On the number of divisors which are values of a polynomial

Katalin Gyarmati*

Abstract

Let $\tau(n)$ be the number of positive divisors of an integer n, and for a polynomial $P(X) \in \mathbb{Z}[X]$, let

$$\tau_P(n) = |(P(m) > 0 : \ m \in \mathbb{Z}, \ P(m) \mid n)| .$$

R. de la Bretèche studied the maximum values of $\tau_P(n)$ in intervals. Here the following is proved: if $P(X) \in \mathbb{Z}[X]$ is not of the form $a(X+b)^k$ with $a, b \in \mathbb{Q}$, and $k \in \mathbb{N}$ then

$$\tau_P(n) \ll (\log n)\tau(n)^{3/5}.$$

This improves partially on La Bretèche's results.

List of keywords and phrases: divisors, polynomial, extremal set theory.

2000 AMS Mathematics subject classification numbers: 11N56; 11N25.

1 Introduction

Paul Erdős asked several problems concerning divisors, for example, he conjectured that the density of integers n which have two divisors d_1, d_2 with

*Research partially supported by Hungarian National Foundation for Scientific Research, Grants T043631, T043623 and T049693

$d_1 < d_2 < 2d_1$ is 1 (e.g. see [9]). This conjecture was proved by Maier and Tenenbaum [16]. In this paper we study the number of certain special divisors of an integer n. We denote positive divisors of n by d, their number by $\tau(n)$, and the number of distinct prime divisors by $\omega(n)$.

P. Erdős and R. R. Hall [10] initiated the study of $\tau_k(n)$, which is the number of positive divisors of n of the form

$$x(x+1)\dots(x+k-1)$$

with $x \in \mathbb{Z}$. In the case $k=2$ an equivalent definition is

$$\tau_2(n) = |\{i : \ d_{i+1} - d_i = 1\}|,$$

where $1 = d_1 < d_2 < \cdots < d_{\tau(n)} = n$ denote the all positive divisors of n. P. Erdős and R. R. Hall [10] proved that

$$\tau_k(n) > (\log n)^{e^{1/k} - \varepsilon}$$

holds for infinitely many n. They also estimated the average value of $\tau_k(n)$ by proving

$$\frac{1}{x}\sum_{n\le x} \tau_k(n) = \frac{1}{(k-1)(k-1)!} + O(x^{-(k-1)/k}).$$

The first upper bound for $\tau_2(n)$ is due to Tenenbaum [17, Theorem 2], who proved that

$$\tau_2(n) \ll \tau(n)^c \tag{1.1}$$

holds with $c = 0.93974\dots$. R. de la Bretèche [6, Theorem 2] improved on the exponent c and obtained (1.1) with $c = 0.91829\dots$. $\tau_2(n)$ was studied by several authors, see in [1], [6], [10], [11] and [17].

Using La Bretèche's method it is easy to prove that

$$\tau_k(n) \le (k+1)\tau(n)^{h(1/(k+1))} \tag{1.2}$$

where

$$h(\alpha) = \frac{1}{\log 2}\left((1-\alpha)\log(1/(1-\alpha)) + \alpha\log(1/\alpha)\right).$$

Indeed at least one of the integers $d, d+1, \ldots, d+k-1, \frac{n}{d(d+1)\ldots(d+k-1)}$ is in the set $\{d: \ \Omega(d) \le \Omega(n)/(k+1)\}$. By using Lemma 2.1 in [5] we get (1.2).

R. de la Bretèche [5] extended the problem to other polynomials.

Definition 1 *For $P(X) \in \mathbb{Z}[X]$, let*

$$\tau_P(n) = \{P(m) > 0: \ m \in \mathbb{Z}, \ P(m) \mid n\}.$$

In the special case $P(X) = X(X+1)\cdots(X+k-1)$ $\tau_p(n)$ is $\tau_k(n)$. R. de la Bretèche [5] estimated the maximum value of $\tau_P(m)$:

Theorem A *If $P(x) \in \mathbb{Z}[x]$ is a polynomial of degree 2 with discriminant Δ, then*

$$\max_{1\le m\le n} \tau_P(m) \le \left(\max_{1\le m\le n} \tau(m)\right)^{c(\Delta)+o(1)} \tag{1.3}$$

where

$$c(\Delta) = \begin{cases} 0.565\ldots & \textit{if } \Delta \neq 0 \textit{ is a square of an integer}, \\ 0.5 & \text{if } \Delta = 0, \\ 0.579\ldots & \textit{if } \Delta \textit{ is not a square of an integer}. \end{cases} \tag{1.4}$$

In [5] it is also mentioned that this theorem can be improved for some special polynomials of higher degree.

Here we will extend La Bretèche's Theorem A to every polynomial and in section 4 we will improve on the constant $c(\Delta)$ if n is a squarefree number and Δ is not a square of an integer.

By Wigert's theorem [18]

$$D(n) \overset{\text{def}}{=} \max_{1\le m\le n} \tau(m) = 2^{(1+o(1))\frac{\log n}{\log\log n}}.$$

For almost all n, $\tau(n)$ is around $c\log n$, which is significally smaller then $D(n)$. Indeed, in the case $\tau(n) < D(n)^{c(\Delta)}$, (1.3) gives a trivial upper bound for $\tau_P(n)$:

$$\tau_P(n) \le \max_{1\le m\le n} \tau_P(m) \le D(n)^{c(\Delta)+o(1)}.$$

This inspired me to look for a bound $\tau_p(n)$ in terms of $\tau(n)$, which can give a sharp estimate for a larger set of integers. I obtained the following

Theorem 1 *If $P(X)$ is not of the form $a(X+b)^k$ with $a, b \in \mathbb{Q}$, and $k \in \mathbb{N}$ then*

$$\tau_P(n) \ll (\log n)\tau(n)^{3/5}. \tag{1.5}$$

Theorem 1 is trivial for $\tau(n) \ll (\log n)^{5/2}$, while the upper bound in (1.1) are always non-trivial. For $k \geq 6$ the exponent $h(1/(k+1))$ in (1.2) is less than $3/5$, so (1.2) gives sharper bound for $\tau_k(n)$ than Theorem 1. However in these special cases Theorem 1 does not give the best possible results, but its proof is a different approach from Tenenbaum's and La Bretèche's and for general polynomials $P(X)$ (for example, for irreducible polynomials over $\mathbb{Q}$) gives a new and sharp bound for $\tau_P(n)$.

The proof of Theorem 1 is based on a generalization of a lemma of B. Lindström [15] on B_2 sequences. Possible improvements on Theorem 1 will be discussed in section 4.

Using Evertse's theorem on S-unit equations [12, Theorem 1] for the linear form $x - y = 1$ we get:

$$\tau_2(n) \ll 7^{2\omega(n)}. \tag{1.6}$$

If n contains only few prime factors, so $\omega(n)$ is small, then (1.6) is a sharper bound than (1.1).

For general polynomials $P(X)$ I will prove the following:

Theorem 2 *If $P(X) \in \mathbb{Z}[X]$ is not of the form $a(X+b)^k$ with $a, b \in \mathbb{Q}$, and $k \in \mathbb{N}$ then*

$$\tau_P(n) \ll \log n(\deg P)^{\omega(n)}. \tag{1.7}$$

If n contains only few prime factors then the upper bound (1.7) is sharper than (1.5).

Acknowledgement. I would like to thank Professors Zoltán Füredi, András Sárközy and Miklós Simonovits for the valuable discussions. I also wish to thank to the referee for his suggestions which leads to (1.2) and the improvement of the original Theorem 1 by a factor $\omega(n)^{1/5}$.

2 Proof of Theorems 1-2

Our first lemma is a generalization of a theorem of B. Lindstörm [15].

Lemma 1 *Let $\mathcal{D}$ be a subset of the divisors of an integer n. Suppose that there are no T different pairs $x_i, y_i \in \mathcal{D}$, such that*

$$1 \neq \frac{x_1}{y_1} = \frac{x_2}{y_2} = \cdots = \frac{x_T}{y_T}.$$

Then

$$|\mathcal{D}| \ll T^{2/5} \tau(n)^{3/5}.$$

The exponent $3/5$ in Theorem 1 strongly depends on the exponent $3/5$ in Lemma 1. This exponent might be improved in some special cases, results in this directions will be discussed in section 4.

Lemma 2 *Let $v \in \mathbb{N}$, $P(X) = a_k X^k + a_{k-1} X^{k-1} + \cdots + a_0 \in \mathbb{Z}[X]$ be a polynomial which is not of the form $a(X+b)^k$ with $a, b \in \mathbb{Q}$, $k \in \mathbb{N}$. Then there exists a (computable) constant T depending only on the polynomial $P(X)$ such that at most T pairs $x_i, y_i \in \mathbb{Z}$ exist with*

$$v < P(x_i), P(y_i) < 2v \tag{2.1}$$

and

$$1 \neq \frac{P(x_1)}{P(y_1)} = \frac{P(x_2)}{P(y_2)} = \cdots = \frac{P(x_T)}{P(x_T)}. \tag{2.2}$$

The history of Lemma 2 is related to a problem of Diophantus. Diophantus found 4 rational numbers such that the product of any two of them increased by 1 is a square of a rational number. The first absolute upper bound for the size of Diophantine tuples was given by A. Dujella, see in [7], [8]. Later Y. Bugeaud and A. Dujella [2] extended the problem for higher power. In [3], [13] and [14] we studied different generalizations of the problem of Diophantus. Lemma 2 is closely related to the proof of these results.

We postpone the proof of Lemma 1 and Lemma 2 to section 3. For $0 \le i \le \frac{\log n}{\log 2}$ let

$$\mathcal{D}_i = \{P(m) > 0 : 2^i < P(m) < 2^{i+1},\ P(m) \mid n\}.$$

By Lemma 2 these sets $\mathcal{D}_i$'s satisfy the conditions of Lemma 1. By using Lemma 1 we get

$$|\mathcal{D}_i| \ll \tau(n)^{3/5}.$$

We have $\left[\frac{\log n}{\log 2}\right] + 1$ different sets $\mathcal{D}_i$, thus we get Theorem 1.

In order to prove Theorem 2 we will need the following lemma.

Lemma 3 *Let $P(X) \in \mathbb{Z}[X]$ be a polynomial of degree k, which is not of the form $a(X+b)^k$. Then there exists a (computable) constant T depending on the polynomial $P(X)$ such that there are at most T integers x_i $(1 \le i \le T)$ such that for $1 \le i, j \le T$*

$$\frac{1}{2} < \frac{P(x_i)}{P(x_j)} < 2 \tag{2.3}$$

and $\frac{P(x_i)}{P(x_j)}$ is the k-th power of a rational number.

We will prove Lemma 3 in section 3.

Denote the prime divisors of n by $p_1, p_2, \dots, p_r$, so $r = \omega(n)$. To every $d \in \mathcal{D}_i$, $d = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ we assign a $\{0, 1, \dots, k-1\}$-vector $(\delta_1, \dots, \delta_r)$ such that

$$\delta_j \equiv \alpha_j \pmod{k}$$

and $0 \le \delta_j \le k-1$. By Lemma 3 to at most T different $d \in \mathcal{D}_i$'s we assign the same $\{0, 1, \dots, k-1\}$-vector. Thus

$$|\mathcal{D}_i| \le T k^{\omega(n)}.$$

Again, we have $\left[\frac{\log n}{\log 2}\right] + 1$ different sets $\mathcal{D}_i$, thus we get Theorem 2.

3 Proof of Lemmas 1-3

Proof of Lemma 1

First we will prove the following:

Lemma 4 *Let $n \in \mathbb{N}$. Then for $1 \leq x < \tau(n)$, there exist positive integers n_1 and n_2 such that*

$$\tau(n_1) \leq x, \ \tau(n_2) \leq \frac{4\tau(n)}{x}, \tag{3.1}$$

and every $d \mid n$ can be written of the form $d = d_1 d_2$ with $d_1 \mid n_1$ and $d_2 \mid n_2$.

Throughout the proof of Lemma 1 we will use this factorization of d's.

Proof of Lemma 4

Consider the prime factorization of n:

$$n = p_1^{\alpha_1} \dots p_r^{\alpha_r}.$$

Let $H - 1(\leq r)$ denote the greatest positive integer with

$$(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_{H-1} + 1) \leq x.$$

Let $0 \leq \beta_H < \alpha_H$ denote the greatest integer with

$$(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_{H-1} + 1)(\beta_H + 1) \leq x. \tag{3.2}$$

By the definition of β_H we get

$$\begin{aligned} \frac{x}{2} &< \frac{1}{2}(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_{H-1} + 1)(\beta_H + 2) \\ &\leq (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_{H-1} + 1)(\beta_H + 1), \end{aligned}$$

thus

$$\begin{aligned} \frac{4\tau(n)}{x} &\geq \frac{2\tau(n)}{(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_{H-1} + 1)(\beta_H + 1)} \\ &\geq \left(\left[\frac{\alpha_H + 1}{\beta_H + 1} \right] + 1 \right) (\alpha_{H+1} + 1)(\alpha_{H+2} + 1) \dots (\alpha_r + 1). \end{aligned} \tag{3.3}$$

Let

$$q_i = \begin{cases} p_i & \text{if } 1 \le i \le H, \\ p_H^{\beta_H} & \text{if } i = H+1, \\ p_{i-1} & \text{if } H+2 \le i \le r, \end{cases}$$

and

$$\gamma_i = \begin{cases} \alpha_i & \text{if } 1 \le i \le H, \\ \beta_H & \text{if } i = H, \\ \left[\frac{\alpha_H+1}{\beta_H+1}\right] & \text{if } i = H+1, \\ \alpha_{i-1} & \text{if } H+2 \le i \le r+1. \end{cases} \tag{3.4}$$

Clearly, every $d \mid n$ can be written in the form $d = q_1^{\delta_1} \dots q_{r+1}^{\delta_{r+1}}$ with $0 \le \beta_i \le \gamma_i$. This proves Lemma 4 with

$$n_1 = q_1^{\gamma_1} \dots q_H^{\gamma_H}$$

and

$$n_2 = q_{H+1}^{\gamma_{H+1}} \dots q_{r+1}^{\gamma_{r+1}}.$$

Indeed, by (3.2) and (3.3) we get (3.1). We remark that then

$$\tau(n_1) = (\gamma_1 + 1)(\gamma_2 + 1) \dots (\gamma_H + 1) \le x \tag{3.5}$$

and

$$\tau(n_2) = (\gamma_{H+1} + 1)(\gamma_{H+2} + 1) \dots (\gamma_{r+1} + 1) \le \frac{4\tau(n)}{x} \tag{3.6}$$

Throughout the proof of Lemma 1 we will use this factorization $d = q_1^{\delta_1} \dots q_{r+1}^{\delta_{r+1}}$ with $0 \le \beta_i \le \gamma_i$ in place of the prime factorization. Our factorization (as the prime factorization) is unique.

Next we return to the proof of Lemma 1. We will fax the value of $1 \le x < \tau(n)$ later.

To every $d \in \mathcal{D}$, $d = q_1^{\delta_1} \dots q_{r+1}^{\delta_{r+1}}$ we assign an $r+1$-dimensional vector $b_d = (\delta_1, \delta_2, \dots, \delta_{r+1})$. Let $\mathcal{B} = \{b_1, b_2, \dots, b_m\}$ be the set of all the $r+1$-dimensional vectors obtained in this way. Then

$$m = |\mathcal{D}| = |\mathcal{B}|.$$

By the conditions of Lemma 1, for every $a \neq 0$, $a \in \mathbb{Z}^{r+1}$ the equation

$$a = b_i - b_j, \quad b_i, b_j \in \mathcal{B}$$

has at most T different solutions in i and j.

We split each b_i in two vectors v_i and w_i of dimensions H and $r + 1 - H$. If $b_i = (\delta_1, \delta_2, \ldots, \delta_{r+1})$, then let $v_i = (\delta_1, \delta_2, \ldots, \delta_H)$ and $w_i = (\delta_{H+1}, \delta_{H+2}, \ldots, \delta_{r+1})$.

By considering the differences $v_i - v_{i'}$ we get that for the j-th component of $v_i - v_{i'}$ we have

$$-\gamma_j \leq \delta_j - \delta'_j \leq \gamma_j.$$

Now let $z_1, z_2, z_3, \ldots, z_p$ be an enumeration of all H-dimensional vectors $\{\delta_1, \delta_2, \ldots, \delta_H\}$ with components

$$-\gamma_j \leq \delta_j \leq \gamma_j,$$

where γ_j's were defined by (3.4). Then

$$p = (2\gamma_1 + 1)(2\gamma_2 + 1) \cdots (2\gamma_H + 1).$$

Let $w^1, w^2, \ldots, w^s$ be an enumeration of all $r + 1 - H$-dimensional vectors $\{\delta_{H+1}, \delta_{H+2}, \ldots, \delta_{r+1}\}$ with components

$$0 \leq \delta_i \leq \gamma_i.$$

Then by (3.6) we have

$$s = (\gamma_{H+1} + 1)(\gamma_{H+2} + 1) \ldots (\gamma_{r+1} + 1) \leq \frac{4\tau(n)}{x}. \tag{3.7}$$

For each i ($1 \leq i \leq s$), let E_i denote the set of all H-dimensional v_j such that $(v_j, w^i) \in \mathcal{B}$. E_i can be empty. Let the cardinality of E_i be e_i. Then we have

$$m = \sum_{i=1}^{s} e_i. \tag{3.8}$$

For each i in $1 \le i \le s$ we consider the differences $v_j - v_k$ where (v_j, w^i) and (v_k, w^i) are vectors in the set $\mathcal{B}$. The zero vector of dimension H occurs m times as a difference, but any other vector z_ℓ occurs at most T times. We will assume that $z_1 = 0$. If x_i is the number of times that z_i occurs as a difference $v_j - v_k$ then

$$x_1 = m, \; x_i \le T \text{ for } i = 2, 3, \dots, p. \tag{3.9}$$

By (3.7), (3.8) and the Cauchy-Shwarz inequality we find that

$$\sum_{i=1}^{p} x_i = \sum_{i=1}^{s} e_i^2 \ge \frac{m^2}{s} \ge \frac{m^2 x}{4\tau(n)}. \tag{3.10}$$

Without loss of generality, we may assume that $\gamma_1 \le \cdots \le \gamma_H$. Let $H^* \le H$ be the greatest integer with

$$1 = \gamma_1 = \gamma_2 = \cdots = \gamma_{H^*}.$$

If all $\gamma_i \ge 2$, then let $H^* = 0$.

If we take all differences in a finite sequence of 0's and 1's, then at least half of all differences are 0: if we have a pieces of 0 and b pieces of 1, then the number of differences 0 is $a^2 + b^2$ and the number of differences ± 1 is $2ab$. Clearly $a^2 + b^2 \ge 2ab$.

Thus if we define $h_{i,j}$ $(1 \le i \le p, 1 \le j \le H^*)$ by 1 when the j-th component of z_i is 0 and $h_{i,j} = -1$ in the other case (when the j-th component is -1 or $+1$), then we get

$$\sum_{i=1}^{p} h_{i,j} x_i \ge 0 \text{ for } j = 1, \dots, H^*. \tag{3.11}$$

Put

$$y_i = \max\{0, 1 + \sum_{j=1}^{H^*} h_{i,j}\}, \text{ for } i = 1, \dots, p. \tag{3.12}$$

It follows then from (3.11),(3.12) and since $x_i \ge 0$ that

$$0 \le \sum_{j=1}^{H^*} \sum_{i=1}^{p} h_{i,j} x_i \le \sum_{i=1}^{p} (y_i - 1) x_i.$$

By this, (3.9) and (3.12) we get

$$\sum_{i=1}^{p} x_i \le \sum_{i=1}^{p} y_i x_i \le m y_1 + T \sum_{i=2}^{p} y_i. \tag{3.13}$$

If in the first H^* components of z_i, k_i components equal to 0, we get

$$\sum_{j=1}^{H^*} h_{i,j} = 2k_i - H^*, \quad i = 1, \ldots, s.$$

By this, (3.12) and since for fixed $(\delta_1, \ldots, \delta_{H^*})$ the number of i's for which z_i first H^* components are $(\delta_1, \ldots, \delta_{H^*})$ is at most $(2\gamma_{H^*+1} + 1) \ldots (2\gamma_H + 1)$, we get

$$T \sum_{i=2}^{p} y_i \le T \sum_{k \ge (H^*-1)/2} \binom{H^*}{k} 2^{H^*-k} (1 + 2k - H^*)(2\gamma_{H^*+1} + 1) \ldots (2\gamma_H + 1). \tag{3.14}$$

The function $f : \mathbb{N} \to \mathbb{R}$, $f(k) = \binom{H^*}{k} 1.7^{H^*/2-k}(1 + 2k - H^*)$ is decreasing in the interval $[H^*/2 + 1, H^*]$. Indeed

$$f(k) > f(k+1)$$

is equivalent with

$$(2k - H^* - 2)(2.7k - H^* + 6.7) + 0.1k + 15.1 > 0,$$

which holds for $k \in [H^*/2 + 1, H^*]$. Thus for $k \in [H^*/2 - 1, H^*]$ we have

$$f(k) \ll f([H^*/2]).$$

By this and the Stirling's formula we get

$$\binom{H^*}{k} 1.7^{H^*/2-k}(1 + 2k - H^*) \ll \binom{H^*}{[H^*/2]} \ll \frac{2^{H^*}}{\sqrt{H^*}}.$$

So

$$\sum_{k\geq(H^*-1)/2}\binom{H^*}{k}2^{H^*-k}(1+2k-H^*)$$

$$=\sum_{k\geq(H^*-1)/2}\binom{H^*}{k}1.7^{H^*/2-k}(1+2k-H^*)2^{H^*/2}\left(\frac{2}{1.7}\right)^{H^*/2-k}$$

$$\ll 2^{H^*/2}\sum_{k\geq(H^*-1)/2}\frac{2^{H^*}}{\sqrt{H^*}}\left(\frac{2}{1.7}\right)^{H^*/2-k}=\frac{2^{3H^*/2}}{\sqrt{H^*}}\sum_{k\geq(H^*-1)/2}\left(\frac{2}{1.7}\right)^{H^*/2-k}$$

$$\ll\frac{2^{3H^*/2}}{\sqrt{H^*}}.$$

By this and (3.14) we get

$$T\sum_{i=2}^{p}y_i\ll\frac{T2^{3H^*/2}}{\sqrt{H^*}}(2\gamma_{H^*+1}+1)\dots(2\gamma_H+1). \tag{3.15}$$

For $1\leq i\leq H^*$ we have $2=\gamma_i+1$ and for $i>H^*$ $\gamma_i\geq 2$, thus $2\gamma_i+1\leq(\gamma_i+1)^{3/2}$, and by (3.15)

$$T\sum_{i=2}^{p}y_i\ll\frac{T}{\sqrt{H^*}}\left((\gamma_1+1)(\gamma_2+1)\dots(\gamma_{H^*}+1)\right)^{3/2}(2\gamma_{H^*+1}+1)\dots(2\gamma_H+1)$$

$$\ll\frac{T}{\sqrt{H^*}}\left((\gamma_1+1)\dots(\gamma_H+1)\right)^{3/2}.$$

Thus by (3.5) we get

$$T\sum_{i=2}^{p}y_i\ll\frac{T}{\sqrt{H^*}}x^{3/2}.$$

By this, (3.10), (3.13) and $y_1\leq H^*+1$ we get

$$\frac{m^2x}{\tau(n)}\ll\sum_{i=1}^{p}x_i\ll mH^*+\frac{T}{\sqrt{H^*}}x^{3/2},$$

$$m^2\ll\frac{mH^*\tau(n)}{x}+\frac{T}{\sqrt{H^*}}x^{1/2}\tau(n),$$

$$m\ll\frac{H^*\tau(n)}{x}+\frac{T^{1/2}}{(H^*)^{1/4}}x^{1/4}\tau(n)^{1/2}. \tag{3.16}$$

Now we fix the value of x in (3.2). Let

$$x=\frac{H^*\tau(n)^{2/5}}{T^{2/5}}. \tag{3.17}$$

Clearly $x \le \tau(n)$. By (3.16) and (3.17) we get

$$m \ll T^{2/5}\tau(n)^{3/5}$$

which was to be proved.

Proof of Lemma 2

Write

$$x_i^* = x_i + \frac{a_{k-1}}{ka_k},\ y_i^* = y_i + \frac{a_{k-1}}{ka_k}$$

and let $Q(X) = P(X - \frac{a_{k-1}}{ka_k})$. Then

$$P(x_i) = Q(x_i^*), \quad P(y_i) = Q(y_i^*).$$

The coefficient of x^{k-1} in $Q(x)$ is 0, let

$$Q(x) = b_k x^k + b_{k-2}x^{k-2} + \cdots + b_0.$$

Clearly $b_k = a_k$. If $|x_i|$ and $|y_i|$ are large enough (depending on the polynomial $P(X)$), $|x_i|, |y_i| > c_1$, then from (2.1)

$$\frac{1}{2}u < |x_i{}^*|, |y_i{}^*| < 2u \tag{3.18}$$

follows with $u = \left|v^{1/k}\right|$. By (2.1) the number of the pairs $x_i, y_i \in \mathbb{Z}$ with $\min\{|x|, |y|\} < c_1$ is finite and depends only on the polynomial of $P(X)$. Thus throughout the proof we may suppose that (3.18) holds for all $x_i{}^*$'s and $y_i{}^*$'s.

Denote by M the greatest coefficients of $Q(x)$ in absolute value:

$$M = \max_{0 \le i \le k} |b_i|.$$

We define a modulus m depending only on the polynomial $P(X)$. Indeed, let

$$m > 2^{4k-1}(k+1)^3 M^2. \tag{3.19}$$

Suppose that T is large enough:

$$T > 4(k+1)m^2,$$

where k is the degree of the polynomial $P(X)$. By the pigeon-hole principle, there exist $k+1$ x_i's and y_i's which are congruent modulo m and all products $x_i y_j$ have the same sign. We may suppose that these x_i's and y_i's are

$$x_1 \equiv x_2 \equiv \cdots \equiv x_{k+1} \pmod m, \quad y_1 \equiv y_2 \equiv \cdots \equiv y_{k+1} \pmod m. \tag{3.20}$$

First we will prove that for all $1 \le i \le k+1$ we have

$$\frac{x_1^*}{y_1^*} = \frac{x_i^*}{y_i^*}. \tag{3.21}$$

By

$$\frac{Q(x_1{}^*)}{Q(y_1{}^*)} = \frac{Q(x_i{}^*)}{Q(y_i{}^*)},$$
$$Q(x_1{}^*)Q(y_i{}^*) = Q(x_i{}^*)Q(y_1{}^*),$$

we get

$$b_k^2\left((x_1{}^* y_i{}^*)^k - (x_i{}^* y_1{}^*)^k\right) = - \sum_{\substack{0\le j,\ell\le k,\\ \min\{j,\ell\}\le k-2}} b_j b_\ell (x_1{}^{*j} y_i{}^{*\ell} - x_i{}^{*j} y_1{}^{*\ell}).$$

By estimating the right-hand side by the triangle-inequality and using $|b_i| \le \max_{1\le i\le k} |b_i| = M$ and (3.18) we get

$$b_k^2 \left|(x_1{}^* y_i{}^*)^k - (x_i{}^* y_1{}^*)^k\right| \le 2(k+1)^2 M^2 (2u)^{2k-2}. \tag{3.22}$$

Next we gave a lower bound for the left hand side of (3.22). $x_1{}^* y_i{}^*$ and $x_i{}^* y_1{}^*$ have the same sign and thus

$$\begin{aligned} b_k^2|(x_1{}^* y_i{}^*)^k - (x_i{}^* y_1{}^*)^k| &= b_k^2 \, |x_1{}^* y_i{}^* - x_i{}^* y_1{}^*| \left(|x_1{}^* y_i{}^*|^{k-1} + \cdots + |x_i{}^* y_1{}^*|^{k-1}\right) \\ &\ge b_k^2 \, |x_1{}^* y_i{}^* - x_i{}^* y_1{}^*| \, k \left(\frac{u}{2}\right)^{2k-2}. \end{aligned}$$

By this, (3.22) and $b_k = a_k$ we get

$$|x_1{}^* y_i{}^* - x_i{}^* y_1{}^*| \le \frac{2^{4k-1}(k+1)^2 M^2}{k a_k^2}. \tag{3.23}$$

The right hand side of (3.23) is a constant which depends only on the polynomial $P(X)$. Thus ${x_1}^*{y_i}^*$ and ${x_i}^*{y_1}^*$ are very close. Suppose that they are not equal. Then we will give a lower bound for the left-hand side of (3.23).

$$|{x_1}^*{y_i}^* - {x_i}^*{y_1}^*| =$$
$$\frac{1}{(ka_k)^2}\left|(ka_kx_1 + a_{k-1})(ka_ky_i + a_{k-1}) - (ka_kx_i + a_{k-1})(ka_ky_1 + a_{k-1})\right|.$$

By (3.20) we get

$$m \mid (ka_kx_1 + a_{k-1})(ka_ky_i + a_{k-1}) - (ka_kx_i + a_{k-1})(ka_ky_1 + a_{k-1}).$$

If ${x_1}^*{y_i}^*$ and ${x_i}^*{y_1}^*$ are not equal, then we obtain

$$|{x_1}^*{y_i}^* - {x_i}^*{y_1}^*| \geq \frac{m}{(ka_k)^2}.$$

By this and (3.23) we get

$$m \leq 2^{4k-1}(k+1)^3M^2$$

which contradicts (3.19), thus we proved (3.21).

By (3.21) we have that there exist $c, d \in \mathbb{Q}$ with

$$c = \frac{Q(x_i^*)}{Q(y_i^*)} \text{ and } d = \frac{x_i^*}{y_i^*} \tag{3.24}$$

for all $1 \leq i \leq (k+1)$. Then

$$0 = Q(dy) - cQ(y)$$

has at least $k+1$ solutions, since for all $1 \leq i \leq k+1$, y_i^* is a solution by (3.24). But the polynomial $Q(dy) - cQ(y)$ is not identically 0 (since $P(X)$ is not the form $a(X+b)^k$) and its degree is $\leq k$, which is a contradiction. Thus we have proved Lemma 2.

Proof of Lemma 3

Define x_i^*'s and polynomial $Q(X)$ as in Lemma 2. The coefficient of x^{k-1} in $Q(x)$ is 0, and let again

$$Q(x) = b_k x^k + b_{k-2} x^{k-2} + \cdots + b_0 \tag{3.25}$$

and

$$M = \max_{0 \le i \le k} |b_i| .$$

If $|x_i|$ and $|x_j|$ are large enough depending on the polynomial $P(X)$, $|x_i|, |x_j| > c_1$, then from (2.3)

$$\frac{1}{2} < \frac{|x_i{}^*|}{|x_j{}^*|} < 2. \tag{3.26}$$

The number of the integers x_i with $|x_i| < c_1$ is finite and depends only on the polynomial of $P(X)$. Thus throughout the proof we may suppose that (3.26) holds for all $x_i{}^*$ and x_j^*.

Let m be a large prime (depending only on the polynomial $P(X)$) such that

$$(k, m-1) = 1 \tag{3.27}$$

and

$$m > k 2^{3k} M^2. \tag{3.28}$$

Suppose that T is large enough:

$$T > 2(k+1)m,$$

where k is the degree of the polynomial $P(X)$. By the pigeon-hole principle, there exist $k+1$ x_i's which are congruent modulo m and all x_i's have the same sign. Let us denote them by $x_1, x_2, \ldots, x_{k+1}$:

$$x_1 \equiv x_2 \equiv \cdots \equiv x_{k+1} \pmod{m}. \tag{3.29}$$

First we will prove that for $1 \le i \le k+1$ we have

$$\frac{P(x_1)}{P(x_i)} = \frac{Q(x_1^*)}{Q(x_i^*)} = \left(\frac{x_1^*}{x_i^*}\right)^k . \tag{3.30}$$

By (2.3) $\frac{P(x_1)}{P(x_i)} = \frac{Q(x_1^*)}{Q(x_i^*)}$ is the k-th power of a positive rational number, so

$$\frac{Q({x_1}^*)}{Q({x_i}^*)} = \left(\frac{p}{q}\right)^k \tag{3.31}$$

with $0 < p, q \in \mathbb{N}$. Then

$$\begin{aligned} p^k &\le Q(x_1^*) \le (k+1)M \left|x_1^*\right|^k, \\ p &\le 2M^{1/k} \left|x_1^*\right|. \end{aligned} \tag{3.32}$$

m is a prime with (3.27), so by (3.29) and (3.31) we have

$$p \equiv q \pmod m \tag{3.33}$$

By (3.25) and (3.31)

$$b_k \left(({x_1}^*q)^k - ({x_i}^*p)^k\right) = -\sum_{0\le j\le k-2} b_j((x_1^*)^j q^k - (x_i^*)^j p^k). \tag{3.34}$$

By (3.26) $\frac{1}{2}\left|x_1^*\right| < \left|x_i^*\right| < 2\left|x_1^*\right|$ and by (2.3) and (3.31) $\frac{1}{2}p^k < q^k < 2p^k$. So by estimating the right-hand side of (3.34) by the triangle-inequality we get

$$\begin{aligned} \left|b_k \left(({x_1}^*q)^k - ({x_i}^*p)^k\right)\right| &\le (k-1)M \max_{0\le j\le k-2} \left|((x_1^*)^j q^k - (x_i^*)^j p^k)\right| \\ &\le (k-1)M(2^k+2)\left|x_1^*\right|^{k-2} p^k. \end{aligned} \tag{3.35}$$

Next we gave a lower bound for the left hand side of (3.35). By (3.26) ${x_1}^*q$ and ${x_i}^*p$ have the same signs and thus

$$\begin{aligned} \left|b_k \left(({x_1}^*q)^k - ({x_i}^*p)^k\right)\right| &= |b_k| \left|{x_1}^*q - {x_i}^*p\right| \left(\left|{x_1}^*q\right|^{k-1} + \cdots + \left|{x_i}^*p\right|^{k-1}\right) \\ &\ge |b_k| \left|{x_1}^*q - {x_i}^*p\right| k \left(\frac{\left|x_1^*\right| p}{4}\right)^{k-1}. \end{aligned}$$

By this, (3.32) and (3.35) we get

$$\begin{aligned} \left|{x_1}^*q - {x_i}^*p\right| &\le \frac{(k-1)(2^k+2)4^{k-1}M}{k\,|b_k|} \frac{p}{\left|x_1^*\right|} \le \frac{(k-1)(2^k+2)4^{k-1}M}{k\,|b_k|} 2M^{1/k} \\ &< \frac{2^{3k}M^2}{|b_k|}. \end{aligned} \tag{3.36}$$

The right hand side of (3.36) is a constant which depends only on the polynomial $P(X)$. Thus $x_1{}^*q$ and $x_i{}^*p$ are very close. Suppose that they are not equal. Then we will give a lower bound for the left-hand side of (3.36).

$$|x_1{}^*q - x_i{}^*p| = \frac{1}{ka_k} \left|(ka_kx_1 + a_{k-1})\, q - (ka_kx_i + a_{k-1})\, p\right|.$$

By (3.29) and (3.33) we get

$$m \mid (ka_kx_1 + a_{k-1})\, q - (ka_kx_i + a_{k-1})\, p.$$

If $x_1{}^*q$ and $x_i{}^*p$ are not equal, then we obtain

$$|x_1{}^*q - x_i{}^*p| \geq \frac{m}{k\,|a_k|} = \frac{m}{k\,|b_k|}.$$

By this and (3.36) we get

$$m \leq k2^{3k}M^2$$

which contradicts (3.28), thus we proved (3.30).

By (3.30) we have that the polynomial

$$Q(x_1^*)y^k - (x_1^*)^kQ(y)$$

has $k+1$ different roots: $y = x_1, x_2, \ldots, x_{k+1}$. But the polynomial $Q(x_1^*)y^k - (x_1^*)^kQ(y)$ is not identically zero (since $P(X)$ is not the form $a(X+b)^k$) and its degree is $\leq k$, which is a contradiction. Thus we have proved Lemma 3.

4 On possible improvements on Theorem 1

One of the main tools in the proof of Theorem 1 was Lemma 1 which is a generalization of the following theorem of Lindström [15, Theorem 2].

Lemma 5 *Let $F_2(d)$ denote the maximum number of vectors of dimension d, whose components are taken from the integers $\{0,1\}$ such that every two vectors have different sum. Then*

$$F_2(d) \ll d2^{3/5d}.$$

A famous conjecture asked whether

$$L \stackrel{\text{def}}{=} \lim_{d\to\infty} F_2(d)^{1/d}$$

equals to 1/2? The constant L is related to our problem. Probably, for all $\varepsilon > 0$

$$\tau_P(n) \ll (\log n)\tau(n)^{L+\varepsilon} \tag{4.1}$$

could be proved. The best known upper bound for the constant L was proved by G. Cohen, S. Litsyn, G. Zémor [4] in 2000. Using coding theory they proved

Lemma 6 *$L \leq 0.57526$, i.e.,*

$$\lim_{d\to\infty} (F_2(d))^{1/d} \leq 0.57526.$$

Unfortunately, I was not able to generalize Lemma 5 to vectors with components taken form a larger set than $\{0, 1\}$. Thus the starting point of the proof of Lemma 1 was Lindström's [15] proof for $L \leq 3/5$. Studying only squarefree numbers I can prove (4.1).

Theorem 3 *Let $\varepsilon > 0$. If n is a squarefree number and $P(X) \in \mathbb{Z}[X]$ is a polynomial, which is not of the form $a(X+b)^k$ with $a, b \in \mathbb{Q}$, and $k \in \mathbb{N}$ then*

$$\tau_P(n) \ll (\log n)\tau(n)^{L+\varepsilon},$$

where the implied factor depends on ε and the polynomial $P(X)$.

From this by using Lemma 6 for squarefree numbers n we get

$$\tau_P(n) \ll (\log n)\tau(n)^{0.5753}. \tag{4.2}$$

This result improves on the constant $c(\Delta)$ in La Bretèche's Theorem C if n is a squarefree number and Δ is not a square of an integer.

I think that (4.2) might be extended to every integer n by generalizing Lemma 5, however I was not able to prove it. Most probably the truth is

$$\tau_P(n) \ll \tau(n)^{o(1)},$$

but it seems hopeless to prove it.

The proof of Theorem 3 uses similar technics than Theorem 1, but the exponent (if we use the best known upper bound for L) is only slightly sharper, thus here we only sketch the proof.

Sketch of the proof of Theorem 3

Let $c_1 > 1$ be a constant small enough, depending only on the polynomial $P(X)$. Write

$$\mathcal{D}_i = \{P(x) > 0 : \ x \in \mathbb{Z}, \ c_1^i \le P(x) < c_1^{i+1}, \ P(x) \mid n\}.$$

We will prove that if $\{d_1, d_2\} \ne \{d_3, d_4\}$, then

$$d_1 d_2 = d_3 d_4 \quad \text{with } d_1, d_2, d_3, d_4 \in \mathcal{D}_i \tag{4.3}$$

is not possible. Then by the definition of L we get

$$|\mathcal{D}_i| \ll 2^{(L+\varepsilon)\omega(n)},$$

from which the theorem follows. Let us see the proof of (4.3).

Define $Q(X) = P(X - \frac{a_{k-1}}{k a_k})$. Then the coefficient of x^{k-1} in $Q(X)$ is 0. Clearly,

$$\mathcal{D}_i = \{Q(x) > 0 : \ x + \frac{a_{k-1}}{k a_k} \in \mathbb{Z}, \ c_1^i \le Q(x) < c_1^{i+1}, \ Q(x) \mid n\}$$

Suppose that contrary to (4.3), there exists $Q(x), Q(y), Q(z), Q(v) \in \mathcal{D}_i$ such that

$$Q(x)Q(y) = Q(z)Q(v).$$

Then there exists integers a, b, c, d such that

$$ac = Q(x), \qquad ad = Q(v),$$
$$bc = Q(z), \qquad bd = Q(y).$$

Then

Lemma 7 *There exists a constant $c_2 > 1$ depending only on the polynomial $P(X)$ such that*

$$c_2 ac < bd.$$

Proof of Lemma 7

This is Lemma 1 in [13] if $xy - zv \neq 0$ and Lemma 5 in [13] if $xy - zv = 0$.

By Lemma 7

$$c_2 Q(x) < Q(y). \tag{4.4}$$

Now we fix the value $c_1 > 1$ in the definition of $\mathcal{D}_i$: let $c_1 = c_2$. By $Q(x), Q(y) \in \mathcal{D}_i$ and (4.4) we have

$$c_1^{i+1} \leq c_1 Q(x) < Q(y) < c_1^{i+1}$$

which is a contradiction.

References

[1] A. Balog, P. Erdős and G. Tenenbaum, *On arithmetic functions involving consecutive divisors*, In: B. Berndt, H. Diamond, H. Halberstam, A. Hildebrand (eds), *Analytic number theory* (Urbana, 1989), Prog. Math. 85, 77-90 (Birkäuser, 1990).

[2] Y. Bugeaud, A. Dujella, *On a problem of Diophantus for higher powers*, Math. Proc. Cambridge Philos. Soc. 135 (2003), 1-10.

[3] Y. Bugeaud, K. Gyarmati, *On generalizations of a problem of Diophantus*, Illinois J. Math. 48 (2004), 1105-1115.

[4] G. Cohen, S. Litsyn, G. Zémor, *Binary B_2-Sequences: A New Upper Bound*, J. Comb. Theory, Ser. A 94, No. 1., 152-155 (2001).

[5] R. de la Bretèche, *Nombre de valeurs polynomials qui divisent un entier*, Math. Proc. Camb. Phil. Soc. 131 (2001), 193-209.

[6] R. de la Bretèche, *Sur une classe de fonctions arithmétiques liées aux diviseurs d'un entier*, Indag. Mathem., New Ser., 11 (2000), 437-452.

[7] A. Dujella, *An absolute bound for the size of Diophantine m-tuples*, J. Number Theory 89 (2001), 126-150.

[8] A. Dujella, *On Diophantine quintuples*, Acta Arith. 81 (1997), 69-79.

[9] P. Erdős, *Some of my new and almost new problems and results in combinatorial number theory*, Number Theory (Eger, 1996) (de Gruyter, 1998), 169-179.

[10] P. Erdős and R. R. Hall, *On some unconventional problems on the divisors of integers*, J. Austral. Math. Soc. (Series A) 25 (1978), 479-485.

[11] P. Erdős and G. Tenenbaum, *Sur les fonctions arithmétiques liées aux diviseurs consécutifs*, J. Number Theory 31 (1989), 285-311.

[12] J. H. Evertse, *On equations in S-units and the Thue-Mahler equation*, Invent. Math. 75 (1984) 561-584.

[13] K. Gyarmati, *A polynomial extension of a problem of Diophantus*, Publ. Math. Debrecen 66/3-4 (2005), 389-405.

[14] K. Gyarmati, *On a problem of Diophantus*, Acta Arith. 97.1 (2001), 53-65.

[15] B. Lindström, *On B_2-Sequences of Vectors*, J. Number Theory 4 (1972), 261-265.

[16] H. Maier and G. Tenenbaum, *On the set of divisors of an integer*, Invent. Math. 76, (1984), 121-128.

[17] G. Tenenbaum, *Une inégalité de Hilbert pour les diviseurs*, Indag. Mathem., New Ser. 2, (1), (1991), 105-114.

[18] S. Wigert, *Sur l'ordre de grandeur du nombre de diviseurs d'un entier*, Arkiv für Mathematik 3 (1906/1907), 1-9.