ON THE THEORY OF PRIME NUMBERS

MATHEMATICS

1966

SovietRxiv

Abstract

Full Text

UDC 511

MATHEMATICS

D. N. LENSKOI

ON THE THEORY OF PRIME NUMBERS

(Presented by Academician Yu. V. Linnik on 5 XI 1965)

In this article we consider a generalization of a problem that we discussed earlier in ([1,2]).

Consider the integral polynomials

$$f_{in}(X_1, X_2, \dots, X_s) = \sum a^{(in)}_{j_1 j_2 \cdots j_s} X_1^{j_1} X_2^{j_2} \cdots X_s^{j_s} \qquad (1)$$

$(i = 1, 2, \dots, k;\ n = 1, 2, \dots)$, whose degrees are bounded by the number d, and we shall assume that $s \geq 2$. Take positive numbers $x_1, x_2, \dots, x_s$ and denote by $T(x_1, x_2, \dots, x_s, n)$ the number of integral points $(u_1, u_2, \dots, u_s)$ of the region $1 \leq u_1 \leq x_1,\ 1 \leq u_2 \leq x_2,\ \dots,\ 1 \leq u_s \leq x_s$, at which all the quantities $|f_{in}(u_1, u_2, \dots, u_s)|$ $(i = 1, 2, \dots, k)$ are prime numbers. The question arises of estimating $T(x_1, x_2, \dots, x_s, n)$ from above, valid at once for all n not exceeding a certain bound depending on

$$x = \min_{1 \leq \nu \leq s} x_\nu.$$

Below we obtain the indicated estimate under certain assumptions concerning the polynomials (1) (Theorem 1), and then this result is used to derive an upper bound for the number of solutions in prime numbers of one indeterminate equation (Theorem 2).

Let us agree on the following notation: p is a prime number; m is a natural number; $\alpha, \beta, \gamma, \delta, \tau, z$ are positive real numbers; $\omega_n(m)$ is the number of solutions, pairwise incongruent modulo m, of the congruence

$$\prod_{i=1}^{k} f_{in}(X_1, X_2, \dots, X_s) \equiv 0 \pmod{m};$$

$\mu(m)$ is the Möbius function; $\Gamma(\tau)$ is the gamma function. x and z will play the role of variables below. Positive constants depending only on k, s, d, α, β are denoted by the letter c with various subscripts. The constants implied by the symbol O do not depend on n.

Theorem 1. *Suppose the following conditions are satisfied:*

1) All the polynomials (1) are absolutely irreducible.

2) For each fixed n, the polynomials (1) are pairwise non-associated in the ring of integral polynomials.

3) For all $i, j_1, j_2, \dots, j_s, n$

$$\left|a^{(in)}_{j_1 j_2 \cdots j_s}\right| \le \alpha n^{\beta}.$$

4) For all n and p, $\omega_n(p) < p^s$.

Furthermore, let $\psi(x)$ be a nonnegative monotonically increasing function,

$$\lim_{x\to\infty} \psi(x) = \infty, \qquad \psi(x) = o(\ln x),$$

and from $\ln z \asymp \ln x$ let it follow that $\psi(z) \asymp \psi(x)$. Put

$$\Phi(x) = \max(\psi(x), \ln\ln x).$$

Then the estimate

$$T(x_1, x_2, \dots, x_s, n) \le 2^k k! \prod_p \frac{1-\omega_n(p)/p^s}{(1-1/p)^k}\, \frac{x_1 x_2 \cdots x_s}{\ln^k x}\left(1 + O\left(\frac{\Phi(x)}{\ln x}\right)\right) \quad (2)$$

holds

$$(x \to \infty,\ \ln\ln n \le \psi(x)).$$

Remark. If condition 4) is dropped, then for every n for which there is a p such that $\omega_n(p) = p^s$, the inequality

$$T(x_1, x_2, \dots, x_s, n) \le c_1 x_1 x_2 \dots x_s / x$$

holds.

For the proof of Theorem 1 we shall use algebraic-geometric considerations in combination with the sieve method (cf. (1)). We shall rely on the following three lemmas.

Lemma 1. *Suppose that conditions 1)–4) of Theorem 1 are fulfilled. Then for any n there exists a set $\mathfrak{P}(n)$ of prime numbers, containing not more than $c_2 \ln(n+1)$ elements, and such that*

$$\omega_n(p) = kp^{s-1} + O(p^{s-3/2}) \qquad (p \to \infty,\ p \notin \mathfrak{P}(n)).$$

Proof. For the proof of this lemma one uses arguments similar to those given in (3), p. 122, as well as the well-known Lang–Weil estimate (4).

Lemma 2. *Let the nonnegative multiplicative functions $F_n(m)$ $(n = 1, 2, \ldots)$ satisfy the following conditions:*

a) $F_n(p) \leq \gamma$ for all n and p;

b)
$$\sum_{p \leq z} \frac{F_n(p)}{p} \ln p = \tau \ln z + O(A(n)) \qquad (z \to \infty),$$

where $A(n)$ is some nonnegative function of n.

Suppose, furthermore, that $\psi(z)$ is a nonnegative function,

$$\lim_{x \to \infty} \psi(z) = \infty,$$

$$\psi(z) = o(\ln z).$$

Then for all n such that $A(n) \leq \delta\psi(z)$, the estimate

$$\sum_{m \leq z} \frac{\mu^2(m) F_n(m)}{m} = \frac{B(n)}{\Gamma(\tau+1)} \ln^\tau z \left(1 + O\left(\frac{\psi(z)}{\ln z}\right)\right) \qquad (z \to \infty),$$

holds, where $B(n)$ denotes the convergent infinite product

$$\prod_p \left(1 + \frac{F_n(p)}{p}\right)\left(1 - \frac{1}{p}\right)^\tau.$$

Proof. This lemma is a further stage in the development of Wirsing's elementary method (5), improved by B. V. Levin. Its proof, in all essentials, follows the ideas of B. V. Levin.

Lemma 3. *Suppose that condition 4 of Theorem 1 is fulfilled. Put*

$$F_n(m) = \frac{\omega_n(m)}{m^{s-1}} \prod_{p/m} \left(1 - \frac{\omega_n(p)}{p^s}\right)^{-1}. \tag{3}$$

Then

$$T(x_1, x_2, \ldots, x_s, n) \leq x_1 x_2 \ldots x_s \left(\sum_{m \leq z} \frac{\mu^2(m) F_n(m)}{m}\right)^{-1} +$$

$$+O\left(\frac{x_1x_2\dots x_s}{x}\,z^2\ln^{c_3}z\right)\qquad (x\to\infty,\ 1\le z\le\sqrt{x}). \tag{4}$$

Proof. The standard application of Selberg' s sieve method (6).

Proof of Theorem 1. We shall assume that all conditions of Theorem 1 are fulfilled. We proceed from inequality (4). Lemma 1 makes it possible to verify that the function $F_n(m)$, defined by equality (3), satisfies the conditions of Lemma 2, with $\tau=k$, $A(n)=\ln\ln n$ $(n\ge 27)$,

$$B(n)=\prod_p\frac{(1-1/p)^k}{1-\omega_n(p)/p^s}.$$

Therefore the sum appearing on the right-hand side of (4) can be estimated by Lemma 2. On the other hand, by virtue of Lemma 1, for the $B(n)$ found the following inequality holds:

$$B(n)\leqslant(\ln\ln n)^{c_4}\qquad (n\geqslant 27).$$

Using the preceding considerations, we obtain from (4) the relation

$$T(x_1,x_2,\dots,x_s,n)\leqslant k!\prod_p\frac{1-\omega_n(p)/p^s}{(1-1/p)^k}\,\frac{x_1x_2\cdots x_s}{\ln^k z}\left(1+O\left(\frac{\psi(z)}{\ln z}\right)+\right.$$

$$\left.+O\left(\frac{z^2}{x}\ln^{c_5}z\,(\psi(z))^{c_4}\right)\right)\quad (x\to\infty,\ z\leqslant\sqrt{x},\ z\to\infty,\ \ln\ln n\leqslant\delta\psi(z)). \tag{5}$$

Putting now in (5) $z=\sqrt{x}\ln^{-c_6}x$ (where c_6 is sufficiently large) and taking into account the properties of $\psi(x)$, we arrive at (2). The theorem is proved.

From Theorem 1 it follows that

Theorem 2. Let $f(X_1,X_2,\dots,X_s)$ be an integer polynomial with nonnegative coefficients $(s\geqslant 2)$; let $d_i>0$ be its degree in X_i $(i=1,2,\dots,s)$; let $n\geqslant 3$ be a natural number; and let $S_f(n)$ be the number of solutions in primes $p,p_1,p_2,\dots,p_s$ of the indeterminate equation

$$p+f(p_1,p_2,\dots,p_s)=n.$$

If the polynomial $f(X_1,X_2,\dots,X_s)-X$ is absolutely irreducible for at least one integral rational value of X, then

$$S_f(n)\leqslant c_f\frac{n^{\sum_{i=1}^{s}\frac{1}{d_i}}}{\ln^{s+1}n}\ln\ln n,$$

where c_f is a positive constant depending only on the polynomial f.

Remark. Using Theorem 1, we introduce into the upper estimate for $S_f(n)$ a factor analogous to the infinite product appearing in (2). It is bounded above by $c_7 \ln\ln n$, and this estimate cannot be improved, for example, for the polynomial $f(X_1, X_2, \dots, X_s) = X_1 X_2 \cdots X_s$ (which, of course, satisfies the conditions of Theorem 2).

For polynomials in one unknown, a result analogous to Theorem 2 was obtained by Schwarz [7].

Theorems 1–2 can be extended to algebraic number fields and function fields.

Saratov State University
named after N. G. Chernyshevsky

Received
28 X 1965

REFERENCES

1. D. N. Lenskoi, DAN, **150**, No. 2, 251 (1963).
2. D. N. Lenskoi, Vestn. LGU, ser. matem., mekh. i astr., issue 4, 162 (1963).
3. N. G. Chebotarev, *Teoriya algebraicheskikh funktsii*, M.–L., 1948.
4. S. Lang, A. Weil, Am. J. Math., **76**, No. 4, 819 (1954).
5. E. Wirsing, Math. Ann., **143**, No. 1, 75 (1961).
6. A. Selberg, XI Skand. Mat. Kongr., 1952, p. 13.
7. W. Schwarz, Math. Nachr., **23**, No. 6, 327 (1961).