AN INFINITE FAMILY OF MULTIPLICATIVELY INDEPENDENT BASES OF NUMBER SYSTEMS IN CYCLOTOMIC NUMBER FIELDS

MANFRED G. MADRITSCH AND VOLKER ZIEGLER

Abstract. Let ζ_k be a k-th primitive root of unity, $m \geq \phi(k)+1$ an integer and $\Phi_k(X) \in \mathbb{Z}[X]$ the k-th cyclotomic polynomial. In this paper we show that the pair $(-m+\zeta_k, \mathcal{N})$ is a canonical number system, with $\mathcal{N} = \{0, 1, \ldots, |\Phi_k(m)|\}$. Moreover we also discuss whether the two bases $-m+\zeta_k$ and $-n+\zeta_k$ are multiplicatively independent for positive integers m and n and k fixed.

1. Introduction

Let $q \geq 2$ be a positive integer. Then the pair $(q, \{0, 1, \ldots, q-1\})$ is a number system in the positive integers, *i.e.* every integer $n \in \mathbb{N}$ has a unique representation of the form

$$n = \sum_{j \geq 0} a_j q^j \quad (a_j \in \{0, 1, \ldots, q-1\}).$$

Taking a negative integer $q \leq -2$ and $\{0, 1, \ldots, |q|-1\}$ as set of digits one gets a number system for all integers $\mathbb{Z}$. This concept of a number system was further extended to the Gaussian integers by Knuth [10]. He showed that the pairs $(-1+i, \{0,1\})$ and $(-1-i, \{0,1\})$ are number systems in the Gaussian integers, *i.e.* every Gaussian integer $n \in \mathbb{Z}[i]$ has a unique representation of the form

$$n = \sum_{j \geq 0} a_j b^j \quad (a_j \in \{0, 1\}),$$

where $b = -1+i$ or $b = -1-i$. It was shown by Kátai and Szabó [9] that all possible bases for the Gaussian integers are of the form $-m \pm i$ with m a positive integer. These results were extended independently by Kátai and Kovács [7,8] and Gilbert [5], who classified all quadratic extensions.

A different point of view on the above systems is the following. Let $P = p_d X^d + p_{d-1}X^{d-1} + \cdots + p_1 X + p_0 \in \mathbb{Z}[X]$ with $p_d = 1$ and $\mathcal{R} = \mathbb{Z}[X]/P(X)\mathbb{Z}[X]$. Then we call the pair $(P, \mathcal{N})$ with $\mathcal{N} = \{0, 1, \ldots, |p_0|-1\}$ a canonical number system if every element $\gamma \in \mathcal{R}$ has a unique representation of the form

$$\gamma = \sum_{j \geq 0} a_j X^j \quad (a_j \in \{0, 1, \ldots, p_0\}).$$

2010 *Mathematics Subject Classification.* 11A63,11D61,11D41.

Key words and phrases. Canonical number systems, Radix representations, Diophantine equations, Nagell-Ljunggren equation.

The second author was supported by the Austrian Science Fund (FWF) under the project P 24801-N26.

If P is irreducible and β is one of its roots, then $\mathcal{R}$ is isomorphic to $\mathbb{Z}[\beta]$. In this case we simply write $(\beta, \mathcal{N})$ instead of $(P, \mathcal{N})$. By setting $P = X + q$ or $P = X^2 + 2mX + (m^2 + 1)$ we obtain the canonical number systems in the integers and Gaussian integers from above, respectively.

Kovács [11] proved that for any algebraic number field K and order $\mathcal{R} = \mathbb{Z}[\alpha]$ of K there exists β such that $(\beta, \mathcal{N})$ is a canonical number system for $\mathcal{R}$. Moreover he proved that if $1 \leq p_{d-1} \leq \cdots \leq p_1 \leq p_0$, $p_0 \geq 2$ and if P is irreducible, then $(P, \mathcal{N})$ is a canonical number system in $\mathcal{R}$. Pethő [15] weakened the irreducibility condition by only assuming that no root of the polynomial is a root of unity.

Kovács and Pethő [12] provided necessary and sufficient conditions on the pair $(\beta, \mathcal{N})$ to be a number system in $\mathbb{Z}[\alpha]$. A decade later Akiyama and Pethő [1] significantly reduced the number of cases one has to check under the additional assumption that

$$\sum_{i=1}^{d} |p_i| < p_0.$$

Let us denote by ζ_k some primitive k-th root of unity. Since $+i$ and $-i$ are primitive fourth roots of unity, we can say that all the bases for the Gaussian integers are of the form $-m + \zeta_4$, with $m \geq 1$. Furthermore an easy computation shows that $-m + \zeta_3$ are bases in $\mathbb{Z}[\zeta_3]$ for $m \geq 1$. Thus our first result answers the question, whether $-m + \zeta_k$ is a basis in $\mathbb{Z}[\zeta_k]$.

Theorem 1.1. *Let $k > 2$ and m be positive integers. If $m \geq \phi(k) + 1$, then $\{-m + \zeta_k, \mathcal{N}\}$ is a canonical number system.*

Our second result considers, whether these bases are multiplicatively independent. We call two algebraic integers α and β multiplicatively independent, if $\alpha^p = \beta^q$ has only the solution $p = q = 0$ over the integers. Considering bases in the Gaussian integers Hansel and Safer [6] proved that $-m + i$ and $-n + i$ are multiplicative independent for all $m > n > 0$. Their motivation was a version of Cobham's theorem [4] for the Gaussian integers. Cobham's theorem states that a set $E \subset \mathbb{N}$ is m- and n-recognizable with m and n multiplicative independent integers if and only if the set E is a union of arithmetic progressions. This means that e.g. except for arithmetic progressions we are not able to deduce the base 3 expansion form the one in base 2.

In the present paper we want to generalize the result of Hansel and Safer [6] on the multiplicative independence to bases of $\mathbb{Z}[\zeta_k]$ of the form $-m + \zeta_k$ for $k \geq 3$.

Theorem 1.2. *Let $k \geq 3$ be a positive integer. Then the algebraic integers $-m+\zeta_k$ and $-n + \zeta_k$ are multiplicatively independent provided $m > n > C(k)$, where $C(k)$ is an effective computable constant depending on k.*

Moreover, if k is a power of $2, 3, 5, 6, 7, 11, 13, 17, 19$ or 23, then $-m + \zeta_k$ and $-n + \zeta_k$ are multiplicatively independent as long as $m > n > 0$.

In order to prove Theorem 1.2 one has to show that the Diophantine equation

$$(-m + \zeta_k)^p = (-n + \zeta_k)^q \tag{1.1}$$

has no solution (n, m, p, q), with $m > n > C(k)$ and p, q are not both zero. Taking norms in (1.1) we obtain $\Phi_k(m)^p = \Phi_k(n)^q$ and therefore the Diophantine equation (1.1) becomes

$$\Phi_k(m)^p = \eta^q, \tag{1.2}$$

where Φ_k is the k-th cyclotomic polynomial and $\eta = \Phi_k(n)$. In case that p and q have greatest common divisor $d > 1$ we take d-th roots and obtain equation (1.2) with p and q co-prime. Therefore we may assume that p and q are coprime and we deduce that η is a p-th power, i.e. we get an equation of the form $\Phi_k(m) = y^q$ with $y = \eta^{1/p}$. Note that since we assume $m, n > C(k)$ the case $\Phi_k(m) = -y^q$ can be excluded. Indeed, we know that $\Phi_k(m) > 0$ for m sufficiently large. In any case we obtain a Diophantine equation of the form

$$\Phi_k(m) = y^q. \tag{1.3}$$

Equation (1.3) is closely related to the well-studied Nagell-Ljunggren equation

$$\frac{x^k - 1}{x - 1} = y^q \qquad x, y > 1,\ q \geq 2,\ k > 2. \tag{1.4}$$

If k is a prime, then the Diophantine equations (1.3) and (1.4) are identical and every solution to (1.1) yields a solution to (1.4). Therefore we conjecture:

Conjecture 1.3. *Let k be an odd prime. Then $-m + \zeta_k$ and $-n + \zeta_k$ are multiplicatively independent provided $m > n > 0$.*

Since it is widely believed that the Nagell-Ljunggren equation (1.4) has only the three solutions

$$\frac{3^5 - 1}{3 - 1} = 11^2, \qquad \frac{7^4 - 1}{7 - 1} = 20^2, \qquad \frac{18^3 - 1}{18 - 1} = 7^3$$

this conjecture seems plausible. Note that none of these solutions to (1.4) implies a solution to (1.1). We guess that even more is true and believe that the following question has an affirmative answer.

Question 1.4. *Given $k > 2$ are $-m + \zeta_k$ and $-n + \zeta_k$ multiplicatively independent provided $m > n > 1$?*

We excluded the case that $n = 1$ since for $k = 6$ we have $-1 + \zeta_6 = \zeta_3$ and ζ_3 and $-m + \zeta_6$ are always multiplicatively dependent.

2. Canonical number systems and the proof of Theorem 1.1

The main tool in our proof is the following result due to Pethő [15].

Lemma 2.1 (Pethő [15, Theorem 7.1]). *Let $P = \sum_{j=0}^{d} p_j X^j \in \mathbb{Z}[X]$ with $p_d = 1$. If $0 < p_{d-1} \leq p_{d-2} \leq \cdots \leq p_0$, $p_0 \geq 2$ and no root of P is a root of unity, then the pair $(P, \mathcal{N})$ is a canonical number system.*

Since ζ_k is a primitive k-th root of unity $-m + \zeta_k$ is a root of $P(X) = \Phi_k(m + X)$. By Vieta's formula we obtain

$$p_{\phi(k)-d} = \tilde{p}_d = \sum_{a_1 < \cdots < a_d \in (\mathbb{Z}/k\mathbb{Z})^*} (m - \zeta_k^{a_1}) \cdots (m - \zeta_k^{a_d}). \tag{2.1}$$

Here we identify elements of $\mathbb{Z}/k\mathbb{Z}$ with their minimal representatives in $\mathbb{Z}$, i.e. with the integers in the set $\{0, 1, \ldots, k-1\}$ in the obvious way. In order to apply

Lemma 2.1 we have to prove that $\tilde{p}_d \leq \tilde{p}_{d+1}$. For a given ordered $(d+1)$-tuple $a_1 < \cdots < a_{d+1}$ there are $d+1$ possibilities to deduce an ordered d-tuple. Thus

$$\begin{aligned}(d+1) & \sum_{a_1<\cdots<a_{d+1}\in(\mathbb{Z}/k\mathbb{Z})^*} (m-\zeta_k^{a_1})\cdots(m-\zeta_k^{a_{d+1}}) \\ &= \sum_{a_1<\cdots<a_d\in(\mathbb{Z}/k\mathbb{Z})^*} (m-\zeta_k^{a_1})\cdots(m-\zeta_k^{a_d}) \sum_{\substack{b\in(\mathbb{Z}/k\mathbb{Z})^*\\ b\neq a_1,\ldots,a_d}} (m-\zeta_k^{b})\end{aligned}$$

Therefore we get for $d < \phi(k)$ that

$$\begin{aligned}\tilde{p}_{d+1} =& \sum_{a_1<\cdots<a_{d+1}\in(\mathbb{Z}/k\mathbb{Z})^*} (m-\zeta_k^{a_1})\cdots(m-\zeta_k^{a_{d+1}}) \\ =&\frac{1}{d+1}\sum_{a_1<\cdots<a_d\in(\mathbb{Z}/k\mathbb{Z})^*} (m-\zeta_k^{a_1})\cdots(m-\zeta_k^{a_d}) \sum_{\substack{b\in(\mathbb{Z}/k\mathbb{Z})^*\\ b\neq a_1,\ldots,a_d}} (m-\zeta_k^{b}) \\ =&\frac{m(\phi(k)-d)}{d+1}\sum_{a_1<\cdots<a_d\in(\mathbb{Z}/k\mathbb{Z})^*} (m-\zeta_k^{a_1})\cdots(m-\zeta_k^{a_d}) \\ &-\frac{1}{d+1}\sum_{a_1<\cdots<a_d\in(\mathbb{Z}/k\mathbb{Z})^*} (m-\zeta_k^{a_1})\cdots(m-\zeta_k^{a_d}) \sum_{\substack{b\in(\mathbb{Z}/k\mathbb{Z})^*\\ b\neq a_1,\ldots,a_d}} \zeta_k^{b} \\ \geq&\frac{\tilde{p}_d m(\phi(k)-d)}{d+1} \\ &-\frac{1}{d+1}\left|\sum_{a_1<\cdots<a_d\in(\mathbb{Z}/k\mathbb{Z})^*} (m-\zeta_k^{a_1})\cdots(m-\zeta_k^{a_d}) \sum_{\substack{b\in(\mathbb{Z}/k\mathbb{Z})^*\\ b\neq a_1,\ldots,a_d}} \zeta_k^{b}\right| \\ \geq&\frac{\tilde{p}_d m(\phi(k)-d)}{d+1} - \binom{\phi(k)}{d}\frac{(m+1)^d(\phi(k)-d)}{d+1}.\end{aligned}$$

Note that in the first four lines in the inequality above all the sums over complex terms yield indeed real numbers. Further the "$\geq$" signs are true due to the triangle inequality and trivial estimates of the form $m-1 \leq |m-\zeta_k^a| \leq m+1$. Furthermore, by (2.1) we have

$$(m+1)^d\binom{\phi(k)}{d} > \tilde{p}_d > (m-1)^d\binom{\phi(k)}{d}$$

and therefore

$$\binom{\phi(k)}{d}\frac{(m+1)^d}{\tilde{p}_d} < \left(\frac{m+1}{m-1}\right)^d = \left(1+\frac{2}{m-1}\right)^d < e^2,$$

where we used that $m-1 \geq \phi(k) > d$ by our assumption. Altogether we obtain the inequality

$$\tilde{p}_{d+1} \geq \frac{\tilde{p}_d(m-e^2)(\phi(k)-d)}{d+1}.$$

Thus the coefficients are increasing if

$$\frac{(m-e^2)(\phi(k)-d)}{d+1} \geq 1. \tag{2.2}$$

We split our considerations into two cases whether $d \leq \phi(k)-2$ or not.

- **Case 1:** $d \leq \phi(k)-2$**.** Together with our assumption that $m \geq \phi(k)+1$ we get that the coefficients $\tilde{p}_d$ up to $\tilde{p}_{\phi(k)-1}$ are increasing if
$$\frac{2(\phi(k)+1-e^2)}{\phi(k)-1} \geq 1.$$
Since $\phi(k)$ only takes positive values a simple calculation yields that this is the case for $\phi(k) \geq 2e^2-3 \approx 11.78$.
On the contrary, since $\phi(k)$ only takes even values except the value 1, we may assume $\phi(k) \leq 10$, which implies $d \leq 8$. Plugging this into (2.2) yields that the coefficients are increasing provided $m \geq e^2+\frac{9}{2} \approx 11.89$.
Finally computing all polynomials $\Phi_k(m+x)$ with $\phi(k)+1 \leq m \leq 11$ by aid of a computer algebra system we see that in any case the coefficients $\tilde{p}_d$ are increasing. In fact we only have to check 92 polynomials, which are certainly to many for writing them down.
- **Case 2:** $d = \phi(k)-1$**.** Thus we are left to show that $p_1 \geq p_0$, i.e.
$$\prod_{a\in(\mathbb{Z}/k\mathbb{Z})^*} (m-\zeta_k^a) \geq \sum_{b\in(\mathbb{Z}/k\mathbb{Z})^*} \prod_{\substack{a\in(\mathbb{Z}/k\mathbb{Z})^* \\ a\neq b}} (m-\zeta_k^a).$$
Since
$$1 \geq \frac{\phi(k)}{m-1} = \sum_{b\in(\mathbb{Z}/k\mathbb{Z})^*} \frac{1}{m-1} \geq \sum_{b\in(\mathbb{Z}/k\mathbb{Z})^*} \frac{1}{m-\zeta_k^b}$$
provided that $m \geq \phi(k)+1$, this case is settled too.

The next requirement, in order to apply Lemma 2.1, is to show that no root of $\Phi_k(m+X)$ is a root of unity. Since we assume $m \geq \phi(k)+1 \geq 3$. So all roots of $\Phi_k(m+X)$ have real part ≥ 2 and therefore cannot be roots of unity.

Finally we have to check that $p_0 \geq 2$. But by (2.1) we have $p_0 \geq (m-1)^{\phi(k)} \geq 2$ provided $m \geq 3$, which we assume.

Therefore $\Phi_k(X+m)$ satisfies all assumptions of Lemma 2.1 and Theorem 1.1 is proved.

Remark 1. In case that $m \leq \phi(k)-1$ we have $p_0 < p_1$ and an application of Lemma 2.1 is no longer possible. Indeed, we have
$$1 \leq \frac{\phi(k)}{m+1} = \sum_{b\in(\mathbb{Z}/k\mathbb{Z})^*} \frac{1}{m+1} < \sum_{b\in(\mathbb{Z}/k\mathbb{Z})^*} \frac{1}{m-\zeta_k^b}$$
and by the same arguments as in Case 2 above we obtain $p_0 < p_1$. In case that $m = \phi(k)$ both situations $p_1 \leq p_0$ and $p_1 > p_0$ occur. For instance, in case that $m = 11$ we have $p_1 \leq p_0$ but in case that $m = 12$ we have $p_1 < p_0$. Therefore in view of the method of proof Theorem 1.1 is best possible.

3. Multiplicative independence

Before we start with the proof of Theorem 1.1, let us note that if p and q have a common factor d then by taking d-th roots on both sides of equation (1.1) we obtain

$$\zeta_k^j(-m+\zeta_k)^p = (-n+\zeta_k)^q, \tag{3.1}$$

with $\gcd(p,q)=1$ and $0\le j<k$.

We start with the proof of the first statement of Theorem 1.2. In view of the discussion below Theorem 1.1 we consider the Diophantine equation

$$f(x)=y^q, \tag{3.2}$$

where f is a polynomial with rational coefficients and with at least two distinct roots. Obviously (1.3) fulfills these requirements as soon as $k>2$. Due to Schinzel and Tijdeman [16] (see also [17, Theorem 10.2]) we know that for all solutions (x,y,q) to (3.2) with $|y|>1$, q is bounded by an effectively computable constant depending only on f. In view of Theorem 1.2 we see that all solutions coming from (1.1) yield $y>1$ provided $n\neq 0$. But it is also well known (see e.g. [17, Theorem 6.1 and 6.2]) that for given $q\ge 2$ all solutions (x,y) to (3.2) satisfy $\max\{|x|,|y|\}<C_{f,q}$, where $C_{f,q}$ is an absolute, effectively computable constant depending on f and q. Thus we conclude that $q=1$ in equation (3.1) if $m,n>C(k)$, and $C(k)$ is an effectively computable constant only depending on k. Exchanging the roles of m and n we deduce that $q=p=1$ if $m,n>C(k)$. But this yields the equation $\zeta_k^j(-m+\zeta_k)=(-n+\zeta_k)$ and taking norms on both sides gives $\Phi_k(m)=\Phi_k(n)$. Since $\Phi_k(m)$ is strictly increasing for m large enough we deduce that $m=n$ which we excluded. Therefore the proof of the first part of Theorem 1.2 is complete.

However, computing the constant $C(k)$ using the methods cited above will yield very huge constants even for small values of k. Therefore we will use a more direct approach in the proof of the second part.

We note that $\Phi_n(X)=\Phi_{n/q}(X^{n/q})$ if $q^2|n$. In particular, if $n=q^\ell$ we have

$$\Phi_{q^\ell}(X)=\Phi_q\left(X^{q^{\ell-1}}\right). \tag{3.3}$$

Let us start with powers of 2. In this case we have that $\Phi_{2^\ell}(X)=X^{2^{\ell-1}}+1$. Therefore the case that k is a power of 2 is deduced from the fact that the Diophantine equation

$$X^2+1=Y^q$$

has no solution. This is a special case of Catalan's equation $X^p-Y^q=1$ which was completely solved by Mihăilescu [14]. Note that this special case was already proved by Chao [3].

In the next step we consider the case that k is a power of 3 or 6.

Lemma 3.1. *Let k be a power of 3 or 6. Then the two algebraic integers $-m+\zeta_k$ and $-n+\zeta_k$ are multiplicatively independent provided $n\neq m$ and $n,m\notin\{0,-1\}$.*

Proof. Let us consider equation (1.3) and let $M=m^{k/3}$ if $9|k$, $M=m^{k/6}$ if $36|k$ and $M=m$ otherwise. Then equation (1.3) turns into

$$M^2\pm M+1=\left(\frac{2M\pm 1}{2}\right)^2+\frac{3}{4}=Y^q,$$

where the "+" sign holds in case that k is a power of 3 and the "−" sign holds in case that k is a power of 6. Multiplying this equation by 4 and putting $X=2M\pm 1$ we get

$$X^2+3=4Y^q.$$

Due to Luca and Tengely [13] we know that $(X,Y,q)=(1,1,q)$ and $(37,7,3)$ are the only solutions with $X,Y,q\ge 1$. The first solution yields $m\in\{0,-1\}$ which we have excluded and the second solution yields $M = \pm 18$ or $M = \pm 19$. Since both, 18 and 19, are not perfect powers we conclude that $k = 3$ or $k = 6$. We may recover m and n from the substitutions that led to equation (1.3). Therefore we are left to check that in case that $k = 3$ equation (1.1) has no solution with $m = 18, -19$, $n = 2, -3$, $q = 3$ and $p = 1$ and in case that $k = 6$ equation (1.1) has no solution with $m = -18, 19$, $n = -2, 3$, $q = 3$ and $p = 1$. This is of course easily done e.g. by a computer. □

We are left to the case that k is a power of $5, 7, 11, 13, 17, 19$ or 23. Since every solution to (1.1) implies a solution to the Nagell-Ljunggren equation (1.4), the following results due to Bugeaud, Hanrot and Mignotte [2, Theorem 1 and 2] are essential in the proof of Theorem 1.1.

Theorem 3.2. *The Nagell-Ljunggren equation* (1.4) *has except the three solutions* $(x, y, k, q) = (3, 11, 5, 2), (7, 20, 4, 2), (18, 7, 3, 3)$ *no further solution in case that*

- *k is a multiple of $5, 7, 11$ or 13, or*
- *k is a multiple of $17, 19$ or 23 and $q \neq 17, 19$ or 23 respectively.*

Since the identity (3.3), we get in case that $k = P^\ell$ is a prime power

$$\Phi_k(X) = \frac{\left(X^{P^{\ell-1}}\right)^P - 1}{\left(X^{P^{\ell-1}}\right) - 1} = \frac{x^P - 1}{x - 1}$$

with $x = X^{P^{\ell-1}}$. If we assume now that $P = 5, 7, 11$ or 13 the only possible solutions to (3.1) imply that $q = 1$. Exchanging the role of m and n we also obtain $p = 1$ and equation (3.1) turns into

$$\zeta_k^j(-m + \zeta_k) = -n + \zeta_k.$$

Taking norms yields

$$\frac{m^k - 1}{m^{k/q} - 1} = \frac{n^k - 1}{n^{k/q} - 1},$$

hence $m = n$, which we excluded. Therefore the we are left to the case that k is a power of $17, 19$ or 23.

Before we consider the remaining cases we want to remind the reader that an integral basis for $\mathbb{Z}[\zeta_k]$ is given by $\{1, \zeta_k, \dots, \zeta_k^{\phi(k)-1}\}$ and therefore every algebraic integer $\alpha \in \mathbb{Z}[\zeta_k]$ has a unique representation of the form

$$\alpha = \sum_{i=0}^{\phi(k)-1} a_i \zeta_k^i, \tag{3.4}$$

with $a_i \in \mathbb{Z}$ for $0 \leq i < \phi(k)$. In the following we will expand the left and right side of equation (3.1) in various cases and bring the result into the unique form (3.4). We will show below that on the left and right side of (3.1) the unique representations (3.4) do not match and conclude that no solution to (3.1) and hence no solution to (1.1) exists.

Assume that (3.1) has a solution (m, n, p, q, j). In case that k is a power of $17, 19$ or 23 Theorem 3.2 implies that the only prime divisors of p and q in equation (1.1) are $17, 19$ or 23 respectively. Therefore we are left to equation (3.1), with $p = 1$

and $q = 17, 19$ or 23. Note that in case of $k = q$ we have

$$\begin{aligned}(-n+\zeta_k)^k &= \sum_{i=0}^{k}(-n)^{k-i}\binom{k}{i}\zeta_k^i \\ &= \sum_{i=0}^{k-2}\left((-n)^{k-i}\binom{k}{i}+kn\right)\zeta_k^i + 1 = \sum_{i=0}^{k-2} p_{k,i}(n)\zeta_k^i.\end{aligned}$$

Let us assume that $0 \leq j < k-2$. Then with $p = 1$ and $k = q$, either the coefficients $p_{k,0}(n)$ and $p_{k,1}(n)$ have to vanish simultaneously or the coefficients $p_{k,3}(n)$ and $p_{k,4}(n)$ vanish simultaneously. Since

$$\gcd(p_{17,0}(n), p_{17,1}(n)) = \gcd(-n^{17}+17n+1, 17n^{16}+17n) = 1$$

as polynomials in n, the coefficients cannot vanish simultaneously. Similarly we obtain

$$\begin{gathered}\gcd(p_{19,0}(n), p_{19,1}(n)) = \gcd(p_{23,0}(n), p_{23,1}(n)) = 1 \\ \gcd(p_{17,3}(n), p_{17,4}(n)) = 17n, \quad \gcd(p_{19,3}(n), p_{19,4}(n)) = 19n, \\ \gcd(p_{23,3}(n), p_{23,4}(n)) = 23n,\end{gathered}$$

where we consider the gcd taken over the polynomial ring $\mathbb{Z}[n]$. Therefore we deduce $n = 0$, a solution which we excluded.

Now consider the case that $k = q$ and $j = k-2$. In this case equation (3.1) turns into

$$-(m+1) - \zeta_k - \cdots - \zeta_k^{k-2} = (-n+\zeta_k)^k = \sum_{i=0}^{k-2} p_{k,i}(n)\zeta_k^i.$$

Considering the coefficient of ζ_k we have

$$-1 = -kn(1+n^{k-2})$$

which cannot hold if $n > 1$. Similarly for $k = j-1$ we obtain

$$(m+1) + m\zeta_k + \cdots + m\zeta_k^{k-2} = (-n+\zeta_k)^k = \sum_{i=0}^{k-2} p_{k,i}(n)\zeta_k^i.$$

And in particular the coefficients of ζ_k and ζ_k^2 have to be equal, i.e.

$$-nk - kn^{k-1} = \frac{k(k-1)n^2}{2} - kn^{k-1},$$

or equivalently

$$0 = nk(nk - n + 2).$$

The last equation can only hold if n or k is zero or $nk - n + 2 = 0$ which implies $k = 0$ and $n = 2$. Since all these options are excluded this case cannot occur.

Now let us consider the case that $k = q^\ell$, with $\ell > 1$, and $q = 17, 19$ or 23. If $j < \phi(k) - 1$ in (3.1) then all coefficients ζ_k^i with $0 \leq i < \phi(k)$ of $\zeta_k^j(-m+\zeta_k)$ vanish except exactly two. Indeed we have

$$\zeta_k^j(-m+\zeta_k) = -m\zeta_k^j + \zeta_k^{j+1}.$$

On the right side of (3.1) all the coefficients of ζ_k^i with $0 \leq i \leq q$ do not vanish, i.e. a contradiction.

In case that $j=\phi(k)+r$ for some $0 \leq r < k-\phi(k)-1 = q^{\ell-1}-1$ we have

$$
\begin{aligned}
(-m+\zeta_k)\zeta_k^j &= (-m+\zeta_k)\left(-\zeta_k^r-\zeta_k^{r+q^{\ell-1}}-\zeta_k^{r+2q^{\ell-1}}-\cdots-\zeta_k^{r+(q-2)q^{\ell-1}}\right)\\
&= -m\zeta_k^r+\zeta_k^{r+1}-\cdots-m\zeta_k^{r+(q-2)q^{\ell-1}}+\zeta_k^{r+1+(q-2)q^{\ell-1}}
\end{aligned}
$$

i.e. there exist non vanishing coefficients of ζ_k^i with $i>q$. But on the right side of (3.1) all coefficients of ζ_k^i vanish for $i>q$ and again no solution is possible.

We are left to the two cases that $j=\phi(k)-1$ and $j=k-1$. In both cases it is easy to see that $\zeta_k^j(-m+\zeta_k)$ has non vanishing coefficients of ζ_k^i for $i>q$ and we deduce again a contradiction.

Acknowledgment

The authors want to thank Shigeki Akiyama (University of Tsukuba) for pointing them to the refinement of Pethő [15, Theorem 7.1].

References

[1] S. Akiyama and A. Pethő. On canonical number systems. *Theoret. Comput. Sci.*, 270(1-2):921–933, 2002.
[2] Y. Bugeaud, G. Hanrot, and M. Mignotte. Sur l'équation diophantienne $(x^n-1)/(x-1)=y^q$. III. *Proc. London Math. Soc. (3)*, 84(1):59–78, 2002.
[3] K. Chao. On the Diophantine equation $x^2=y^n+1$, $xy\neq 0$. *Sci. Sinica*, 14:457–460, 1965.
[4] A. Cobham. Uniform tag sequences. *Math. Systems Theory*, 6:164–192, 1972.
[5] W. J. Gilbert. Radix representations of quadratic fields. *J. Math. Anal. Appl.*, 83(1):264–274, 1981.
[6] G. Hansel and T. Safer. Vers un théorème de Cobham pour les entiers de Gauss. *Bull. Belg. Math. Soc. Simon Stevin*, 10(suppl.):723–735, 2003.
[7] I. Kátai and B. Kovács. Kanonische Zahlensysteme in der Theorie der quadratischen algebraischen Zahlen. *Acta Sci. Math. (Szeged)*, 42(1-2):99–107, 1980.
[8] I. Kátai and B. Kovács. Canonical number systems in imaginary quadratic fields. *Acta Math. Acad. Sci. Hungar.*, 37(1-3):159–164, 1981.
[9] I. Kátai and J. Szabó. Canonical number systems for complex integers. *Acta Sci. Math. (Szeged)*, 37(3-4):255–260, 1975.
[10] D. E. Knuth. *The art of computer programming. Vol. 2*. Addison-Wesley Publishing Co., Reading, Mass., second edition, 1981. Seminumerical algorithms, Addison-Wesley Series in Computer Science and Information Processing.
[11] B. Kovács. Canonical number systems in algebraic number fields. *Acta Math. Acad. Sci. Hungar.*, 37(4):405–407, 1981.
[12] B. Kovács and A. Pethő. Number systems in integral domains, especially in orders of algebraic number fields. *Acta Sci. Math. (Szeged)*, 55(3-4):287–299, 1991.
[13] F. Luca, S. Tengely, and A. Togbé. On the Diophantine equation $x^2+C=4y^n$. *Ann. Sci. Math. Québec*, 33(2):171–184, 2009.
[14] P. Mihăilescu. Primary cyclotomic units and a proof of Catalan's conjecture. *J. Reine Angew. Math.*, 572:167–195, 2004.
[15] A. Pethő. On a polynomial transformation and its application to the construction of a public key cryptosystem. In *Computational number theory (Debrecen, 1989)*, pages 31–43. de Gruyter, Berlin, 1991.
[16] A. Schinzel and R. Tijdeman. On the equation $y^m=P(x)$. *Acta Arith.*, 31(2):199–204, 1976.
[17] T. N. Shorey and R. Tijdeman. *Exponential Diophantine equations*, volume 87 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 1986.

Manfred Madritsch
1. Université de Lorraine, Institut Elie Cartan de Lorraine, UMR 7502, Vandoeuvre-lès-Nancy, F-54506, France;
2. CNRS, Institut Elie Cartan de Lorraine, UMR 7502, Vandoeuvre-lès-Nancy, F-54506, France
E-mail address: manfred.madritsch@univ-lorraine.fr

Volker Ziegler
Johann Radon Institute for Computational and Applied Mathematics (RICAM)
Austrian Academy of Sciences
Altenbergerstr. 69
A-4040 Linz, Austria
E-mail address: volker.ziegler@ricam.oeaw.ac.at