On multiplicative bases of finite sets

Katalin Fried
Eötvös Loránd University, Institute of Mathematics,
Department of Mathematics Teaching and Education Center
H-1117 Budapest, Pázmány Péter st. 1/C, Hungary
Email: kfried@cs.elte.hu

and

Katalin Gyarmati
Eötvös Loránd University, Institute of Mathematics,
Department of Algebra and Number Theory and
MTA–ELTE Geometric and Algebraic Combinatorics
Research Group
H-1117 Budapest Pázmány Péter sétány 1/C, Hungary
Email: gykati@cs.elte.hu

2010 Mathematics Subject Classification: Primary: 11B75, 11B13, Secondary: 11B83.

Keywords and phrases: multiplicative basis

Research supported by Hungarian National Research Development and Innovation Funds NK 104183 and K 119528,

Abstract

We study the density of multiplicative bases of subsets of $\mathbb{Z}$ formed by values of polynomials.

1 Introduction

Throughout the paper we will use the following notation: For a set $\mathcal{S} \subseteq \mathbb{Z}$ we denote by $\mathcal{S}(n)$ the cardinality of the set $\mathcal{S} \cap [1, 2, \ldots, n]$. We say that a set $\mathcal{B} \subseteq \mathbb{Z}$ forms a multiplicative basis of order h of $\mathcal{S}$ if every element of $\mathcal{S}$ can be written as the product of h members of $\mathcal{B}$. While the study of additive bases is an intensively studied topic in additive number theory, much less attention is devoted to multiplicative bases. First multiplicative basis of $[n] \stackrel{\text{def}}{=} [1, 2, \ldots, n]$ were studied. It is easy to see that every multiplicative basis of $[n]$ contains the prime numbers up to n. On the other hand in 2011 Chan [2] prove that there is a multiplicative basis with less than $\pi(n) + c(h+1)^2 \frac{n^{2/(h+1)}}{\log^2 n}$ elements (however he did not use this terminology of multiplicative bases). This upper bound has been recently sharpened by a factor h by Pach and Sándor [22]. Namely if $G_h(n)$ denotes the size of the smallest multiplicative basis of order h of $[n]$ then

$$\pi(n) + 0.5h\frac{n^{2/(h+1)}}{\log^2 n} \leq G_h(n) \leq \pi(n) + 150.4h\frac{n^{2/(h+1)}}{\log^2 n}.$$

Slightly related problems were studied by Erdős [9]. Next a few definitions follow.

Definition 1 *In general for a set $\mathcal{S}$ we denote by $G_h(\mathcal{S})$ the size of the smallest multiplicative basis of order h. A basis $\mathcal{B}$ of order h is a* ***minimal basis of order*** *h* ***of*** *$\mathcal{S}$ if $|\mathcal{B}| = |G_h(\mathcal{S})|$. We call $\mathcal{B}$ a* ***giant basis of order*** *h* ***of*** *$\mathcal{S}$ if $|\mathcal{B}| \geq |\{1\} \cup \mathcal{S}|$.*

In this paper we will study multiplicative basis of order 2 of the set $S(f(x), n) \stackrel{\text{def}}{=} [f(1), f(2), \ldots, f(n)]$ where $f(x) \in \mathbb{Z}[x]$ is a polynomial. (A related problem was studied by Hajdu and Sárközy in [12], namely they studied multiplicative decomposability of polynomial sets.)

Clearly, if $f(x)$ is of the form $f(x) = x^r$ then from Chan [2] and Pach and Sándor's [22] the following result immediately follows

Proposition 1

$$\pi(n) \le G_h(S(x^r, n)) \le \pi(n) + 150.4h\frac{n^{2/(h+1)}}{\log^2 n}.$$

So, for these polynomials $f(x) = x^r$ we know the exact order of magnitude of $G_h(S(f(x), n))$. Now we will study the case of other polynomials. First we study the simplest case $f(x) = x^2 + 1$. One may conjecture that the set $S(x^2 + 1, n)$ has only giant bases, but it turned out that this is not the case. There exists a basis with slightly less elements than $|\{1\} \cup S(f(x), n)|$. On the other hand we will prove that every multiplicative basis of $S(x^2 + 1, n)$ has at least as many elements as the number of prime numbers of the form $4k + 1$ between n and $2n$. In other words:

Theorem 1 *For every $\varepsilon > 0$ there exists a constant $n_0 = n_0(\varepsilon)$ such that for $n > n_0$ we have*

$$\left(\frac{1}{2} - \varepsilon\right)\frac{n}{\log n} \le G_h(S(x^2 + 1, n)) \le n - n^{1/2} + (1 + \varepsilon)n^{1/4}.$$

There is a huge gap between the lower and upper bound. It is an interesting question which one is closer to the truth.

Problem 1 *Does there exist a constant $\varepsilon_1 > 0$ such that*

$$\varepsilon_1 n \le G_2(S(x^2 + 1, n)) \le (1 - \varepsilon_1)n$$

is always true?

Next we study the case of general polynomials $f(x)$. In this case we will be able to prove the following:

Theorem 2 *Let $f(x) \in \mathbb{Z}[x]$ be a polynomial of degree $r \geq 2$ and write $f(x)$ as a product of irreducible polynomials over $\mathbb{Z}[x]$, say*

$$f(x) = f_1(x) f_2(x) \cdots f_s(x), \tag{1}$$

where s denotes the number of irreducible factors in (1). Then

$$\frac{n}{(\log n)^{s \log r / \log 2}} \ll G_2(S(f(x), n)).$$

We remark that from Theorem 2 immediately follows the following:

Corollary 1 *Let $f(x) \in \mathbb{Z}[x]$ be a polynomial of degree $r \geq 2$. Then*

$$\frac{n}{(\log n)^{r \log r / \log 2}} \ll G_2(S(f(x), n)).$$

In case of the polynomial $f(x) = x^2 + 1$, the lower bound in Theorem 2 gives the same result as the one in Theorem 1.

As a general upper bound we are able to give the trivial bound $|\{1\} \cup S(f(x), n)| \leq n + 1$. Related to the upper bound we ask the following questions.

Problem 2 *Is there any polynomial $f(x)$ such that for every n the set $S(f(x), n)$ has only giant bases of order 2, in other words do we have for every basis $\mathcal{B}$ of order 2 the following*

$$|\mathcal{B}| \geq |\{1\} \cup S(f(x), n)|?$$

Or, is there a general non-trivial upper bound for $G_2(S(f(x), n))$?

Perhaps the lower bound in Theorem 2 can be sharpened. We also ask the following:

Problem 3 *Is it possible to give a general better lower bound for $G_2(S(f(x), n))$ than the bound $\frac{n}{(\log n)^{s \log r / log 2}}$ in Theorem 2?*

So far we have been studying multiplicative bases of $S(f(x), n) = \{f(1), f(2), f(3), \ldots, f(n)\}$. Next we study the multiplicative bases of its subsets, i.e. sets of the form

$$\mathcal{W} \stackrel{\text{def}}{=} \{f(a_1), f(a_2), f(a_3), \ldots, f(a_k)\}, \tag{2}$$

where $1 \le a_1 < a_2 < \cdots < a_k \le n$ are integers. If $\mathcal{B}$ is a multiplicative basis of order 2 of $\mathcal{W}$, then each elements of $\mathcal{W}$ can be written in the form $b_i b_j$ with $b_i, b_j \in \mathcal{B}$, thus

$$|\mathcal{W}| \le |\mathcal{B}|^2,$$

and so

$$|\mathcal{W}|^{1/2} \le |\mathcal{B}|. \tag{3}$$

In case of polynomials $f(x)$ of degree 2, this problem is slightly related to the study of Diophantine tuples (see e.g. [1], [4], [5], [6], [7], [8], [13]).

We will study whether (3) is the best possible general lower bound? Under some not too restrictive conditions on the a_i's in $\mathcal{W}$ we will prove $|\mathcal{W}|^{2/3} \ll |\mathcal{B}|$:

Theorem 3 *Let $f(x) \in \mathbb{Z}[x]$ be a polynomial of degree $\deg f \ge 2$ and $u, a_1, a_2, \ldots, a_k$ be positive integers such that*

$$u \le a_1 < a_2 < \cdots < a_k < 2u. \tag{4}$$

We define $\mathcal{W}$ by (2). If $\mathcal{B}$ is a multiplicative basis of order 2 of $\mathcal{W}$ then

$$|\mathcal{W}|^{2/3} \ll |\mathcal{B}|. \tag{5}$$

Remark 1 *If $f(x)$ is of the form $f(x) = x^r + a_{r-3}x^{r-3} + \cdots + a_{r-4}x^{r-4} + \cdots + a_0$ (so the coefficients of the terms x^{r-1} and x^{r-2} are 0), then Theorem 3 also holds if in place of (4) only $u \le a_1 < a_2 < \cdots < a_k < u^2$ holds.*

Related to Theorem 3 we ask the following

Problem 4 *Is it true that the lower bound* (5) *holds for arbitrary a_i's, i.e. is condition* (4) *indeed necessary in Theorem 3? In this general case which lower bound can be given for* $|\mathcal{B}|$*?*

Remark 2 *Let $\mathcal{B}$ be a multiplicative basis of order 2 of the set $\mathcal{W}$ defined in Theorem 3. Probably, the lower bound* (5) *in case of certain special polynomials might be sharpened to* $|\mathcal{W}|^{3/4} \ll |\mathcal{B}|$. *For more details see the end of the proof of Theorem 3.*

Finally we will say a few words about sets having only giant bases. Clearly the set $I = [a^2, a^2+1, a^2+2, \ldots, a^2+a]$ has only giant bases: Let $\mathcal{B}$ be a multiplicative basis of I of order 2. We split $\mathcal{B}$ into two disjoint subsets, so $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$ where

$$\mathcal{B}_1 \stackrel{\text{def}}{=} \{b \in \mathcal{B} : \ b \le a\}$$
$$\mathcal{B}_2 \stackrel{\text{def}}{=} \{b \in \mathcal{B} : \ b \ge a+1\}.$$

If $b_i b_j \in I$ and $b_i < b_j$, then $b_i \le a$ and $b_j \ge a+1$. Thus for $b_i b_j \in I$ and $b_i < b_j$, we have $b_i \in \mathcal{B}_1$ and $b_j \in \mathcal{B}_2$.

For each $b \in \mathcal{B}_2$ there exists at most one element i of I for which $b \mid i$ since $|I| = a+1 \le b$. Thus

$$a+1 = |I| \le |\mathcal{B}_2| < |\mathcal{B}|,$$

from which the statement follows.

Our final problem is the following:

Problem 5 *Let $I = [m+1, m+2, \ldots, m+n]$ and $d \ge 2$ is an integer. For which m and n's does I have only giant bases?*

2 Proofs of Theorem 1 and 2

Proof of Theorem 1

First we prove that for $n > n_0(\varepsilon)$ we have

$$\left(\frac{1}{2} - \varepsilon\right) \frac{n}{\log n} \leq G_h(S(x^2+1, n)). \tag{6}$$

Let $\mathcal{B}$ be a multiplicative basis of order h of $S(x^2+1, n)$. Let $\mathcal{P}$ denote the following set

$$\mathcal{P} \overset{\text{def}}{=} \{p : \ p \text{ is a prime of form } 4k+1 \text{ and } n < p < 2n\}. \tag{7}$$

For every prime $p \in \mathcal{P}$ we assign the smallest positive integer $g = g(p)$ with

$$p \mid g(p)^2 + 1.$$

Since for $p \in \mathcal{P}$, p is a prime number of form $4k+1$, the congruence

$$x^2 \equiv -1 \pmod{p}$$

has two different solutions, and one of them is between 1 and $(p-1)/2$, thus

$$1 \leq g(p) \leq \frac{p-1}{2} < n. \tag{8}$$

Since $\mathcal{B}$ is a multiplicative basis of $S(x^2+1, n)$ it is also a multiplicative basis of its subsets, namely $\mathcal{B}$ is a multiplicative basis of

$$S_1 \overset{\text{def}}{=} \{g(p)^2 + 1 : \ p \in \mathcal{P}\}$$

since $S_1 \subset S(x^2+1, n)$ by (8).

For every $p \in \mathcal{P}$, S_1 contains a multiple of p since $p \mid g(p)^2 + 1$. Thus $\mathcal{B}$ contains a multiple of p, which we denote by $h(p)$. Thus $h(p) \in \mathcal{B}$ and $p \mid h(p)$.

We will prove that for $p, q \in \mathcal{P}$, $p \neq q$

$$h(p) = h(q)$$

is not possible. Contrary, suppose that $p \neq q$ and $h(p) = h(q)$. Then

$$p \mid h(p), \ q \mid h(q).$$

Thus

$$pq \mid h(p) = h(q).$$

Since $p, q \in \mathcal{P}$ we have $n+1 \leq p, q$ so

$$(n+1)^2 \leq pq \leq h(p) = h(q). \tag{9}$$

But $\mathcal{B}$ is a multiplicative basis of $S(x^2+1, n)$ so its elements are less or equal to n^2+1, thus

$$h(p) = h(q) \leq n^2 + 1,$$

which contradicts (9).

Thus the function $h: \ \mathcal{P} \to \mathcal{B}$ is injective, so

$$|\mathcal{P}| \leq |\mathcal{B}|,$$

which proves (6).

In order to prove

$$G_h(S(x^2+1, n)) \leq n - n^{1/2} + (1+\varepsilon)n^{1/4}.$$

we will prove a slightly stronger upper bound, namely $G_h(S(x^2+1, n)) \leq n - n^{1/2} + n^{1/4} + 2$. It is enough to construct a multiplicative basis $\mathcal{B}$ of order h of $S(x^2+1, n)$ with

$$|\mathcal{B}| \leq n - n^{1/2} + n^{1/4} + 2.$$

First observe that

$$\left(a^2+1\right)\left((a+1)^2+1\right) = \left(a^2+a+1\right)^2 + 1. \tag{10}$$

Let

$$\mathcal{B} \stackrel{\text{def}}{=} \{x^2+1: \ 0 \leq x \leq n\} \setminus \{\left(a^2+a+1\right)^2+1: \ n^{1/2}+0.5 \leq a^2+a+1 \leq n\}.$$

In order to prove that $\mathcal{B}$ is a multiplicative basis of order h it is enough to prove that for $1 \leq x \leq n$ the integer x^2+1 can be written as a product of h

elements of $\mathcal{B}$. If x is not of the form a^2+a+1 where $n^{1/2}+0.5 \le a^2+a+1 \le n$, then it is clear that

$$x^2 + 1 = b_1 b_2 b_3 \cdots b_h \tag{11}$$

where $b_1 = x^2 + 1 \in \mathcal{B}$ and $b_2 = b_3 = \cdots = b_h = 1 \in \mathcal{B}$.

If $x = a_1^2 + a_1 + 1$ for some integer a_1 and $n^{1/2} + 0.5 \le a_1^2 + a_1 + 1 \le n$, then by (10)

$$x^2 + 1 = \left(a_1^2 + a_1 + 1\right)^2 + 1 = \left(a_1^2 + 1\right) \left((a_1 + 1)^2 + 1\right).$$

Thus

$$x^2 + 1 = b_1 b_2 b_3 \cdots b_h,$$

with $b_1 = a_1^2 + 1,\ b_2 = (a_1 + 1)^2 + 1,\ b_3 = \cdots = b_h = 1$. It is easy to see that from $a_1^2 + a_1 + 1 \le n$ follows

$$a_1 < a_1 + 1 < n^{1/2} + 0.5.$$

So

$$b_1, b_2 \notin \{y^2 + 1 : n^{1/2} + 0.5 \le y \le n\},$$

therefore

$$b_1, b_2 \notin \{\left(a^2 + a + 1\right)^2 + 1 :\ n^{1/2} + 0.5 \le a^2 + a + 1 \le n\}.$$

Thus by the definition of $\mathcal{B}$ we have $b_1, b_2 \in \mathcal{B}$ and we also have $b_3 = b_4 = \cdots = b_h = 1 \in \mathcal{B}$. Computing the number of elements of $\mathcal{B}$ we get

$$|\mathcal{B}| \le n - n^{1/2} + n^{1/4} + 2,$$

which was to be proved.

Proof of Theorem 2

Throughout the proof $c_1, c_2, c_3, \ldots$ will denote constants depending only on the polynomial $f(x)$. We may also suppose that the leading coefficient of $f(x)$ is positive.

Let $\tau(a)$ denote the number of positive divisors of a positive integer a. It is well-known that

$$\sum_{a=1}^{n} \tau(a) = n \log n + O(n).$$

In 1952 Erdős [10] extended this result to polynomials, namely he proved the following:

Lemma 1 (Erdős) *Let $f(x) \in \mathbb{Z}[x]$ be an irreducible polynomial. There exist positive integers c_1 and c_2 depending on $f(x)$ such that for $n \geq 2$ we have*

$$c_1 n \log n < \sum_{a=1}^{n} \tau(f(a)) < c_2 n \log n. \qquad (12)$$

Here we mention that Erdős gave an existence proof, and he could not give bounds on the order of magnitude of the constants c_1 and c_2 in Lemma 1. Recently Lapkova [17] achieved some good bounds in the case of polynomials of degree 2. Related results can be found in [3].

In order to prove Theorem 2 we will need only the upper bound in (12). Let s denote the number of irreducible factors $f_j(x)$ in (1). Using Erdős's lemma we will prove the following:

Lemma 2 *There exists a constant c_3 depending only on the polynomial $f(x)$ such that for every integer n large enough we have that the set*

$$E(f(x), n) \stackrel{\text{def}}{=} \{a : n/4 \leq a \leq n \text{ and } \tau(f(a)) < c_3 (\log n)^s\} \qquad (13)$$

has at least $n/4$ different elements.

Proof of Lemma 2

Let s denote the number of irreducible factors $f_j(x)$ in (1). By Erdős's lemma for $1 \leq j \leq s$ we have

$$\sum_{a=1}^{n} \tau(f_j(a)) < c_2 n \log n.$$

Thus

$$\sum_{a=1}^{n}\left(\tau(f_1(a))+\tau(f_2(a))+\cdots+\tau(f_s(a))\right)<sc_2 n\log n=c_4 n\log n. \tag{14}$$

Let

$$\mathcal{A}_1 \stackrel{\text{def}}{=} \{1\le a\le n:\ \tau(f_1(a))+\tau(f_2(a))+\cdots+\tau(f_s(a))\ge 2c_4\log n,\}$$
$$\mathcal{A}_2 \stackrel{\text{def}}{=} \{1\le a\le n:\ \tau(f_1(a))+\tau(f_2(a))+\cdots+\tau(f_s(a))< 2c_4\log n.\}$$

Clearly $\mathcal{A}_1$ and $\mathcal{A}_2$ are disjoint and

$$|\mathcal{A}_1|+|\mathcal{A}_2|=n. \tag{15}$$

By (14)

$$\begin{aligned}|\mathcal{A}_1|\cdot 2c_4\log n &\le \sum_{a\in\mathcal{A}_1}\left(\tau(f_1(a))+\tau(f_2(a))+\cdots+\tau(f_s(a))\right)\\ &\le \sum_{a=1}^{n}\left(\tau(f_1(a))+\tau(f_2(a))+\cdots+\tau(f_s(a))\right)\\ &< c_4 n\log n.\end{aligned}$$

Thus

$$|\mathcal{A}_1|<n/2.$$

From this and (15) we have

$$|\mathcal{A}_2|>n/2. \tag{16}$$

Next we will use the inequality $\tau(xy)\le\tau(x)\tau(y)$ and the inequality of arithmetic and geometric means. For $a\in\mathcal{A}_2$ we have

$$\begin{aligned}\tau(f(a)) &= \tau\left(f_1(a)f_2(a)\cdots\tau f_s(a)\right)\\ &\le \tau\left(f_1(a)\right)\tau\left(f_2(a)\right)\cdots\tau\left(f_s(a)\right)\\ &\le \left(\frac{\tau\left(f_1(a)\right)+\tau\left(f_2(a)\right)+\cdots+\tau\left(f_s(a)\right)}{s}\right)^s\\ &< \left(\frac{2c_4\log n}{s}\right)^s\\ &= c_5(\log n)^s.\end{aligned} \tag{17}$$

Define $\mathcal{C}$ by

$$\mathcal{C} \stackrel{\text{def}}{=} \{a: \ n/4 \le a < n \text{ and } a \in \mathcal{A}_2\}.$$

Clearly by (16) we have

$$|\mathcal{C}| \ge |\mathcal{A}_2| - n/4 > n/4. \tag{18}$$

Since $\mathcal{C} \subseteq \mathcal{A}_2$ by (17) we have for $a \in \mathcal{C}$

$$\tau(f(a)) < c_5 (\log n)^s.$$

Thus if we define $E(f(x), n)$ by (13) with c_5 in place of c_3 we have $\mathcal{C} \subseteq E(f(x), n)$. By this and (18) we have

$$n/4 < |\mathcal{C}| \le |E(f(x), n)|,$$

which proves Lemma 2.

Define $F(f(x), n)$ by

$$F(f(x), n) \stackrel{\text{def}}{=} \{f(a) : n/4 \le a \le n \text{ and } \tau(f(a)) < c_3 (\log n)^s\} \tag{19}$$

Since for fixed number c the equation $f(x) = c$ has at most $r = \deg f$ solutions we have

$$|F(f(x), n)| \ge \frac{1}{r} |E(f(x), n)| > \frac{n}{4r} = c_6 n. \tag{20}$$

Next we prove the following:

Lemma 3 *Let $\mathcal{B}$ be a multiplicative basis of $F(f(x), n)$ of order 2. Then*

$$|\mathcal{B}| \gg \frac{n}{(\log n)^{s \log r / \log 2}}.$$

From Lemma 3 we immediately get Theorem 2. If $\mathcal{B}$ is a multiplicative basis of $S(f(x), n)$ then it is also a multiplicative basis of $F(f(x), n)$ by $F(f(x), n) \subseteq S(f(x), n)$.

Proof of Lemma 3

Define a graph $\mathcal{G}$ by the following: its vertices are the elements of $\mathcal{B}$. Two vertices v_1, v_2 are joined by an edge $\{v_1, v_2\}$ if and only if

$$v_1 v_2 \in F(f(x), n).$$

In other words there exists $a \in E(f(x), n)$ (so $n/4 \leq a < n$ and $\tau(f(a)) < c_3(\log n)^s$) such that

$$v_1 v_2 = f(a). \tag{21}$$

By the definition of $F(f(x), n)$ we have

$$\max\{\tau(v_1), \tau(v_2)\} \leq \tau(v_1 v_2) < c_3(\log n)^s. \tag{22}$$

Then for the number of vertices and edges of $\mathcal{G}$ we have

$$|V(\mathcal{G})| = |\mathcal{B}| \tag{23}$$

$$|E(\mathcal{G})| \geq |F(f(x), n)| > c_6 n. \tag{24}$$

Let $f(x)$ be of the form $f(x) = a_r x^r + a_{r-1} x^{r-1} + \cdots + a_1 x + a_0$. Since in (21) $a \geq n/4$, provided that n is large enough, we have

$$v_1 v_2 = f(a) > \frac{a_r}{2} a^r > \frac{a_r}{2}(n/4)^r = c_7^2 n^r \geq c_7^2 n^2.$$

So for an arbitrary edge $e = \{v_1, v_2\}$ of $\mathcal{G}$ we have

$$v_1 > c_7 n \text{ or } v_2 > c_7 n. \tag{25}$$

We split the set of vertices $\mathcal{B}$ into two disjoint sets:

$$\mathcal{B}_1 = \{v \in \mathcal{B} : \ v > c_7 n\}$$

$$\mathcal{B}_2 = \{v \in \mathcal{B} : \ v \leq c_7 n\}$$

By (25) clearly for every edge $e = \{v_1, v_2\}$ of $\mathcal{G}$ we have $v_1 \in \mathcal{B}_1$ or $v_2 \in \mathcal{B}_1$. Thus if we denote by $d(v)$ the degree of a vertex $v \in \mathcal{B}$ in $\mathcal{G}$ then

$$|E(\mathcal{G})| \leq \sum_{v \in \mathcal{B}_1} d(v). \tag{26}$$

In Lemma 4 we give an estimate on the degree of a vertex of $\mathcal{B}_1$:

Lemma 4 *For $v \in \mathcal{B}_1$ we have*

$$d(v) \ll (\log n)^{s \log r / \log 2}$$

Before proving Lemma 4 we show that from Lemma 4 we immediately get Lemma 3. From Lemma 4, (24) and (26) follows

$$\begin{aligned} c_6 n < |E(\mathcal{G})| \le \sum_{v \in \mathcal{B}_1} d(v) \ll \sum_{v \in \mathcal{B}_1} (\log n)^{s \log r / \log 2} \ll |\mathcal{B}_1| (\log n)^{s \log r / \log 2} \\ \ll |\mathcal{B}| (\log n)^{s \log r / \log 2} \end{aligned}$$

from which follows

$$\frac{n}{(\log n)^{s \log r / \log 2}} < |\mathcal{B}|$$

which proves Lemma 3. Thus in order to prove Theorem 2 it is enough to prove Lemma 4.

Proof of Lemma 4

If $d(v) = 0$ then the statement of the lemma is trivial. Suppose that there exist $v' \in \mathcal{B}$ such that $e = \{v, v'\}$ is an edge of $\mathcal{G}$, so there exists $n/4 \le a < n$ for which $\tau(f(a)) < c_3 (\log n)^s$ and

$$vv' = f(a).$$

Then

$$\tau(v) \le \tau(vv') = \tau(f(a)) < c_3 (\log n)^s. \tag{27}$$

Next a few notations will follow. Let $D(f)$ denote the discriminant of the polynomial $f(x)$. For a prime p denote by $\ell(p)$ the largest integer for which

$$p^{\ell(p)} \mid D(f)$$

(thus $p^{\ell(p)+1} \nmid D(f)$). For $m \in \mathbb{N}$ denote by $N(f(x), m)$ the number of solutions of the congruence

$$f(x) \equiv 0 \pmod{m}.$$

In 1921 Nagel [18] and Ore [19] proved that if p is a prime and $k \in \mathbb{N}$ then

$$N(f(x), p^k) \le rp^{2\ell(p)}. \tag{28}$$

This was considerably improved by Sándor [20], Huxley [14] and Stewart [21], but for our purpose (28) is sufficient. Let m be a composite number. By the Chinese Remainder Theorem we have

$$N(f(x), m) = \prod_{p^k || m} N(f(x), p^k).$$

Using (28) we have

$$\begin{aligned} N(f(x), m) &\le \prod_{p|m} rp^{2\ell(p)} = r^{\omega(m)} \prod_{p|m} p^{2\ell(p)} \\ &= r^{\omega(m)} \prod_{p|m,\ \ell(p)\neq 0} p^{2\ell(p)} \le r^{\omega(m)} \prod_{p,\ \ell(p)\neq 0} p^{2\ell(p)} \\ &\le r^{\omega(m)} \prod_{p|D(f)} p^{2\ell(p)} = r^{\omega(m)} D(f)^2 \\ &= c_8 r^{\omega(m)}. \end{aligned} \tag{29}$$

Now we are ready to give an upper bound for $d(v)$ if $v \in \mathcal{B}_1$. We get

$$\begin{aligned} d(v) &= |\{v' \in \mathcal{B} :\ vv' = f(a) \text{ with } a \in E(f(x), n)\}| \\ &\le |\{a \in E(f(x), n) :\ f(a) \equiv 0 \pmod{v}\}| \\ &\le |\{1 \le a \le n :\ f(a) \equiv 0 \pmod{v}\}| \end{aligned}$$

Since $v \in \mathcal{B}_1$ thus $v > c_7 n$. Let $c_9 = \lceil \frac{1}{c_7} \rceil$ then

$$\begin{aligned} d(v) &\le \left| \{1 \le a \le \frac{1}{c_7} v :\ f(a) \equiv 0 \pmod{v}\} \right| \\ &\le |\{1 \le a \le c_9 v :\ f(a) \equiv 0 \pmod{v}\}| \\ &\le c_9 \, |\{1 \le a \le v :\ f(a) \equiv 0 \pmod{v}\}| \\ &= c_9 N(f(x), v). \end{aligned}$$

By (29) we have

$$\begin{aligned} d(v) &\leq c_9 c_8 r^{\omega(v)} = c_{10} r^{\omega(v)} \\ c_{10}\left(2^{\omega(v)}\right)^{\log r/\log 2} &= c_{10}\tau(v)^{\log r/\log 2}. \end{aligned}$$

By (27) we have

$$d(v) < c_{10}\left(c_3(\log n)^s\right)^{\log r/\log 2} = c_{11}(\log n)^{s\log r/\log 2},$$

which completes the proof of Lemma 4, from which Theorem 2 follows.

Proof of Theorem 3

Let $f(x)$ be a polynomial of the form

$$f(x) = a_r x^r + a_{r-1}x^{r-1} + \cdots + a_1 x + a_0.$$

Define β by $\beta \stackrel{\text{def}}{=} \frac{a_{r-1}}{ra_r}$ and the polynomial $p(x)$ is

$$\begin{aligned} p(x) &\stackrel{\text{def}}{=} f(x-\beta) \\ &= a_r\left(x - \frac{a_{r-1}}{ra_r}\right)^r + a_{r-1}\left(x - \frac{a_{r-1}}{ra_r}\right)^{r-1} + \ldots a_1\left(x - \frac{a_{r-1}}{ra_r}\right) + a_0. \end{aligned}$$

Clearly $p(x)$ is of the form

$$p(x) = q_r x^r + q_m x^m + q_{m-1}x^{m-1} + q_{m-2}x^{m-2} + \cdots + q_1 x + q_0, \tag{30}$$

where $q_m \neq 0$ and $m \leq r-2$ (or, in other words the coefficients $q_{r-1}, q_{r-2}, \ldots, q_{m+1}$ of $p(x)$ are 0). Here we also remark that if $a_{r-1} = 0$ then $f(x) = p(x)$.

Let $\mathcal{B} = \{b_1, b_2, \ldots, b_t\}$ be a multiplicative basis of $\mathcal{W}$ of order 2.

We will use the following lemma

Lemma 5 *There exist constants c_1 and $c_2 > 1$ depending only on the polynomial $f(x)$ $(= p(x-\beta))$ such that if b_1, b_2, b_3, b_4 are integers greater than c_1*

for which

$$b_1b_3 = f(x_1) = p(x_1 - \beta)$$
$$b_1b_4 = f(x_2) = p(x_2 - \beta)$$
$$b_2b_3 = f(x_3) = p(x_3 - \beta)$$
$$b_2b_4 = f(x_4) = p(x_4 - \beta)$$

hold for some integers x_1, x_2, x_3, x_4. Then

$$c_2b_1b_3 < b_2b_4 \text{ if } m = r - 2 \text{ in } (30) \text{ and}$$
$$c_2\left(b_1b_3\right)^2 < b_2b_4 \text{ if } m \leq r - 3 \text{ in } (30).$$

Proof of Lemma 5. This is a combination of Lemma 1 and Lemma 2 in [15].

We define the following graph $\mathcal{G}$. Its vertices are the elements of $\mathcal{B}$, so $V(\mathcal{G}) = \mathcal{B}$. There is an edge between the vertices $b_1 \in \mathcal{B}$ and $b_2 \in \mathcal{B}$ if and only if there exists an $1 \leq i \leq s$ such that

$$b_1b_2 = f(a_i) = p(a_i - \beta).$$

We will denote this edge by $\{b_1, b_2\}$.

Since $\mathcal{B}$ is a multiplicative basis of order 2 of $\mathcal{W}$, for the number of the edges of $\mathcal{G}$ we have

$$|E(\mathcal{G})| \geq |\mathcal{W}|. \tag{31}$$

Next we will use the constants c_1 and c_2 defined in Lemma 5. We will color the edges of $\mathcal{G}$ by different colors. We color an edge $\{b_1, b_2\}$ of $\mathcal{G}$ by the first color if $b_1 \leq c_1$ or $b_2 \leq c_1$. Clearly, the number of edges colored by the first color is $\leq 2c_1|\mathcal{B}|$. For $i \geq 2$ we color the edge $\{b_1, b_2\}$ of $\mathcal{G}$ by the i-th color if

$$c_2^{i-2}u \leq b_1b_2 < c_2^{i-1}u. \tag{32}$$

Here $b_1b_2 = f(a_i)$ for some $1 \le i \le s$. Since the leading coefficients of $f(x)$ is positive and by (4) we have

$$\frac{a_r}{2} < f(a_1), \dots, f(a_k) < 2a_r u^r$$

if u is large enough depending on the polynomial $f(x)$. By this and (32) the number of different colors is less than a constant c_4 depending on the polynomial $f(x)$.

By Lemma 5 the graph $\mathcal{G}$ does not contain a cycle of length 4, where the edges of the cycle are colored by the same i-th color for an $i \ge 2$. By the Kövári-Sós-Turán theorem [16] we have that if a graph $\mathcal{G}$ has n vertices and it does not contain a cycle of length 4, than it has at most

$$1 + n + \left[\frac{1}{2}n^{3/2}\right] \tag{33}$$

edges. (Here we remark that in [16] the authors studied matrices containing 0's and 1's and not graphs, but considering the adjacency matrix of $\mathcal{G}$ one may get the upper bound in (33).) Since we have at most c_4 different colors we have

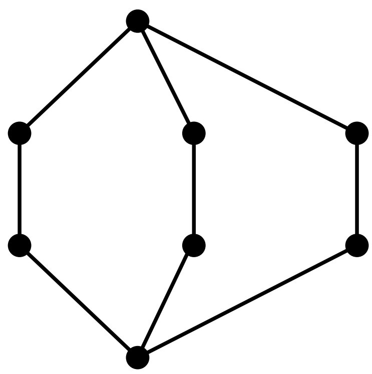
$$|E(\mathcal{G})| \ll |V(\mathcal{G})|^{3/2} = |\mathcal{B}|^{3/2},$$

where the implied constant depend on the polynomial $f(x)$. Using (31) we get

$$|\mathcal{W}| \ll |\mathcal{B}|^{3/2},$$

from which the theorem follows.

Probably, it can be proved that if m in (30) is significantly smaller than r which is the degree of the polynomial, then the subgraphs $\mathcal{G}_i$ of $\mathcal{G}$ formed by the edges of $\mathcal{G}$ colored by the i-th color (where $i \ge 2$) do not contain the following graph $\theta_{3,3}$:



From this, using Faudree and Simonovits theorem [11] in extremal graph theory one may obtain the bound

$$|\mathcal{W}| \leq \sum_i E(\mathcal{G}_i) \ll c_1 |\mathcal{B}| + \sum_{i \geq 2} |V(\mathcal{G}_i)|^{1+1/3} \ll |\mathcal{B}|^{4/3},$$

from which

$$|\mathcal{B}| \gg |\mathcal{W}|^{3/4} \tag{34}$$

follows. Here, we remark that the proof that these subgraphs of $\mathcal{G}$ do not contain $\theta_{3,3}$ can be rather lengthly and complicated, and the desired lower bound (34) is just slightly stronger than the one in Theorem 3 and it is also far from the truth. Thus we do not work out the details of the proof here.

Acknowledgments The authors would like to thank the referee for his careful reading and valuable comments.

References

[1] A. Baker and H. Davenport, *The equations* $3x^2-2=y^2$ *and* $8x^2-7=z^2$, Quart J. Math. Oxford Ser. (2) 20 (1969), 129-137.

[2] T. H. Chan, *On sets of integers, none of which divides the product of k others*, Eur. J. Comb. (3) 32 (2011), 443-447.

[3] F. Delmer, *Probléme de diviseurs*, Séminaire de théorie des nombres de Bordeaux, Volume (1970-1971), Talk no. 22, p. 1-20.

[4] L. E. Dickson, *History of the Theory of Numbers* Vol. 2, Chelsea, New-York 1966, 514-519.

[5] Diophantus of Alexandria, *Arithmetics and the Book of Polygonal Numbers*, (I. G. Bashmakova, Ed.), Nauka, Moscow, 1974 (Russian), 103-104, 232.

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

[7] A. Dujella, *There are only finitely many Diophantine quintuples*, J. Reine Angew. Math. 566 (2004), 183-214.

[8] A. Dujella and A. Pethő, *A generalization of a theorem of Baker and Davenport*, Quart. J. Math. Oxford Ser. (2), 49 (1998), 291-306.

[9] P. Erdős, *On sequences of integers no one of which divides the product of two others and some related problems*, Mitt. Forsch.-Inst. Math. Mech. Univ. Tomsk 2 (1938), 74-82.

[10] P. Erdős, *On the sum* $\sum_{k=1}^{x} d(f(k))$, J. London Math. Soc. 27 (1952), 7-15.

[11] R. J. Faudree and M. Simonovits, *On a class of degenerate extremal graph problems*, Combinatorica 3 (1) (1983), 83-93.

[12] L. Hajdu and A. Sárközy, *On multiplicative decompositions of polynomial sequences I*, Acta Arith., to appear.

[13] Bo He, A. Togbé and V. Ziegler, *There is no Diophantine quintuple*, Trans. Am. Math. Soc., to appear.

[14] M. N. Huxley, *A note on polynomial congruence*, in: Recent progress in analytic number theory, volume I, eds.: H. Halberstam, C. Hooley, 193-196, 1981, London, Academic Press.

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

[16] T. Kövári, V. T. Sós, P. Turán, *On a problem of K. Zarankiewicz*, Colloquium Math. 3, (1954). 50-57.

[17] K. Lapkova, *Explicit upper bound for an average number of divisors of irreducible quadratic polynomials*, Monatsh. Math. (2017).

[18] T. Nagel, *Généralisation d'un théorème de Tchebicheff*, Journ. de Math. 8 (1921) 343-356.

[19] O. Ore, *Anzahl der Wurseln höherer Kongruenzen*, Norsk Matematisk Tidsskrift, 3 Aagang, Kristiana (1921), 343-356.

[20] G. Sándor, *Uber die Anzahl der Lösungen einer Kongruenz*, Acta Math. 87 (1952), 13-17.

[21] C. L. Stewart, *On the number of solutions of polynomial congruences*, C. R. Math. Rep. Acad. Sci. Canada, Vol. XIII 6 (1991), 271-273.

[22] P. P. Pach, Cs. Sándor, *Multiplicative bases and an Erdős Problem*, Combinatorica, to appear.