VOL. 148

2017

NO. 2

AN ASYMPTOTIC FORMULA FOR GOLDBACH'S CONJECTURE WITH MONIC POLYNOMIALS IN $\mathbb{Z}[\theta][x]$

BY ABÍLIO LEMOS and ANDERSON LUÍS ALBUQUERQUE DE ARAUJO (Viçosa)

Abstract. Let $k \geq 2$ be a squarefree integer, and

 $\theta = \begin{cases} \sqrt{-k} & \text{if } -k \not\equiv 1 \pmod{4}, \\ (\sqrt{-k}+1)/2 & \text{if } -k \equiv 1 \pmod{4}. \end{cases}$

We prove that the number R(y) of representations of a monic polynomial $f(x) \in \mathbb{Z}[\theta][x]$, of degree $d \geq 1$, as a sum of two monic irreducible polynomials g(x) and h(x) in $\mathbb{Z}[\theta][x]$, with the coefficients of g(x) and h(x) bounded in modulus by y, is asymptotic to $(4y)^{2d-2}$.

1. Introduction. In 1965, Hayes [H1] showed that Goldbach's conjecture is considerably simpler for polynomials with integer coefficients.

THEOREM 1.1. If f(x) is a monic polynomial in $\mathbb{Z}[x]$ of degree d > 1, then there are monic irreducible polynomials g(x) and h(x) in $\mathbb{Z}[x]$ with f(x) = g(x) + h(x).

In a recent note, Saidak [S], improving on a result of Hayes, obtained a Chebyshev-type estimate for the number $R(y) = R_f(y)$ of representations of the monic polynomial $f(x) \in \mathbb{Z}[x]$ of degree d > 1 as a sum of two irreducible monics g(x) and h(x) in $\mathbb{Z}[x]$, with the coefficients of g(x) and h(x) bounded in absolute value by y. Saidak's argument with slight modifications shows that, for y sufficiently large,

$$c_1 y^{d-1} < R(y) < c_2 y^{d-1},$$

where c_1 and c_2 are constants that depend on the degree and coefficients of the polynomial f(x).

Recently, Kozek [K] proved that R(y) is asymptotic to $(2y)^{d-1}$, i.e.,

$$\lim_{y \to \infty} \frac{R(y)}{(2y)^{d-1}} = 1.$$

Published online 9 March 2017.

²⁰¹⁰ Mathematics Subject Classification: Primary 11R09; Secondary 11C08. Key words and phrases: irreducible polynomial, Goldbach's problem for polynomials. Received 11 April 2016; revised 5 July 2016.

His approach implies that there is a constant c_3 , depending only on d, such that if y is sufficiently large, then

$$R(y) = (2y)^{d-1} + E$$
, where $|E| \le c_3 y^{d-2} \ln y$.

In 2011, Dubickas [D1] proved a more general result for the number of representations of f as a sum of r monic irreducible (over \mathbb{Q}) integer polynomials f_1, \ldots, f_r of height at most y, i.e.,

 $f(x) = f_1(x) + \dots + f_r(x).$

For r = 2, he proved that

(1)
$$R(y) = (2y)^{d-1} + O(y^{d-2})$$

for $d \ge 4$,

(2)
$$R(y) = (2y)^2 + O(y\ln(y))$$

for d = 3, and

(3) $R(y) = 2y + O(\sqrt{y})$

for d = 2. Moreover, for each $d \ge 4$, the error term in (1) is the best possible for some f. Note that these results improve the error term proved by Kozek [K].

In 2013, Dubickas [D2] proved a necessary and sufficient condition on the list of nonzero integers $u_1, \ldots, u_r, r \ge 2$, under which a monic polynomial $f(x) \in \mathbb{Z}[x]$ is expressible by a linear form $u_1f_1(x) + \cdots + u_rf_r(x)$ in monic polynomials $f_1(x), \ldots, f_r(x) \in \mathbb{Z}[x]$.

We say that a ring D has property (GC) if

every element of D[x] of degree $d \ge 1$ can be written as the sum of two irreducibles in D[x].

If D is the ring of integers, then Theorem 1.1 implies that \mathbb{Z} has property GC. Pollack proved the following:

PROPOSITION 1.1 ([P2, Theorem 1]). Suppose that D is an integral domain which is Noetherian and has infinitely many maximal ideals. Then D has property (GC).

COROLLARY 1.1 ([P2, Theorem 2]). If S is any integral domain, then D = S[x] has property (GC).

When $D = \mathbb{F}_q$ is a finite field (note that in this case, the assumptions of Proposition 1.1 do not hold), Hayes [H2], in 1966, gave an asymptotic formula for the number R(f) of representations of an odd polynomial $f(x) \in$ $\mathbb{F}_q[x]$ as a sum $\alpha g(x) + \beta h(x) + \gamma t(x) = f(x)$ with three monic irreducible polynomials g(x), h(x) and t(x) in $\mathbb{F}_q[x]$, where α, β, γ in \mathbb{F}_q^* are such that $\alpha + \beta + \gamma = f_r$ and f_r is the leading coefficient of f(x). Hayes' formula is

$$R(f) = r^{-3}q^{2r}S(f) + O(q^{1/4}q^{(5/4+\epsilon)r}),$$

where $r = \deg f$, S(f) is the singular series (see [H2, (6.10)]), and the constant implied in O is independent of both f and q. The number ϵ is defined as $\max\{1/2, \epsilon^*\}$, where ϵ^* is the least upper bound of the real parts of the zeros of certain *L*-functions. Advances in this direction can be found in Pollack [P1, P3], Webb [W] and Car [C1, C2, C3].

In this paper, we do not distinguish the sum g(x) + h(x) from h(x) + g(x)and we recall that a monic polynomial in $\mathbb{Z}[x]$ is irreducible over \mathbb{Z} if and only if it is irreducible over \mathbb{Q} .

Following the results of Hayes and Pollack with $D = \mathbb{Z}[\theta]$, where θ has the properties described in Lemma 2.1 below, and following the ideas of Kozek [K], we prove that the number R(y) of representations of a monic polynomial $f(x) \in \mathbb{Z}[\theta][x]$ as a sum of two monic irreducible polynomials g(x) and h(x) in $\mathbb{Z}[\theta][x]$, with the coefficients of g(x) and h(x) bounded in modulus by y, is asymptotic to $(4y)^{2d-2}$.

2. Notation and preliminary results. Some well known facts are presented below. Let $f(x) = \sum_{i=0}^{d} f_i x^i$ be a polynomial in $\mathbb{C}[x]$. Set

$$H(f) = \max_{0 \le i \le d} |f_i| \quad \text{and} \quad M(f) = \exp\left(\int_0^1 \ln|f(e^{2\pi it})|\,dt\right).$$

The expressions H(f) and M(f) are known as the *height* and *Mahler's* measure of f, respectively (see [M1, M2]). Mahler [M2] showed that for $0 \le i \le n$, $|f_i| \le {n \choose i} M(f)$, and that M(f) is multiplicative. Another result of Mahler is

(4)
$$\frac{M(f)}{\sqrt{d+1}} \le H(f) \le 2^{d-1}M(f).$$

An important property of Mahler's measure is

(5)
$$1 \le M(f) \le \left(\sum_{i=0}^{d} |f_i|^2\right)^{1/2},$$

which was proved by Landau [L].

Assume that f(x) = a(x)b(x) with deg $a = d_1$ and deg $b = d_2$, i.e., $d = d_1 + d_2$. A direct application of Jensen's formula (see [M1]) results in $H(f) = H(ab) \leq (1 + d_1)H(a)H(b)$ if $d_1 \leq d_2$. To see this, let

$$f(x) = \sum_{i=0}^{d} f_i x^i, \quad a(x) = \sum_{k=0}^{d_1} a_k x^k, \quad b(x) = \sum_{t=0}^{d_2} b_t x^t.$$

Then

$$|f_i| = \left|\sum_{j=0}^{a_1} a_j b_{i-j}\right| \le (1+d_1) \max |a_k| \max |b_t| = (1+d_1)H(a)H(b)$$

Moreover,

(6)
$$H(ab) \ge \frac{H(a)H(b)}{2^{d-2}\sqrt{d+1}},$$

which follows from the fact that M(f) is multiplicative and from (4) for a(x) and b(x), i.e., $H(a) \leq 2^{d_1-1}M(a)$, $H(b) \leq 2^{d_2-1}M(b)$ and $M(ab) \leq H(ab)\sqrt{d+1}$.

Using the above, we prove the result below.

LEMMA 2.1. Let f(x) = a(x)b(x) be a polynomial of degree d in $\mathbb{Z}[\theta][x]$, where $a(x), b(x) \in \mathbb{Z}[\theta][x]$ and

(7)
$$\theta = \begin{cases} \sqrt{-k} & \text{if } -k \not\equiv 1 \pmod{4}, \\ (\sqrt{-k}+1)/2 & \text{if } -k \equiv 1 \pmod{4}, \end{cases}$$

where k is a squarefree integer and $k \geq 2$. Let

$$a(x) = \sum_{i=0}^{m} a_i x^i$$
 and $f(x) = \sum_{i=0}^{d} f_i x^i$.

Then, for $0 \leq l \leq m$,

$$|a_l| \le 2^{2d-2}\sqrt{d+1} \Big(\sum_{i=0}^d |f_i|^2\Big)^{1/2}.$$

Proof. First, we observe that $|r + s\theta| \ge 1/2$ for any θ as above and $r, s \in \mathbb{Z}$ with $r \neq 0$ or $s \neq 0$. Indeed,

$$|r+s\theta| = \begin{cases} \sqrt{r^2 + s^2k} & \text{if } -k \not\equiv 1 \pmod{4}, \\ \frac{1}{2}\sqrt{r_1^2 + s^2k} & \text{if } -k \equiv 1 \pmod{4}, \end{cases}$$

where $r_1 = 2r + s$. Since r and s are integers with $r \neq 0$ or $s \neq 0$, and k > 1, we have $\sqrt{r^2 + s^2 k} \ge 1$ and $\sqrt{r_1^2 + s^2 k} \ge 1$. Consequently, $H(b) \ge 1/2$.

From (4) and (6), we have

$$H(a)H(b) \le 2^{2d-3}\sqrt{d+1}M(f)$$

Now, using (5), it follows that

$$\frac{1}{2}|a_l| \le \frac{1}{2}H(a) \le H(a)H(b) \le 2^{2d-3}\sqrt{d+1} \left(\sum_{i=0}^d |f_i|^2\right)^{1/2}.$$

Consequently,

$$|a_l| \le 2^{2d-2}\sqrt{d+1} \left(\sum_{i=0}^d |f_i|^2\right)^{1/2}$$
.

Before we state the next lemma, we recall the big O notation. For two functions r(y) and $\phi(y)$, we write $r(y) = O(\phi(y))$ as $y \to \infty$ if there is a y_0 and a C > 0 such that $|r(y)| \leq C\phi(y)$ for all $y > y_0$. In the event that the constant C depends only on a value s, we write $|r(y)| \leq C_s \phi(y)$, and also $r(y) = O_s(\phi(y))$. If C depends on the coefficients and the degree of a polynomial f(x), we use O_f instead.

LEMMA 2.2. Let d > 1 be an integer and let $g_{d-1} \in \mathbb{Z}[\theta]$ be fixed, with θ as in Lemma 2.1. For each $y \geq 2$, let r_y denote the number of d-tuples $(g_{d-1}, g_{d-2}, \ldots, g_1, g_0)$ of elements in $\mathbb{Z}[\theta]$ satisfying $|g_i| \leq y$ for each i with $0 \leq i \leq d-1$ such that the polynomial

$$g(x) = \sum_{i=0}^{d-1} g_i x^i + x^d$$

is reducible. Then $r_y = O_g(y^{2d-4} \ln y)$. In particular, $r_y = 0$ if $y < |g_{d-1}|$.

Proof. Let $g(x) \in \mathbb{Z}[\theta](x)$ be as above with g_{d-1} fixed. Then there are monic polynomials $a(x), b(x) \in \mathbb{Z}[\theta][x]$ of degree ≥ 1 such that g(x) = a(x)b(x). Let

$$\deg(a) = m \ge n = \deg b,$$

where m + n = d. We write

$$a(x) = x^m + a_{m-1}x^{m-1} + \dots + a_1x + a_0,$$

$$b(x) = x^n + b_{n-1}x^{n-1} + \dots + b_1x + b_0.$$

We assert that the number of monic polynomials g(x) that we are considering with $g_0 = 0$ is $O_g(y^{2d-4})$. Indeed, denoting by $g_j = g_{j,1} + i\sqrt{k} g_{j,2}$, we have $|g_j| = \sqrt{g_{j,1}^2 + kg_{j,2}^2} \leq y$. Therefore, the number of possibilities for g_j is bounded by

(8)

$$(2y+1)\left(2\frac{y}{\sqrt{k}}+1\right) - 2\frac{y}{\sqrt{k}} - \left[2\frac{y}{\sqrt{k}} - 2\frac{\sqrt{2y-1}}{\sqrt{k}}\right] - \dots - \left[2\frac{y}{\sqrt{k}} - 2\frac{\sqrt{y^2-1}}{\sqrt{k}}\right],$$

with the sum having y terms, i.e., (8) is $O_k(y^2)$, and the assertion follows.

The argument above is sufficient to show that the number of *d*-tuples

$$(a_{m-1}, a_{m-2}, \dots, a_1, a_0, b_{n-1}, b_{n-2}, \dots, b_1, b_0)$$

as above with $a_0b_0 \neq 0$ is equal to $O_g(y^{2d-4}\ln y)$.

We consider a(x), which has degree $m \leq d - 1$. A similar argument applies to b(x). For $1 \leq l \leq m - 1$, Lemma 2.1 implies

$$|a_l| \le 2^{2d-2}\sqrt{d+1} \left(\sum_{i=0}^d |g_i|^2\right)^{1/2} \le 2^{2d-2}\sqrt{d+1}((d+1)y^2)^{1/2} = C_d y,$$

where C_d depends only on d. Thus, the number of (d-4)-tuples

 $(a_{m-2},\ldots,a_1,b_{n-2},\ldots,b_1)$

is $O_g(y^{2m-4}y^{2n-4}) = O_g(y^{2d-8}).$

Observe that when we multiply a(x) and b(x), the value of the coefficient g_{d-1} is $a_{m-1} + b_{n-1}$, since a(x) and b(x) are both monic. Also, since g_{d-1} is fixed, when a_{m-1} is determined, b_{n-1} is determined as well. Hence, the number of pairs (a_{m-1}, b_{n-1}) is $O_k(y^2)$.

Since $a_0b_0 = g_0$, we have $1 \le |a_0b_0| \le y$, i.e.,

$$1 \le (a_{0,1}^2 + ka_{0,2}^2)(b_{0,1}^2 + kb_{0,2}^2) \le y^2.$$

2

Thus, the number of pairs (a_0, b_0) is bounded by

$$\begin{split} 16 \sum_{q \le y^2} \sum_{\delta | y^2} 1 &= 16 \sum_{\delta \le y^2} \sum_{\substack{q \le y^2 \\ \delta | q}} 1 \le 16 \sum_{\delta \le y^2} \frac{y^2}{\delta} \\ &\leq 16y^2 \sum_{\delta \le y^2} \frac{1}{\delta} \le 16y^2 \left(1 + \int_1^y \frac{1}{t} \, dt \right) \\ &= O(y^2 \ln y^2) = O(y^2 \ln y), \end{split}$$

where 16 appears because each term of a_0 and b_0 may be either positive or negative.

Finally, for an integer d > 1 and a fixed $g_{d-1} \in \mathbb{Z}[\theta]$, the number of d-tuples

$$(a_0, a_1, \ldots, a_{m-1}, b_0, b_1, \ldots, b_{n-1}),$$

corresponding to the coefficients of two monic polynomials a(x) and b(x) in $\mathbb{Z}[\theta][x]$ of degrees $m, n \ge 1$ such that g(x) = a(x)b(x) and the coefficients of g(x) are bounded in absolute value by y is

$$r_y = O_g(y^{2m-4}y^{2n-4}y^2(\ln y)y^2) = O_g(y^{2d-4}\ln y)$$
 as $y \to \infty$,

with the constants depending only on d and k.

REMARK 2.1. If we replace (7) by

$$\theta = \begin{cases} \sqrt{k} & \text{if } k \not\equiv 1 \pmod{4}, \\ (\sqrt{k}+1)/2 & \text{if } k \equiv 1 \pmod{4}, \end{cases}$$

where $k \geq 2$ is a squarefree integer and we consider $\mathbb{Z}[\theta]$ with the usual norm induced by \mathbb{Q} , our argument cannot be applied because, for y large enough, there are infinitely many possibilities for $g_j = g_{j,1} + \sqrt{k} g_{j,2}$ with $g_{j,1}, g_{j,2} \in \mathbb{Z}$ and $|g_j| \leq y$. Therefore, we could not achieve the limitation (8).

REMARK 2.2. If we remove the condition in Lemma 2.2 that g_{d-1} is fixed, then $r_y = O_g(y^{2d-2}\ln y)$. This is a direct consequence of the same arguments used to prove (8). If the degree of g is d-1, and in this case g_{d-2} is not fixed, then $r_y = O_g(y^{2d-4}\ln y)$.

LEMMA 2.3. Let f(x) be a monic polynomial in $\mathbb{Z}[\theta][x]$ of degree d > 1. Consider pairs (g(x), h(x)) of monic polynomials such that f(x) = g(x) + h(x), where g(x) or h(x) is reducible with deg g = d and $1 \leq \deg h \leq d - 1$, and the coefficients of g(x) and h(x) are bounded in modulus by y. The number of such pairs is $O_f(y^{2d-4} \ln y)$.

Proof. Write

(9)
$$f(x) = x^d + \sum_{j=0}^{d-1} f_j x^j, \quad g(x) = x^d + \sum_{j=0}^{d-1} g_j x^j, \quad h(x) = x^n + \sum_{j=0}^{n-1} h_j x^j,$$

where $f_j = g_j + h_j$ and $1 \le n \le d - 1$.

Suppose at least one of g(x) or h(x) is reducible. Once g(x) or h(x) is fixed, it determines the other. Thus, we can count separately when g(x) is reducible and when h(x) is reducible. We count the ways that g(x) might be reducible. Since f(x) = g(x) + h(x), by (9), we have either $g_{d-1} = f_{d-1}$ or $g_{d-1} = f_{d-1} - 1$. Therefore, in any case, g_{d-1} is fixed. Now, the coefficients of g are bounded in modulus by y, and thus by Lemma 2.2, the number of monic reducible polynomials g(x) is $O_f(y^{2d-4} \ln y)$. Now, we count the ways that g(x) might be reducible. If deg h = d - 1, then by Remark 2.2, the number of monic reducible polynomials h(x) is $O_f(y^{2d-4} \ln y)$, and if deg h < d - 1, this number is smaller, also by Remark 2.2.

3. Main result

THEOREM 3.1. Let f(x) be a monic polynomial in $\mathbb{Z}[\theta][x]$ of degree d > 1and with θ as in Lemma 2.1. The number R(y) of representations of f(x) as a sum of two monic irreducible g(x) and h(x) in $\mathbb{Z}[\theta][x]$, with the coefficients of g(x) and h(x) bounded in modulus by y, is asymptotic to $(4y)^{2d-2}$.

Proof. Let

$$f(x) = x^d + \sum_{j=0}^{d-1} f_j x^j,$$

where $f_j = f_{j,1} + i\sqrt{k} f_{j,2}$. We are looking for pairs of monic polynomials $g(x), h(x) \in \mathbb{Z}[\theta][x]$ such that f(x) = g(x) + h(x) and the coefficients of g(x) and h(x) are bounded in modulus by y. Without loss of generality, let

 $\deg g > \deg h$, and observe that $\deg g = d$ and $1 \leq \deg h \leq d - 1$. In this case,

$$g(x) = x^d + \sum_{j=0}^{d-1} g_j x^j, \quad h(x) = x^n + \sum_{j=0}^{n-1} h_j x^j,$$

where $g_j = g_{j,1} + i\sqrt{k} g_{j,2}$, $h_j = h_{j,1} + i\sqrt{k} h_{j,2}$, $f_j = g_j + h_j$ and $1 \le n \le d-1$. If $y \ge 1 + \{|f_0|, |f_1|, \dots, |f_{d-1}|\}$, then the total number of pairs of monic

(not necessarily irreducible) polynomials g(x), h(x) is

$$\sum_{S=0}^{d-2} \prod_{j=0}^{S} (2\lfloor y \rfloor + 1 - |f_{j,1}|) (2\lfloor y \rfloor + 1 - |f_{j,2}|) = (4y)^{2d-2} + O_f(y^{2d-4}),$$

since $f_{j,1} + i\sqrt{k} f_{j,2} = g_{j,1} + h_{j,1} + i\sqrt{k} (g_{j,2} + h_{j,2}).$

By Lemma 2.3, almost all of these pairs of monic polynomials g(x), h(x) are irreducible. In fact, the number of pairs (g(x), h(x)) where g(x) or h(x) is reducible is $O_f(y^{2d-4} \ln y)$. Thus,

$$\begin{aligned} R(y) &= \sum_{S=0}^{d-2} \prod_{j=0}^{S} (2\lfloor y \rfloor + 1 - |f_{j,1}|) (2\lfloor y \rfloor + 1 - |f_{j,2}|) + O_f(y^{2d-4} \ln y) \\ &= ((4y)^{2d-2} + O_f(y^{2d-4} \ln y)) + O_f(y^{2d-4} \ln y) \\ &= (4y)^{2d-2} + O_f(y^{2d-4} \ln y). \end{aligned}$$

Since any constant depending only on the coefficients and degree of f(x) is small compared to $\ln y$ when y is sufficiently large, we get

$$R(y) \sim (4y)^{2d-2}. \bullet$$

REFERENCES

- [C1] M. Car, Le problème de Goldbach pour l'anneau des polynômes sur un corps fini,
 C. R. Acad. Sci. Paris Sér. A-B 273 (1971), A201–A204.
- [C2] M. Car, Sommes de carrés de polynômes irréductibles dans $\mathbb{F}_q[X]$, Acta Arith. 44 (1984), 307–321.
- [C3] M. Car, Sommes de carrés et d'irréductibles dans $\mathbb{F}_q[X]$, Ann. Fac. Sci. Toulouse Math. (5) 3 (1981), 129–166.
- [D1] A. Dubickas, Polynomials expressible by sums of monic integer irreducible polynomials, Bull. Math. Soc. Sci. Math. Roumanie 54 (2011), 65–81.
- [D2] A. Dubickas, Linear forms in monic integer polynomials, Canad. Math. Bull. 56 (2013), 510–519.
- [H1] D. R. Hayes, A Goldbach theorem for polynomials with integral coefficients, Amer. Math. Monthly 72 (1965), 45–46.
- [H2] D. R. Hayes, The expression of a polynomial as a sum of three irreducibles, Acta Arith. 11 (1966), 461–488.
- [K] M. Kozek, An asymptotic formula for Goldbach's conjecture with monic polynomials in Z[x], Amer. Math. Monthly 117 (2010), 365–369.

- [L] E. Landau, Sur quelques théorèmes de M. Petrovich relatifs aux zéros des fonctions analytiques, Bull. Soc. Math. France 33 (1905), 251–261.
- [M1] K. Mahler, An application of Jensen's formula to polynomials, Mathematika 7 (1960), 98–100.
- [M2] K. Mahler, On some inequalities for polynomials in several variables, J. London Math. Soc. 37 (1962), 341–344.
- [P1] P. Pollack, Irreducible polynomials with several prescribed coefficients, Finite Fields Appl. 22 (2013), 70–78.
- [P2] P. Pollack, On polynomial rings with a Goldbach property, Amer. Math. Monthly 118 (2011), 71–77.
- [P3] P. Pollack, The exceptional set in the polynomial Goldbach problem, Int. J. Number Theory 7 (2011), 579–591.
- [S] F. Saidak, On Goldbach's conjecture for integer polynomials, Amer. Math. Monthly 113 (2006), 541–545.
- [W] W. A. Webb, On the representation of polynomials over finite fields as sums of powers and irreducibles, Rocky Mountain J. Math. 3 (1973), 23–29.

Abílio Lemos, Anderson Luís Albuquerque de Araujo

CCE, Departamento de Matemática

Universidade Federal de Viçosa

36570-900, Viçosa, MG, Brasil

E-mail: abiliolemos@ufv.br

anderson.araujo@ufv.br