

## About the number of $\tau$ -numbers relative to polynomials with integer coefficients

MART ABEL, HELENA LAUER, AND ELLEN REDI

ABSTRACT. We show that for all polynomials  $Q(x)$  with integer coefficients, that satisfy the extra condition  $|Q(0) \cdot Q(1)| \neq 1$ , there are infinitely many positive integers  $n$  such that  $n$  is a  $\tau$ -number relative to the polynomial  $Q(x)$ . We also find some examples of polynomials  $Q(x)$  for which 1 is the only  $\tau$ -number relative to the polynomial  $Q(x)$  and some examples of polynomials  $Q(x)$  with  $|Q(0) \cdot Q(1)| = 1$ , which have infinitely many positive integers  $n$  such that  $n$  is a  $\tau$ -number relative to the polynomial  $Q(x)$ . In addition, we prove one result about the generators of a  $\tau$ -number.

### 1. Introduction

The subset of positive integers called  $\tau$ -numbers was introduced by Kennedy and Cooper in [2] in 1990. They showed that the natural density of the set of  $\tau$ -numbers is zero and asked about the characterization of  $\tau$ -numbers. In 1999, Colton rediscovered the  $\tau$ -numbers in [1], calling them refactorable numbers. He studied the distribution of  $\tau$ -numbers that are smaller than a certain fixed real number  $x$  and formulated a conjecture on it, related to the distribution of prime numbers. In 2002, in the attempt of proving Colton's Conjecture, Zelinsky checked in [8] that this conjecture is valid under some extra assumptions, proved several other properties of the distribution of  $\tau$ -numbers and introduced several new generalizations, like the notion of a  $\tau$ -number relative to a polynomial  $Q(x) \in \mathbb{Z}[x]$  or the notion of an anti- $\tau$ -number. The present paper is concerned with the topics studied by Zelinsky, more precisely with Zelinsky's Theorems 34 and 54.

---

Received October 8, 2020.

2020 *Mathematics Subject Classification*. Primary 11A07; Secondary 11C08.

*Key words and phrases*.  $\tau$ -numbers, polynomials with integer coefficients, number of divisors, anti- $\tau$ -numbers,  $\tau$ -numbers relative to polynomials, generators of a  $\tau$ -number.

<https://doi.org/10.12697/ACUTM.2021.25.07>

Corresponding author: Mart Abel

Let us first recall some definitions needed in the following. Most of these definitions can be found in several books and papers about  $\tau$ -numbers and number theory (e.g., [1], [3], [5], [8]).

A positive integer  $n$  is called a  $\tau$ -number, if the number  $\tau(n)$  of positive divisors of  $n$  divides  $n$  (in short,  $\tau(n) \mid n$ ), i.e., if  $n \equiv 0 \pmod{\tau(n)}$ .

A positive number  $n$  is called an *anti- $\tau$ -number*, if  $n$  and  $\tau(n)$  are coprime, that is  $(n, \tau(n)) = \gcd(n, \tau(n)) = 1$ .

Let  $m$  be a non-negative integer and  $Q(x) = a_m x^m + \dots + a_1 x + a_0$  a polynomial with integer coefficients  $a_0, \dots, a_m$  (in short,  $Q(x) \in \mathbb{Z}[x]$ ). A positive integer  $n$  is said to be a  $\tau$ -number relative to the polynomial  $Q(x)$ , if  $Q(n)$  is divisible by  $\tau(n)$  (in short,  $\tau(n) \mid Q(n)$ ), i.e., if  $Q(n) \equiv 0 \pmod{\tau(n)}$ . A positive integer  $n$  is said to be an *anti- $\tau$ -number relative to the polynomial  $Q(x)$* , if  $(Q(n), \tau(n)) = 1$ .

A  $\tau$ -number  $n$  is called a  $p$ -generator, if for any prime  $p$  with  $(n, p) = 1$ , the number  $np$  is a  $\tau$ -number. If  $n$  is a  $\tau$ -number,  $p$  is a prime,  $(n, p) = 1$  and  $np$  is also a  $\tau$ -number, then it is said that  $n$  is a generator of  $np$ .

For fixed positive integers  $k, a_1, \dots, a_k$ , a positive number  $n$  is called an  $(a_1, \dots, a_k)$ -generator, if for all  $k$ -tuples of distinct primes  $(p_1, \dots, p_k)$  which do not divide  $n$ , the number  $np_1^{a_1} \cdot \dots \cdot p_k^{a_k}$  is a  $\tau$ -number.

For a positive integer  $n$ , the number of distinct sets of positive integers greater than 1 such that the product of all the elements of the set is  $n$ , is denoted by  $h(n)$ . For example,  $h(1) = 0$ , because 1 cannot be represented as a product of positive integers greater than 1;  $h(2) = 1$ , because  $\{2\}$  is the only suitable set of positive integers greater than 1 such that the product of all integers in this set is 2;  $h(4) = 2$ , because the suitable sets are  $\{4\}$  and  $\{2, 2\}$ ;  $h(6) = 2$ , because the suitable sets are  $\{6\}$  and  $\{2, 3\}$ ;  $h(8) = 3$ , because the suitable sets are  $\{8\}$ ,  $\{2, 4\}$  and  $\{2, 2, 2\}$ , etc.

*Dirichlet's theorem* (on arithmetic progressions) says that for any coprime  $a \in \mathbb{Z}$  and  $b \in \mathbb{Z}^+$ , there are infinitely many primes  $p$  in the form  $p = a + kb$ , where  $k \in \mathbb{Z}^+$ . In other words, these primes  $p \equiv a \pmod{b}$ .

*Fermat's little theorem* says that if prime  $p$  does not divide  $a$ , then  $a^{p-1} \equiv 1 \pmod{p}$ .

The term " $\tau$ -number relative to a polynomial  $Q(x)$ " was introduced by Zelinsky in [8]. This was a natural generalization, prepared by many papers on  $\tau$ -numbers relative to arithmetic functions  $f : \mathbb{Z}[x] \rightarrow \mathbb{A}$ , where  $\mathbb{A}$  is the field of algebraic numbers. From the results of C. A. Spiro in 1985, we know that there are infinitely many  $\tau$ -numbers relative to  $I(x) = x$  (see [7]) and to  $S(x) = x + 1$  (see [6]). J. Zelinsky stated the same for  $C_k(x) = k$  (see [8], Conjecture 53), but proved it only partially.

F. Luca studied upper bounds for the number of  $0 < n \leq x$  with  $\tau(n) \mid f(n)$ , where  $f(x) \in \mathbb{Q}[x]$ . The main result of the paper [4] is that such count is  $o(x)$ , so "most numbers" are not  $\tau$ -numbers relative to any

fixed polynomial. Moreover, J. Zelinsky formulated in 2002 the following two statements:

- 1) For any  $Q(x) \in \mathbb{Z}[x]$  there exists infinitely many  $n$  such that  $\tau(n) \mid Q(n)$  (see [8], Theorem 54).
- 2) Apart from the order of the exponents, any given tau number  $n$  has  $\sum_{d \mid (n/\tau(n))} h(d)$  generators (see [8], Theorem 34 d)).

Unfortunately, the proofs of these two results were wrong (it has been understood by several mathematicians, for example in [3]).

What concerns the proof of the first statement by Zelinsky, then it is true that  $\tau(p^{Q(c)-1}) = Q(c)$  and  $Q(c) \mid Q(p)$ , but what we actually needed in this proof, is that  $\tau(p^{Q(c)-1}) \mid Q(p^{Q(c)-1})$ . Unfortunately, this is not true, in general.

What concerns the second statement of Zelinsky, then we have a counterexample. The  $\tau$ -number 80 is (1)-generator, (1,1)-generator, (1,1,1)-generator, (3)-generator, (3,1)-generator and (7)-generator and  $\sum_{d \mid (80/\tau(80))} h(d) = h(2) + h(4) + h(8) = 1 + 2 + 3 = 6$ , i.e., 80 is an  $(a_1, \dots, a_k)$ -generator for  $\sum_{d \mid (80/\tau(80))} h(d)$  different  $k$ -tuples  $(a_1, \dots, a_k)$  of numbers, but there are no generators of 80.

Our paper is mainly concerned with proving the first statement of Zelinsky in case  $|Q(0) \cdot Q(1)| \neq 1$  and reformulating the second statement of Zelinsky in a way it could be proved, as it is demonstrated in the present paper.

The main results of the present paper are Theorems 1, 2, and 4.

## 2. On the number of $\tau$ -numbers

At first, let us notice that, for any prime  $p$ , positive integer  $k$  and all primes  $q \neq p$ , the equality  $\tau(q^{p^k-1}) = p^k$  holds, i.e., there are infinitely many  $\tau$ -numbers relative to  $Q(x) = p^k$ . As  $\tau$ -function is multiplicative, it holds that there are infinitely many  $\tau$ -numbers relative to all constant polynomials  $Q(x) = a$ , where  $a \notin \{0, \pm 1\}$ .

**Lemma 1.** Assume that  $Q(x) = Q_1(x)^{e_1} \cdot \dots \cdot Q_t(x)^{e_t} \in \mathbb{Z}[x]$ , where  $t$  is a positive integer and  $Q_1(x), \dots, Q_t(x) \in \mathbb{Z}[x]$  are pairwise different polynomials. Then the following two statements hold:

- 1) if  $n \in \mathbb{Z}^+$  is a  $\tau$ -number relative to some  $Q_i(x)$ , where  $i \in \{1, \dots, t\}$ , then  $n$  is a  $\tau$ -number relative to  $Q(x)$ ;
- 2) if  $n \in \mathbb{Z}^+$  is not a  $\tau$ -number relative to  $Q(x)$ , then  $n$  is not a  $\tau$ -number relative to any  $Q_i(x)$  where  $i \in \{1, \dots, t\}$ .

*Proof.* 1) Let  $n$  be a  $\tau$ -number relative to some  $Q_i(x)$  with  $i \in \{1, \dots, t\}$ , i.e.,  $\tau(n) \mid Q_i(n)$ . Then  $\tau(n) \mid (Q_1(n)^{e_1} \cdot \dots \cdot Q_t(n)^{e_t}) = Q(n)$ , i.e.,  $n$  is a  $\tau$ -number relative to  $Q(x)$ .

2) Suppose that  $n$  is not a  $\tau$ -number relative to  $Q(n)$ , i.e.,  $\tau(n)$  does not divide  $Q(n) = Q_1(n)^{e_1} \cdot \dots \cdot Q_t(n)^{e_t}$ . Then it is clear that  $\tau(n)$  cannot divide

$Q_i(n)$  for any  $i \in \{1, \dots, t\}$ , because otherwise we would get by part 1) that  $n \mid Q(n)$ , which is false. Hence,  $n$  is not a  $\tau$ -number relative to any  $Q_i(x)$  where  $i \in \{1, \dots, t\}$ .  $\square$

*Remark 1.* If one could show that for every non-constant irreducible polynomial  $Q(x) \in \mathbb{Z}[x]$  there are infinitely many  $\tau$ -numbers relative to  $Q(x)$ , then, by Lemma 1, we would obtain that there are infinitely many  $\tau$ -numbers relative to every non-constant polynomial, because every non-constant polynomial is representable as a product of irreducible non-constant polynomials.

Using Lemma 1 and the comments before Lemma 1, we obtain the following result.

**Corollary 1.** *There are infinitely many  $\tau$ -numbers relative to  $Q(x) \in \mathbb{Z}[x]$  if at least one of the following conditions holds:*

- 1)  $Q(x)$  is not primitive (i.e., the greatest common divisor of its coefficients is  $a > 1$ );
- 2)  $Q(x)$  is non-constant and  $Q(0) = 0$ ;
- 3)  $Q(x)$  is non-constant and  $Q(1) = 0$ .

*Proof.* These follow from Lemma 1. Indeed, in case 1), we can write  $Q(x) = aQ_2(x)$  where  $a > 1$ , and there are infinitely many  $\tau$ -numbers for  $Q_1(x) = a$ , as it was noted before Lemma 1.

In case 2), we can write  $Q(x) = xQ_2(x)$ . For any  $\tau$ -number  $n$ , it is true that  $\tau(n) \mid n \mid nQ_2(n) = Q(n)$ . It is known that there are infinitely many  $\tau$ -numbers (e.g.,  $p^{p-1}$  with prime  $p$ ). So, there are infinitely many  $\tau$ -numbers relative to  $Q(x)$ .

In case 3), we can write  $Q(x) = (x-1)Q_2(x)$ . Let  $p < q$  be arbitrary primes. Then (by Fermat's little theorem)  $p \mid (q^{p-1} - 1)$ . Set  $n = q^{p-1}$ . Then we have  $\tau(n) = p \mid (q^{p-1} - 1) = (n-1) \mid (n-1)Q_2(n) = Q(n)$  and there are infinitely many such integers  $n$ .  $\square$

Next, we study the case, where  $|Q(0)| > 1$ .

**Lemma 2.** *If  $Q(x) \in \mathbb{Z}[x]$  and  $|Q(0)| = v > 1$ , then there are infinitely many  $\tau$ -numbers relative to  $Q(x)$ .*

*Proof.* Let  $p$  be a prime factor of  $v$  which exists since  $v > 1$ . Set  $T(x) := Q(x^{p-1})$ . It is known (see, for example, [5], E.1.2.5) that the set of prime factors of values of  $T(n)$  is infinite as  $n$  runs over positive integers. So, there exist some  $w \in \mathbb{Z}^+$  and a prime  $r > v$  so that  $r \mid T(w) \mid Q(w^{p-1})$ .

Clearly,  $r$  does not divide  $w$ , since from  $r \mid w$  and  $r \mid Q(w^{p-1})$ , we would get  $r \mid v$ , which is false. Choose a prime  $q$  so that  $r < q \equiv w \pmod{r}$ . There are infinitely many of them, by Dirichlet's theorem. Take  $n = p^{r-1}q^{p-1}$ . Then  $\tau(n) = rp$ . Since  $p \mid v$ , we have  $p \mid Q(n)$ . Since  $r > v > p$ , we get by Fermat's little theorem that  $p^{r-1} \equiv 1 \pmod{r}$ . Hence,  $Q(n) \equiv Q(w^{p-1}) \equiv 0 \pmod{r}$ , showing that  $rp \mid Q(n)$ , i.e.,  $\tau(n) \mid Q(n)$ .  $\square$

Next, we study the case, where  $|Q(1)| > 1$ .

**Lemma 3.** *If  $Q(x) \in \mathbb{Z}[x]$  and  $|Q(1)| > 1$ , then there are infinitely many  $\tau$ -numbers relative to  $Q(x)$ .*

*Proof.* As  $|Q(1)| > 1$ , then  $(|Q(1)|, 1) = 1$ . Take any prime  $p \equiv 1 \pmod{|Q(1)|}$ . There are infinitely many of them, by Dirichlet's theorem. Set  $n = p^{|Q(1)|-1}$ . Then  $n = p^{|Q(1)|-1} \equiv 1 \pmod{|Q(1)|}$  and  $Q(n) = Q(p^{|Q(1)|-1}) \equiv Q(1) = 0 \pmod{|Q(1)|}$ . Clearly,  $\tau(n) = |Q(1)|$ , so we have  $Q(n) \equiv 0 \pmod{\tau(n)}$ . All these integers  $n = p^{|Q(1)|-1} \equiv 1$  are  $\tau$ -numbers relative to  $Q(x)$  and there are infinitely many of them, since the exponent  $|Q(1)| > 0$ . Hence, there are infinitely many  $\tau$ -numbers relative to  $Q(x)$ .  $\square$

We can have a corollary for the special case of some cyclotomic polynomials (see also the example after the corollary).

**Corollary 2.** *There are infinitely many  $\tau$ -numbers relative to cyclotomic polynomial  $\Phi_{p^k}(x) = x^{p^{k-1}(p-1)} + x^{p^{k-1}(p-2)} + \dots + x^{p^{k-1}} + 1$  with prime  $p$ .*

*Proof.* It is a partial case of Lemma 3 for cyclotomic polynomial  $\Phi_{p^k}(x)$ , because  $\Phi_{p^k}(1) = p > 1$ .  $\square$

**Example 1.** In the increasing order of degrees, the first cyclotomic polynomials with index  $p^k$  for some prime  $p$  are:  $\Phi_2(x) = x+1$ ,  $\Phi_3(x) = x^2+x+1$ ,  $\Phi_4(x) = x^2+1$ ,  $\Phi_5(x) = x^4+x^3+x^2+x+1$ ,  $\Phi_7(x) = x^6+x^5+\dots+x+1$ ,  $\Phi_8(x) = x^4+1$ ,  $\Phi_9(x) = x^6+x^3+1$ ,  $\Phi_{11}(x) = x^{10}+x^9+\dots+x+1$ ,  $\Phi_{13}(x) = x^{12}+\dots+x+1$ ,  $\Phi_{16}(x) = x^8+1$ , etc.

Now we are ready to prove our first theorem.

**Theorem 1.** *If  $Q(x) \in \mathbb{Z}[x]$  and  $|Q(0) \cdot Q(1)| \neq 1$ , then there are infinitely many  $\tau$ -numbers relative to  $Q(x)$ .*

*Proof.* Notice, that the condition  $|Q(0) \cdot Q(1)| \neq 1$  is equivalent to the condition that either  $|Q(0)| \neq 1$  or  $|Q(1)| \neq 1$ . In case we have a constant polynomial  $Q(x) = 0$ , then every positive integer  $n$  is a  $\tau$ -number relative to  $Q(x)$ , because  $Q(n) = 0 \equiv 0 \pmod{\tau(n)}$  for every integer  $n > 0$ . We will go through all other different allowed values of  $Q(0)$  and  $Q(1)$ .

- a) If  $Q(x)$  is non-constant and  $Q(0) = 0$ , then the claim follows from Corollary 1, case 2).
- b) If  $Q(x)$  is non-constant and  $Q(1) = 0$ , then the claim follows from Corollary 1, case 3).
- c) If  $|Q(0)| > 1$ , then the claim follows from Lemma 2.
- d) If  $|Q(1)| > 1$ , then the claim follows from Lemma 3.  $\square$

### 3. Results concerning anti- $\tau$ -numbers

**Theorem 2.** *There are infinitely many anti- $\tau$ -numbers relative to any  $Q(x) \in \mathbb{Z}[x]$  except for the constant polynomial  $Q(x) = 0$ .*

*Proof.* In case we have a constant polynomial  $Q(x) = c$  and  $c \neq 0$ , then  $n = p^{|c|}$  is an anti- $\tau$ -number relative to  $Q(x)$  for any prime  $p$ .

Let us assume that  $Q(x) = a_d x^d + \dots + a_0$  and  $d > 0$ . Choose large primes  $q_1, q_2$  such that both are larger than the maximum of numbers  $2d+1, |a_d|, |a_0|$  and such that  $(q_1 - 1, q_2 - 1) = 2$ . There are  $(q_1 - 1)/2$  quadratic residues modulo  $q_1$  and they cannot all be roots of  $Q(x) \pmod{q_1}$ , as  $d < (q_1 - 1)/2$ . So, we can choose  $r_1 \in \{1, \dots, q_1 - 1\}$  such that  $Q(r_1^2) \not\equiv 0 \pmod{q_1}$ . Similarly, we can choose  $r_2 \in \{1, \dots, q_2 - 1\}$  such that  $Q(r_2^2) \not\equiv 0 \pmod{q_2}$ .

Since  $((q_1 - 1)/2, (q_2 - 1)/2) = 1$ , the number  $(q_1 - 1)/2$  is invertible modulo  $(q_2 - 1)/2$  and vice-versa. So, there is  $u_1 \in \mathbb{Z}^+$  such that

$$u_1(q_1 - 1)/2 \equiv 1 \pmod{(q_2 - 1)/2}$$

(from which we get  $u_1(q_1 - 1) \equiv 2 \pmod{(q_2 - 1)}$ ). Choose a prime  $p_1 \equiv r_2^{u_1} \pmod{q_2}$ .

Similarly, choose a prime  $p_2 \equiv r_1^{u_2} \pmod{q_1}$ , where  $u_2(q_2 - 1)/2 \equiv 1 \pmod{(q_1 - 1)/2}$ . Then  $u_2(q_2 - 1) \equiv 2 \pmod{(q_1 - 1)}$ .

Consider the integer  $n = p_1^{q_1 - 1} p_2^{q_2 - 1}$ . Clearly,  $p_1^{q_1 - 1} \equiv 1 \pmod{q_1}$  (by Fermat's little theorem) and  $p_2^{q_2 - 1} \equiv r_1^{u_2(q_2 - 1)} \equiv r_1^2 \pmod{q_1}$ , since the exponents are equivalent modulo  $q_1 - 1$ . Thus,  $n = p_1^{q_1 - 1} p_2^{q_2 - 1} \equiv r_1^2 \pmod{q_1}$ , which implies  $Q(n) \equiv Q(r_1^2) \not\equiv 0 \pmod{q_1}$ . Hence,  $q_1 \nmid Q(n)$ . Similarly we get that  $q_2 \nmid Q(n)$ . So  $Q(n)$  is coprime with  $q_1 q_2 = \tau(n)$ . Since there are infinitely many possibilities for choosing primes  $p_1$  and  $p_2$ , there are infinitely many anti- $\tau$ -numbers  $n = p_1^{q_1 - 1} p_2^{q_2 - 1}$  relative to  $Q(x)$ .  $\square$

Next, let us describe some relations between the  $\tau$ -numbers relative to some polynomial and anti- $\tau$ -numbers.

**Lemma 4.** *Suppose that  $Q(x) \in \mathbb{Z}[x]$  is such that  $Q(0) \in \{-1, 1\}$ . If  $n \in \mathbb{Z}^+$  is a  $\tau$ -number relative to  $Q(x)$ , then  $n$  is an anti- $\tau$ -number.*

*Proof.* It is clear that  $n = 1$  is an anti- $\tau$ -number.

Let  $n > 1$  be an arbitrary positive integer, which is not an anti- $\tau$ -number. Then  $(n, \tau(n)) > 1$  and there exists some prime  $p$  such that  $p | n$  and  $p | \tau(n)$ .

Set  $Q(x) - Q(0) = xT(x)$ . Then  $Q(n) = nT(n) + Q(0) = nT(n) \pm 1$ . Clearly,  $n \nmid Q(n)$ . Therefore,  $p \nmid Q(n)$  and  $\tau(n) \nmid Q(n)$ , as well. So  $n$  cannot be a  $\tau$ -number relative to  $Q(x)$ . Hence, any  $\tau$ -number relative to  $Q(x)$  must be an anti- $\tau$ -number.  $\square$

The following proposition helps us to say something about the total number of  $\tau$ -numbers relative to a polynomial with integer coefficients.

**Proposition 1.** *Let  $Q(x) \in \mathbb{Z}[x]$ . If there exists an anti- $\tau$ -number  $n > 1$  which is a  $\tau$ -number relative to  $Q(x)$ , then there are infinitely many such anti- $\tau$ -numbers, which are  $\tau$ -numbers relative to  $Q(x)$ .*

*Proof.* Let  $n > 1$  be an anti- $\tau$ -number which is a  $\tau$ -number relative to  $Q(x)$ . Then  $(n, \tau(n)) = 1$  and  $\tau(n) \mid Q(n)$ . As  $n > 1$ , we can consider its canonical form  $n = p_1^{t_1} \cdot \dots \cdot p_k^{t_k}$  where  $k \geq 1$ , primes  $p_1, \dots, p_k$  are pairwise different and  $t_1, \dots, t_k \in \mathbb{Z}^+$ . Then  $\tau(n) = (t_1 + 1) \cdot \dots \cdot (t_k + 1)$ . Since  $(\tau(n), n) = 1$ , then also  $(\tau(n), p_i) = 1$  for each  $i \in \{1, \dots, k\}$ . By Dirichlet's theorem, there are infinitely many different primes

- 1)  $q_1$  such that  $q_1 \equiv p_1 \pmod{\tau(n)}$ ;
- .....
- k)  $q_k$  such that  $q_k \equiv p_k \pmod{\tau(n)}$ .

Set  $m = q_1^{t_1} \cdot \dots \cdot q_k^{t_k}$  for some  $k$ -tuple of pairwise different primes  $(q_1, \dots, q_k)$  that satisfy conditions 1) - k), respectively. Then

$$\tau(m) = (t_1 + 1) \cdot \dots \cdot (t_k + 1) = \tau(n),$$

$(m, \tau(m)) = 1$  (i.e.,  $m$  is an anti- $\tau$ -number),  $m \equiv n \pmod{\tau(n)}$  and  $Q(m) \equiv Q(n) \equiv 0 \pmod{\tau(n)}$ , because  $\tau(n)$  divides  $Q(n)$ . Hence,  $\tau(m) = \tau(n)$  divides also  $Q(m)$ . With that, we have constructed infinitely many anti- $\tau$ -numbers  $m$ , which are  $\tau$ -numbers relative to  $Q(x)$ .  $\square$

*Remark 2.* By Lemma 4 and Proposition 1, we can now say that for  $Q(x) \in \mathbb{Z}[x]$  with  $Q(0) \in \{-1, 1\}$ , there are exactly 2 possibilities:

- 1) number 1 is the only  $\tau$ -number relative to  $Q(x)$ ;
- 2) there are infinitely many  $\tau$ -numbers relative to  $Q(x)$ .

**Example 2.** Some non-constant polynomials with  $|Q(0) \cdot Q(1)| = 1$ , which belong to the case 2) of Remark 2, are listed in the following table.

$Q(x)$	suitable values for $n$	$Q(0) \cdot Q(1)$
$2x - 1$	$p^{16} \cdot q^6$ with $p \equiv \pm 3 \pmod{7}$ and $q \equiv \pm 7 \pmod{17}, q \neq 7$	-1
$4x^4 - 5x^2 + 3x - 1$	$p^4 \cdot q^6$ with primes $p \equiv 2 \pmod{35}$ and $q \equiv 3 \pmod{35}$	-1
$x^4 + 32x^2 - 33x - 1$		1
$x^4 - 3x^2 + 2x - 1$		1
$x^4 - 7x^2 + 8x - 1$	$p^6 \cdot q^4$ with primes $p \equiv 2 \pmod{35}$ and $q \equiv 3 \pmod{35}$	-1
$x^4 + 17x^2 - 18x - 1$		1
$x^3 - 2x^2 + x - 1$		1
$x^4 + 7x^2 - 8x - 1$	$p^4 \cdot q^{10}$ with primes $p \equiv 2 \pmod{55}$ and $q \equiv 3 \pmod{55}$	1
$x^4 - 32x^2 + 33x - 1$		-1
$x^2 - 3x + 1$		-1
$x^4 - 17x^2 + 18x - 1$	$p^{10} \cdot q^4$ with primes $p \equiv 2 \pmod{55}$ and $q \equiv 3 \pmod{55}$	-1
$x^4 + 10x^2 - 11x - 1$	$p^6 \cdot q^{10}$ with primes $p \equiv 2 \pmod{77}$ and $q \equiv 3 \pmod{77}$	1

#### 4. A result, which does not use the values of $Q(0)$ and $Q(1)$

We have obtained also a result, which does not use the values of  $Q(0)$  and  $Q(1)$  in order to classify some more polynomials relative to which there are infinitely many  $\tau$ -numbers.

**Theorem 3.** *Let  $Q(x) \in \mathbb{Z}[x]$  be a polynomial for which there exist different primes  $q_1, q_2$  with  $(q_1 - 1, q_2 - 1) = 2$  and positive integers  $r_1 < q_1, r_2 < q_2$  such that  $Q(r_1^2) \equiv 0 \pmod{q_1}$  and  $Q(r_2^2) \equiv 0 \pmod{q_2}$ . Then there are infinitely many  $\tau$ -numbers relative to  $Q(x)$ .*

*Proof.* Since  $q_1, q_2$  are primes and  $r_1 < q_1, r_2 < q_2$ , we have  $(r_1, q_1) = 1$  and  $(r_2, q_2) = 1$ . As  $(q_1 - 1, q_2 - 1) = 2$ , then  $((q_1 - 1)/2, (q_2 - 1)/2) = 1$ , which means that  $(q_1 - 1)/2$  is invertible modulo  $(q_2 - 1)/2$  and  $(q_2 - 1)/2$  is invertible modulo  $(q_1 - 1)/2$ . So, there exist positive integers  $u_1, u_2$  such that  $u_1(q_1 - 1)/2 \equiv 1 \pmod{(q_2 - 1)/2}$  and  $u_2(q_2 - 1)/2 \equiv 1 \pmod{(q_1 - 1)/2}$ . It gives us  $u_1(q_1 - 1) \equiv 2 \pmod{(q_2 - 1)}$  and  $u_2(q_2 - 1) \equiv 2 \pmod{(q_1 - 1)}$ . By Dirichlet's theorem, we can choose infinite number of pairs  $(p_1, p_2)$  of primes such that  $p_1 \equiv r_1^{u_1} \pmod{q_2}$  and  $p_2 \equiv r_2^{u_2} \pmod{q_1}$ .

Consider the integer  $n = p_1^{q_1-1} p_2^{q_2-1} > 1$ . Clearly,  $p_1^{q_1-1} \equiv 1 \pmod{q_1}$  (by Fermat's little theorem) and  $p_2^{q_2-1} \equiv r_1^{u_2(q_2-1)} \equiv r_1^2 \pmod{q_1}$ , since the exponents are equivalent modulo  $q_1 - 1$ . Thus,  $n = p_1^{q_1-1} p_2^{q_2-1} \equiv r_1^2 \pmod{q_1}$  and  $Q(n) \equiv Q(r_1^2) \equiv 0 \pmod{q_1}$ . Hence,  $q_1 \mid Q(n)$ . Similarly, we get that  $q_2 \mid Q(n)$ . So  $Q(n)$  is divisible by  $q_1 q_2 = \tau(n)$ .

As there were infinitely many different ways to choose the primes  $p_1, p_2$ , there are infinitely many numbers  $n = p_1^{q_1-1} p_2^{q_2-1}$ , which are  $\tau$ -numbers relative to  $Q(x)$ .  $\square$

*Remark 3.* Notice, that  $n = p_1^{q_1-1} p_2^{q_2-1}$  in Theorem 3 is also an anti- $\tau$ -number.

#### 5. About the generators of a $\tau$ -number

We think that the reason why we could find a counterexample for Theorem 34 d) in [8] is that actually the result was formulated wrongly. Hereby we offer another formulation of this result with a proof.

**Theorem 4.** *Apart from the order of the numbers  $a_1, \dots, a_k$ , any given  $\tau$ -number  $n$  is an  $(a_1, \dots, a_k)$ -generator for  $\sum_{d \mid (n/\tau(n))} h(d)$  different  $k$ -tuples  $(a_1, \dots, a_k)$  of positive integers (here  $k$  can take different values for fixed  $n$ ).*

*Proof.* Take any  $\tau$ -number  $n$  and set  $t = \frac{n}{\tau(n)}$ . Then  $t$  is a positive integer.

If  $n = 1$  or  $n = 2$ , then  $t = 1$ , the only positive divisor of  $t$  is  $d = 1$  and  $\sum_{d \mid (n/\tau(n))} h(d) = h(1) = 0$ , which corresponds to the fact that the integers 1 and 2 are not  $(a_1, \dots, a_k)$ -generators for any integer  $k > 0$  and any  $k$ -tuple  $(a_1, \dots, a_k)$  of positive integers.



If  $2 < n$ , then there exist a positive integer  $s$ , pairwise different prime numbers  $p_1, \dots, p_s$  and positive integers  $b_1, \dots, b_s$  such that  $n = p_1^{b_1} \cdot \dots \cdot p_s^{b_s}$ . As  $n$  was a  $\tau$ -number,  $\tau(n)$  divides  $n$ , which means that all primes, which divide  $t = \frac{n}{\tau(n)}$ , have to be from the set  $\{p_1, \dots, p_s\}$  of prime divisors of  $n$ .

Let  $d > 1$  be any positive integer that is a divisor of  $t$ . Then  $d = p_1^{d_1} \cdot \dots \cdot p_s^{d_s}$ , where  $d_1 \leq b_1, \dots, d_s \leq b_s$  are non-negative integers such that  $m = d_1 + \dots + d_s > 0$ . By the definition, there are exactly  $h(d)$  different  $k$ -tuples of positive integers  $(c_1, \dots, c_k)$  such that  $k$  is a positive integer,  $1 \leq k \leq m$ ,  $1 < \min\{c_1, \dots, c_k\}$  and  $c_1 \cdot \dots \cdot c_k = d$ .

Take any set  $\{q_1, \dots, q_k\}$  of pairwise different primes such that  $(q_i, n) = 1$  for all  $i \in \{1, \dots, k\}$  and define  $a_i = c_i - 1$  for each  $i \in \{1, \dots, k\}$ . Then  $(q_i, p_j) = 1$  for every  $i \in \{1, \dots, k\}$  and every  $j \in \{1, \dots, s\}$ , which means that  $(q_1^{a_1} \cdot \dots \cdot q_k^{a_k}, n) = 1$ . Define  $n' = nq_1^{a_1} \cdot \dots \cdot q_k^{a_k}$ . Then

$$\tau(n') = \tau(n)\tau(q_1^{a_1} \cdot \dots \cdot q_k^{a_k}) = \tau(n)c_1 \cdot \dots \cdot c_k = \tau(n)d.$$

It is clear that  $\tau(n') = \tau(n)d$  is a divisor of  $n$ . Hence,  $\tau(n')$  is also a divisor of  $n'$  and  $n'$  is a  $\tau$ -number. So, we have that  $n$  is an  $(a_1, \dots, a_k)$ -generator.

We see that for every positive divisor  $d$  of  $t$ , apart from the order of the numbers  $a_1, \dots, a_k$ , the number  $n$  is an  $(a_1, \dots, a_k)$ -generator for  $h(d)$  different  $k$ -tuples  $(a_1, \dots, a_k)$ , where  $k$  is a positive integer. Moreover, for different positive divisors  $d, d'$  of  $t$ , their respective tuples  $(a_1, \dots, a_k)$  and  $(a'_1, \dots, a'_k)$ , where  $k$  and  $k'$  are positive integers, are also different, because

$$(a_1 + 1) \cdot \dots \cdot (a_k + 1) = d \neq d' = (a'_1 + 1) \cdot \dots \cdot (a'_k + 1).$$

Hence, every  $\tau$ -number  $n$  is an  $(a_1, \dots, a_k)$ -generator for at least  $\sum_{d|(n/\tau(n))} h(d)$  different  $k$ -tuples  $(a_1, \dots, a_k)$  of positive integers (where  $k$  is a positive integer that can vary).

On the other hand, suppose that a  $\tau$ -number  $n$  is an  $(a_1, \dots, a_k)$ -generator for some positive integer  $k$  and positive integers  $a_1, \dots, a_k$ . Then there exist pairwise different primes  $p_1, \dots, p_k$  such that  $(p_i, n) = 1$  and  $(p_i, a_j + 1) = 1$  for every  $i, j \in \{1, \dots, k\}$ . As  $n$  is an  $(a_1, \dots, a_k)$ -generator,  $n' = np_1^{a_1} \cdot \dots \cdot p_k^{a_k}$  is a  $\tau$ -number, which means that  $\tau(n') = \tau(n)(a_1 + 1) \cdot \dots \cdot (a_k + 1)$  divides  $n'$ . As  $(p_i, a_j + 1) = 1$  for all  $i, j \in \{1, \dots, k\}$ , the number  $\tau(n)(a_1 + 1) \cdot \dots \cdot (a_k + 1)$  has to divide  $n$ , which means that  $d = (a_1 + 1) \cdot \dots \cdot (a_k + 1)$  is a divisor of  $t = \frac{n}{\tau(n)} \in \mathbb{Z}$ . Hence all  $k$ -tuples  $(a_1, \dots, a_k)$ , for which  $n$  is an  $(a_1, \dots, a_k)$ -generator for some positive integer  $k$  and positive integers  $a_1, \dots, a_k$ , are of the form described above.

With that we have demonstrated that apart from the order of the numbers  $a_1, \dots, a_k$ , any given  $\tau$ -number  $n$  is an  $(a_1, \dots, a_k)$ -generator for exactly  $\sum_{d|(n/\tau(n))} h(d)$  different  $k$ -tuples  $(a_1, \dots, a_k)$  of positive integers (where  $k$  can take different positive values for a fixed  $n$ ).  $\square$

## 6. Open problems

Let  $Q(x) = a_mx^m + \dots + a_1x + a_0$  be a polynomial with integer coefficients. First, let us remark that the condition “ $|Q(0) \cdot Q(1)| \neq 1$ ” is equivalent to the condition “ $a_ma_0 + \dots + a_1a_0 + a_0^2 \notin \{-1, 1\}$ ”, because  $a_ma_0 + \dots + a_1a_0 + a_0^2 = Q(0) \cdot Q(1)$ .

Similarly, the condition “ $|Q(0) \cdot Q(1)| = 1$ ” is equivalent to the condition “ $a_ma_0 + \dots + a_1a_0 + a_0^2 \in \{-1, 1\}$ ”.

Formally, the new equivalent conditions seem not to use the values of the polynomial and they can be easily checked by doing similar calculations with the coefficients of the polynomial. We give the following definition in order to shorten the texts of open problems.

**Definition 1.** We say that a polynomial  $Q(x) = a_mx^m + \dots + a_1x + a_0$  with integer coefficients is

- a) of type I, if  $a_ma_0 + \dots + a_1a_0 + a_0^2 \notin \{-1, 1\}$ ;
- b) of type II, if  $a_ma_0 + \dots + a_1a_0 + a_0^2 \in \{-1, 1\}$ .

By Theorem 1, we know that, for every polynomial  $Q(x)$  of type I, there are infinitely many integers  $n$  such that  $n$  is a  $\tau$ -number relative to polynomial  $Q(x)$ .

For polynomials of type II we have two examples ( $Q(x) = 1$  and  $Q(x) = -1$ ) such that only  $n = 1$  is a  $\tau$ -number relative to polynomial  $Q(x)$ . But we also have several examples, where there are infinitely many  $\tau$ -numbers relative to a polynomial  $Q(x)$  of type II. For several polynomials of type II (e.g.,  $x^2 - x + 1$ ,  $x^2 + x - 1$ ,  $x^3 + x^2 - 1$ ,  $2x^2 - 2x + 1$ ,  $2x^2 - 2x - 1$ , etc) we have checked by a computer program that the only  $\tau$ -number relative to these polynomials, in the range from 1 to  $10^8$ , is 1. Unfortunately, we were not able to classify the polynomials of type II by the number of  $\tau$ -numbers relative to the polynomial yet. We just remark here, that the only common thing for polynomials of type II, for which we were able to find an infinite family of  $\tau$ -numbers with respect to the polynomial, was that  $|a_m| + \dots + |a_0|$  was a prime. From this, the following open problem arises.

**Open problem 1.** Determine the conditions (using only the values of  $a_m, \dots, a_0$ ), which are necessary and sufficient for a polynomial  $Q(x)$  of type II to have infinitely many  $\tau$ -numbers relative to  $Q(x)$ .

In our results, we constructed for each polynomial of type I only one infinite family of  $\tau$ -numbers to polynomial  $Q(x)$ . Actually, there are more different families of  $\tau$ -numbers  $n$  with different values of  $\tau(n)$ . For example, for a polynomial  $Q(x) = x - 2$ , there are families  $n_1 = 2p$  and  $n_2 = 4p$ , where  $p > 2$  is a prime,  $n_3 = 2pq$ , where  $p$  and  $q$  are primes with  $p \equiv 3 \equiv q \pmod{8}$ , with  $\tau(n_1) = 4$ ,  $\tau(n_2) = 6$  and  $\tau(n_3) = 8$ . Perhaps there are even more

families of  $\tau$ -numbers relative to the polynomial  $Q(x) = x - 2$  with different number of positive divisors. From this the following open problems arise.

**Open problem 2.** Determine all possible values for  $\tau(n)$  such that  $n$  is a  $\tau$ -number relative to a fixed polynomial  $Q(x) = a_mx^m + \dots + a_1x + a_0$  with integer coefficients, using only the values of  $a_m, \dots, a_0$ .

**Open problem 3.** Determine all possible values  $n \in \mathbb{Z}^+$  which are  $\tau$ -numbers relative to fixed polynomial  $Q(x) = a_mx^m + \dots + a_1x + a_0$  with integer coefficients, using only the values of  $a_m, \dots, a_0$ .

### Acknowledgements

The research of the first author was supported by the institutional research funding PRG877 of the Estonian Ministry of Education and Research. The authors thank the anonymous referees for historical remarks and good ideas for shortening the proofs of this paper. The first author would like to thank Ott Eric Oopkaup from University of Tartu for help with modifying the computer programs for finding the lists of  $\tau$ -numbers relative to specific polynomials and making a list of the numbers of positive divisors of integers 1 to  $10^8$ . Running these programs simplified the life of the first author and gave new ideas for stating the results of the present paper.

### References

- [1] S. Colton, *Refactorable numbers - a machine invention*, J. Integer Seq. **2** (1999), Article 99.1.2, 15 pp.
- [2] R. R. Kennedy and C. N. Cooper, *Tau numbers, natural density, and Hardy and Wright's Theorem 437*, Int. J. Math. Math. Sci. **13**(2) (1990), 383–386.
- [3] H. Lauer, *Overview of  $\tau$ -numbers*, Master's Thesis, Tallinn University, Tallinn, 2014, 60 pp. (Estonian)
- [4] F. Luca, *On  $f(n)$  modulo  $\Omega(n)$  and  $\omega(n)$  when  $f$  is a polynomial*, J. Aust. Math. Soc. **77**(2) (2004), 149–164.
- [5] M. R. Murty and J. Esmonde, *Problems in Algebraic Number Theory*, 2nd edition, Graduate Texts in Mathematics **190**, Springer-Verlag, New York, 2005, 352 pp.
- [6] C. A. Spiro, *How often does the number of divisors of an integer divide its successor?*, J. London Math. Soc. (2) **31**(1) (1985), 30–40.
- [7] C. Spiro, *How often is the number of divisors of  $n$  a divisor of  $n$ ?*, J. Number Theory **21**(1) (1985), 283–302.
- [8] J. Zelinsky, *Tau numbers: a partial proof of a conjecture and other results*, J. Integer Seq. **5**(2) (2002), Article 02.2.8, 17 pp.

SCHOOL OF DIGITAL TECHNOLOGIES, TALLINN UNIVERSITY, 25 NARVA STR., 10120 TALLINN, ESTONIA; INSTITUTE OF MATHEMATICS AND STATISTICS, UNIVERSITY OF TARTU, 18 NARVA STR., 51009 TARTU, ESTONIA

*E-mail address:* `mart.abel@tlu.ee`, `mart.abel@ut.ee`

SCHOOL OF DIGITAL TECHNOLOGIES, TALLINN UNIVERSITY, 25 NARVA STR., 10120 TALLINN, ESTONIA

*E-mail address:* `helena.lauer@mail.com`

*E-mail address:* `eredi@tlu.ee`