Bull. Math. Soc. Sci. Math. Roumanie
Tome 54(102) No. 1, 2011, 65–81

Polynomials expressible by sums of monic integer irreducible polynomials

by
Artūras Dubickas

Abstract

We prove an asymptotical formula for the number of representations of a given monic polynomial $f \in \mathbb{Z}[x]$ by the sum of $k \geqslant 2$ monic irreducible polynomials in $\mathbb{Z}[x]$ whose heights are bounded by T. The main term turns out to be $c_{d,k}T^{(d-1)(k-1)}$, where $d = \deg f$ and $c_{d,k}$ is some positive rational number. The binary case $k = 2$ was first considered by Hayes in 1965 as a version of a binary Goldbach problem for polynomials. In this case, we improve the error term in a recent asymptotical formula (due to Kozek) and show that our error term is best possible for each $d \geqslant 2$.

Key Words: Irreducible polynomial, height, Goldbach's problem for polynomials.
2010 Mathematics Subject Classification: Primary 11R09; Secondary 11C08.

1 Introduction

Let f be a monic polynomial in $\mathbb{Z}[x]$ of degree $d \geqslant 2$, and let $k \geqslant 2$ and T be two positive integers. We write $\mathcal{N}(f, k, T)$ for the number of representations of f by the sum of k monic irreducible (over $\mathbb{Q}$) integer polynomials $f_1, f_2, \dots, f_k$ of height at most T, i.e.,

$$f(x) = f_1(x) + f_2(x) + \dots + f_k(x), \tag{1}$$

where $H(f_i) \leqslant T$ for $i = 1, 2, \dots, k$. Recall that the polynomial

$$g(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x],$$

where $a_n \neq 0$, is called *monic* if $a_n = 1$, and its *height* is defined by the formula $H(g) := \max_{0 \leqslant i \leqslant n} |a_i|$. We say that $g \in \mathbb{Z}[x]$ is *reducible* if it is a product of some two non-constant polynomials in $\mathbb{Z}[x]$ and *irreducible* otherwise. Of course, by (1), for each permutation σ of the set $\{1,\dots,k\}$, the sum $f_{\sigma(1)}(x)+f_{\sigma(2)}(x)+\dots+f_{\sigma(k)}(x)$ is also equal to $f(x)$. This is understood as the same representation of f by the sum of $f_1,\dots,f_k$, i.e., in $\mathcal{N}(f,k,T)$ we only take into account distinct collections of monic irreducible polynomials $f_1,\dots,f_k$ summing to f.

For $k=2$, the problem of representations of a given polynomial by the sum of two irreducible polynomials was first considered by Hayes [6] who looked at this problem as a version of Goldbach's conjecture for polynomials. He showed that every polynomial of degree d in $\mathbb{Z}[x]$ can be expressed by the sum of two irreducible polynomials in $\mathbb{Z}[x]$, both of degree d. This result was later rediscovered by Rattan and Stewart [12]. See also the subsequent papers Hayes [7], Effinger and Hayes [5], Car [3] for an asymptotical formula for the number of representations of f by sums of the form $g_1f_1+g_2f_2+g_3f_3$, where g_1,g_2,g_3 are some fixed polynomials over a finite field $\mathbb{F}_q[x]$. Recently, Pollack [11] generalized the result of Hayes [6] to polynomials in the ring $R[x]$, where R is a Noetherian domain with infinitely many maximal ideals. Using methods similar to those initiated by Hayes, one can also restrict the problem to monic polynomials and show that $\mathcal{N}(f,2,T)\geqslant 1$ for T large enough. See, e.g., the paper of Betts [1].

There is a simple explanation why sometimes those problems are referred to as Goldbach's problems for polynomials. In 1742, Goldbach conjectured that every integer greater than 5 can be written as the sum of three primes and that every even integer greater than 2 can be written as the sum of two primes. In the context of polynomials, it is natural to replace a "positive integer" by a "monic integer polynomial" and a "prime number" by a "monic irreducible integer polynomial". Then the inequality $\mathcal{N}(f,2,T)\geqslant 1$ asserts that each monic integer polynomial is the sum of some two monic irreducible integer polynomials of height at most T.

In fact, there are many such representations. By a result of Saidak [13], the true size of $\mathcal{N}(f,2,T)$ is T^{d-1}. More precisely, he showed that, for T large enough,

$$T^{d-1}\ll\mathcal{N}(f,2,T)\ll T^{d-1}$$

for each monic integer polynomial of degree d, where the constants in Vinogradov's symbol $\ll$ are independent of T. Finally, Kozek [9] established the asymptotical formula

$$\mathcal{N}(f,2,T)=(2T)^{d-1}+O(T^{d-2}\log T) \tag{2}$$

as $T\to\infty$. Although in [9] the formula (2) is stated for $d\geqslant 2$, but it only holds for $d\geqslant 3$. This is because Lemma 2 of [9] only holds for $d\geqslant 3$ rather than for $d\geqslant 2$. (In the notation of Lemma 5 below, Lemma 2 of [9] asserts that $|M(a,d,T)|\ll T^{d-2}\log T$, where $M(a,d,T)$ is the set of monic integer reducible polynomials of degree d and of height at most T whose coefficients for x^{d-1} are equal to a. So, by Lemma 5 (*iii*) below, the correct upper bound for $d=2$ should be $|M(a,2,T)|\ll\sqrt{T}$.) Our first theorem gives the best possible error terms in (2):

Theorem 1. *Let $f \in \mathbb{Z}[x]$ be a monic polynomial of degree $d \geqslant 2$. Then, as $T \to \infty$,*

$$\mathcal{N}(f, 2, T) = (2T)^{d-1} + O(T^{d-2}) \tag{3}$$

for $d \geqslant 4$,

$$T \log T \ll (2T)^2 - \mathcal{N}(f, 2, T) \ll T \log T \tag{4}$$

for $d = 3$, and

$$\sqrt{T} \ll 2T - \mathcal{N}(f, 2, T) \ll \sqrt{T} \tag{5}$$

for $d = 2$. Moreover, for each $d \geqslant 4$, the error term in (3) *is best possible for some f.*

Given nonnegative real numbers u, v, we define

$$\Lambda(n, u, v) := \{0 \leqslant x_1, \ldots, x_n \leqslant u,\ \ x_1 + \cdots + x_n \leqslant v\} \subset \mathbb{R}^n, \tag{6}$$

and put

$$V_n := \mathrm{vol}(\Lambda(n, 1, (n-1)/2)). \tag{7}$$

Our second theorem extends the asymptotical formula (2) from $k = 2$ to $k \geqslant 2$:

Theorem 2. *Let $f \in \mathbb{Z}[x]$ be a monic polynomial of degree $d \geqslant 2$, and let $k \geqslant 2$ be an integer. Then, as $T \to \infty$,*

$$\mathcal{N}(f, k, T) = \frac{(2^{k-1}(1 - 2V_{k-1}))^{d-1}}{(k-1)!} T^{(d-1)(k-1)} + O(T^{dk-d-k}) \tag{8}$$

for $d \geqslant 4$,

$$\mathcal{N}(f, k, T) = \frac{(2^{k-1}(1 - 2V_{k-1}))^{2}}{(k-1)!} T^{2(k-1)} + O(T^{2k-3} \log T) \tag{9}$$

for $d = 3$, and

$$\mathcal{N}(f, k, T) = \frac{2^{k-1}(1 - 2V_{k-1})}{(k-1)!} T^{k-1} + O(T^{k-3/2}) \tag{10}$$

for $d = 2$.

Note that the polyhedron $\Lambda(n, 1, (n-1)/2)$ (that is, the intersection of a finite number of closed half-spaces) is contained in the polyhedron $\Lambda(n, 1, n/2)$ whose volume is $1/2$. (This is easily seen by expressing the volume by a corresponding integral and changing the variables $x_i \mapsto 1 - x_i$ for $i = 1, \ldots, n$.) Thus, by (6) and (7), it follows that

$$0 \leqslant V_n < 1/2.$$

It is easy to see that the volume of the polyhedron $V(n, u, v)$ is a rational number for rational u, v, because the (oriented) volume of a convex body with $n + 1$ vertices $e_0, \ldots, e_n$ in $\mathbb{R}^n$ is expressible by a determinant with coordinates of the vertices as $\frac{1}{n!}\det(e_1 - e_0, \dots, e_n - e_0)$ and we can cut $V(n, u, v)$ into finitely many of such convex bodies. Thus V_{k-1} is a rational number for every integer $k \geqslant 2$.

Evidently, for $k = 2$, by (6) and (7), we have $V_{k-1} = V_1 = 0$, so (8) implies (3). The values of the constant V_n for $n \in \{2, 3, 4, 5\}$ can be easily calculated:

Proposition 3. *For V_n defined in* (6) *and* (7), *we have $V_2 = 1/8$, $V_3 = 1/6$, $V_4 = 77/384$ and $V_5 = 9/40$.*

Proof: Clearly, $\Lambda(2, 1, 1/2)$ is a right triangle with coordinates $(0, 0)$, $(0, 1/2)$, $(1/2, 0)$. Its area is $V_2 = (1/2)^3 = 1/8$. Similarly, $\Lambda(3, 1, 1) = \{0 \leqslant x_1, x_2, x_3 \leqslant 1,\ x_1 + x_2 + x_3 \leqslant 1\}$ is a simplex with coordinates $(0, 0, 0)$, $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$. Its volume is $V_3 = 1/3! = 1/6$.

To compute V_4 and V_5, we first recall that the volume of the simplex

$$V(n, s, s) = \{0 \leqslant x_1, \dots, x_n \leqslant s,\ \ x_1 + \dots + x_n \leqslant s\} \subset \mathbb{R}^n$$

with side s is equal to $s^n/n!$. By (6), $\Lambda(4, 1, 3/2)$ is a simplex with side $3/2$ minus four "small" simplexes with sides $1/2$. Thus

$$V_4 = \frac{(3/2)^4}{4!} - 4\frac{(1/2)^4}{4!} = \frac{81 - 4}{2^4 \cdot 4!} = \frac{77}{384}.$$

Finally, $\Lambda(5, 1, 2)$ is a simplex with side 2 minus five "small" simplexes with sides 1. Hence

$$V_5 = \frac{2^5}{5!} - 5\frac{1}{5!} = \frac{9}{40}$$

which completes the proof. $\square$

The results of Theorem 2 and Proposition 3 can be given in the following table (where the last column is the asymptotical formula as $T \to \infty$):

k	V_{k-1}	$2^{k-1}(1 - 2V_{k-1})$	$(k-1)!$	$\mathcal{N}(f, k, T)$, $\deg f = d$
2	0	2	1	$(2T)^{d-1}$
3	1/8	3	2	$\left(3T^2\right)^{d-1}/2$
4	1/6	16/3	6	$\left(16T^3/3\right)^{d-1}/6$
5	77/384	115/12	24	$\left(115T^4/12\right)^{d-1}/24$
6	9/40	88/5	120	$\left(88T^5/5\right)^{d-1}/120$

In the next section we state some earlier relevant results and also prove some auxiliary lemmas. Then in Sections 3 and 4 we shall complete the proofs of Theorems 2 and 1, respectively.

2 Monic polynomials with one fixed coefficient

Let $d, T \geqslant 1$ be two integers. We denote by $M(d,T)$ the set of monic integer reducible polynomials of degree d and of height at most T. The result of Chela [4] asserts that

$$|M(d,T)| \sim 2^d(\zeta(d-1) + 1/2 - 2V_{d-1})T^{d-1} \quad \text{as} \quad T \to \infty \tag{11}$$

for each $d \geqslant 3$ (because the constant k_d defined [4] equals $2^{d-1}(1-2V_{d-1})$) and

$$|M(2,T)| \sim 2T \log T \quad \text{as} \quad T \to \infty. \tag{12}$$

To prove (11) Chela used the following result of van der Waerden [14] (which will also use below):

Lemma 4. *Let $M_\ell(d,T)$ be the set of monic integer polynomials of degree $d \geqslant 2$ and of height at most T with a factor of degree ℓ, where $1 \leqslant \ell \leqslant d/2$. Then, as $T \to \infty$,*

$$T^{d-\ell} \ll |M_\ell(d,T)| \ll T^{d-\ell} \tag{13}$$

for $\ell < d/2$ and

$$T^{d/2} \log T \ll |M_{d/2}(d,T)| \ll T^{d/2} \log T \tag{14}$$

for $\ell = d/2$ and d even, where the constants in $\ll$ depend only on d and ℓ.

Let us denote by $M(a,d,T)$ the set of monic integer reducible polynomials of degree d and of height at most T whose coefficients for x^{d-1} are equal to a. In this section we shall prove the next lemma.

Lemma 5. *If $d, T \geqslant 2$ and a are three integers then, as $T \to \infty$,*
(i) $T^{d-2} \ll |M(a,d,T)| \ll T^{d-2}$ *for* $d \geqslant 4$,
(ii) $T \log T \ll |M(a,3,T)| \ll T \log T$,
(iii) $\sqrt{T} \ll |M(a,2,T)| \ll \sqrt{T}$,
where all the implied constants in $\ll$ depend only on d.

For the proof of Lemma 5 we shall need the following:

Lemma 6. *Let a, d, T, s be four integers such that $T \geqslant |s| \geqslant 2$ and $d \geqslant 3$. Then the number of solutions $(h_{d-2}, \dots, h_0) \in \mathbb{Z}^{d-1}$ of the linear equation*

$$s^d + as^{d-1} + h_{d-2}s^{d-2} + \dots + h_0 = 0$$

satisfying $|h_i| \leqslant T$ for each $i = 0, \dots, d-2$ does not exceed $(2T/|s| + 1)^{d-1}$.

Proof: It suffices to prove the lemma for $s > 0$, because in case $s < 0$ we can replace s by $-s$ and a by $-a$. Note that $s | h_0$. Set $H_0 := h_0/s \in \mathbb{Z}$. From $s|H_0| \leqslant T$ we see that the integer H_0 takes at most $2[T/s] + 1 \leqslant 2T/s + 1$ values. So h_0 takes at most $2T/s + 1$ values. From

$$s^{d-1} + as^{d-2} + h_{d-2}s^{d-3} + \dots + h_1 + h_0/s = 0$$

we derive that s divides $h_1+h_0/s = h_1+H_0$. So, for each fixed h_0, the integer h_1 belongs to the residue class $-H_0 \pmod{s}$ and $|h_1| \leqslant T$. There at most $2T/s+1$ of such integers h_1. Arguing in this way, namely, each time dividing by s and considering h_j with some fixed $h_{j-1},\dots,h_0$, we obtain the factor $2T/s+1$ at each step up to h_{d-2} which must be uniquely determined by $h_{d-3},\dots,h_0$. Thus the number of vectors $(h_{d-2},\dots,h_0) \in \mathbb{Z}^{d-1} \cap [-T,T]^{d-1}$ for which the above linear equation holds does not exceed $(2T/s+1)^{d-1}$. This completes the proof of the lemma. □

The next lemma will be used several times below:

Lemma 7. *Let $N(b_1,\dots,b_n,b_0,T)$ denote the number of solutions $(y_1,\dots,y_n) \in \mathbb{Z}^n$ of the linear equation*

$$b_1y_1+\dots+b_ny_n=b_0 \tag{15}$$

satisfying $-T \leqslant y_i \leqslant T$ for each $i=1,\dots,n$, where $b_0 \in \mathbb{Z}$, $n \geqslant 2$, and $b_1,\dots,b_n$ are nonzero integers. Then

$$N(b_1,\dots,b_n,b_0,T) \leqslant (2T+1)^{n-1} \tag{16}$$

for each $T \in \mathbb{N}$. Moreover,

$$N(1,\dots,1,b_0,T) = 2^{n-1}(1-2V_{n-1})T^{n-1}+O(T^{n-2}) \quad \text{as} \quad T \to \infty. \tag{17}$$

Proof: The first claim is trivial, because there is most one value of y_n corresponding to every vector $(y_1,\dots,y_{n-1}) \in \mathbb{Z}^{n-1} \cap [-T,T]^{n-1}$ for which (15) holds for the vector $(y_1,\dots,y_{n-1},y_n)$. There are at most $(2T+1)^{n-1}$ of such vectors $(y_1,\dots,y_{n-1})$. Thus $N(b_1,\dots,b_n,b_0,T) \leqslant (2T+1)^{n-1}$, giving (16).

In order to prove the asymptotical formula (17), since $-T \leqslant y_n \leqslant T$, we need to estimate the number of solutions $(y_1,\dots,y_{n-1}) \in \mathbb{Z}^{n-1} \cap [-T,T]^{n-1}$ for which

$$-T+b_0 \leqslant y_1+\dots+y_{n-1} \leqslant T+b_0.$$

In case $n=2$, it is clear that $N(1,1,b_0,T)=2T+O(1)$. Assume that $n \geqslant 3$. By replacing each y_i by y_i-T, we obtain

$$(n-2)T+b_0 \leqslant y_1+\dots+y_{n-1} \leqslant nT+b_0, \tag{18}$$

where $(y_1,\dots,y_{n-1}) \in \mathbb{Z}^{n-1} \cap [0,2T]^{n-1}$.

Suppose that $|\Lambda(n,u,v)|$ is the number of integer points of the lattice $\mathbb{Z}^{n-1}$ lying in the polyhedron $\Lambda(n,u,v)$ defined in (6). Then (18) implies

$$N(1,\dots,1,b_0,T) = |\Lambda(n-1,2T,nT+b_0)|-|\Lambda(n-1,2T,(n-2)T+b_0-1)| \tag{19}$$

for $T \geqslant |b_0|+1$, since then $(n-2)T+b_0-1 \geqslant 0$.

We next claim that, for any fixed numbers $u>0$, $v \in \mathbb{R}$, and any integer $n \geqslant 3$,

$$|\Lambda(n-1,2T,uT+v)| = 2^{n-1}\mathrm{vol}(\Lambda(n-1,1,u/2))T^{n-1}+O(T^{n-2}) \,\mathrm{as}\, T \to \infty. \tag{20}$$

Then, combining (19) with (20), we would have

$$N(1,\dots,1,b_0,T) =$$
$$= 2^{n-1}(\mathrm{vol}(\Lambda(n-1,1,n/2)) - \mathrm{vol}(\Lambda(n-1,1,n/2-1)))T^{n-1} + O(T^{n-2})$$

as $T \to \infty$. This would complete the proof of (17), because, by (6) and (7),

$$\mathrm{vol}(\Lambda(n-1,1,n/2)) - \mathrm{vol}(\Lambda(n-1,1,n/2-1)) =$$
$$= 1 - 2\mathrm{vol}(\Lambda(n-1,1,n/2-1)) = 1 - 2V_{n-1}.$$

To prove (20) note that the diagonal of the unit cube in $\mathbb{R}^{n-1}$ is equal to $\sqrt{n-1}$. Hence, by continuity, there is a $\theta \in [-1,1]$ such that

$$|\Lambda(n-1,2T,uT+v)| = \mathrm{vol}(\Lambda(n-1,2T,uT+v+\theta\sqrt{n-1}))$$

provided that $uT+v+\theta\sqrt{n-1} \geqslant 0$. Note that, for every positive number r, the polyhedron $\Lambda(n-1,2T,r)$ is a blown-up body of the polyhedron $\Lambda(n-1,1,r/2T)$ scaled by $2T$, hence $\mathrm{vol}(\Lambda(n-1,2T,r)) = (2T)^{n-1}\mathrm{vol}(\Lambda(n-1,1,r/2T))$. It follows that

$$\frac{|\Lambda(n-1,2T,uT+v)|}{(2T)^{n-1}} = \mathrm{vol}(\Lambda(n-1,1,u/2+(v+\theta\sqrt{n-1})/2T))$$

$$= \mathrm{vol}(\Lambda(n-1,1,u/2)) + \frac{c(v,\theta,n)}{T}$$

with some constant $c(v,\theta,n) \in \mathbb{R}$. Multiplying both sides by $(2T)^{n-1}$ we obtain (20). $\square$

It is well-known (see, e.g., [10]) that, in general, this simple estimate for the difference between the number of lattice points in a blown-up body and its volume is best possible up to a constant. See also [2] for the best possible constants in case $n \leqslant 5$. Better bounds for the error term can be obtained if the boundary of the convex body is smooth [8] (which is not the case in (20)).

Proof of Lemma 5: In case $d = 2$ we need to estimate the number of quadratic monic reducible polynomials $x^2+ax+b \in \mathbb{Z}[x]$, where a is fixed and $|b| \leqslant T$. Such a polynomial is reducible if and only if it has an integer root, say, s. Then $b = -s^2 - as$. The number of integer solutions of the inequality $|s^2+as| \leqslant T$ is asymptotically equal to $2\sqrt{T}$. Hence $|M(a,2,T)| \leqslant 3\sqrt{T}$ for T large enough. Moreover, at most two distinct integer roots s and s' are the roots of the same polynomial x^2+ax+b. It follows that $\sqrt{T}/2 \leqslant |M(a,2,T)|$ for T large enough. This proves (iii). In fact, since each integral root is counted twice (except for some "small" set of polynomials with a double root), one can easily show that $|M(a,2,T)| \sim \sqrt{T}$ as $T \to \infty$.

To prove the lower bound in (ii), we fix a nonzero polynomial $g(x) \in \mathbb{Z}[x]$ and consider the set of reducible polynomials $M_g(T)$ of the form $g(x)x^2+h_1x+h_0$, where $|h_1|, |h_0| \leqslant T$. (In our case $g(x) = x+a$, so $M_{x+a}(T) = M(a,3,T)$.) Set

$r := \deg g \geqslant 0$. Consider all pairs $(y_1, y_2) \in \mathbb{Z}^2$ satisfying $1 \leqslant y_1 \leqslant [T^{1/(r+3)}]$, $y_1 < y_2$ and $y_1 y_2 \leqslant T/2$. Since $y_1 < y_2 \leqslant T/2y_1$, the number of such pairs is

$$\sum_{y_1=1}^{[T^{1/(r+3)}]} ([T/2y_1] - y_1) > \frac{T}{3} \sum_{y_1=1}^{[T^{1/(r+3)}]} \frac{1}{y_1} > \frac{T \log T}{3r+10} \tag{21}$$

for T large enough.

Consider the polynomial

$$f_{y_1,y_2}(x) := g(x)x^2 - (y_2 + y_1 g(y_1))x + y_1 y_2 \in \mathbb{Z}[x]. \tag{22}$$

Since g is fixed and $|y_1 y_2| \leqslant T/2$, using the upper bound for y_1, we have $|y_1 g(y_1)| < T/2$ for each sufficiently large T. Thus

$$|y_2 + y_1 g(y_1)| \leqslant T/2 + |y_1||g(y_1)| < T/2 + T/2 = T$$

for T large enough. Also, $1 \leqslant y_1 y_2 \leqslant T/2 < T$. Hence $H(f_{y_1,y_2}) \leqslant T$ provided that $T \geqslant H(g)$. Furthermore, by (22), at $x = y_1$ we have $f_{y_1,y_2}(y_1) = 0$. Thus f_{y_1,y_2} is a reducible integer polynomial of height at most T, i.e., $f_{y_1,y_2} \in M_g(T)$ for each sufficiently large T. We next claim that f_{y_1,y_2} is the same polynomial for at most $r+2$ pairs (y_1, y_2) with the restrictions as above. Combined with (21) this would imply the inequality

$$|M_g(T)| > \frac{T \log T}{(3r+10)(r+2)} \tag{23}$$

for T large enough.

To prove the above claim, let us fix any pair of positive integers (s_1, s_2). Assume that $f_{y_1,y_2} = f_{s_1,s_2}$ for some pair of positive integers (y_1, y_2). Then $y_1 y_2 = s_1 s_2$ and $y_2 + y_1 g(y_1) = s_2 + s_1 g(s_1)$, by (22). Put $\lambda := y_1/s_1 \in \mathbb{Q}$. Then the first equality yields $y_2 = s_2/\lambda$. Inserting this into the second equality we obtain

$$s_2 + s_1 g(s_1) = s_2/\lambda + \lambda s_1 g(\lambda s_1).$$

Multiplying this equality by λ gives us a polynomial in λ of degree $r+2$, so there are at most $r+2$ distinct rational numbers λ for which $f_{\lambda s_1, \lambda^{-1} s_2} = f_{s_1,s_2}$. This completes the proof of the claim. In particular, from (23) we obtain

$$T \log T \ll |M_g(T)|$$

as $T \to \infty$ for every nonzero integer polynomial g. This yields the lower bound in *(ii)*, by selecting $g(x) = x + a$.

Observe that, for each $d \geqslant 3$, the number of polynomials in $M(a, d, T)$ which have a root at $s = 0$ does not exceed $(2T+1)^{d-2}$. Also, by (16), the number of polynomials in $M(a, d, T)$ which have a root at $s = 1$ (or at $s = -1$) does not exceed $(2T+1)^{d-2}$. Hence the number of polynomials in $M(a,d,T)$ with a root in $\{-1,0,1\}$ does not exceed

$$3(2T+1)^{d-2}. \tag{24}$$

To prove the upper bound in (ii), note that $f \in M(a,3,T)$ implies that f has an integer root s in the range $[-T,T]$. By (24) (with $d=3$) and Lemma 6, we find that

$$|M(a,3,T)| \leqslant 3(2T+1) + 2\sum_{s=2}^{T}(2T/s+1) < 5T\log T$$

for each sufficiently large T. This proves the upper bound in (ii).

It is clear that each polynomial with constant coefficient zero is reducible. The set $M(a,d,T)$ contains exactly $(2T+1)^{d-2}$ of such polynomials if $T \geqslant |a|$. Thus $|M(a,d,T)| > T^{d-2}$ for $T \geqslant |a|$, giving the lower bound in (i).

It remains to prove the upper bound in (i). Let $M_1(a,d,T)$ be the subset of $M(a,d,T)$ consisting of reducible polynomials with a linear factor and an irreducible factor of degree $d-1$. Obviously,

$$M(a,d,T) \setminus M_1(a,d,T) \subset \cup_{\ell=2}^{[d/2]} M_\ell(d,T)$$

for $T \geqslant |a|$. Hence, by Lemma 4,

$$|M(a,d,T) \setminus M_1(a,d,T)| \ll T^{d-2} \tag{25}$$

for each $d \geqslant 5$. We next prove that (25) also holds for $d=4$.

Indeed, by (13) and (14), the estimate (25) holds for the set all polynomials of degree 4 lying in the set $M(a,4,T) \setminus M_1(a,4,T)$ except for a subset consisting of those which are products of two irreducible quadratic polynomials. Let us write each such a polynomial as $(x^2+a_1x+b_1)(x^2+a_2x+b_2)$. Taking into account that the coefficient for x^3 must be a, we have $a_1+a_2=a$. Considering the constant coefficient and the coefficient for x^2 we also obtain

$$|b_1b_2| \leqslant T \quad \text{and} \quad |b_1+b_2+a_1(a-a_1)| \leqslant T.$$

The number of pairs (b_1,b_2) satisfying $1 \leqslant b_1 \leqslant b_2 \leqslant T/b_1$ is equal to

$$\sum_{b_1=1}^{[\sqrt{T}]}([T/b_1]-b_1+1) \ll T\log T.$$

Thus the number of integer pairs (b_1,b_2) for which $|b_1b_2| \leqslant T$ is also $\ll T\log T$. For each such a pair we have $|b_1+b_2| \leqslant T+1$. Hence

$$|a_1(a-a_1)| \leqslant T + |b_1+b_2| \leqslant 2T+1.$$

The number of integers a_1 satisfying this inequality is $\ll \sqrt{T}$. It follows that the number of products of two irreducible quadratic polynomials is $\ll T^{3/2} \log T$. This proves (25) for $d = 4$.

Now, since each polynomial lying in $M_1(a,d,T)$ has an integral root $s \in [-T,T]$, using (24) and Lemma 6, we find that

$$|M_1(a,d,T)| \leqslant 3(2T+1)^{d-2} + 2\sum_{s=2}^{T}(2T/s+1)^{d-2} \leqslant$$
$$\leqslant 3(2T+1)^{d-2} + 3^{d-1}T^{d-2}\sum_{s=2}^{\infty} s^{2-d} \ll T^{d-2},$$

because $d \geqslant 4$. Adding this inequality to (25), we obtain

$$|M(a,d,T)| \leqslant |M_1(a,d,T)| + |M(a,d,T) \setminus M_1(a,d,T)| \ll T^{d-2} + T^{d-2} \ll T^{d-2}$$

for every $d \geqslant 4$, as claimed. □

3 Proof of Theorem 2

Lemma 8. *Let $f \in \mathbb{Z}[x]$ be a monic polynomial of degree $d \geqslant 2$, and let $\mathcal{N}_1(f,k,T)$ be the number of representations of f by the sum of k monic irreducible integer polynomials $f_1, f_2, \dots, f_k$ of height at most T and of degrees $d, d-1, \dots, d-1$, respectively. Then*

$$0 \leqslant \mathcal{N}(f,k,T) - \mathcal{N}_1(f,k,T) \ll T^{dk-d-k}, \tag{26}$$

where the constant in $\ll$ depends only on d and k.

Proof: Each representation of the polynomial

$$f(x) = x^d + a_{d-1}x^{d-1} + \dots + a_0 \in \mathbb{Z}[x]$$

by the sum of monic polynomials $f_1, \dots, f_k$ contains exactly one polynomial of degree $\deg f = d$, say f_1, and $k-1$ polynomials of degrees at most $d-1$. We need to estimate the number of representations $f(x) = f_1(x) + \dots + f_k(x)$, where $\deg f_1 = d$ and $\deg f_i < d-1$ for at least one $i \in \{2, \dots, k\}$. Assume that there are exactly q polynomials for which $\deg f_i < d$, where $1 \leqslant q \leqslant k-1$. Then the coefficient for x^{d-1} in f_1 equals $a_{d-1} - k + q + 1$. Let us denote the coefficients for x^{d-j} (where $j = 2, \dots, d$) in $f_1, \dots, f_k$ by $y_{1,d-j}, \dots, y_{k,d-j}$, respectively. Some of $y_{i,d-j}$ may be equal to zero. For example, $y_{2,d-2} = 0$ if $\deg f_2 < d-2$. In any case, $f = f_1 + \dots + f_k$ implies

$$\sum_{i=1}^{k} y_{i,d-j} = a_{d-j} \tag{27}$$

for $j = 2, \dots, d$.

It remains to estimate the number of integer solutions of the linear system (27) satisfying $|y_{i,d-j}| \leqslant T$. For $j = 2$, at least q terms in the sum $\sum_{i=2}^{k} y_{i,d-j}$ are equal to 1, and the first linear equation in (27) (corresponding to $j = 2$) contains $k - q$ unknowns. By (15) and (16), there are at most $(2T + 1)^{k-q-1}$ solutions corresponding to this linear equation. For each j in the range $3 \leqslant j \leqslant d$, the corresponding equality in (27) is a linear equation with at most k unknowns. As above, by (15) and (16), there are at most $(2T + 1)^{k-1}$ solutions corresponding to this linear equation. It follows that, for every fixed $q \in \{1, \ldots, k - 1\}$, the number of integer solutions of (27) satisfying $|y_{i,d-j}| \leqslant T$ does not exceed

$$(2T+1)^{k-q-1}(2T+1)^{(k-1)(d-2)} = (2T+1)^{(d-1)(k-1)-q} \leqslant 3^{(d-1)(k-1)}T^{dk-d-k}.$$

For each $q \in \{1, \ldots, k-1\}$, there are $\binom{k-1}{q}$ possibilities to choose the corresponding q polynomials f_i, $2 \leqslant i \leqslant k - 1$, whose degrees are strictly smaller than d. Thus

$$\mathcal{N}(f, k, T) - \mathcal{N}_1(f, k, T) \leqslant 3^{(d-1)(k-1)}T^{dk-d-k} \sum_{q=1}^{k-1} \binom{k-1}{q} \ll T^{dk-d-k},$$

which proves (26). $\square$

Lemma 9. *Let $f \in \mathbb{Z}[x]$ be a monic polynomial of degree $d \geqslant 2$, and let $\mathcal{N}_2(f, k, T)$ be the number of representations of f by the sum of k monic integer polynomials $f_1, f_2, \ldots, f_k$ of height at most T and of degrees $d, d - 1, \ldots, d - 1$, respectively. Then, as $T \to \infty$,*

$$\mathcal{N}_2(f, k, T) = \frac{(2^{k-1}(1 - 2V_{k-1}))^{d-1}}{(k-1)!} T^{(d-1)(k-1)} + O(T^{dk-d-k}) \qquad (28)$$

for each $d \geqslant 2$.

Proof: This time, in the notation of the preceding lemma, $q = 0$, $a = a_{d-1} - k + 1$,

$$f_1(x) = x^d + ax^{d-1} + \sum_{j=2}^{d} y_{1,d-j}x^{d-j},$$

$$f_i(x) = x^{d-1} + \sum_{j=2}^{d} y_{i,d-j}x^{d-j}$$

for $i = 2, \ldots, k$. Clearly, $f = f_1 + \cdots + f_k$ if and only if the $k(d - 1)$ unknowns $y_{i,d-j}$ satisfy the linear system (27).

First, let us find the total number of integer solutions of the linear system (27) satisfying $|y_{i,d-j}| \leqslant T$. Applying (17) to each of $d - 1$ linear equations (27), we derive that (27) has

$$\big(2^{k-1}(1 - 2V_{k-1})T^{k-1} + O(T^{k-2})\big)^{d-1} =$$

$$\left(2^{k-1}(1-2V_{k-1})\right)^{d-1}T^{(d-1)(k-1)}+O(T^{dk-d-k}) \tag{29}$$

integer solutions satisfying $|y_{i,d-j}| \leqslant T$. Next, we claim that the number of solutions of (1) for which $f_i = f_t$ for some $i \neq t$ is $O(T^{dk-d-k})$. Evidently, $f_1 \neq f_t$ for every $t > 1$. If $f_i = f_t$ holds for some indices i, t satisfying $2 \leqslant i < t \leqslant k$ then $k \geqslant 3$ and $y_{i,d-j} = y_{t,d-j}$ for $j = 2, \dots, t$. So the system of linear equations (27) has only $(k-1)(d-1)$ unknowns. Applying (16) with $n = k-2$ to each linear equation, we find that the number of integer solutions of (27) does not exceed

$$(2T+1)^{(d-1)(k-2)} = O(T^{(d-1)(k-2)}) = O(T^{dk-d-k+2-d}) = O(T^{dk-d-k}),$$

because $d \geqslant 2$. This proves our claim.

So we can assume that the polynomials $f_1, \dots, f_k$ of degrees $d, d-1, \dots, d-1$, respectively, are distinct. Obviously, all collections of polynomials $f_1, f_{\sigma(2)}, \dots, \dots, f_{\sigma(k)}$, where σ runs through all permutations of the set $\{2, \dots, k\}$, are the same. Therefore, when counting the number of solutions of (27), in (29) we took into account each collection of distinct polynomials $f_1, \dots, f_k$ exactly $(k-1)!$ times. Thus

$$\mathcal{N}_2(f,k,T)(k-1)! = \left(2^{k-1}(1-2V_{k-1})\right)^{d-1}T^{(d-1)(k-1)}+O(T^{dk-d-k}),$$

by (29). This proves (28). $\square$

Lemma 10. *With the notation of Lemmas 8 and 9, we have*

$$0 \leqslant \mathcal{N}_2(f,k,T)-\mathcal{N}_1(f,k,T) \ll \begin{cases} T^{dk-d-k} & \text{for } d \geqslant 4, \\ T^{2k-3}\log T & \text{for } d = 3, \\ T^{k-3/2} & \text{for } d = 2, \end{cases} \tag{30}$$

where $\deg f = d$ *and the constant in* $\ll$ *depends only on* d *and* k.

Proof: Note that in the definition of $\mathcal{N}_2$ compared with $\mathcal{N}_1$ the irreducibility is omitted. So we need to estimate from above the number of representations $f = f_1 + \dots + f_k$, where $\deg f_1 = d$, $\deg f_i = d-1$ for $i = 2, \dots, k$, and at least one f_i, $i = 1, \dots, d$, is reducible. Fix any $i \in \{1, \dots, k\}$. For $i \geqslant 2$, we have $\deg f_i = d-1$, so the number of choices for reducible polynomials f_i is $\ll T^{d-2}$ for $d \geqslant 4$, by (11), and $\ll T \log T$ for $d = 3$, by (12). (The polynomial f_i is always irreducible for $d = 2$.) For $i = 1$, $\deg f_1 = d$. In the same manner, by Lemma 5, we can see that the number of choices for reducible polynomials f_1 is $\ll T^{d-2}$ for $d \geqslant 4$, $\ll T \log T$ for $d = 3$, and $\ll \sqrt{T}$ for $d = 2$. Summarizing, we can claim that, for each fixed $i \in \{1, \dots, k\}$, there are $\ll T^{d-2}$ choices for reducible polynomials f_i when $d \geqslant 4$, $\ll T \log T$ choices when $d = 3$, and $\ll \sqrt{T}$ choices when $d = 2$.

On the other hand, by (16) and (27), the number of representations of $f - f_i$ by the sum of $k-1$ monic integer polynomials $f_1, f_2, \dots, f_{i-1}, f_{i+1}, \dots, f_k$ of height at most T does not exceed $(2T+1)^{(k-2)(d-1)}$. It follows that, for $d \geqslant 4$,

$$\mathcal{N}_2(f,k,T)-\mathcal{N}_1(f,k,T) \ll T^{(k-2)(d-1)+d-2} = T^{dk-d-k}.$$

Similarly, for $d = 3$, we obtain

$$\mathcal{N}_2(f,k,T) - \mathcal{N}_1(f,k,T) \ll T^{2(k-2)}T\log T = T^{2k-3}\log T,$$

whereas, for $d = 2$,

$$\mathcal{N}_2(f,k,T) - \mathcal{N}_1(f,k,T) \ll T^{k-2}\sqrt{T} = T^{k-3/2}.$$

This proves (30). □

Proof of Theorem 2: Combining Lemmas 8 and 10 we obtain

$$|\mathcal{N}_2(f,k,T) - \mathcal{N}(f,k,T)| \ll \begin{cases} T^{dk-d-k} \text{ for } d \geqslant 4, \\ T^{2k-3}\log T \text{ for } d = 3, \\ T^{k-3/2} \text{ for } d = 2. \end{cases}$$

This yields (8)–(10) in view of Lemma 9. □

4 Proof of Theorem 1

To prove (5) suppose that f is a monic quadratic integer polynomial $f(x) = x^2 + bx + c$. Without loss of generality assume that

$$T \geqslant 2 + |b| + |c|.$$

The polynomial f can be the sum of two monic polynomials only if they have degrees either $2, 0$ or $2, 1$. In the first case, there is only one such representation $f = f_1 + f_2$, where $f_1(x) = x^2 + bx + c - 1$ and $f_2(x) = 1$. Obviously, $H(f_1), H(f_2) \leqslant T$, so this representation must be counted if and only if the polynomial $x^2 + bx + c - 1$ is irreducible. Set $\delta := 1$ if $x^2 + bx + c - 1$ is irreducible and $\delta := 0$ otherwise.

In the second case, $2, 1$, we must have $f_1(x) = x^2 + (b-1)x + c_1$ and $f_2(x) = x + c_2$ with $c_1 + c_2 = c$. Note that f_2 is irreducible for any $c_2 \in \mathbb{Z}$. Then $H(f_1), H(f_2) \leqslant T$ if $|c_1|, |c_2| \leqslant T$. Since $c_2 = c - c_1$, we must have

$$\max(-T, c-T) \leqslant c_1 \leqslant \min(T, c+T). \tag{31}$$

This interval contains exactly $2T - |c| + 1$ integers c_1. Hence the number

$$\delta + 2T - |c| + 1 - \mathcal{N}(f,2,T)$$

is equal to the number of distinct integers c_1 in the interval (31) for which the polynomial $x^2 + (b-1)x + c_1$ is reducible.

The interval (31) contains the interval $[-T + |c|, T - |c|]$ and is contained in the interval $[-T - |c|, T + |c|]$. Hence, with notation of Lemma 5, we have

$$|M(b-1, 2, T - |c|)| \leqslant \delta + 2T - |c| + 1 - \mathcal{N}(f,2,T) \leqslant |M(b-1, 2, T + |c|)|.$$

This inequality combined with Lemma 5 (*iii*) implies

$$\sqrt{T} \ll 2T - \mathcal{N}(f,2,T) \ll \sqrt{T}$$

for T large enough. This proves (5).

Assume next that f is a monic irreducible polynomial of degree $d \geqslant 3$. If f is the sum of two monic integer polynomials f_1 and f_2, where $\deg f_1 \geqslant \deg f_2$, then these must be of degrees d and ℓ, respectively, where $\ell \in \{0,\dots,d-1\}$. Let $t(f,\ell,T)$ be the number of representations of f by the sum $f = f_1 + f_2$, with monic polynomials f_1, f_2 of degrees d and ℓ, respectively, and of heights at most T. Let also $t^*(f,\ell,T)$ be the number of such representations with both f_1 and f_2 irreducible, so that $\mathcal{N}_1(f,2,T) = t^*(f,d-1,T)$ and $\mathcal{N}_2(f,2,T) = t(f,d-1,T)$.

Write

$$f(x) = x^d + a_{d-1}x^{d-1} + \dots + a_\ell x^\ell + \dots + a_0.$$

Clearly,

$$f_1(x) = x^d + \dots + a_{\ell+1}x^{\ell+1} + (a_\ell - 1)x^\ell + g_1(x), \qquad f_2(x) = x^\ell + g_2(x)$$

with $g_1, g_2 \in \mathbb{Z}[x]$, $\deg g_1, \deg g_2 \leqslant \ell - 1$. Since $H(g_1) \leqslant T$, there are exactly $(2T+1)^\ell$ different possibilities to choose g_1. Each choice of g_1 gives a unique polynomial g_2, because

$$g_1(x) + g_2(x) = a_{\ell-1}x^{\ell-1} + \dots + a_0$$

if $\ell > 0$ and $g_1(x) = g_2(x) = 0$ if $\ell = 0$. It follows that

$$t(f,\ell,T) \leqslant (2T+1)^\ell \tag{32}$$

for each sufficiently large T.

We next estimate the number of representations $f = f_1 + f_2$ with $\ell = \deg f_2 = d-1$ from below. Then

$$f_1(x) = x^d + (a_{d-1} - 1)x^{d-1} + g_1(x), \qquad f_2(x) = x^{d-1} + g_2(x)$$

with $g_1, g_2 \in \mathbb{Z}[x]$, $\deg g_1, \deg g_2 \leqslant d-2$. Assume that $H(f) = h$. Then total number of such representations (which does not take into account reducibility), $\mathcal{N}_2(f,2,T) = t(f,d-1,T)$, is at least $(2T-2h+1)^{d-1}$ (because each coefficient of g_1 can be taken in the interval $[-T+h, T-h]$) and, by (32), at most $(2T+1)^{d-1}$. Therefore,

$$(2T-2h+1)^{d-1} \leqslant t(f,d-1,T) \leqslant (2T+1)^{d-1}. \tag{33}$$

For a special polynomial

$$f_h(x) := x^d + x^{d-1} + h(x^{d-2} + \dots + x + 1), \tag{34}$$

each coefficient of g_1 can be in the interval $[-T+h, T]$, so we have

$$t(f_h, d-1, T) = (2T-h+1)^{d-1}. \tag{35}$$

The number

$$\sum_{\ell=0}^{d-1}(t(f,\ell,T)-t^*(f,\ell,T))=\sum_{\ell=0}^{d-1}t(f,\ell,T)-\mathcal{N}(f,2,T)$$

is equal to to the number of distinct pairs of monic polynomials (f_1,f_2), where $\deg f_1=d$, $\deg f_2<d$, and at least one of the polynomials f_1,f_2 is reducible. Taking into account only monic reducible polynomials of degree d with coefficient for x^{d-1} equal to $a_{d-1}-1$, we find that

$$|M(a_{d-1}-1,d,T)|\leqslant\sum_{\ell=0}^{d-1}t(f,\ell,T)-\mathcal{N}(f,2,T) \tag{36}$$

On the other hand, using $t(f,\ell,T)-t^*(f,\ell,T)\leqslant t(f,\ell,T)$ for $\ell\leqslant d-2$ and

$$t(f,d-1,T)-t^*(f,d-1,T)=\mathcal{N}_2(f,2,T)-\mathcal{N}_1(f,2,T)\leqslant$$

$$|M(a_{d-1}-1,d,T)|+|M(d-1,T)|,$$

we obtain

$$\sum_{\ell=0}^{d-1}t(f,\ell,T)-\mathcal{N}(f,2,T)\leqslant|M(a_{d-1}-1,d,T)|+|M(d-1,T)|+\sum_{\ell=0}^{d-2}t(f,\ell,T).$$

Therefore,

$$\mathcal{N}(f,2,T)\geqslant-|M(a_{d-1}-1,d,T)|-|M(d-1,T)|+t(f,d-1,T). \tag{37}$$

Now, we can complete the proof of Theorem 1. Assume first that $d=3$. Then, from (12), Lemma 5 (*ii*), (33) and (37), we obtain

$$\begin{aligned}(2T)^2-\mathcal{N}(f,2,T)&\leqslant(2T)^2+|M(a_2-1,3,T)|+|M(2,T)|-(2T-2h+1)^2\\&\leqslant 4(2h-1)T+|M(a_2-1,3,T)|+|M(2,T)|\ll T\log T\end{aligned}$$

for T large enough. On the other hand, from Lemma 5 (*ii*), (32) and (36), we derive that

$$T\log T\ll 1+(2T+1)+(2T+1)^2-\mathcal{N}(f,2,T)=(2T)^2-\mathcal{N}(f,2,T)+6T+2.$$

This proves (4).

As we already observed earlier, (8) implies (3). It remains to prove that the error term in (3) is optimal. For this, we shall consider the polynomial f_h defined in (34). Employing (32), (35) and (36), we find that

$$\mathcal{N}(f_h,2,T)\leqslant\sum_{\ell=0}^{d-1}t(f_h,\ell,T)\leqslant 1+(2T+1)+\cdots+(2T+1)^{d-2}+(2T+1-h)^{d-1}.$$

Fix any $h \geqslant 2$. Since $d \geqslant 4$, for T large enough, we derive that

$$\mathcal{N}(f_h, 2, T) \leqslant 3 \cdot 2^{d-3}T^{d-2} + (2T-h+1)^{d-1} \leqslant 3 \cdot 2^{d-3}T^{d-2} + (2T-1)^{d-1}$$
$$< 3 \cdot 2^{d-3}T^{d-2} + (2T)^{d-1} - (d-2)(2T)^{d-2} = (2T)^{d-1} - (2d-7)2^{d-3}T^{d-2}$$
$$\leqslant (2T)^{d-1} - T^{d-2}.$$

This implies
$$T^{d-2} < (2T)^{d-1} - \mathcal{N}(f_h, 2, T),$$
so the error term $O(T^{d-2})$ in (3) for $f = f_h$ cannot be strengthened.

References

[1] C. Betts, *Additive and subtractive irreducible monic decompositions in* $\mathbb{Z}[x]$, C. R. Math. Acad. Sci. Soc. R. Can., **20** (1998), 86–90.

[2] J. Bokowski, *Gitterpunktsanzahl und Parallelkörpervolumen von Eikörpern,* Monatsh. Math., **79** (1975), 93–101.

[3] M. Car, *The generalized polynomial Goldbach problem,* J. Number Theory, **57** (1996), 22–49.

[4] R. Chela, *Reducible polynomials,* J. London Math. Soc., **38** (1963), 183–188.

[5] G.W. Effinger and D.R. Hayes, *A complete solution to the polynomial 3-primes problem,* Bull. Amer. Math. Soc. (N.S.), **24** (1991), 363–369.

[6] D.R. Hayes, *A Goldbach theorem for polynomials with integer coefficients,* Amer. Math. Monthly, **72** (1965), 45–46.

[7] D.R. Hayes, *The expression of a polynomial as a sum of three irreducibles,* Acta Arith., **11** (1966), 461–488.

[8] E. Hlawka, *Über integrale auf konvexen Körpern. I, II,* Monatsh. Math., **54** (1950), 1–36, 81–99.

[9] M. Kozek, *An asymptotic formula for Goldbach's conjecture with monic polynomials,* Amer. Math. Monthly, **117** (2010), 365–369.

[10] M. Peter, *Lattice points in convex bodies with planar points on the boundary,* Monatsh. Math., **135** (2002), 37–57.

[11] P. Pollack, *On polynomial rings with a Goldbach property,* Amer. Math. Monthly, **118** (2011), 71–77.

[12] A. Rattan and C. Stewart, *Goldbach's conjecture for* $\mathbb{Z}[x]$, C. R. Math. Acad. Sci. Soc. R. Can., **20** (1998), 83–85.

[13] F. Saidak, *On Goldbach's conjecture for integer polynomials,* Amer. Math. Monthly, **113** (2006), 541–545.

[14] B.L. van der Waerden, *Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt,* Monatscheft für Matematik und Physik, **43** (1936), 133–147.

Received: 26.12.2010
Accepted: 06.01.2011.

Department of Mathematics and Informatics
Vilnius University
Naugarduko 24, Vilnius LT-03225
Lithuania
E-mail: arturas.dubickas@mif.vu.lt