Applicable Analysis and Discrete Mathematics
available online at http://pefmath.etf.rs

Appl. Anal. Discrete Math. **10** (2016), 308–324. doi:10.2298/AADM160714014D

COUNTING INTEGER REDUCIBLE POLYNOMIALS WITH BOUNDED MEASURE

Artūras Dubickas

The purpose of this work is to give an asymptotic formula for the number of integer reducible polynomials with fixed degree $d \geq 2$ and Mahler measure bounded above by T and also for the number of such monic polynomials as $T \to \infty$. We also consider the case of monic polynomials which have all their roots in the disc $|z| \leq R$ and find asymptotics for the number of such reducible polynomials too as $R \to \infty$. In all cases the constants in the main terms are related to the constants of the corresponding counting formulas for the number of such irreducible polynomials due to Chern and Vaaler (in case of Mahler measure) and Akiyama and Pethő (in case of a disc).

1. INTRODUCTION

In this paper, we shall give some asymptotic formulas for the number of reducible polynomials with integer coefficients of fixed degree $d \geq 2$ and restricted height. Throughout, reducibility of a polynomial $f \in \mathbb{Z}[x]$ is understood over the field $\mathbb{Q}$, unless indicated otherwise. Sometimes, we also use the concept of reducibility of f in the ring of polynomials $\mathbb{Z}[x]$. (For example, the polynomial $f(x) = 2x^2 + 4$ is irreducible over $\mathbb{Q}$, since it is not a factor of two polynomials with positive degrees and rational coefficients, but it is reducible in the ring $\mathbb{Z}[x]$.) Below, we shall use the Landau symbol O and the Vinogradov symbol $\ll$. Recall that the assertions $U = O(V)$ and $U \ll V$ are both equivalent to the inequality $|U| \leq CV$ with some constant $C > 0$. In case U and V are of the same size, i. e. $U \ll V \ll U$, the notation $V \asymp U$ will be used. Also, the constants implied in the

2010 Mathematics Subject Classification. 11R09, 11R04, 11R11.
Keywords and Phrases. Reducible polynomials, Mahler measure, polynomials with bounded zeros, totally real algebraic integers.

symbols $O, \ll$ and $\asymp$ only depend on the degree d, unless indicated otherwise, but are independent of the constants T and R standing as bounds of various heights of a polynomial.

The first author who worked on a problem with the restriction $H(f) := \max_{j=0}^{d} |a_j| \le T$ on the coefficients a_i of $f(x) = a_d x^d + \cdots + a_0 \in \mathbb{Z}[x]$, was VAN DER WAERDEN [**26**]. Clearly, there are $2\lfloor T \rfloor (2\lfloor T \rfloor + 1)^d \sim (2T)^{d+1}$ such polynomials. It was shown in [**26**] that for each $d \ge 3$ and each sufficiently large T all but $O(T^{d+1-1/(6(d-2)\log\log T)})$ of them are irreducible and have Galois group isomorphic to the full symmetric group S_d. This direction was then developed and the error term improved by GALLAGHER [**15**] and DIETMANN [**9**], [**10**].

The case of reducible polynomials turned out to be more subtle. After the estimates given in [**25**, Example 266], [**11**] and [**16**], the asymptotics was only recently established by the author in [**12**]. See also the previous work of CHELA [**7**], who proved a corresponding asymptotic formula for the number of reducible monic polynomials, and the paper of BHARGAVA et al. [**6**] for an asymptotic formula for quadratic forms in d variables with integral zero (the case $d = 2$ corresponds to the number of reducible quadratic polynomials).

Later, SPECHT [**24**] investigated the same problem with another quite natural height restriction $\left(\sum_{j=0}^{d} a_j^2\right)^{1/2} \le T$ and gave several asymptotic formulas for the number of such irreducible and reducible polynomials of degree d.

In this paper, we consider the polynomials with bounded Mahler measure which is of a similar size as its height. Indeed, for any $f \in \mathbb{C}[x]$ in view of the inequality

$$H(f)2^{-d} \le M(f) \le H(f)\sqrt{d+1}, \tag{1}$$

where $d = \deg f$, the Mahler measure and the height of a polynomial have the same size, i. e. $H(f) \ll M(f) \ll H(f)$ or, equivalently,

$$M(f) \asymp H(f). \tag{2}$$

The left inequality of (1) is given, e. g., in [**27**, Lemma 3.11], whereas the right one follows from an old inequality of LANDAU [**17**].

Throughout, we assume that $d \ge 2$. Put

$$V_d := 2^d d^{\lfloor d/2 \rfloor - 1} \prod_{j=1}^{\lfloor d/2 \rfloor - 1} \frac{(2j)^{d-2j-1}}{(2j+1)^{d-2j}}, \tag{3}$$

where an empty product is 1, so that $V_2 = 4$, $V_3 = 8$, $V_4 = 128/9$, etc. In [**8**], CHERN and VALLER proved that the number of integer polynomials of degree at most d and Mahler measure at most T is

$$V_{d+1} T^{d+1} + O(T^d), \tag{4}$$

whereas the number of monic integer polynomials of degree exactly d and Mahler measure at most T is asymptotic to

$$V_d T^d \quad \text{as} \quad T \to \infty. \tag{5}$$

This last formula is not explicitly given in [**8**]. To derive (5) from the results of [**8**] one can combine the formulas (1.10) and (1.29) of [**8**] and then verify that the product of $2^d \prod_{j=1}^{\lfloor (d-1)/2 \rfloor} (2j/(2j+1))^{d-2j}$ and $(d/2)^{\lfloor (d-1)/2 \rfloor}/\lfloor (d-1)/2 \rfloor!$ is equal to V_d defined in (3).

In fact, it is easy to see that the same formula (4) also gives the asymptotics for the number of integer polynomials of degree exactly d and Mahler measure at most T (see, e. g., [**18**]). Distributing all such polynomials into two classes, irreducible and reducible, and using the fact that the number of reducible ones is $O(T^d)$ for $d \geq 3$ and $O(T^2 \log T)$ for $d = 2$ (by (2) and [**12**, Theorem 1] or [**16**, Theorems 1 and 2]) we find that the number of irreducible integer polynomials of degree $d \geq 2$ and Mahler measure at most T is

$$V_{d+1} T^{d+1} + O(T^d (\log T)^{\lfloor 2/d \rfloor}). \tag{6}$$

In [**18**] it was also shown that the number of integer irreducible polynomials in the ring $\mathbb{Z}[x]$ with positive leading coefficient and Mahler measure at most T is

$$\frac{V_{d+1}}{2\zeta(d+1)} T^{d+1} + O(T^d (\log T)^{\lfloor 2/d \rfloor}), \tag{7}$$

for each $d \geq 2$. Consequently, the number of algebraic numbers of degree $d \geq 2$ and Mahler measure at most T is

$$\frac{dV_{d+1}}{2\zeta(d+1)} T^{d+1} + O(T^d (\log T)^{\lfloor 2/d \rfloor}). \tag{8}$$

Other results implying some special cases of (8) have been earlier obtained by Schanuel [**21**] and Schmidt [**22**], whereas various generalizations of (8) over the fields other than $\mathbb{Q}$ have been subsequently investigated in [**4**], [**5**], [**19**]. By the same argument, using (5) instead of (6), one can see that the number of algebraic integers of degree d and Mahler measure at most T is asymptotic to $dV_d T^d$ as $T \to \infty$.

2. MAIN RESULTS

In the next theorem, we find the asymptotics for the number of reducible polynomials with bounded Mahler measure.

Theorem 1. *The number of integer reducible (over $\mathbb{Q}$) polynomials of degree $d \geq 5$ and Mahler measure at most T is*

$$\Big(4\frac{\zeta(d-1)}{\zeta(d)} - 1\Big) V_d T^d + O(T^{d-1}).$$

The number of such quartic polynomials is

$$\Big(\frac{5120\zeta(3)}{\pi^4} - \frac{128}{9}\Big)T^4 + O(T^3 \log T),$$

the number of such cubic polynomials is

$$8\Big(\frac{2\pi^2}{3\zeta(3)} - 1\Big)T^3 + O(T^2(\log T)^2),$$

and the number of such quadratic polynomials is

$$\frac{48}{\pi^2}T^2 \log T + O(T^2).$$

One can see that all these formulas are explicit and much simpler than those obtained for the height $H(f) \le T$ in [**12**]. We take this opportunity to correct a small error of our result given in [**12**, Theorem 1]. In the quartic case (when $d = 4$) the error term there should be $O(T^3 \log T)$ as it is here in Theorem 1 and not $O(T^3)$ as given in [**12**]. The reason for the error to occur is that we used the result of KUBA [**16**, Theorem 4] whose second part is incorrectly stated for $n = 4$. Its correct version follows from Lemma 6 below: the number of quartic integer polynomials of height at most H that can be expressed by a product of two irreducible quadratic polynomials is $O(H^3 \log H)$ (and this bound is sharp).

In the next theorem we establish the same result for monic polynomials (except that we do not give any error term, since no error term is given in (5)).

Theorem 2. *The number of monic integer reducible polynomials of degree $d \ge 3$ and Mahler measure at most T is asymptotic to*

$$(2\zeta(d-1) + 1)V_{d-1}T^{d-1} \quad \textit{as} \quad T \to \infty,$$

whereas the number of such monic integer quadratic polynomials is

$$2T \log T + O(T).$$

Let us consider another natural height of a polynomial which is the modulus of its largest root. The constant naturally coming into the picture is the volume v_d of d-dimensional real vectors $(b_{d-1}, \dots, b_0)$ for which monic polynomials $x^d + b_{d-1}x^{d-1} + \cdots + b_0$ have all their roots in the unit disc $|z| \le 1$. This d-dimensional body was considered by SCHUR [**23**] in 1918. Then, in [**14**] FAM proved that

$$v_d = 2^{2m^2} \prod_{j=1}^{m} \frac{(j-1)!^4}{(2j-1)!^2}$$

for $d = 2m$ and

$$v_d = 2^{2m^2+2m+1} \prod_{j=1}^{m} \frac{j!^2(j-1)!^2}{(2j-1)!(2j+1)!}$$

for $d = 2m+1$ (see also [**1**], [**2**]). In fact, by a standard calculation, in view of $\prod_{j=1}^{t} j! = \prod_{j=1}^{t} j^{t+1-j}$ and

$$\prod_{j=1}^{t}(2j-1)! = 2^{t(t-1)/2}\prod_{j=1}^{t}\big((2j-1)(j-1)\big)^{t+1-j}$$

one can easily compose both formulas into one having a pattern similar to that of the constant V_d defined in (3):

$$v_d = 2^d \prod_{j=1}^{\lfloor (d-1)/2\rfloor} \Big(\frac{2j}{2j+1}\Big)^{d-2j}. \tag{9}$$

For a given integer s in the range $0 \le s \le \lfloor d/2\rfloor$, let $v_d^{(s)}$ be the volume of d-dimensional real vectors $(b_{d-1},\dots,b_0)$ for which monic polynomials $x^d+b_{d-1}x^{d-1}+\cdots+b_0$ have $2s$ complex roots, $d-2s$ real roots, and all d roots lie in the unit disc $|z|\le 1$. The value of $v_d^{(s)}$ in terms of a (quite complicated) integral was established by Akiyama and Pethő in [**1**]. Note that

$$v_d = \sum_{j=0}^{\lfloor d/2\rfloor} v_d^{(s)}. \tag{10}$$

As shown in [**1**], each $v_d^{(s)}$ is a rational number which is conjectured to be an integer multiple of $v_d^{(0)}$. There are several explicit formulas for $v_d^{(0)}$ given in [**1**]. For instance, combining Theorem 4.1 and Lemma 5.1 of [**1**] we have

$$v_d^{(0)} = 2^{d(d+1)/2}\prod_{j=1}^{d}\frac{(j-1)!^2}{(2j-1)!}.$$

As above, it can be rewritten it in the following equivalent form (similar to (3) and (9)):

$$v_d^{(0)} = 2^{-d(d-3)/2}\prod_{j=1}^{d-1}\Big(\frac{2j}{2j+1}\Big)^{d-j}. \tag{11}$$

In [**2**], it was shown that the number of monic integer irreducible polynomials of degree d whose roots ($2s$ complex and $d-2s$ real) all lie in the disc $|z|\le R$ is

$$v_d^{(s)}R^{(d+1)d/2} + O(R^{(d+1)d/2-1}), \tag{12}$$

where the constant in O depends on d and s. Summing over s from 0 to $\lfloor d/2\rfloor$ and applying (10), one obtains the total number of such monic integer irreducible polynomials

$$v_d R^{(d+1)d/2} + O(R^{(d+1)d/2-1}). \tag{13}$$

In particular, since $2^{-d(d-3)/2} = 4^d \cdot 2^{-d(d+1)/2}$ and each monic irreducible polynomial of degree d has d distinct roots that are real algebraic integers lying with their conjugates in $[-R, R]$, the formulas (11) and (12) with $s = 0$ imply that

Corollary 3. *The number of algebraic integers of degree d that lie with their conjugates in the interval $[-R, R]$ is*

$$d4^d (R/2)^{d(d+1)/2} \prod_{j=1}^{d-1} \Big(\frac{2j}{2j+1}\Big)^{d-j} + O(R^{d(d+1)/2-1}).$$

For applications (see, e. g., the paper of Royer [**20**]), an upper bound $O(R^{d(d+1)/2})$ coming from Corollary 3 is better than the bound $O(R^{d(d+1)})$ coming from [**13**] which was actually used in [**20**].

For $d = 1$ all $2\lfloor R \rfloor + 1$ monic integer polynomials with roots in $|z| \le R$ are irreducible. For $d = 2$, only the polynomials of form $(x - a)(x - b)$, where a, b are integers in the range $-R \le a \le b \le R$, are reducible, so there are exactly $(2\lfloor R \rfloor + 1)(\lfloor R \rfloor + 1)$ of such quadratic reducible polynomials. For other d in [**2**, Corollary 3.1] it was shown that the number of reducible polynomials with roots in $|z| \le R$ is $O(R^{d(d+1)/2-1})$.

The next theorem gives the true order and asymptotics for $d \ge 3$:

Theorem 4. *The number of monic integer reducible polynomials of degree $d \ge 3$ whose roots all lie in the disc $|z| \le R$ is*

$$2^d \prod_{j=1}^{\lfloor d/2 \rfloor - 1} \Big(\frac{2j}{2j+1}\Big)^{d-2j-1} R^{d(d-1)/2+1} + O(R^{d(d-1)/2}). \tag{14}$$

Also, for each s in the range $0 \le s \le \lfloor d/2 \rfloor$, the number of monic integer reducible polynomials of degree d with $2s$ complex roots and $d - 2s$ real roots all lying in the disc $|z| \le R$ is

$$2v_{d-1}^{(s)} R^{d(d-1)/2+1} + O(R^{d(d-1)/2}) \tag{15}$$

when $d \ne 2s$,

$$\frac{8}{3}\, v_{d-2}^{(d/2-1)} R^{(d-1)(d-2)/2+3} + O(R^{(d-1)(d-2)/2+2}) \tag{16}$$

when $d = 2s \ge 6$, and

$$\frac{32}{9}\, R^6 + O(R^5) \tag{17}$$

when $d = 2s = 4$. Here, the constants implied in O depend on d and s.

Note that, by (9), (10) and (11), we have

$$v_2^{(1)} = v_2 - v_2^{(0)} = 4 - \frac{4}{3} = \frac{8}{3}, \tag{18}$$

so the constant $32/9$ in (17) is equal to the half of the constant $8v_2^{(1)}/3 = 64/9$ that would occur in (16) for $d = 4$.

In the next section we will prove several lemmas and also recall two well known asymptotic formulas for sums involving Euler's totient function. Then, in Sections 4, 5, 6 we will prove Theorems 1, 2, 4, respectively.

3. AUXILIARY RESULTS

We begin with the following analytical estimate:

Lemma 5. *Let $k, t, s, k_1, \dots, k_t$ be some positive integers satisfying $1 \le s \le t$ and $k_1 \le \cdots \le k_{t-s} < k_{t-s+1} = \cdots = k_t = k$. Let also*

$$\Delta_t := \{(x_1, \dots, x_t) \in \mathbb{R}^t \ : \ \text{where } x_1, \dots, x_t \ge 1 \text{ and } x_1 \dots x_t \le X\}.$$

Then,

$$\int_{\Delta_t} x_1^{k_1} x_2^{k_2} \dots x_t^{k_t} \mathrm{d}x_1 \mathrm{d}x_2 \dots \mathrm{d}x_t \asymp X^{k+1} (\log X)^{s-1},$$

where the implied constants depend on k, t, s, but not on X.

Proof. Integrating over the last variable x_t, we find that

$$\int_1^{X/(x_1 \dots x_{t-1})} x_t^k \mathrm{d}x_t \asymp X^{k+1} x_1^{-k-1} \dots x_{t-s}^{-k-1} x_{t-s+1}^{-k-1} \dots x_{t-1}^{-k-1}.$$

Hence, for our integral I we have $I \asymp X^{k+1} J$, with

$$J := \int_{\Delta_{t-1}} x_1^{k_1-k-1} \dots x_{t-s}^{k_{t-s}-k-1} x_{t-s+1}^{-1} \dots x_{t-1}^{-1} \mathrm{d}x_1 \mathrm{d}x_2 \dots \mathrm{d}x_{t-1}, \tag{19}$$

where Δ_{t-1} is the domain consisting of the vectors $(x_1, \dots, x_{t-1}) \in \mathbb{R}^{t-1}$ such that $x_1, \dots, x_{t-1} \ge 1$ and $x_1 \dots x_{t-1} \le X$. Therefore, the task is now to show that

$$J \asymp (\log X)^{s-1}. \tag{20}$$

To get the required upper bound on the integral J defined in (19) we observe that the domain of integration Δ_{t-1} is contained in the domain $\mathcal{D}' := [1, +\infty]^{t-s} \cup [1, X]^{s-1}$. Integrating over $\mathcal{D}'$ instead of Δ_{t-1}, we see that the integrals over the first $t-s$ variables are all bounded above by 1, since $\int_1^{+\infty} x_j^{k_j-k-1} \mathrm{d}x_j = 1/(k-k_j) \le 1$ for $1 \le j \le t-s$. The integral over each of the last $s-1$ variables is equal to $\int_1^X x_j^{-1} \mathrm{d}x_j = \log X$ for $t-s+1 \le j \le t-1$. This yields the upper bound $J \le (\log X)^{s-1}$.

For a lower bound on J we integrate over the domain

$$\mathcal{D} := [1, 2]^{t-s} \cup \{1 \le x_{t-s+1} \le \cdots \le x_{t-1} \le X^{1/(s-1)} 2^{(s-t)/(s-1)}\}.$$

(Here, the first element of the union is empty for $t = s$ and the second element of the union is empty for $s = 1$.) This domain $\mathcal{D}$ is contained in Δ_{t-1} for $X \geq 2^{t-s}$, since for each $(x_1, \dots, x_{t-1}) \in \mathcal{D}$ the product $x_1 \dots x_{t-1}$ does not exceed $2^{t-s}X2^{s-t} = X$. Now, each integral over the first $t - s$ variables is

$$\int_1^2 x_j^{k_j-k-1}\mathrm{d}x_j = \frac{1}{k-k_j} - \frac{1}{(k-k_j)2^{k-k_j}} \geq \frac{1}{2(k-k_j)} > \frac{1}{2k}.$$

Hence, we immediately get the the required lower bound in (20) when $s = 1$.

Assume that $s > 1$. Put $r := s - 1 \geq 1$ and $Y := X^{1/(s-1)}2^{(s-t)/(s-1)}$. Also, for simplicity of notation, set $y_1 := x_{t-s+1}, \dots, y_r := x_{t-1}$. Since $\log Y \gg \log X$ and, as we just showed, $J \geq (2k)^{s-t}J_1$, with

$$J_1 := \int_{\mathcal{D}_r} y_1^{-1} \dots y_r^{-1}\mathrm{d}y_1 \dots \mathrm{d}y_r,$$

where $\mathcal{D}_r := \{1 \leq y_1 \leq \dots \leq y_r \leq Y\}$, in order to get the required lower bound in (20) it remains to show that

$$J_1 \gg (\log Y)^r.$$

Indeed, integrating over y_1 in the range $1 \leq y_1 \leq y_2$, we obtain

$$J_1 = \int_{\mathcal{D}_{r-1}} (\log y_2) y_2^{-1} \dots y_r^{-1}\mathrm{d}y_2 \dots \mathrm{d}y_r$$

where $\mathcal{D}_{r-1} := \{1 \leq y_2 \leq \dots \leq y_r \leq Y\}$. Next, integrating over y_2 in the range $1 \leq y_2 \leq y_3$, we further find that

$$J_1 = \frac{1}{2}\int_{\mathcal{D}_{r-2}} (\log y_3)^2 y_3^{-1} \dots y_r^{-1}\mathrm{d}y_3 \dots y_r,$$

where $\mathcal{D}_{r-2} := \{1 \leq y_3 \leq \dots \leq y_r \leq Y\}$, etc. In this way, after r steps we will finally arrive to the formula $J_1 = (\log Y)^r/r!$, which completes the proof of the lemma. □

The next lemma is similar to the results given by VAN DER WAERDEN [**26**] and KUBA [**16**].

Lemma 6. *Let k, s, d and $k_1, \dots, k_t$ be positive integers satisfying $k_1 + \dots + k_t = d$ and $k_1 \leq \dots \leq k_{t-s} < k_{t-s+1} = \dots = k_t = k$. Let $R(k_1, \dots, k_t, H)$ be the set of integer polynomials f of degree d and height at most H that can be factorized as $f = f_1 f_2 \dots f_t$, where f_1 is irreducible over $\mathbb{Q}$ polynomial of degree $\deg f_1 = k_1$ and f_i, $i = 2, \dots, t$, are irreducible in $\mathbb{Z}[x]$ polynomials with positive leading coefficients and degrees $\deg f_i = k_i$. Then,*

$$|R(k_1, \dots, k_t, H)| \asymp H^{k+1}(\log H)^{s-1}.$$

For the set of such monic integer polynomials $R^*(k_1, \dots, k_t, H)$, where $f_1, f_2, \dots, f_t$ as above are monic, we have

$$|R^*(k_1, \dots, k_t, H)| \asymp H^k(\log H)^{s-1}.$$

Proof. For $t = 1$ the claim is trivial, so assume that $t \geq 2$. By the multiplicativity of the Mahler measure, the product of Mahler measures $M(f_1)M(f_2)\dots M(f_t)$ is equal to $M(f) \ll H(f) \leq H$ (see (2)). Put

$$x_1 := H(f_1),\ x_2 := H(f_2),\ \dots,\ x_t := H(f_t).$$

In view of $x_i \asymp M(f_i)$ for $1 \leq i \leq t$, we have $x_1 x_2 \dots x_t \ll H$.

The number of integer polynomials with height equal to $x_i \in \mathbb{N}$ and degree equal to k_i is less than

$$2(k_i+1)(2x_i+1)^{k_i} \ll x_i^{k_i},$$

since we have $k_i + 1$ choices to choose the coefficient $\pm x_i$, two choices to choose its sign, and at most $2x_i + 1$ choices for each of the remaining k_i coefficients of the polynomial of degree k_i. This gives the upper bound for $|R(k_1, \dots, k_t, H)|$ as in the formula (21) below.

Next, for a lower bound, by (2) and (7), we can assert that the number of such polynomials that are irreducible in $\mathbb{Z}[x]$ is at least $x_i^{k_i}$ (up to multiplication by a constant depending on k_i but not on x_i). Furthermore, given any vector $(x_1, \dots, x_t) \in \mathbb{N}^t$, each polynomial $f \in R(k_1, \dots, k_t, H)$ which is a factor of polynomials f_i $(1 \leq i \leq t)$ as above with degrees k_i and heights x_i is counted at most $t! \leq d!$ times. Hence, for the number of possible polynomials f under consideration, we deduce that

$$|R(k_1, \dots, k_t, H)| \asymp \sum x_1^{k_1} x_2^{k_2} \dots x_t^{k_t}, \tag{21}$$

where the sum is taken over all positive integers $x_1, x_2, \dots, x_t$ satisfying $x_1 x_2 \dots x_t \ll H$.

In order to evaluate the sum on the right hand side of (21) it suffices to estimate the corresponding integral with integrand $x_1^{k_1} \dots x_t^{k_t}$ over the variables $x_1, x_2, \dots, x_t \geq 1$ in the range $x_1 x_2 \dots x_t \leq CH$ with some constant C depending on d. (Here, k, t, s are all bounded above by d.) The required result now follows from Lemma 5.

The proof for the monic polynomials is exactly the same except that in the analogue of (21) for $R^*(k_1, \dots, k_t)$ we will have the powers $k_i - 1$ instead of k_i. Hence, by Lemma 5, the resulting exponent for H will be k instead of $k + 1$.

Lemma 7. *The number of monic integer polynomials f of degree $d \geq 3$ with all roots in the disc $|z| \leq R$ that can be factorized as $f = f_1 f_2 \dots f_t$, where $f_1, \dots, f_t$ are monic irreducible polynomials with degrees* $\deg f_i$ *satisfying* $\deg f_i \leq d - 2$ *for each $i = 1, 2, \dots, t$, is $O(R^3)$ for $d = 3$ and $O(R^{(d^2-3d+8)/2})$ for $d \geq 4$.*

Proof. We use the fact that the number of monic integer irreducible polynomials of degree k with all roots in $|z| \leq R$ is $O(R^{k(k+1)/2})$ (see (13)). For $d = 3$, the inequality $\deg f_i \leq d - 2 = 1$ implies that f is a product of three linear factors. Clearly, the number of such polynomials is equal to the number of triplets $(a, b, c) \in \mathbb{Z}^3$ satisfying $-R \leq a \leq b \leq c \leq R$ which is $O(\lfloor R \rfloor^3) = O(R^3)$.

For $d \geq 4$, setting $k_i := \deg f_i$, we obtain $O(R^{k_i(k_i+1)/2})$ choices for $f_i \in \mathbb{Z}[x]$, since there are $O(R^{k_i-j})$ choices for its coefficient for x^j $(j = 0, 1, \ldots, k_i - 1)$. So the number of possible f as described in the lemma is $O(R^S)$, where

$$S := \sum_{i=1}^{t} \frac{k_i(k_i+1)}{2} = \frac{1}{2}\sum_{i=1}^{t} k_i + \frac{1}{2}\sum_{i=1}^{t} k_i^2 = \frac{d}{2} + \frac{1}{2}\sum_{i=1}^{t} k_i^2. \tag{22}$$

Since $t \geq 2$, from $u^2 + v^2 < (u+v)^2$ for $u, v \in \mathbb{N}$ it is easy to see that the sum of squares $\sum_{i=1}^{t} k_i^2$ attains its maximal value $d^2 - 4d + 8$ when $t = 2$ and $\{k_1, k_2\} = \{2, d-2\}$. This yields $S \leq (d^2-3d+8)/2$, whence the result for $d \geq 4$. □

Finally, recall that

$$\sum_{a=2}^{m} \frac{\varphi(a)}{a^d} = \frac{\zeta(d-1)}{\zeta(d)} - 1 + O(m^{1-d}) \tag{23}$$

for each $d \geq 3$ and

$$\sum_{a=2}^{m} \frac{\varphi(a)}{a^2} = \frac{6}{\pi^2}\log m + O(1), \tag{24}$$

where $\varphi(a)$ is Euler's totient function (see, e. g., [**3**]).

4. PROOF OF THEOREM 1

We first consider the case $d \geq 3$. To be consistent with our notation of Lemma 6, for any positive integers $k_1 \leq \cdots \leq k_t$ summing to d, let $M(k_1, \ldots, k_t, T)$ be the set of polynomials of degree d and Mahler measure at most T that can be factorized as $f = f_1 f_2 \ldots f_t$, where f_1 is an irreducible over $\mathbb{Q}$ polynomial of degree $\deg f_1 = k_1$ and f_i, $i = 2, \ldots, t$, are irreducible in $\mathbb{Z}[x]$ polynomials with positive leading coefficients and degrees $\deg f_i = k_i$. In view of (2) we have

$$|M(k_1, \ldots, k_t, T)| \asymp |R(k_1, \ldots, k_t, T)|. \tag{25}$$

Consequently, by Lemma 6 and (25), the number of reducible polynomials of degree d lying outside the set $M(1, d-1, T)$ is

$$O(T^2(\log T)^2) \quad \text{for} \quad d = 3 \tag{26}$$

(those lying in the set $M(1, 1, 1, T)$),

$$O(T^3 \log T) \quad \text{for} \quad d = 4 \tag{27}$$

(those lying in the union of the sets $M(1, 1, 1, 1, T)$, $M(1, 1, 2, T)$ and $M(2, 2, T)$), and

$$O(T^{d-1}) \quad \text{for} \quad d \geq 5 \tag{28}$$

(where the main contribution comes from those lying in the union of the sets $M(1,1,d-2,T)$ and $M(2,d-2,T)$).

It remains to evaluate the cardinality of the set $M(1,d-1,T)$ which gives the main contribution. Let $M_{1,r}(d,T)$ be the set of polynomials of degree d and Mahler measure at most T which have a fixed rational root r and an irreducible in $\mathbb{Z}[x]$ factor of degree $d-1$ with positive leading coefficient. In [**12**], a similar notation $R_{1,r}(d,T)$ was used for the set polynomials, where "height" was standing for "Mahler measure". Then, for each $d \ge 3$, since the sets $M_{1,r}(d,T)$ and $M_{1,r'}(d,T)$, $r \ne r'$, are disjoint and nonempty only when the numerator and the denominator of $|r|$ are both at most $\lfloor T \rfloor$, exactly as in [**12**, Lemma 6], we deduce that $|M(1,d-1,T)|$ is equal to

$$|M_{1,0}(d,T)| + 2|M_{1,1}(d,T)| + 4\sum_{a=2}^{\lfloor T \rfloor} \sum_{\substack{1 \le b < a, \\ \gcd(a,b)=1}} |M_{1,a/b}(d,T)|. \tag{29}$$

Here, the factor 4 comes from the fact that the following four sets

$$M_{1,a/b}(d,T),\ M_{1,b/a}(d,T),\ M_{1,-a/b}(d,T),\ M_{1,-b/a}(d,T), \tag{30}$$

where $a \ge 2$, $b \ne 0$ and $\gcd(a,b) = 1$, are all of the same cardinality, whereas the sum

$$|M_{1,0}(d,T)| + 2|M_{1,1}(d,T)| = |M_{1,0}(d,T)| + |M_{1,1}(d,T)| + |M_{1,-1}(d,T)|$$

stands for the number of polynomials which have a root in $\{0,1,-1\}$.

By the definition, the set $M_{1,0}(d,T)$ contains polynomials of the form $cxf_2(x)$, where c is a nonzero integer and $f_2 \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Z}[x]$ polynomial of degree $d-1$ with positive leading coefficient. Hence, $g(x) = cf_2(x)$ is irreducible over $\mathbb{Q}$ polynomial of degree $d-1$ and Mahler measure at most T. By (6), we see that there are

$$V_d T^d + O(T(\log T)^{\lfloor 2/(d-1) \rfloor}) = V_d T^d + O(T(\log T)^{\lfloor 3/d \rfloor})$$

of such polynomials g. Hence,

$$|M_{1,0}(d,T)| = V_d T^d + O(T^{d-1}(\log T)^{\lfloor 3/d \rfloor}) \tag{31}$$

for $d \ge 3$. Since the Mahler measure of $x-1$ is 1, we also have

$$|M_{1,1}(d,T)| = |M_{1,0}(d,T)| \tag{32}$$

for $d \ge 3$.

To evaluate $M_{1,a/b}(d,T)$ in (29), we first observe that the set $M_{1,a/b}(d,T)$ contains polynomials of the form $c(bx-a)f_2(x)$, where c is a nonzero integer and $f_2 \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Z}[x]$ polynomial of degree $d-1$ with positive leading coefficient. Then, $g(x) = cf_2(x)$ is irreducible over $\mathbb{Q}$ of degree $d-1$ and its Mahler

measure is at most T/a, since $1 \le b < a$ and $M(bx-a) = a$. By (6), the number of such polynomials g is $V_d(T/a)^d + O((T/a)^{d-1}(\log T)^{\lfloor 3/d \rfloor})$. Thus,

$$\sum_{\substack{1\le b<a,\\ \gcd(a,b)=1}} |M_{1,a/b}(d,T)| = V_d T^d \frac{\varphi(a)}{a^d} + O\Big(T^{d-1}(\log T)^{\lfloor 3/d\rfloor}\frac{\varphi(a)}{a^{d-1}}\Big).$$

Summing over a in the range $2 \le a \le T$ and using (23) we find that

$$\sum_{a=2}^{\lfloor T\rfloor} \sum_{\substack{1\le b<a,\\ \gcd(a,b)=1}} |M_{1,a/b}(d,T)| = V_d T^d\Big(\frac{\zeta(d-1)}{\zeta(d)} - 1\Big) + O(T^{d-1}(\log T)^{\lfloor 3/d\rfloor}) \tag{33}$$

for each $d \ge 4$. The formula (33) also holds for $d = 3$, but in view of (24) and $(\log T)^{\lfloor 3/d\rfloor} = \log T$ the error term is $T^2(\log T)^2$.

Consequently, for each $d \ge 4$, by (31), (32) and (33), it follows that the sum given in (29) is equal to

$$|M(1,d-1,T)| = \Big(4\frac{\zeta(d-1)}{\zeta(d)} - 1\Big)V_d T^d + O(T^{d-1}). \tag{34}$$

For $d = 3$ the formula (34) is the same, but the error term $T^2(\log T)^2$.

Now, for $d \ge 5$, combining (28) with (34) we deduce the assertion of the theorem. Similarly, for $d = 4$ the corresponding claim follows from (27), (34), $\zeta(4) = \pi^4/90$ and $V_4 = 128/9$. For $d = 3$ the result follows from (26), (34) (with $d = 3$), $\zeta(2) = \pi^2/6$ and $V_3 = 8$.

It remains to establish the assertion of the theorem for $d = 2$. For this we need to evaluate the number of polynomials in $M(1,1,T)$. Recall that $M_{1,r}(2,T)$ is the set of quadratic integer polynomials of Mahler measure at most T which have a rational root r. We claim that

$$\Big||M(1,1,T)| - 2\sum_{a=2}^{\lfloor T\rfloor} \sum_{\substack{1\le b<a,\\ \gcd(a,b)=1}} |M_{1,a/b}(2,T)|\Big| \ll T^2 \tag{35}$$

as $T \to \infty$.

To deduce (35) we first observe that each polynomial in $M(1,1,T)$ must have a rational root $r = a/b$, where $a \in \mathbb{Z}$, $b \in \mathbb{N}$, $\gcd(a,b) = 1$ and $|a|, |b| \le \lfloor T\rfloor$. In the union $\mathcal{U}_T := \cup_r M_{1,r}(2,T)$ (where r runs through all rational numbers a/b as above) that contains $M(1,1,T)$ each polynomial is counted exactly twice except for polynomials with a double root, i. e., $c(bx-a)^2$, where $c \in \mathbb{Z}\setminus\{0\}$, $a \in \mathbb{Z}$, $b \in \mathbb{N}$, $\gcd(a,b) = 1$ and $|c|\max\{|a|,b\}^2 \le T$.

We first show that the number of polynomials with a double root is small. For this assume first that $1 \le b \le a \le T$ and $c > 0$. Then $c \le T/a^2$ and $1 \le a \le \sqrt{T}$. Clearly, by (24), there are at most

$$\sum_{a=1}^{\lfloor\sqrt{T}\rfloor} T\frac{\varphi(a)}{a^2} \ll T\log T$$

of such f. In all the other cases ($0 \le a \le b$ and also for negative a and negative c) the estimates are the same.

Furthermore, it is clear that $|M_{1,r}(2,T)| \ll T^2$ for each fixed value of r. Hence, in the union $\mathcal{U}_T$ we can ignore the values $r = -1, 0, 1$. Observing that the four sets given in (30) for $d = 2$ are of the same cardinality for each pair $a, b \in \mathbb{N}$ satisfying $a \ge 2$, $a > b$ and $\gcd(a,b) = 1$, we obtain (35).

To find the cardinality of $M_{1,a/b}(2,T)$ for a fixed pair a, b, where $1 \le b < a$, we just need to cound the number of integer pairs u, v ($u \ne 0$) for which $M((bx - a)(ux - v)) \le T$. Since $M(bx - a) = a$ and $M(ux - v) = \max\{|u|, |v|\}$, the only condition on u and v is $\max\{|u|, |v|\} \le T/a$. There are $2\lfloor T/a \rfloor$ possibilities for u and $2\lfloor T/a \rfloor + 1$ possibilities for v. Hence, $|M_{1,a/b}(2,T)| = 4\lfloor T/a \rfloor^2 + 2\lfloor T/a \rfloor$. Consequently, taking the sum over b coprime to a we obtain

$$\sum_{\substack{1 \le b < a, \\ \gcd(a,b)=1}} |M_{1,a/b}(2,T)| = (4\lfloor T/a \rfloor^2 + 2\lfloor T/a \rfloor)\varphi(a).$$

Now, summing over a, by (24) and $\varphi(a) < a$, we find that

$$\sum_{a=2}^{\lfloor T \rfloor} \sum_{\substack{1 \le b < a, \\ \gcd(a,b)=1}} |M_{1,a/b}(2,T)| = \frac{24}{\pi^2} T^2 \log T + O(T^2).$$

Combined with inequality (35), this implies the assertion of the theorem for $d = 2$.

5. PROOF OF THEOREM 2

For any positive integers $k_1 \le \cdots \le k_t$ with $k_1 + \cdots + k_t = d$, let $M^*(k_1, \dots, k_t, T)$ be the set of polynomials of degree d and of Mahler measure at most T that can be factorized as $f = f_1 f_2 \dots f_t$, where f_i, $i = 1, \dots, t$, are irreducible monic polynomials with degrees $\deg f_i = k_i$. (This time, since the polynomials are monic, their irreducibility over $\mathbb{Q}$ and in the ring $\mathbb{Z}[x]$ means the same.) As above, by (2), we have

$$|M^*(k_1, \dots, k_t, T)| \asymp |R^*(k_1, \dots, k_t, T)|.$$

Consequently, by the second part of Lemma 6, the number of reducible polynomials of degree d lying outside the set $M^*(1, d-1, T)$ is

$$O(T(\log T)^2) \quad \text{for} \quad d = 3$$

(those lying in the set $M^*(1,1,1,T)$),

$$O(T^2 \log T) \quad \text{for} \quad d = 4$$

(those lying in the union of the sets $M^*(1,1,1,1,T)$, $M^*(1,1,2,T)$ and $M^*(2,2,T)$), and

$$O(T^{d-2}) \quad \text{for} \quad d \ge 5$$

(where the main contribution comes from those lying in the union of the sets $M^*(1,1,d-2,T)$ and $M^*(2,d-2,T)$).

All the above bounds fall into the error term. Therefore, to find asymptotics for $d \geq 3$ it suffices to count the polynomials of the form $(x-a)f(x)$, where a is an integer satisfying $|a| \leq T$ and f is a monic integer irreducible polynomial of degree $d-1$ satisfying $M(f) \leq T/\max\{|a|,1\}$. By (5), the number of such polynomials is asymptotic to

$$V_{d-1}(T/\max\{|a|,1\})^{d-1} \quad \text{as} \quad T/a \to \infty. \tag{36}$$

Note that, by (2), the number of monic integer polynomials of degree $d-1$ with Mahler measure at most $\log T$ is $O((\log T)^{d-1})$. Thus, for each integer a in the range $T/\log T \leq |a| \leq T$ there are $O((\log T)^{d-1})$ monic integer polynomials with degree $d-1$ and Mahler measure at most $T/|a|$. Therefore, for all such a there are

$$O(T(\log T)^{d-1}) \tag{37}$$

such polynomials.

Summing over other a, by (36), we find the number of such polynomials with $|a| \leq T/\log T$ (so $a=0$ or $|a| \in \{1,2,\dots,\lfloor T/\log T\rfloor\}$) is asymptotic to

$$V_{d-1}T^{d-1}\Big(1+2\sum_{a=1}^{\lfloor T/\log T\rfloor}\frac{1}{a^{d-1}}\Big) \sim V_{d-1}(1+2\zeta(d-1))T^{d-1}.$$

Combined with (37) this completes the proof of the theorem for each $d \geq 3$.

For $d=2$, each reducible monic quadratic polynomial has the form $(x-a)(x-b)$, where a,b are integers satisfying $|ab| \leq T$. For $ab=0$, there are $2\lfloor T\rfloor+1$ of such polynomials. For $1 \leq |a| = |b| \leq \lfloor\sqrt{T}\rfloor$ there are $3\lfloor\sqrt{T}\rfloor$ of them.

Suppose $|a| \neq |b|$. Then, without loss of generality we may assume that $|a| < |b|$. Next, we will evaluate the number of pairs $1 \leq a < b$ satisfying $ab \leq T$, and multiply the result by 4. Clearly, at least one pair $a<b$ with fixed a exists if $a(a+1) \leq T$, namely, $a \leq \lfloor\sqrt{T+1/2}-1/2\rfloor$. Then, one can take $b = a+1, a+2, \dots, a+j$ until $a(a+j) \leq T$, i. e. $j \leq \lfloor T/a\rfloor - a$.

It follows that the total number of such quadratic reducible polynomials is exactly

$$5\lfloor T\rfloor + 1 + 4\sum_{a=1}^{\lfloor\sqrt{T+1/2}-1/2\rfloor}(\lfloor T/a\rfloor - a) = 2T\log T + O(T),$$

as claimed.

5. PROOF OF THEOREM 4

In order to prove (15) for some fixed s and d, where $0 \leq s \leq \lfloor d/2\rfloor$, we first find the cardinality of the set of polynomials with a linear factor and an irreducible factor of degree $d-1$. Evidently, all such polynomials have the form $(x-a)f(x)$,

where a is an integer satisfying $|a| \le R$ and f is a monic irreducible polynomial of degree $d-1$ with exactly $2s$ complex (nonreal) roots (since a is a real root) and all $d-1$ roots lying in the disc $|z| \le R$. Clearly, there are $2\lfloor R \rfloor + 1$ of such integers a. So, multiplying (12) (with the same s but $d-1$ instead of d) by $2\lfloor R \rfloor + 1$, we find that our set contains

$$2v_{d-1}^{(s)} R^{d(d-1)/2+1} + O(R^{(d(d-1)/2}) \tag{38}$$

polynomials, which is exactly as claimed in (15).

In case $d = 2s$ any reducible polynomial of degree d whose all roots are complex (nonreal) has only factors of even degree, so the factorization cannot be $(x-a)f(x)$ as above. Let L_d be the number of such polynomials with all roots in $|z| \le R$ that are products of a quadratic factor and an irreducible factor of degree $d-2$. By (12) and (18), the number of quadratic factors is $8R^3/3 + O(R^2)$, whereas the number of irreducible factors of degree $d-2$ is $v_{d-2}^{(d/2-1)} R^{(d-1)(d-2)/2} + O(R^{(d-1)(d-2)/2-1})$. Thus, in case $d \ge 6$ the set L_d contains

$$\frac{8}{3}\, v_{d-2}^{(d/2-1)} R^{(d-1)(d-2)/2+3} + O(R^{(d-1)(d-2)/2+2}) \tag{39}$$

polynomials, which is exactly as claimed in (16). In evaluating the cardinality $|L_4|$ of the set L_4 we should take into account the fact that both factors of a quartic polynomial are quadratic. Hence, $|L_4|$ is equal to $\binom{|L_2|}{2} + |L_2| = |L_2|(|L_2|+1)/2$. Here, $|L_2| = 8R^3/3 + O(R^2)$, so $|L_4| = 32R^6/9 + O(R^5)$ as claimed in (17).

Next, by Lemma 7, the number of other reducible polynomials of degree d (irrespectively of the number of their real roots) is $O(R^{(d^2-3d+8)/2}$ for $d \ge 4$ and $O(R^3)$ for $d = 3$. In view of $(d^2-3d+8)/2 \le d(d-1)/2$, this contribution falls into the error term of (38). This completes the proof of (15). Similarly, in case $d = 2s$, by (22) (see the proof of Lemma 7), one can easily see that the number of other reducible polynomials falls into the error term of (39). In fact, for $d = 2s = 4$, all reducible polynomials belong to the set L_4. This completes the proofs of (16) and (17).

Now, it easy to see that (14) follows from (10) and (15)-(17).

Acknowledgements. The author thanks the referee for careful reading and correcting a misstatement in the first version of Theorem 4.

REFERENCES

1. S. Akiyama, A. Pethő: *On the distribution of polynomials with bounded roots.* I. *Polynomials with real coefficients.* J. Math. Soc. Japan, **66** (2014), 927–949.
2. S. Akiyama, A. Pethő: *On the distribution of polynomials with bounded roots.* II. *Polynomials with integer coefficients.* Unif. Distrib. Theory, **9** (2014), 5–19.
3. T. M. Apostol: *Introduction to Analytic Number Theory.* Springer, New York, 1998.
4. F. Barroero: *Counting algebraic integers of fixed degree and bounded height.* Monatsh. Math., **175** (2014), 25–41.

5. F. Barroero, M. Widmer: *Counting lattice points and O-minimal structures.* Int. Math. Res. Not. IMRN, **18** (2014), 4932–4957.

6. M. Bhargava, J. E. Cremona, T. Fisher, N. G. Jones, J. P. Keating: *What is the probability that a random integral quadratic form in n variables has an integral zero*? Int. Math. Res. Not. IMRN, **12** (2016), 3828–3848.

7. R. Chela: *Reducible polynomials.* J. Lond. Math. Soc., **38** (1963), 183–188.

8. S. Chern, J. D. Vaaler: *The distribution of values of Mahler's measure.* J. Reine Angew. Math., **540** (2001), 1–47.

9. R. Dietmann: *On the distribution of Galois groups.* Mathematika, **58** (2012), 35–44.

10. R. Dietmann: *Probabilistic Galois theory.* Bull. Lond. Math. Soc., **45** (2013), 453–462.

11. K. Dörge: *Abschätzung der Anzahl der reduziblen Polynome.* Math. Ann., **160** (1965), 59–63.

12. A. Dubickas: *On the number of reducible polynomials of bounded naive height.* Manuscripta Math., **144** (2014), 439–456.

13. A. Dubickas, S. V. Konyagin: *On the number of polynomials of bounded measure.* Acta Arith., **86** (1998), 325–342.

14. A. Fam: *The volume of the coefficient space stability domain of monic polynomials.* In: *IEEE International Symposium on Circuits and Systems*, **3** (1989), 1780–1783.

15. P. X. Gallagher: *The large sieve and probabilistic Galois theory.* In: Analytic number theory (Proceedings of Symposia in Pure Mathematics, vol. 24), pp. 91–101, American Mathematical Society, 1973.

16. G. Kuba: *On the distribution of reducible polynomials.* Math. Slovaca, **59** (2009), 349–356.

17. E. Landau: *Über eine Aufgabe der Funktionentheorie.* Tohoku Math. J., **5** (1914), 97–116.

18. D. Masser, J. D. Vaaler: *Counting algebraic numbers with large height. I.* In: *Diophantine Approximation. Festschrift for Wolfgang Schmidt.* (H. P. Schlickewei et al., eds), 2003, Springer, Vienna, Developments in Mathematics **16** (2008), 237–243.

19. D. Masser, J. D. Vaaler: *Counting algebraic numbers with large height.* II. Trans. Amer. Math. Soc., **359** (2007), 427–445.

20. E. Royer: *Facteurs $\mathbb{Q}$-simples de $J_0(N)$ de grande dimension et de grand rang.* Bull. Soc. Math. France, **128** (2000), 219–248.

21. S. H. Schanuel: *Heights in number fields.* Bull. Soc. Math. France, **107** (1979), 433–449.

22. W. M. Schmidt: *Northcott's theorem on heights.* II. *The quadratic case.* Acta Arith., **74** (1995), 343–375.

23. I. Schur: *Über Potenzreihen, die im Inneren des Einheitskreises beschränkt sind.* II. J. Reine Angew. Math., **148** (1918), 122–145.

24. W. Specht: *Zur Zahlentheorie der Polynome.* IV. Math. Z., **57** (1953), 291–335.

25. G. Pólya, G. Szegö: *Problems and theorems in analysis,* vol. II. Springer, Berlin, Heidelberg, New York, 1976.

26. B. L. van der Waerden: *Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt.* Monatsh. Math., **43** (1936), 133–147.

27. M. Waldschmidt: *Diophantine approximation on linear algebraic groups. Transcendence properties of the exponential function in several variables.* Grundlehren der Mathematischen Wissenschaften **326**, Springer, Berlin, 2000.

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

(Received December 4, 2015)
(Revised July 4, 2016)