REDUCIBLE POLYNOMIALS

R. Chela

All the polynomials considered have rational integral coefficients.

Let N be any positive real number and $\rho_\kappa(n, N)$ the number of polynomials

$$f(x) = x^n + a_1 x^{n-1} + \ldots + a_n, \quad (n > 1), \tag{1}$$

which are reducible with a factor of degree $1 \leqslant k \leqslant \frac{1}{2}n$ and satisfying

$$|a_i| \leqslant N, \quad (i = 1, \ldots, n). \tag{2}$$

B. L. van der Waerden proved the following relations (*cf.* [1]):

$$A_1 N^{n-k} < \rho_\kappa(n, N) < B_1 N^{n-k}, \quad (k < \tfrac{1}{2}n) \tag{3}$$

$$A_2 N^{n-k} \log N < \rho_\kappa(n, N) < B_2 N^{n-k} \log N, \quad (k = \tfrac{1}{2}n) \tag{4}$$

where A_1, B_1, A_2, B_2, are positive constants independent of N.

When $n > 2$ from (3) and (4) we get:

$$AN^{n-1} < \rho(n, N) < BN^{n-1}, \quad (n > 2), \tag{5}$$

where $\rho(n, N)$ is the total number of reducible polynomials (1) with condition (2) and where A, B are positive constants independent of N.

This result still leaves open the question whether

$$\lim_{N\to\infty} \frac{\rho(n, N)}{N^{n-1}}, \quad (n > 2), \tag{6}$$

exists. We shall show that this is the case.

Let

$$k_n = \int \ldots \int_{(R)} dx_1 \ldots dx_{n-1}, \tag{7}$$

where (R) is the region of the $n-1$-dimensional Euclidean space (coordinates $x_1, \ldots, x_{n-1}$) defined by

$$|x_i| \leqslant 1, \quad i = 1, \ldots, n-1, \tag{8}$$

$$\left|\sum_{i=1}^{n-1} x_i\right| \leqslant 1, \tag{9}$$

and let $\zeta(z)$ be the Riemann zeta function of the complex variable z.

Received 9 January, 1962. This paper is part of a Ph.D. thesis submitted this year to the University of London. I wish to thank my supervisor Dr. A. Fröhlich for his guidance and encouragement, the Universidad Central of Venezuela for the grant and the Department of Mathematics of the King's College for the facilities which enabled me to pursue my course of study.

THEOREM 1.

$$\lim_{N\to\infty}\frac{\rho(n, N)}{N^{n-1}} = 2^n\left\{\zeta(n-1)-\tfrac{1}{2}+\frac{k_n}{2^{n-1}}\right\}, \quad (n>2). \tag{10}$$

We need several lemmas.

Let

$T_{n,N}(\nu)$ = number of polynomials (1) with condition (2) and having the linear factor $x+\nu$, ν = integer.

$\bar{\rho}_1(n, N)$ = number of polynomials (1) with condition (2) and having two (not necessarily distinct) linear factors.

LEMMA 1.

$$\rho_1(n\ N) = \sum_{\nu} T_{n,N}(\nu)+o(N^{n-1}) \tag{11}$$

where o is the Landau symbol and where the summation extends over all integers ν in the interval $[-N, N]$.

Proof. We have

$$\sum_{\nu} T_{n,N}(\nu) \geqslant \rho_1(n, N) \tag{12}$$

since in the left-hand side a polynomial may be counted repeatedly. Let $R_i (i = 1, \ldots, n)$ be the number of polynomials (1) with exactly i distinct linear factors. Each of these is counted in $\sum_{\nu} T_{n,N}(\nu)$ exactly i times. Moreover

$$R_i \leqslant \bar{\rho}_1(n, N) < \rho_2(n, N), \text{ for } i>1.$$

But from (3) and (4) we have

$$\rho_2(n, N) = o(N^{n-1}).$$

Therefore, $\rho_1(n, N)$ and $\sum_{\nu} T_{n,N}(\nu)$ differ in a term of the form $o(N^{n-1})$.

LEMMA 2.

$$\lim_{N\to\infty}\frac{\sum_{|\nu|>1} T_{n,N}(\nu)}{N^{n-1}} = 2^n\{\zeta(n-1)-1\}, \quad (n>2), \tag{13}$$

where for fixed N the summation extends over all integers ν with $1<|\nu|\leqslant N$.

Proof. Since $T_{n,N}(\nu) = T_{n,N}(-\nu)$, we may assume $2\leqslant\nu\leqslant N$. Let

$$f(x) = (x+\nu)(x^{n-1}+b_1x^{n-2}+\ldots+b_{n-1}). \tag{14}$$

$T_{n,N}(\nu)$ is equal to the number of $n-1$-tuples $(b_1, \ldots, b_{n-1})$ satisfying (14) when the coefficients of $f(x)$ vary according to (2).

From (14) we get

$$b_{i-1} = \frac{a_i-b_i}{\nu}, \quad (2\leqslant i\leqslant n), \quad b_n = 0, \tag{15}$$

$$a_1 = b_1+\nu. \tag{16}$$

If b_i is fixed and in (15) a_i varies in the interval $[-N, N]$, then b_{i-1} takes all the integral values of the interval

$$\left[\frac{-N+b_i}{\nu}, \frac{N-b_i}{\nu}\right],$$

whose amplitude is $2N/\nu$ and, therefore, independent of b_i. To any b_i there correspond, therefore,

$$\left[\frac{2N}{\nu}\right] \text{ or } \left[\frac{2N}{\nu}\right]+1$$

integral values of b_{i-1}. Hence the number of solutions of (15) is of form

$$\prod_{i=1}^{n}\left(\frac{2N}{\nu}+r_{\nu i}\right), \quad (|r_{\nu i}| \leqslant 1).$$

Moreover, using the inequality

$$|b_1| \leqslant N\left(\frac{1}{\nu}+\frac{1}{\nu^2}+\ldots+\frac{1}{\nu^{n-1}}\right)$$

which follows from (15) and (2), we can see that for $2 \leqslant \nu < N$ the values of b_1 also satisfy (16) with $|a_1| \leqslant N$, provided N is large enough. We have therefore,

$$\sum_{|\nu|>1} T_{n,N}(\nu) = 2\sum_{\nu=2}^{[N]-1}\prod_{i=1}^{n}\left(\frac{2N}{\nu}+r_{\nu i}\right)+2T_{n,N}([N])$$

$$= 2\sum_{\nu=2}^{N}\left(\frac{2N}{\nu}\right)^{n-1}+o(N^{n-1}). \tag{17}$$

From (17) follows (13). This completes the proof.

Let

$$t\big(f(x)\big) = a_1+\ldots+a_n, \tag{18}$$

$L_n(N, h) =$ number of polynomials $f(x)$ satisfying (2) and $t\big(f(x)\big) = h$. (19)

We have clearly

$$T_{n,N}(1) = L_n(N, -1), \tag{20}$$

$$L_n(N, h) = L_n(N, -h). \tag{21}$$

LEMMA 3.
$$\lim_{N\to\infty}\frac{L_n(N, h)}{N^{n-1}} = k_n, \tag{22}$$

for all h, where k_n is given by (7).

Proof. Assume for the moment that

$$\lim_{N}\frac{L_n(N, 0)}{N^{n-1}} = k_n. \tag{23}$$

We shall show that (23) implies (22) or, equivalently

$$\lim_{N\to\infty} \frac{L_n(N, h)}{L_n(N, 0)} = 1, \text{ for all } h. \tag{24}$$

By (21) we may assume $h > 0$. Let

$\mathscr{L}_n(N, h)$ = set of polynomials (1) with condition (2) and $t\big(f(x)\big) = h$.

Let $f(x) \varepsilon \mathscr{L}_n(N, 0)$ and let $f'(x) = x^n + a_1' x^{n-1} + \ldots + a_n'$ where $a_1' = a_1, \ldots, a'_{n-1} = a_{n-1}, a_n' = a_n + h$. Then

$$f'(x) \varepsilon \mathscr{L}_n(N+h, h).$$

The mapping $f(x) \to f'(x)$ is a binmique map

$$\mathscr{L}_n(N, 0) \to \mathscr{L}_n(N+h, h).$$

Hence

$$L_n(N, 0) \leqslant L_n(N+h, h). \tag{25}$$

Let $f(x) \varepsilon \mathscr{L}_n(N, h)$ and $f'(x)$ be given now by

$$a_1' = a_1, \ldots, a_{n-1} = a'_{n-1}\; a_n' = a_n - h.$$

By the same argument we have

$$L_n(N, h) \leqslant L_n(N+h, 0). \tag{26}$$

From (25) and (26) it follows

$$\frac{L_n(N-h, 0)}{L_n(N, 0)} \leqslant \frac{L_n(N, h)}{L_n(N, 0)} \leqslant \frac{L_n(N+h, 0)}{L_n(N, 0)}. \tag{27}$$

From (27) and our assumption follows (24).

We shall now prove (23) and this will complete the proof of Lemma 3.

We shall work in $E_n = n$-dimensional Euclidean space (coordinates: $x_1, \ldots, x_n$). Let Λ_n be the lattice of integral points in E_n. Moreover, if S is any region $\subset E_n$, we shall denote with $\|S\|$ the number of points of $S \cap \Lambda_n$ and with $V(S)$ the volume of S.

$L_n(N, 0)$ is equal to the number of points of Λ_n which lie inside the cube $C_N : |x_i| \leqslant N$ $(i = 1, \ldots, n)$ and in the hyperplane $H : x_1 + \ldots + x_n = 0$, *i.e.*

$$L_n(N, 0) = \|\Lambda_n \cap C_N \cap H\|. \tag{28}$$

H is an $(n-1)$-dimensional space. We take in it $x_1, \ldots, x_{n-1}$ as coordinates and we identify H with E_{n-1}.

We then have also $\Lambda_n \cap H = \Lambda_{n-1}$.

$C_N \cap H$ is given by $|x_i| \leqslant N$, $(i = 1, \ldots, n-1)$, and $\left|\sum_{i=1}^{n-1} x_i\right| \leqslant N$.

But

$$\lim_{N\to\infty} \frac{\|\Lambda_n \cap C_N \cap H\|}{N^{n-1}} = V(R_1), \tag{29}$$

where R_1 is the region obtained transforming $C_N \cap H$ by the substitution $x_i = Ny_i$ $(i = 1, \ldots, n-1)$, *i.e.* R_1 is given by

$$|y_i| \leqslant 1 \quad (i = 1, \ldots, n-1_1, \quad \left|\sum_{i=1}^{n-1} y_i\right| \leqslant 1.$$

From (28) and (29) we get

$$\lim_{N\to\infty} \frac{L_n(N, 0)}{N^{n-1}} = V(R_1) = \int \ldots \int_{(R_1)} dy_1 \ldots dy_{n-1}$$
$$= k_n.$$

COROLLARY.
$$\lim_{N\to\infty} \frac{T_{n,N}(1)}{N^{n-1}} = k_n. \tag{31}$$

Proof of Theorem 1. We have

$$\sum_{\nu} T_{n,N}(\nu) = \sum_{|\nu|>1} T_{n,N}(\nu) + 2T_{n,N}(1) + T_{n,N}(0). \tag{32}$$

From (32), (31), (13) and $T_{n,N}(0) \sim 2^{n-1}N^{n-1}$, we get

$$\lim_{N\to\infty} \frac{\sum_{\nu} T_{n,N}(\nu)}{N^{n-1}} = 2^n\left\{\zeta(n-1) - \tfrac{1}{2} + \frac{k_n}{2^{n-1}}\right\}, \quad (n > 2). \tag{33}$$

Finally, from (33), Lemma (1), (3) and (4), follows (10).

Remark 1. Formula (10) is not valid when $n = 2$. However, we can show that for quadratic polynomials we have:

THEOREM 2.
$$\lim_{N\to\infty} \frac{\rho(2, N)}{2N \log N} = 1. \tag{34}$$

Remark 2. Let

$\rho^*(n, N)$ = number of polynomials (1) satisfying the sphere-condition

$$\sum_{i=1}^{n} a_i^2 \leqslant N^2. \tag{35}$$

W. Specht established asymptotic formulae for $\rho^*(n, N)$ when $N \to \infty$ (*cf.* [2]). From his results and ours it follows:

$$\lim_{N\to\infty} \frac{\rho(n, N)}{\rho^*(n, N)} = l_n > 1 \text{ if } n > 2, \tag{36}$$

$$\lim_{N\to\infty} \frac{\rho(2, N)}{\rho^*(2, N)} = 1. \tag{37}$$

On the other hand, if we put

$v_n(N)$ = volume of the sphere of radius N,

$$g_n = \lim_{N \to \infty} \frac{(2N)^n}{v_n(N)},$$

then

$$\lim_{n \to \infty} \frac{l_n}{g_n} = \infty.$$

(36) and (37) give a more precise picture of the distribution inside the cube of the integral points attached to reducible polynomials.

Bibliography.

1. B. L. van der Waerden, " Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt ", *Monatsheft für Matematik und Physik*, 43 (1936), S. 133–147.
2. W. Specht, " Zur Zahlentheorie der Polynome ", *Math. Nachr.*, 7 (1952), S. 105–126.

Mathematics Department,
Facultad de Ciencias,
Universidad Central,
Caracas, Venezuela.

Printed by C. F. Hodgson & Son, Ltd., Pakenham Street, London, W.C.1