G = \frac{2^{\frac{(d+1)(4-d)}{2}}}{d!} \; \varphi(m)^2 \, \alpha \, \beta \, \gamma.$$

We first need several technical lemmas.

Lemma 7.2. *If m is not a power of 2, then every $N \in \mathcal{O}_K$ may be written in the following form:*

$$N = \sum_{i \in I} \left(\varepsilon_i + \varepsilon_i' \right) f(k_i) \;\; with \;\; \varepsilon_i, \varepsilon_i' \in \mu_K, k_i \in \mathbb{N},$$

with

$$Card(I) \leq (d+1) \times \varphi(m)^2 \times \delta(m) \times \beta \times \gamma \times V \times \widetilde{N}.$$

Proof. Obviously,

$$N = \sum_{k=0}^{d} N v_k f(k).$$

Let us write

$$N v_k = \sum_{0 \leq j < \varphi(m)} w_{k,j} \zeta^j \;\; (w_{k,j} \in \mathbb{Z}).$$

Then

$$N = \sum_{k=0}^{d} \left(\sum_{0 \leq j < \varphi(m)} w_{k,j} \zeta^j \right) f(k).$$

As already noticed in the proof of Theorem 5.3, the element $\xi = \zeta^{\frac{m}{m'}}$ satisfies

$$\sum_{i=1}^{m'-1} \xi^i = -1.$$

Consequently,

$$N = \sum_{k=0}^{d} \left(\sum_{0 \leq j < \varphi(m)} w_{k,j} \zeta^j \left(- \sum_{i=1}^{\delta(m)} \xi^i (1 + \xi^{\delta(m)}) \right) \right) f(k),$$

and then

$$N = \sum_{k=0}^{d} \left(\sum_{0 \le j < \varphi(m)} n_{k,j} \sum_{i=1}^{\delta(m)} (\varepsilon_{i,j,k} + \varepsilon'_{i,j,k}) \right) f(k),$$

where $\varepsilon_{i,j,k}, \varepsilon'_{i,j,k} \in \mu_K$ and $n_{k,j} \in \mathbb{N}$. It follows from Lemma 6.3 that

$$n_{k,j} = |w_{k,j}| \le E \times \widetilde{Nv_k} \le E \times \widetilde{v}_k \times \widetilde{N} \le E \times V \times \widetilde{N} = \varphi(m) \, \beta \, \gamma \, V \, \widetilde{N}.$$

$\square$

Lemma 7.3. *If m is a power of 2, then every $N \in \mathcal{O}_K$ may be written in the following form:*

$$N = N_0 + \sum_{i \in I} (\varepsilon_i + \varepsilon'_i) f(k_i), \quad \text{where } \varepsilon_i, \varepsilon'_i \in \mu_K, k_i \in \mathbb{N},$$

with

$$N_0 = 0 \ \text{ or } \ N_0 = \sum_{k=1}^{k_0} f(k) \ \text{ for some } k_0 \le d+1$$

and

$$Card(I) \le (d+1) \times \varphi(m) \times \delta(m) \times V \times (\widetilde{N} + F).$$

Proof. As seen in the proof of Theorem 5.3, there exists a least integer k_0 ($1 \le k_0 \le d+1$) such that $f(k_0) \notin (1-\zeta)\mathcal{O}_K$, and then such that

$$N_* = \sum_{k=1}^{k_0} f(k) \notin (1-\zeta)\mathcal{O}_K.$$

We also know that every $N \in \mathcal{O}_K$ is of the form

$$N = N_0 + (1-\zeta)N_1 \quad \text{with} \quad N_0 = 0 \text{ or } N_* \text{ and } N_1 \in \mathcal{O}_K.$$

As for the previous lemma, we may write

$$N_1 = \sum_{k=0}^{d} N_1 v_k f(k) = \sum_{k=0}^{d} \left(\sum_{0 \le j < \varphi(m)} w_{k,j} \zeta^j \right) f(k).$$

Thus

$$N - N_0 = (1-\zeta)N_1 = \sum_{k=0}^{d} \left(\sum_{0 \le j < \varphi(m)} n_{k,j} (\varepsilon_{k,j} + \varepsilon'_{k,j}) \right) f(k),$$

with $n_{k,j} \in \mathbb{N}$, $\varepsilon_{k,j}, \varepsilon'_{k,j} \in \mu_K$ and

$$n_{k,j} = |w_{k,j}| \le E\widetilde{N_1 v_k} \le E\widetilde{N}_1 \widetilde{v}_k \le E \times V \times (\widetilde{N} + \widetilde{N}_*) \times \widetilde{\frac{1}{1-\zeta}}.$$

We may conclude, since

$$E = 1 \ , \quad \widetilde{N}_* \le \sum_{k=1}^{d+1} \widetilde{f}(k) = F,$$

and

$$\min_{\sigma \in G} |1 - \sigma(\zeta)| = 2 \sin \frac{\pi}{m} = \delta(m)^{-1}.$$

$\square$

Lemma 7.4. *Let* $N \in \mathcal{O}_K$ *and* $k \in \mathbb{N}$ *be such that* $k > \lambda(N)$. *Then, for all* $\varepsilon, \varepsilon' \in \mu_K$,

$$\lambda(N + (\varepsilon + \varepsilon')f(k)) \leq \lambda(N) + 2 \max(2^d, k - \lambda(N)).$$

Proof. The proof of Proposition 4.2 shows that, if $N = A[f](0)$ where $l(A) = \lambda(N)$, then $N + (\varepsilon + \varepsilon')f(k) = B[f](0)$ for some B such that $l(B) = l(A) + 2^m$ with $m > d$ and $k \leq 2^m + l(A)$. The least integer m is $\max(d + 1, \lceil \log_2(k - \lambda(N)) \rceil)$, and hence

$$2^m \leq 2 \max(2^d, k - \lambda(N)).$$

$\square$

Lemma 7.5. *For all* $N \in \mathcal{O}_K$, $\varepsilon, \varepsilon' \in \mu_K$, *and* $k \in \mathbb{N}$,

$$\lambda(N + (\varepsilon + \varepsilon')f(k)) \leq h(\lambda(N)),$$

where h *is the following polynomial of degree* d:

$$h(X) = 2d!c + X + G \widetilde{f}(X + d!c)$$

with

$$G = \frac{2^{\frac{(d+1)(4-d)}{2}}}{d!} \varphi(m)^2 \alpha \beta \gamma.$$

Proof. Let $k' \in \mathbb{N}$ be such that $k' - k \in d!c\mathbb{Z}$ and $k' > \lambda(N)$. One may choose k' in $[\lambda(N), \lambda(N) + d!c]$. Then it follows from Lemma 7.3 that

$$\lambda(N + (\varepsilon + \varepsilon')f(k')) \leq \lambda(N) + 2 \max(2^d, d!c) = \lambda(N) + 2d!c.$$

On the other hand,

$$(\varepsilon + \varepsilon')(f(k') - f(k)) = Cy, \quad \text{where} \quad y \in \mathcal{O}_K.$$

Obviously,

$$\widetilde{y} \leq 2 \widetilde{\frac{1}{C}} \, (\widetilde{f}(k) + \widetilde{f}(k')) \leq 4 \widetilde{\frac{1}{C}} \, \widetilde{f}(\lambda(N) + d!c).$$

Writing $y = \sum_{0 \leq i < \varphi(m)} y_i \zeta^i$, we see from Lemma 6.2 that

$$|y_i| \leq 4 E \times \widetilde{\frac{1}{C}} \, \widetilde{f}(\lambda(N) + d!c).$$

Then,

$$N + (\varepsilon + \varepsilon')f(k) = N + (\varepsilon + \varepsilon')f(k') + (\varepsilon + \varepsilon')(f(k) - f(k'))$$

implies that

$$\lambda(N + (\varepsilon + \varepsilon')f(k)) \leq \lambda(N) + 2d!c + 2^d \sum_{0 \leq i < \varphi(m)} |y_i|$$

$$\leq \lambda(N) + 2d!c + 2^{d+2}\varphi(m) \times E \times \widetilde{\frac{1}{C}} \times \widetilde{f}(\lambda(N) + d!c).$$

To conclude, it suffices to use the values for E and C. $\square$

Proof of Proposition 7.1. Let $N \in \mathcal{N}$; then $\widetilde{N} \leq \frac{c}{2}\varphi(m)$. We first consider the case when m is not a power of 2. Lemma 7.2 shows that it suffices to use Lemma 7.5 $Card(I)$ times starting with $N = 0$ and $\lambda(0) \leq 2^{d+1}$. We have

$$Card(I) \leq (d+1) \, \varphi(m)^2 \, \delta(m) \, \beta \, \gamma \times V \times \widetilde{N}$$

$$\leq (d+1) \, \varphi(m)^3 \, \delta(m) \, \beta \, \gamma \, V \times \frac{c}{2},$$

that is,
$$Card(I) \leq \omega(m).$$

Consider the increasing sequence $\{\lambda_n\}_{n \in \mathbb{N}}$ defined inductively by
$$\lambda_0 = 2^{d+1} \quad \text{and} \quad \lambda_{n+1} = h(\lambda_n).$$

Then,
$$\Lambda(\mathcal{N}) \leq \lambda_{\omega(m)}.$$

Assume now that m is a power of 2. Lemma 7.3 shows that it suffices to use Lemma 7.5 $Card(I)$ times starting with $N = 0$ or $N = N_*$ and $\lambda(0) \leq 2^{d+1}$ or $\lambda(N_*) \leq d + 1$. We have

$$Card(I) \leq (d+1)\varphi(m)\delta(m) \, V \times (\widetilde{N} + F)$$
$$\leq (d+1) \, \varphi(m) \, \delta(m) \, V \times \left(\frac{c}{2}\varphi(m) + F\right),$$

that is,
$$Card(I) \leq \omega(m).$$

The conclusion is the same because we still start with $\lambda_0 = \max(2^{d+1}, d+1) = 2^{d+1}$. $\square$

Remark 7.6. The bounds that we obtained are very large, especially those given for $\Lambda(\mathcal{N})$. But, as seen in Remarks 6.6, one may find better bounds when one considers specific polynomials. In particular, if there exists $k \in \{0, 1, \ldots, d\}$ such that $f(k) = 1$, then 1 may replace V and $d+1$ in Lemmas 7.2 and 7.3 for the upper bound of $Card(I)$.

For instance, assume that $K = \mathbb{Q}$ and that $f(x)$ is the binomial polynomial
$$\binom{X}{d} = \frac{X(X-1)\cdots(X-d+1)}{d!}.$$

Then $a_d = \frac{1}{d!}$, $c = |C| = 2^{\frac{d(d-1)}{2}}$, $\delta(1) = \frac{1}{2}$, $V = 1$, $1 - \zeta = 2$, N_0 is $f(0) = 0$ or $f(d) = 1$, and F may be replaced by d, so that $Card(I) \leq \frac{1}{2}(|N| + d)$ with $|N| \leq \frac{c}{2}$ for every $N \in \mathcal{N}$. Consequently, $\omega = \left[2^{\frac{d^2-d-4}{2}} + \frac{d}{2}\right]$ with $\lambda_0 = d$. Recall that

$$A = 2^{\frac{d(3-d)}{2}} \quad \text{and} \quad B = 2^{d-1} + \Lambda(\mathcal{N}).$$

In the particular case when $d = 2$ we have $c = 2$, $\mathcal{N} = \{0, 1\}$, $\Lambda(\mathcal{N}) = 3$ and

$$\lambda_{\mathbb{Q}}\left(\frac{X(X-1)}{2}, N\right) \leq 2|N| + 5.$$

References

[1] P. T. BATEMAN, Note on the coefficients of the cyclotomic polynomial, *Bull. Amer. Math. Soc.* **55** (1949), 1180–1181. MR 11:329e

[2] M. N. BLEICHER, On Prielipp's problem on signed sums of kth powers, *J. Number Theory* **56** (1996), 36–51. MR 96j:11011

[3] O. BODINI, P. DUCHET, AND S. LEFRANC, Autour d'un théorème d'Erdös sur les combinaisons à coefficients ±1 des premiers carrés, *La Nouvelle Revue des Mathématiques de l'Enseignement Supérieur* **112** (2001/2002), 3–8.

[4] J. W. S. CASSELS, On the representation of integers as the sums of distinct summands taken from a fixed set, *Acta Sci. Math. Szeged* **21** (1960), 111–124. MR 24:A103

[5] P. ERDÖS AND R. L. GRAHAM, Old and new problems and results in combinatorial number theory, Monographie 28 de *L'enseignement mathématique*, Geneva, 1980. MR 82j:10001

[6] R. L. GRAHAM, Complete sequences of polynomial values, *Duke Math. J.*, **31** (1964), 275–285. MR 29:63

[7] H. KOCH, *Number Theory, Algebraic Numbers and Function*, American Mathematical Society, Providence, 2000. MR 2001a:11176

[8] M. B. NATHANSON, *Elementary Methods in Number Theory*, Springer, 2000. MR 2001j:11001

[9] N.J.A. SLOANE, *The On-Line Encyclopedia in Integer Sequences*, http://www.research. att.com/ñjas/sequences/index.html

[10] H. B. YU, Signed sums of polynomial values, *Proc. Amer. Math. Soc.* **130** (2002), 1623–1627. MR 2002m:11007

DEPARTMENT OF MATHEMATICS, UNIVERSITÉ DE PICARDIE, 80039 AMIENS, FRANCE, LAMFA CNRS-UMR 6140, FRANCE

E-mail address: `jaboulanger@wanadoo.fr`

DEPARTMENT OF MATHEMATICS, UNIVERSITÉ DE PICARDIE, 80039 AMIENS, FRANCE, LAMFA CNRS-UMR 6140, FRANCE

E-mail address: `jean-luc.chabert@u-picardie.fr`