Polynomials with prescribed vanishing at roots of unity

Polynomials with prescribed vanishing at roots of unity.

Francesco Amoroso

Sommario.

Dati due interi positivi $r < N$, consideriamo lo spazio vettoriale $\mathbf{V}(r, N)$ dei polinomi a coefficienti razionali di grado $< N$ e molteplicità in $x = 1$ almeno r. In questo lavoro si studia il comportamento asintotico di

$$\min_{\substack{G \in \mathbf{V}(r,N) \\ G \neq 0}} h(G)$$

($h(G)$=altezza logaritmica di G) quando $N, r \to +\infty$ e $r/N \to 0$, migliorando stime precedenti di M. Mignotte e di E. Bommbieri - J. Vaaler.

Polynomials with prescribed vanishing at roots of unity. *

Francesco Amoroso

§1 Introduction.

Let N, r be two integers with $0 < r < N$ and let $\mathbf{V}(r, N)$ be the vector space of polynomials with rational coefficients, having degree $< N$ and vanishing at 1 with multiplicity at least r. We are interested in lower and upper bounds for the minimal logarithmic height of nontrivial polynomials $G \in \mathbf{V}(r, N)$. This problem was first considered by M. Mignotte (see [M]), who found

$$\frac{1}{4} \cdot \frac{r^2}{N} - \log N \leq \min_{\substack{G \in \mathbf{V}(r,N) \\ G \neq 0}} h(G) \leq \frac{1}{2} \cdot \frac{r(r+1)}{N-r} \log N + \frac{r \log 4}{N-r}.$$

The upper bound in the previous formula was obtained by an ingenious use of Siegel's lemma, while the lower bound was a consequence of an old theorem of Schmidt and Schur about the number of real zeros of polynomials. We are interested in the asymptotic for the above minimum as $N, r \to +\infty$ and $r/N \to 0$. Therefore it is worth rewriting Mignotte's results as

$$\frac{1}{4}(r/N)^2\big(1 + o(1)\big) \leq \frac{1}{N} \min_{\substack{G \in \mathbf{V}(r,N) \\ G \neq 0}} \leq \frac{1}{2}(r/N)^2 \log(N/r)\big(1 + o(1)\big) \tag{0}$$

where $o(1)$ is a function of r and N satisfying

$$o(1) \to 0, \qquad \text{for} \quad N, r \to +\infty, \quad \text{and} \quad r/N \to 0.$$

In 1984, Bombieri and Vaaler (see [BV]) considered this problem again, finding similar bounds but with different methods. They found Mignotte's upper bound as a consequence of a new version of Siegel's lemma which uses as its main tool the geometry of numbers instead of the box-principle. This does not only give a polynomial $G \in \mathbf{V}(r, N)$ with

* Research supported by NSF grant DMS-9100383

small height, but also a family $G_1, \dots, G_{N-r}$ of linearly independent polynomials with $\sum h(G_l)$ bounded from above by essentially the same quantity that occurs in the right side of Mignotte's estimate. For the lower bound, the main idea of Bombieri and Vaaler is the following "automatic vanishing" principle: if a polynomial $G \in \mathbf{V}(r, N)$ has small height it must vanish also at p-th roots of unity for small primes.

In this paper we exploit Bombieri and Vaaler's method to give somewhat sharper bounds. More precisely, we have the following theorems:

Theorem 1.

For any nontrivial polynomial $G \in \mathbf{V}(r, N)$ and for any $\varepsilon > 0$, we have

$$N^{-1} h(G) \geq \frac{c - \varepsilon}{2} (r/n)^2 \cdot \big(1 + o_\varepsilon(1)\big)$$

where

$$c = \sum_{s=1}^{+\infty} \frac{s!}{(2s-1)!} = 1.38844...$$

and $o_\varepsilon(1)$ tends to zero when $N, r \to +\infty$ so that

$$r/N \to 0 \quad \text{and} \quad \frac{\sqrt{N \log N}}{r} \to 0.$$

Theorem 2.

There exists a nontrivial polynomial $G \in \mathbf{V}(r, N)$ satisfying

$$N^{-1} h(G) \leq \frac{1}{4} (r/N)^2 \log(N/r) \cdot \big(1 + o(1)\big)$$

where $o(1)$ tends to zero when $N, r \to +\infty$ so that

$$r/N \to 0 \quad \text{and} \quad \frac{\sqrt{N/\log N}}{r} \to 0.$$

As explained before, the main tool of Bombieri and Vaaler's lower bound is the automatic vanishing principle. This essentially depends on the fact that the norm of a primitive p-th root of unity is large, so we cannnot apply this method directly to roots of unity with composite module. However, it is easy to see that for every prime number p the resultant of the n-th and the np-th cyclotomic polynomials is still large. This suggests the following idea: if a polynomial with integer coefficients and low height vanishes to a high multiplicity at n-th roots of unity, it must behave similarly at np-th roots of unity for small primes p. In this way we are able to take into account n-th roots of unity for composite modules as well, and we arrive at a general version of the automatic vanishing principle (proposition 1 below). More precisely, there are two kinds of influence concerning the vanishing of a polynomial at primitive n-th roots. In fact, vanishing at n-th roots implies vanishing both at np-th roots for small primes p and vanishing at n/p-th roots for small primes p dividing n. This gives a system of inequalities which must be satisfied for all $G \in \mathbf{V}(r,n)$, and we have to find the minimum of $h(G)$ when G satisfies such a system. Unfortunately, the contribution up-to-down (from n-th roots to n/p-th roots) is hard to take into account, and we are only able to solve our minimum problem forgetting this contribution. In any case,this gives an improvement in the constant in the right hand side of (0), and we believe that a more accurate analysis of these inequalities can give better results. For the moment, using the general form of our inequalities, we can prove that this system is actually a system of approximate equalities when the height of G is small.

Our lower bounds can also be used to improve the right hand side of (0). Let $r < N$ be two positive integers; using Siegel's lemma in the more elaborate form of [BV] we find a family of $n = N - e$ linearly independent polynomials $G_1, \dots, G_n$ with integer coefficients and degree $< N$, vanishing at 1 with order at least r and satisfying

$$\sum_{s=1}^{n} h(G_s) \leq N^2 (r/N)^2 \log(N/r)\big(1 + o(1)\big).$$

Since the G_i are linearly independent, at least one of them, say G_1, does not vanish at -1 and so $2^r \leq |G_1(-1)| \leq NH(G_1)$ gives a lower bound for $h(G_1)$. Among the remaining

$n-1$ polynomials, at least two, say G_2 and G_3, do not vanish at cubic roots of unity and therefore their heights are not too small. With the aid of a combinatorial lemma we arrive in this way at a lower bound for the sum of the heights of the first m polynomials among the G_i, where $m < n$ is a parameter at our disposal. Taking into account the above upper bound for $\sum h(G_i)$, we deduce that at least one of the polynomials $G_{m+1}, \ldots, G_n$ has relatively low height.

For simplicity we have applied this method only at a "first level", i.e. taking only into account the contributions of p-th roots. A more elaborate use of the arithmetic information related to the vanishing at generic roots of unity will give other numerical improvements for the constant.

The plan of the paper is as follows. In §2 we state our general version of the automatic vanishing principle, which takes the form of a system of inequalities. In §3 we show that this is actually a system of approximate inequalities, at least for polynomials with small height. In §4 we apply the vanishing principle to obtain a new lower bound for the minimal height of non-zero polynomials $G \in \mathbf{V}(r, N)$. Finally, in the last paragraph, using simple considerations from the geometry of numbers, we show the existence of polynomials with prescribed vanishing at 1 having relatively low height and degree.

Acknowledgement. I am grateful to Prof. Bombieri for the discussions we had about this problem. I am also indebted to Olivier Ramaré who pointed out to me some techniques and results from analytic number theory.

§2 Lower bounds for the height.

Our first aim is to give a lower bound for the height of polynomials with integer coefficients vanishing at primitive n-th roots of unity with prescribed multiplicity. We begin with two classical lemmas concerning the resultants of cyclotomic polynomials. In the following the letter p will be reserved for prime numbers.

Lemma 1.

Let $m < n$ be two integers. Then the resultant $\mathrm{Res}(F_m, F_n)$ of the n-th and the m-th cyclotomic polynomials satisfies

$$|\mathrm{Res}(F_m, F_n)| = \begin{cases} p^{\phi(m)}, & \text{if } n = p^l m; \\ 1, & \text{otherwise.} \end{cases}$$

Lemma 2.

For any integer n the discriminant of the n-th cyclotomic polynomial satisfies

$$|\mathrm{Disc}(F_n)| = n^{\phi(n)} \Big(\prod_{p|n} p^{\frac{1}{p-1}} \Big)^{-\phi(n)}.$$

There are several proofs of the previous lemmas. For instance, see [A], [L] and [S1].

Now, we state our vanishing principle (see also [S2]).

Proposition 1.

Let $G \in \mathbf{Z}[x]$ be a polynomial with integer coefficients and degree $d < N$ vanishing at primitive n-th roots of 1 with multiplicity r_n. Then for any integer n we have

$$\sum_{k|n} r_{n/k} \phi(n/k) \Lambda(k) + \sum_{k} r_{nk} \phi(n) \Lambda(k) + r_n \phi(n) \Big(\log n - \sum_{p|n} \frac{\log p}{p-1} \Big) \leq \phi(n) h(G) + \phi(n) \log \binom{N}{r_n + 1}. \quad (1)$$

Proof.

We write $G = F_n^{r_n} R$ where R is a polynomial with integer coefficients not divisible by F_n, vanishing at primitive m-th roots of 1 with multiplicity r_m for any $m \neq n$. Let us consider the polynomial

$$G_n(x) = \frac{1}{r_n!} \Big(\frac{d}{dx} \Big)^{r_n} G(x) \in \mathbf{Z}[x].$$

The congruence $G_n(x) \equiv \big(F_n'\big)^{r_n} R(x) \ \big(\mathrm{mod} F_n\big)$ joints with lemma 1 and lemma 2 yields the lower bound

$$\begin{aligned}\log|\mathrm{Res}(G_n, F_n)| &\geq \sum_{m\neq n} r_m \log|\mathrm{Res}(F_m, F_n)| + r_n \log|\mathrm{Disc}(F_n)| \\ &\geq \sum_{k|n} r_{n/k}\phi(n/k)\Lambda(k) + \sum_{k} r_{nk}\phi(n)\Lambda(k) \\ &\qquad + r_n\phi(n)\bigg(\log n - \sum_{p|n}\frac{\log p}{p-1}\bigg).\end{aligned} \tag{2}$$

On the other hand, if $G(x) = \sum_{l=0}^{N-1} g_l x^l$, we have for any primitive n-th root of unity ω

$$|G_n(\omega)| \leq \sum_{l=r_n}^{N-1} |g_l| \binom{h}{r_n} \leq \left(\sum_{l=r_n}^{N-1}\binom{l}{r_n}\right) \max_l |g_l| = \binom{N}{r_n+1} \exp\big(h(G)\big).$$

Therefore

$$\log|\mathrm{Res}(G_n, F_n)| \leq \phi(n)h(G) + \phi(n)\log\binom{N}{r_n+1}. \tag{3}$$

Combining (2) and (3) we obtain (1).

Q.E.D.

§3 Rigidity.

Let G, N, r_n as before and let x be a positive real number. We define

$$\begin{aligned}\delta_{n,x}(G) = \phi(n)^{-1}\Bigg\{ &\sum_{k|n} r_{n/k}\phi(n/k)\Lambda(k) + \sum_{k\leq x/n} r_{nk}\phi(n)\Lambda(k) \\ &+ r_n\phi(n)\bigg(\log n - \sum_{p|n}\frac{\log p}{p-1}\bigg) - \phi(n)\log\binom{N}{r_n+1}\Bigg\}\end{aligned}$$

for a positive integer $n \leq x$. From proposition 1, we have

$$\delta_{n,x}(G) \leq h(G).$$

We claim that if $h(G)$ and x are small, then $\delta_{n,x}(G)$ are small too. Since $\phi(n/k)\Lambda(k) \geq \phi(n)\Lambda(k)/k$ and $\log\binom{N}{M} \leq M\log(\varepsilon N/M)$, we deduce that

$$\delta_{n,x}(G) \geq \sum_{k|n} r_{n/k}\frac{\Lambda(k)}{k} + \sum_{k\leq x/n} r_{nk}\Lambda(k) - (r_n+1)\log\left\{\frac{eN}{n(r_n+1)}\prod_{p|n}p^{1/(p-1)}\right\} - \log n.$$

Lemma 3.

$$\sum_{n\leq x}\frac{1}{n}\prod_{p|n}p^{\frac{1}{p-1}} \lesssim c\log x$$

where

$$c = \prod_p\left(1+\frac{p^{\frac{1}{p-1}}-1}{p}\right) = 2.4061....$$

Proof.

Let $s>1$. Using Rankin's trick we get

$$\begin{aligned}\sum_{n\leq x}\frac{1}{n}\prod_{p|n}p^{\frac{1}{p-1}} &\leq x^{s-1}\sum_{n=1}^{\infty}\frac{1}{n^s}\prod_{p|n}p^{\frac{1}{p-1}}\\ &= x^{s-1}\prod_p\left(1+\frac{1}{p^{s-1/(p-1)}}+\frac{1}{p^{2s-1/(p-1)}}+\cdots\right)\\ &= x^{s-1}\prod_p\frac{1+p^{-s}\left(p^{\frac{1}{p-1}}-1\right)}{1-p^{-s}} = x^{s-1}\zeta(s)f(s)\end{aligned}$$

where

$$f(s) = \prod_p\left(1+p^{-s}\left(p^{-1/(p-1)}-1\right)\right) \to c, \qquad \text{for} \quad s\to 1.$$

Now we chose $s = 1+(\log x)^{-1}$.

Q.E.D.

We are now able to find a lower bound for $\sum\delta_{n,x}(G)$.

Proposition 2.

$$\sum_{n\leq x}\delta_{n,x}(G) \geq -ce^{\gamma}\frac{N\log x}{x}\big(1+o(1)\big)$$

where c is as in lemma 3 and $o(1)\to 0$ for $x\to+\infty$ and $x^2/N\to 0$.

Proof.

We have

$$\sum_{m\le x} r_m \sum_{k\le x/m} \frac{\Lambda(k)}{k} + \sum_{m\le x} r_m \sum_{k|m} \Lambda(k)$$
$$\le \sum_{n\le x} d_n + \sum_{n\le x} (r_n+1)\log\left\{\frac{eN}{n(r_n+1)}\prod_{p|n} p^{1/(p-1)}\right\}. \tag{4}$$

Let $I = \sum_{n\le x} r_n$. Since $t \to t\log 1/t$ is concave, we easily see that

$$\sum_{n\le x}(r_n+1)\log\left\{\frac{eN}{n(r_n+1)}\prod_{p|n} p^{1/(p-1)}\right\} \le (I+x)\log\frac{eNS}{I+x} \tag{5}$$

where

$$S = \sum_{n\le x}\frac{1}{n}\prod_{p|n} p^{1/(p-1)} \lesssim c\log x \tag{6}$$

by lemma 3. On the other hand, taking into account

$$\sum_{k\le T}\frac{\Lambda(k)}{k} \sim \log T - \gamma + o(1)$$
$$\sum_{k|m}\Lambda(k) = \log m$$

and $\sum \phi(n) r_n < N$, we find

$$\sum_{m\le x} r_m \sum_{k\le x/m}\frac{\Lambda(k)}{k} + \sum_{m\le x} r_m\sum_{k|m}\Lambda(k) = \big(\log x - \gamma + o(1)\big)I + O\Big(\frac{N\log\log x}{x}\Big). \tag{7}$$

Substitution of (5), (6) and (7) into (4) yields

$$\big(\log x - \gamma + o(1)\big)I + O\Big(\frac{N\log\log x}{x}\Big)$$
$$\le \Big(\sum_{n\le x}\delta_{n,x}(G)\Big) + (I+x)\log\frac{ceN(\log x)\big(1+o(1)\big)}{I+x} + x\log x$$

or

$$(I+x)\Big(-\gamma + o(1) + \log\frac{x(I+x)}{ceN(\log x)\big(1+o(1)\big)}\Big) + O\Big(\frac{N\log\log x}{x}\Big)$$
$$\le \Big(\sum_{n\le x}\delta_{n,x}(G)\Big)x\big(\log x + \gamma + o(1)\big).$$

Since the minimum of

$$t \mapsto t\Big(-\gamma + o(1) + \log \frac{xt}{ceN(\log x)\big(1+o(1)\big)}\Big), \qquad t \geq x$$

is $\sim ce^{\gamma}x^{-1}\log x$, the last displayed line yields

$$\sum_{n\leq x}\delta_{n,x}(G) \geq -ce^{\gamma}\frac{N\log x}{x}\big(1+o(1)\big) + O\Big(x\log x + \frac{N\log\log x}{x}\Big) = -ce^{\gamma}\frac{N\log x}{x}\big(1+o(1)\big).$$

Q.E.D.

We have the following corallaries:

Corollary 1.

For any $x \geq 1$ and for any positive integer $n \leq x$ we have

$$|\delta_{n,x}(G)| \leq xh(G) + ce^{\gamma}\frac{N\log x}{x}\big(1+o(1)\big).$$

Corollary 2.

Let us assume that $N \to +\infty$ so that

$$h(G) = o(N), \qquad \frac{\log N/h(G)}{h(G)} \to 0.$$

Then for any

$$x \leq \sqrt{\frac{ce^{\gamma}}{2}N/h(G)\log\frac{N}{h(G)}}$$

and for any $n \leq x$ we have

$$|\delta_{n,x}(G)| \lesssim N\sqrt{2ce^{\gamma}\frac{h(G)}{N}\log\frac{N}{h(G)}}$$

§4 Proof of theorem 1.

For a non-negative integer s and for a real $x \geq 1$, let $T_s(x)$ be the set of positive square-free integers n having s prime factors and satisfying the inequality $\phi(n) \leq x \prod_{p|n} \log p$. Let f be a multiplicative function; in what follows we repeatedly use

$$\sum_{n \in T_s(x)} f(n) = \frac{1}{s} \sum_{p \in T_1(x)} f(p) \sum_{m \in T_{s-1}(xp/\log p)} f(m).$$

Lemma 4.

For $x \to +\infty$ we have

$$\sum_{n \in T_s(x)} 1 \sim \frac{x(\log x)^{s-1}}{s!^2};$$
$$\sum_{n \in T_s(x)} \prod_{p|n} \log p \sim \frac{x(\log x)^{2s-1}}{s!(2s-1)!};$$
$$\sum_{n \in T_s(x)} \phi(n) \sim \frac{x^2(\log x)^{2s-1}}{2s!(2s-1)!}.$$

Proof.

If $s = 1$ our claim follows from the Prime Number Theorem. Let us assume $s > 1$ and the formulas held for $s - 1$. Then

$$\sum_{n \in T_s(x)} 1 \sim \frac{1}{s} \sum_{p \in T_1(x)} \frac{x \frac{\log p}{p} (\log x - \log p)^{s-2}}{(s-1)!^2}$$
$$\sim \frac{x}{(s-1)!s!} \sum_{h=0}^{s-2} \binom{s-2}{h} (-1)^h (\log x)^{s-2-h} \sum_{p/\log p \leq x} \frac{(\log p)^{h+1}}{p}.$$

Using again the Prime Number Theorem we obtain

$$\sum_{n \in T_s(x)} 1 \sim \frac{x(\log x)^{s-1}}{s!^2} \sum_{h=0}^{s-1} \binom{s}{h+1} (-1)^h = \frac{x(\log x)^{s-1}}{s!^2}.$$

Similarly,

$$\sum_{n\in T_s(x)}\prod_{p|n}\log p \sim \frac{1}{s}\sum_{p\in T_1(x)}(\log p)\cdot\frac{x\frac{\log p}{p}(\log x-\log p)^{2s-3}}{(s-1)!(2s-3)!}$$
$$\sim \frac{x}{s!(2s-3)!}\sum_{h=0}^{2s-3}\binom{2s-3}{h}(-1)^h(\log x)^{2s-3-h}\sum_{p/\log p\le x}\frac{(\log p)^{h+2}}{p}$$
$$\sim \frac{x(\log x)^{2s-1}}{s!(2s-3)!}\sum_{h=0}^{2s-3}\binom{2s-3}{h}\frac{(-1)^h}{h+2}=\frac{x(\log x)^{2s-1}}{s!(2s-1)!}.$$

The last asymptotic equality is proved similarly.

Q.E.D.

Proof of theorem 1.

Let $0<r<N$ be two integers which tend to $+\infty$ so that

$$r/N\to 0,\quad \frac{\sqrt{N\log N}}{r}\to 0.$$

Let also $G\in\mathbf{Z}[x]$ of degree $<N$ and height $h=h(G)$, vanishing at 1 with multiplicity $r_1\ge r=\varepsilon N$ and at primitive n-th roots of unity with multiplicity $r_n=N\theta_n/\phi(n)$. Then we have $\sum\theta_n\le 1$ and

$$\varepsilon,\ \frac{\log 1/\varepsilon}{Nr^2}\to 0.$$

Taking into account $\log\binom{N}{M}\le M\log(eN/M)$ and $\sum_{p|n}(\log p)/(p-1)\le\log(2\log n)$ $(n>1)$ we obtain from proposition 1

$$\sum_{p|n}\theta_{n/p}\log p\le\phi(n)\frac{h(g)}{N}+(\theta_n+n/N)\log\frac{6\log n}{\theta_n+n/N},\quad n>1. \tag{8}$$

We take the sum of these inequalites over the set $T_s(x)$, where $x\ll\varepsilon^{-1}(\log 1/\varepsilon)^{1-s}$ tends to ∞ and s is a fixed positive integer. Taking into account the asymptotic equalities of lemma 4, we obtain

$$\sum_{n\in T_s(x)}\sum_{p|n}\theta_{n/p}\log p\lesssim\frac{x^2(\log x)^{2s-1}}{s!(2s)!}\frac{h}{N}$$
$$+\Big(\sum_{n\in T_s(x)}(\theta_n+n/N)\log\frac{6\log n}{\theta_n+n/N}\Big)+O\big(x^2(\log x)^{2s}/N\big).$$

Since $x \mapsto x \log 1/x$ is concave for $x > 0$, the sum on the right gives the following contribution

$$\sum_{n\in T_s(x)} (\theta_n + n/N) \log \frac{6\log n}{\theta_n + n/N}$$
$$\leq \big(A_s(x) + O(x^2(\log x)^{2s-1}/N\big) \log \frac{6x(logx)^s}{A_s(x) + O(x^2(\log x)^{2s-1}/N)}$$

where $A_s(x) = \sum_{n\in T_s(x)} \theta_n$. Therefore, from

$$\sum_{n\in T_s(x)} \sum_{p|n} \theta_{n/p} \log p = \sum_{p\in T_1(x)} (\log p) A_{s-1}\Big(\frac{x\log p}{p-1}\Big)$$

we obtain

$$\sum_{p\in T_1(x)} (\log p) A_{s-1}\Big(\frac{x\log p}{p-1}\Big) \leq \frac{x^2(\log x)^{2s-1}}{s!(2s)!}\frac{h}{N}$$
$$+ \big(A_s(x) + O(x^2(\log x)^{2s-1}/N\big) \log \frac{6x(\log x)^s}{A_s(x) + O(x^2(\log x)^{2s-1}/N)} + o(1). \quad (9)$$

From now on we assume $h = o(Nr^2 \log 1/r)$. We claim that

$$\frac{s!\varepsilon}{(\log 1/\varepsilon)^s} \sum_{n\in T_s(x)} \prod_{p|n} \log p \lesssim A_s(x) \quad (10)$$

provided that $x \ll \varepsilon^{-1}(\log 1/\varepsilon)^{-s}$. Since $A_0(x) = \theta_0 \geq \varepsilon$, the previous assertion holds for $s = 0$. Let $s > 1$ and assume that (10) holds for $s-1$. Then, if $x \ll \varepsilon^{-1}(\log 1/\varepsilon)^{-s}$,

$$\frac{s!\varepsilon}{(\log 1/\varepsilon)^{s-1}} \sum_{n\in T_s(x)} \prod_{p|n} \log p \lesssim \sum_{p\in T_1(x)} (\log p) A_{s-1}\Big(x\frac{\log p}{p-1}\Big).$$

Substituting in (9) we get

$$\frac{s!\varepsilon}{(\log 1/\varepsilon)^{s-1}} \sum_{n\in T_s(x)} \prod_{p|n} \log p$$
$$\lesssim \Big\{A_s(x) + o\big((\log 1/\varepsilon)^{-1}\big)\Big\} \log \frac{7(\log 1/\varepsilon)^s}{\varepsilon\Big\{A_s(x) + o\big((\log 1/\varepsilon)^{-1}\big)\Big\}} + o(1).$$

The left hand side of the last line is $O(1)$ by lemma 4, therefore we find

$$\frac{s!\varepsilon}{(\log 1/\varepsilon)^{s-1}} \sum_{n\in T_s(x)} \prod_{p|n} \log p \lesssim A_s(x) \log 1/\varepsilon$$

and (10) follows. Let now $x_s = c_s\varepsilon^{-1}(\log 1/\varepsilon)^{1-s}$ where c_s is a constant which will be chosen later. The lower bound (10) for A_{s-1} gives

$$\begin{aligned}\sum_{p\in T_1(x_s)} (\log p) A_{s-1}\Big(\frac{x_s \log p}{p-1}\Big) &\gtrsim \frac{(s-1)!\varepsilon}{(\log 1/\varepsilon)^{s-1}} \sum_{p\in T_1(x_s)} (\log p) \sum_{n\in T_{s-1}\left((x_s \log p)/(p-1)\right)} \prod_{q|n} \log q \\ &= \frac{s!\varepsilon}{(\log 1/\varepsilon)^{s-1}} \sum_{n\in T_s(x_s)} \prod_{p|n} \log p \\ &\sim \frac{c_s}{(2s-1)!} \log 1/\varepsilon.\end{aligned}$$

Substituting this into (9) we obtain

$$\begin{aligned}&\frac{c_s}{(2s-1)!} \log 1/\varepsilon \\ &\qquad \lesssim \frac{c_s^2}{2\cdot s!(2s-1)!} \cdot \frac{h \log 1/\varepsilon}{N\varepsilon^2} + \big(A_s(x_s) + o(1)\big) \log \frac{7(\log 1/\varepsilon)^s}{\varepsilon\Big(A_s(x_s) + o(1)\Big)} \qquad + o(1).\end{aligned}$$

We sum the last inequality over the set of positive integers $s \le k$, where k is fixed. Since $t \mapsto t \log 1/t$ is concave and $\sum A_s(x_s) < 1$, we find

$$\Big(\sum_{s=1}^{k} \frac{c_s}{(2s-1)!}\Big) \log 1/\varepsilon \lesssim \Big(\sum_{s=1}^{k} \frac{c_s^2}{2\cdot s!(2s-1)!}\Big) \cdot \frac{h \log 1/\varepsilon}{N\varepsilon^2} + \log 1/\varepsilon$$

and

$$h \gtrsim N\varepsilon^2 \left\{ \Big(\sum_{s=1}^{k} \frac{c_s}{(2s-1)!}\Big) - 1 \right\} \Big/ \Big(\sum_{s=1}^{k} \frac{c_s^2}{2\cdot s!(2s-1)!}\Big)$$

Putting

$$c_s = 2s! \left\{ \sum_{s=1}^{k} \frac{s!}{(2s-1)!} \right\}^{-1}$$

we obtain our assertion.

Q.E.D.

Remark.

Forgetting error terms, the inequalities (8) can be rewritten as

$$N^{-1}h(G) \geq \phi(n)^{-1}\Big\{ \sum_{p|n} \theta_{n/p} \log p - \theta_n \log 1/\theta_n \Big\}, \qquad n \geq 1.$$

Let S be the set of sequences $(\theta_n)_{n\geq 1}$ of non-negative real numbers, satisfying $\theta_n = 0$ for all sufficiently large n and $\sum \theta_n \leq 1$. Let $F\colon S \to \mathbf{R}$ defined by

$$F\big((\theta_n)\big) = \max_n \frac{1}{\phi(n)} \Big\{ \sum_{p|n} \theta_{n/p} \log p - \theta_n \log 1/\theta_n \Big\}.$$

We shall show that for any sufficiently large $k \in \mathbf{N}$ there exists $\varepsilon_k > 0$ such that

$$\inf_{\substack{(\theta_n)\in S \\ \theta_1 \geq \varepsilon}} F \leq \Big\{ \sum_{s=1}^{k} \frac{s!}{(2s-1)!} \Big\} \varepsilon^2, \qquad \forall \varepsilon \leq \varepsilon_k.$$

i.e. the lower bound obtained from (8) for $h(G)$ is the best possible one.

Let $k \geq 2$ such that

$$c_k = \sum_{s=1}^{k} \frac{s!}{(2s-1)!} > 1.$$

Let also $\theta_1 = \varepsilon$ and

$$\begin{cases} \theta_n = \frac{s!\varepsilon}{(\log 1/\varepsilon)^s} \prod_{p|n} \log p - c_k \dfrac{\varepsilon^2}{\log 1/\varepsilon} \phi(n), & \text{if } n \in T_s(x_s) \text{ for some } s \leq k-1; \\ 0, & \text{otherwise} \end{cases}$$

where

$$x_s = \frac{s!(\log 1/\varepsilon)^{1-s}}{\varepsilon c_k}.$$

Then $0 \leq t_n \leq \varepsilon$ (the last inequality can be checked by direct computation; indeed the function

$$(t_1, \ldots, t_s) \mapsto \frac{s!\varepsilon}{(\log 1/\varepsilon)^s} \prod_{h=1}^{s} \log t_h - c_k \frac{\varepsilon^2}{\log 1/\varepsilon} \prod_{h=1}^{s} (t_h - 1), \qquad t_h \geq 2$$

has a maximum which is $\leq \varepsilon$ if ε is sufficiently small and if $c_k > 1$ or $s > 1$). Using lemma 4,

$$\begin{aligned} \sum_{n\in T_s} \theta_n &= \frac{s!\varepsilon}{(\log 1/\varepsilon)^s} \sum_{p\in T_s(x_s)} \sum_{p|n} \log p - \frac{c_k\varepsilon^2}{\log 1/\varepsilon} \sum_{p\in T_s(x_s)} \phi(n) \\ &\sim \frac{s!}{(2s-1)!c_k} - \frac{s!}{2(2s-1)!c_k} \sim \frac{1}{c_k} \cdot \frac{s!}{2(2s-1)!} \end{aligned}$$

and so $\sum_n \theta_n \leq 1$, if ε is sufficiently small. Therefore $(\theta_n) \in S$. Assume now $n \in T_s(x_s)$ for some $s \leq k-1$; then:

$$\sum_{p|n} \theta_{n/p} \log p - \theta_n \log 1/\theta_n \leq \sum_{p|n} \frac{(s-1)!\varepsilon}{(\log 1/\varepsilon)^{s-1}} \Big(\prod_{q|\frac{n}{p}} \log q \Big) \log p$$
$$- \frac{s!\varepsilon}{(\log 1/\varepsilon)^{s-1}} \prod_{p|n} \log p + c_k \varepsilon^2 \phi(n) = c_k \varepsilon^2 \phi(n).$$

If, instead, n is square-free with s distinct factor, but $n \notin T_s(x_s)$,

$$\sum_{p|n} \theta_{n/p} \log p - \theta_n \log 1/\theta_n \leq \sum_{p|n} \frac{(s-1)!\varepsilon}{(\log 1/\varepsilon)^{s-1}} \Big(\prod_{q|\frac{n}{p}} \log q \Big) \log p$$
$$= \frac{s!\varepsilon}{(\log 1/\varepsilon)^{s-1}} \prod_{p|n} \log p$$
$$\leq \frac{s!\varepsilon}{x_s (\log 1/\varepsilon)^{s-1}} \phi(n) = c_k \varepsilon^2 \phi(n).$$

Therefore, in any case $F\big((\theta_n)\big) \leq c_k \varepsilon^2$.

§5 Proof of theorem 2.

We shall use our lower bounds for the heights proved in proposition 1 to obtain a good upper bound. The keys are the two following lemmas.

Lemma 5.

Let $\mathbf{V}$ *be a vector space of finite dimension* n *spanned by* $v_1, \ldots, v_n$ *and let* h *be an arbitrary real function defined on* $V \backslash \{0\}$. *Let also*

$$\mathbf{V} = \mathbf{V}_0 \supset \mathbf{V}_1 \supset \cdots \supset \mathbf{V}_k \neq \{0\}$$

a family of decreasing subspaces. Put $d_i = \dim \mathbf{V}_{i-1} - \dim \mathbf{V}_i$ *and*

$$h_i = \inf_{V \backslash V_i} h.$$

Then

$$\min_{s=1,\ldots,n} h(G_s) \leq \frac{1}{\dim \mathbf{V}_k} \left\{ \sum_{s=1}^{n} h(v_s) - \sum_{i=1}^{k} d_i h_i \right\}.$$

Proof.

Comparing dimensions, we can assume the vectors v_s arranged so that $v_s \notin \mathbf{V}_i$ for $i = 1, \ldots, k$ and $d_1 + \cdots + d_{i-1} < s \leq d_1 + \cdots + d_i$. Therefore for any s in the previous range we have $h(v_s) \geq h_i$. This gives

$$\sum_{s=1}^{d_1+\cdots+d_k} h(v_s) \geq d_1 h_1 + \cdots + d_k h_k$$

and our claim follows since $n - (d_1 + \cdots + d_k) = \dim \mathbf{V}_k$.

Q.E.D.

Let now $D > d \geq 0$ be two integers and let $F_0 \in \mathbf{Q}[x]$ be a polynomial of degree d. We consider the vector space $\mathbf{V}$ of dimension $n = D - d$ defined by

$$\mathbf{V} = \{G \in \mathbf{Q}[x],\ \mathrm{deg}G < D,\ F_0 | G\}.$$

Then, for any polynomial H of degree $< n$ and co-prime with F, the subspace

$$\mathbf{W} = \{G \in \mathbf{V},\ H | G\}$$

has dimension $n - \mathrm{deg}H$. As before, we fix a basis $G_1, \ldots, G_n$ of $\mathbf{V}$ and we consider an arbitrary real function h defined on $\mathbf{V} \backslash \{0\}$.

Lemma 6.

Let l be a non-negative integer and let $F_1, \ldots, F_l \in \mathbf{Q}[x]$ be polynomials of degrees $d_1, \ldots, d_l$ and assume $F_0, \ldots, F_l$ pairwise co-prime. Let also $e_1, \ldots, e_l$ be positive integers such that $m = e_1 d_1 + \cdots + e_l d_l < n = \dim \mathbf{V}$ and let

$$\phi_i \colon \{1, \ldots, e_i\} \to \mathbf{R}, \qquad i = 1, \ldots, l$$

be decreasing real functions satisfying

$$\min_{G \in \mathbf{V},\ F_i^{e-1} || G} h(G) \geq \phi_i(e), \qquad e = 1, \ldots, e_i; \quad i = 1, \ldots, l.$$

Then we have

$$h(G_s) \leq \frac{1}{n-m}\left\{\sum_{s=1}^{n} h(G_s) - \sum_{i=1}^{l}\sum_{e=1}^{e_i} d_i\phi_i(e)\right\}.$$

Proof.

We introduce a total order $\prec$ on the set

$$\Lambda = \{(i,e) \in \mathbf{N}\times\mathbf{N},\ e = 1,\dots,e_i,\ i = 1,\dots,l\}$$

of cardinality $k = e_1 + \cdots + e_l$ putting

$$(i,e) \prec (j,f) \Longleftrightarrow \phi_i(e) > \phi_j(f)$$

Let ψ be the increasing bijection $\psi\colon \Lambda \to [1,k]$; since ϕ_i is decreasing, $\psi(i,\cdot)$ is increasing for any i. For $i \in \{1,\dots,l\}$ and $s \in \{1,\dots,k\}$ we define $x(i,s)$ as the last integer $e \leq e_i$ for which $\psi(i,e) \leq s$ †. We remark that $\psi(i,x(i,s)) \leq s$. Let $p = \pi \circ \psi^{-1}\colon [1,k] \to [1,l]$, where $\pi\colon \Lambda \to [1,l]$ is the projection. Then $x(i,s) = x(i,s-1)$ if $i \neq p(s)$. If, instead, $i = p(i,s)$,

$$\psi(i,x(i,s)) = s > s-1 \geq \psi(i,x(i,s-1)),$$

and we have $x(i,s) \geq x(i,s-1)+1$. On the other hand $\psi(i,x(i,s)-1) < \psi(i,x(i,s)) = s$, hence $\psi(i,x(i,s)-1) \leq s-1$ and so $x(i,s-1) \geq x(i,s)-1$. We have proved

$$x(i,s) = \begin{cases} x(i,s-1) & , \quad \text{if } i \neq i_s; \\ x(i,s-1)+1 & , \quad \text{if } i = i_s. \end{cases}$$

Let us define a family of subspaces $(\mathbf{V}_s)_{s=1,\dots,k}$ of $\mathbf{V}$ putting

$$\mathbf{V}_s = \left\{G \in \mathbf{V},\ \prod_{i=0}^{l} F_i^{x(i,s)} | G\right\}.$$

By our last remark, we have

$$\mathbf{V} = \mathbf{V}_0 \supset \mathbf{V}_1 \supset \cdots \supset \mathbf{V}_k \neq \{0\}$$

† $x(i,s) = 0$ if $\psi(i,e) > s$ for any $s \leq e_i$

and $\dim \mathbf{V}_{s-1} - \dim \mathbf{V}_s = \deg F_{p(s)} = d_{p(s)}$. Let $G \in \mathbf{V}\backslash\mathbf{V}_s$; then there exist $i \in \{1, \dots, u\}$ and $e \leq x(i,s)$ such that $F_i^{e-1} || G$. Therefore, $h(G) \geq \phi_i(e) \geq \phi_i(x(i,s))$. Since $\psi(i, x(i,s)) \leq s$ and ψ is order-preserving, $(i, x(i,s)) \preceq \psi^{-1}(s)$ and, by definition, $\phi_i(x(i,s)) \geq \phi_{p(s)}\big(\pi_2 \circ \psi^{-1}(s)\big)$, where π_2 is the projection on the e-axis. This gives $h(G) \geq \phi_{p(s)}\big(\pi_2 \circ \psi^{-1}(s)\big)$. Now we apply lemma 5, taking into account

$$\sum_{s=1}^{k} d_{p(s)} \phi_{p(s)}\big(\pi_2 \circ \psi^{-1}(s)\big) = \sum_{i=1}^{l} \sum_{e=1}^{e_i} d_i \phi_i(e).$$

Q.E.D.

Proof of theorem 2.

Let $0 < r < N$ be two integers which tend to $+\infty$ so that

$$r/N \to 0, \quad \frac{\sqrt{N \log N}}{r} \to 0.$$

As a corollary of the main theorem of [BV], we can find $n = N - r$ linearly independent polynomials $G_1, \dots, G_n$ of degrees $\leq N$ and multiplicity at 1 at least r, such that

$$\sum_{h=1}^{n} h(G_s) \leq N^2 (r/N)^2 \log(N/r)\big(1 + o(1)\big). \tag{11}$$

Let $\varepsilon = r/N$, $X = 1/(\varepsilon \log 1/\varepsilon)$ and, for any prime $p \leq X$, let r_p be the integer part of

$$\frac{\varepsilon (\log p) N}{p \log 1/\varepsilon}.$$

Our assumption on r and N implies

$$r_p \geq \frac{\varepsilon}{\log 1/\varepsilon} \cdot \frac{\log X}{X} N - 1 \geq \varepsilon^2 (\log 1/\varepsilon) N - 1 \to +\infty.$$

We apply the last lemma with $h =$ logarithmic height, $l = \pi(X)$, $F_i = F_p$, $d_i = d_p = p - 1$, $e_i = r_{p_i}$ (where p_i is the sequence of primes) and

$$\phi_i(e) = \phi_p(e) = r \frac{\log p}{p-1} - e \log \frac{N}{pe} - 2e - \log p.$$

Since the functions $\phi_p(e)$ are decreasing on $1,\dots,r_p$, lemma 3 gives an index $l\in\{1,\dots,n\}$ such that the corresponding polynomial $G=G_l$ satisfies

$$h(G)\le\Big(n-\sum_{p\le X}pr_p\Big)^{-1}\bigg\{\sum_{h=1}^{n}h(G_s)-\sum_{p\le X}\sum_{e=1}^{r_p}\Big(r\log p-pe\log\frac{N}{pe}-2ep-p\log p\Big)\bigg\}. \quad (12)$$

Taking into account $\sum_{i=1}^{x} i\log i=(1/2)x^2\log x+O(x^2)$ for $x\to+\infty$ and the Prime Number Theorem, it follows that

$$\begin{aligned}
&\sum_{p\le X}\sum_{e=1}^{r_p}\Big(r\log p-pe\log\frac{N}{pe}-2ep-p\log p\Big)\\
&\qquad=\sum_{p\le X}\bigg\{rr_p\log p-\frac12 pr_p^2\log\frac{N}{pr_p}+O\big(pr_p(r_p+\log p+\log N)\big)\bigg\}\\
&\qquad\le\sum_{p\le X}\bigg\{\frac{\varepsilon^2}{\log 1/\varepsilon}\cdot\frac{(\log p)^2}{p}N^2-\frac{\varepsilon^2}{2(\log 1/\varepsilon)^2}\cdot\frac{(\log p)^2}{p}\big(\log 1/\varepsilon+\log\log 1/\varepsilon\big)N^2\\
&\qquad\quad+O\Big(\frac{\varepsilon^2}{(\log 1/\varepsilon)^2}\cdot\frac{(\log p)^2}{p}N^2+\frac{\varepsilon}{\log 1/\varepsilon}(\log p)^2N+\frac{\varepsilon}{\log 1/\varepsilon}(\log p)N\log N\Big)\bigg\}\\
&\qquad=\frac{\varepsilon^2N^2}{2\log 1/\varepsilon}\sum_{p\le X}\frac{(\log p)^2}{p}+R=\frac14 e^2\log 1/\varepsilon\big(1+o(1)\big)N^2+R \qquad (13)
\end{aligned}$$

where

$$R=O\bigg(\frac{\varepsilon^2(\log\log 1/\varepsilon)N^2}{(\log 1/\varepsilon)^2}\sum_{p\le X}\frac{(\log p)^2}{p}+\frac{\varepsilon N}{\log 1/\varepsilon}\sum_{p\le X}(\log p)^2+\frac{\varepsilon N\log N}{\log 1/\varepsilon}\sum_{p\le X}\log p\bigg).$$

Using Chebyshev inequalities and our assumptions on r and N we find

$$\begin{aligned}
|R|&\ll\frac{\varepsilon^2(\log\log 1/\varepsilon)N^2}{(\log 1/\varepsilon)^2}\sum_{p\le X}\frac{(\log p)^2}{p}+\frac{\varepsilon N}{\log 1/\varepsilon}\sum_{p\le X}(\log p)^2+\frac{\varepsilon N\log N}{\log 1/\varepsilon}\sum_{p\le X}\log p\\
&\ll\varepsilon^2(\log\log 1/\varepsilon)N^2+N+\frac{N\log N}{\log 1/\varepsilon}=o\big(\varepsilon^2(\log 1/\varepsilon)N^2\big) \qquad (14)
\end{aligned}$$

and

$$n-\sum_{p\le X}pr_p=N-\varepsilon N-\frac{\varepsilon N}{\log 1/\varepsilon}\sum_{p\le X}\log p=N\big(1-o(1)\big). \qquad (15)$$

Combining (11), (12), (13), (14) and (15) we obtain our claim.

Q.E.D.

REFERENCES.

[A] T.M. Apostol, "Resultants of Cyclotomic Polynomials", Proc. Amer. Math. Soc. 24 (1970), 457-462;

[BV] E. Bombieri and J.D. Vaaler, "Polynomials with low height and prescribed vanishing", Analytic Number Theory and Diophantine Problems, Oklahoma 1984, Ed. A.C. Adolphson, J.B. Conrey, A. Ghosh and R.I. Yager, Birkhäuser PM 70 (1987), 53-73;

[M] M. Mignotte "Estimation élémentaires effectives sur les nimbres algébriques", Journées Aritmétiques1980, éd. J.V. Armitage, London Math. Soc. Lecture Notes Ser. 56, Cambridge U. Press (1982), 24-34;

[S1] A. Schinzel, "On the number of irreducible factors of a polynomial", Colloq. Math. Soc. János Bolyai 13 (1976), 305-314;

[S2] A. Schinzel, "On the number of irreducible factors of a polynomial II", Annales Polonici Math. 42, 309-320.

Francesco Amoroso,

Dipartimento di Matematica
Via Buonarroti 2
56127 PISA (ITALY)