Mathematics

1964

SovietRxiv

Abstract

Full Text

Mathematics

N. A. Khmyrova

On Polynomials with Small Prime Divisors

(Presented by Academician I. M. Vinogradov on 6 I 1964)

I. M. Vinogradov in ([1]) introduced numbers with small prime divisors. Subsequently they were studied by many authors ([2–6]) and found numerous applications in various problems of number theory. However, in all the works listed, the laws of distribution of these numbers were studied either in the natural sequence or in progressions. But, in view of the importance of these numbers, it is of interest to study the laws of their distribution in polynomials with integral rational coefficients.

In this note we consider the problem of the number of values of an irreducible polynomial

$$f(y) = y^n + a_1 y^{n-1} + \ldots + a_n,$$

each prime factor of which is $\leq z$; y runs through the integral rational numbers $\leq x$. The case of a more general polynomial is trivially reduced to this one.

The method of the paper ([6]) can no longer be applied to polynomials. To achieve the aim, one has to use the theory of normal algebraic number fields and the laws of factorization of prime numbers in these fields. In connection with the complication of the problem, the estimates for the function $F_f(x, z)$ obtained in the present work will be somewhat weaker than the corresponding estimates for $F(x, z)$ in ([6]). This deficiency is apparently hidden in the method of proof used here. Let us formulate precisely the theorem to whose proof the work is devoted.

Theorem. Let $F_f(x, z)$ be the number of values of the polynomial $f(m)$, $m \leq x$, under the condition that every prime divisor $p \mid f(m)$ satisfies

$$p \leq z \leq x.$$

If $\alpha = \ln z / \ln x$, then in the interval $\ln \ln x / \ln x \leq \alpha \leq 1$ the estimate

$$F_f(x, z) \leq c(K)\, x \exp\left(-\frac{1}{4\alpha} \ln \frac{1}{\alpha}\right),$$

holds, where $c(K)$ is an absolute constant depending only on the constants of the normal field K generated by the polynomial f.

Proof. Consider the normal field K of the polynomial f. In this field $f(y)$ decomposes into linear factors:

$$f(y) = \prod_{i \le n} (y - \omega_i). \tag{1}$$

By assumption, $f(m)$ (m an integral rational number) has as prime divisors only numbers $p \le z$. Consequently, in the field K any linear factor (1)

$$(m - \omega_i) \tag{2}$$

has as prime divisors only prime ideals $\mathfrak{p}$ satisfying the condition:

$$N\mathfrak{p} = p^r, \qquad p \le z, \qquad r \le g(n), \tag{3}$$

where $g(n)$ is the degree of the field K, with the estimate $g(n) \le n!$. Let us take some fixed number ω_i. In this case $F_f(x, z)$ will not exceed the number of $m \le x$ for which the linear expression (2) in the field K has only those prime divisors $\mathfrak{p}$ that are subject to condition (3).

Consider two possibilities for α.

1. Let α lie in the range

$$1 \le \frac{1}{\alpha} \le g(n) + \frac{2 \ln \ln x}{\ln \ln \ln x}. \tag{4}$$

In this interval we apply to the sequence (2) the method of A. A. Buchstab, set forth in the paper (3), with the corresponding interpretation of it for the field K. We obtain, in a completely analogous way to (3), the estimate

$$F_f(x, z) \le c(K)\, x \exp\left(-\frac{1}{\alpha} \ln \frac{1}{\alpha}\right) + O\left(\frac{x}{\sqrt{\ln x}}\right).$$

But in the interval (4) the inequality holds:

$$\frac{1}{\sqrt{\ln x}} \le \exp\left(-\frac{1}{4\alpha} \ln \frac{1}{\alpha}\right).$$

Therefore, finally, for the interval (4) we obtain the estimate

$$F_f(x, z) \le c(K)\, x \exp\left(-\frac{1}{4\alpha} \ln \frac{1}{\alpha}\right). \tag{5}$$

2. Let α lie in the interval

$$g(n) + \frac{2 \ln \ln x}{\ln \ln \ln x} \leq \frac{1}{\alpha} \leq \frac{\ln x}{\ln \ln x}.$$

Decompose $m - \omega_i$ into prime factors in the field K:

$$m - \omega_i = \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_r. \tag{6}$$

From the factorization (6) one can always choose an ideal $\mathfrak{b}$ subject to the condition

$$\frac{x}{z^{g(n)}} \leq N\mathfrak{b} \leq x. \tag{7}$$

Indeed, let in (6)

$$N\mathfrak{p}_1 < x,$$

$$N\mathfrak{p}_1 \mathfrak{p}_2 < x,$$

$$\ldots\ldots\ldots\ldots$$

$$N\mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_j < x,$$

but already

$$N\mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_j \mathfrak{p}_{j+1} \geq x.$$

Consequently, for $\mathfrak{b} = \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_j$ we have

$$\frac{x}{N\mathfrak{p}_{j+1}} \leq N\mathfrak{b} < x.$$

But, by assumption, $N\mathfrak{p}_{j+1} \leq z^{g(n)}$. Hence (7) is obtained. Consequently, $F_f(x, z)$ does not exceed the number of solutions of the congruence

$$m \equiv \omega_i \pmod{\mathfrak{d}}, \tag{8}$$

summed over all $\mathfrak{d}$ of the interval (7) subject to condition (3). Let m_0 be the least integer rational number from the interval $(0, x)$ satisfying the congruence

$$\omega_i \equiv m_0 \pmod{\mathfrak{d}}$$

(if there is no such number, then the congruence (8) has no solutions). Replacing ω_i by m_0 in (8), we obtain that the number of solutions of (8) does not exceed twice the number of solutions of the congruence

$$m \equiv 0 \pmod{\mathfrak{d}}, \qquad m \le 2x.$$

But if an integer rational number m is divisible by the ideal $\mathfrak{d}$, then it is divisible also by $N\mathfrak{d}$; therefore the number of solutions of the congruence (8) is no more than $4x/N\mathfrak{d}$. Consequently,

$$F_f(x,z) \le 4x \sum_{\frac{x}{z^{g(n)}} < N\mathfrak{d} \le x} \frac{1}{N\mathfrak{d}}. \tag{9}$$

To estimate the sum on the right-hand side of (9), split it into sums of the form

$$\sum_{Q_i < N\mathfrak{d} \le 2Q_i} \frac{1}{N\mathfrak{d}}; \qquad Q_i = \frac{x}{z^{g(n)}}\, 2^i, \quad 0 \le i \le g(n)\frac{\ln z}{\ln 2}. \tag{10}$$

But the sum (10) does not exceed the quantity

$$\frac{1}{Q_i} \sum_{N\mathfrak{d} \le 2Q_i} 1. \tag{11}$$

We estimate the sum in (11) under the condition that each prime factor $\mathfrak{p}/\mathfrak{d}$ is subject to condition (3). We have

$$\sum_{N\mathfrak{d} \le Q} 1 \le e \sum_{\mathfrak{d}} \exp\left(-\frac{N\mathfrak{d}}{Q}\right) = \frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} Q^s \Gamma(s) \Pi_K(s,z)\, ds, \tag{12}$$

where

$$\Pi_K(s,z) = \prod_{\substack{N\mathfrak{p} = p^r \\ p = z,\ r \ge 1}} \left(1 - \frac{1}{N\mathfrak{p}^s}\right)^{-1}.$$

Applying to the function $\Pi_K(s,z)$ and to the integral (12) the technique of estimates developed in (6), with the corresponding correction for the field K, we obtain the estimate

$$\sum_{N\mathfrak{d}\leq 2Q_i} 1 \leq c(K)\, Q_i \exp\left(-\frac{\ln Q_i}{\ln z}\, \ln\frac{\ln Q_i}{\ln z}\right). \tag{13}$$

Substituting (13) into (11) and then summing over all i, we find

$$F_f(x,z) \leq c'(K)\, x \ln z\, \exp\left(-\left(\frac{1}{\alpha}-g(n)\right)\ln\left(\frac{1}{\alpha}-g(n)\right)\right).$$

But, by assumption,

$$\frac{1}{\alpha}-g(n) \geq \frac{2\ln\ln x}{\ln\ln\ln x}.$$

Therefore,

$$\ln z \exp\left[-\frac{2}{3}\left(\frac{1}{\alpha}-g(\eta)\right)\ln\left(\frac{1}{\alpha}-g(\eta)\right)\right] < 1.$$

Moreover,

$$\frac{1}{3}\left(\frac{1}{\alpha}-g(\eta)\right)\ln\left(\frac{1}{\alpha}-g(\eta)\right) > \frac{1}{4\alpha}\ln\frac{1}{\alpha}.$$

Consequently, for the second interval as well, the estimate

$$F_f(x,z) < c(K)x\exp\left(-\frac{1}{4\alpha}\ln\frac{1}{\alpha}\right)$$

is valid.

Combining it with estimate (5), we obtain the validity of the theorem.

Received
23 XII 1963

REFERENCES

[1] I. M. Vinogradov, *Izv. OMEN AN SSSR*, **20**, 47 (1926).
[2] Yu. V. Linnik, *DAN*, **36**, No. 4-5, 131 (1942).
[3] A. A. Bukhshtab, *DAN*, **67**, No. 1, 5 (1949).
[4] N. G. de Bruijn, *Nederl. Acad. Wetensch. Proc.*, Ser. A, **53**, 813 (1950).
[5] S. Chowla, W. E. Briggs, *Proc. Am. Math. Soc.*, **6**, No. 4 (1955).
[6] A. I. Vinogradov, *DAN*, **109**, No. 4 (1956).

Note: Figure translations are in progress. See original paper for figures.