ACTA ARITHMETICA
VI (1961)

On the distribution with respect to a prime modulus of the products of primes with a given value of a character

by

O. M. FOMENKO (Krasnodar, USSR)

Notations. We shall use thorough the following notation. The letter N will denote a number satisfying the condition $N > c_0$ where c_0 is sufficiently large; we put $r = \log N$. The letter Θ will denote a number $-1 < \Theta < 1$; c — a positive constant, and ε — an arbitrarily small positive number. For $B > 0$ the symbol $A \ll B$ shows that $|A| < cB$. For real x the symbol $\{x\}$ denotes the fractional part of x, i.e. the difference $x-[x]$. We will write $\exp x = e^x$.

The letter n will denote an arbitrary fixed integer >1; q — will be a prime number, with $q-1$ divisible by n. The letter s will denote one of the numbers $0, 1, \ldots, n-1$ and β will be a number such that $0 < \beta \leqslant 1$; $\mu(d)$ will denote the Möbius function. The symbol $\chi(a)$ will denote the character with respect to the modulus q which is different from the main character; it is known that

$$\chi(a) = \begin{cases} \exp\left(2\pi i \dfrac{t \operatorname{ind} a}{n}\right) & \text{if} \quad (a, q) = 1, \\ 0 & \text{if} \quad (a, q) = q, \end{cases}$$

where in this formula, and in the sequel, the index is taken with respect to the modulus q for a fixed primitive root. We shall assume that $(t, n) = 1$. Further, l will denote a positive integer; $w_l^{(s)}$ runs over all products of l different prime factors, where $\operatorname{ind} w_l^{(s)} \equiv s \pmod{n}$. The symbol $R_{l,\beta}^{(s)}(N)$ will denote the number of those $w_l^{(s)}$ which do not exceed N and whose smallest non-negative remainders with respect to the $\operatorname{mod} q$ are smaller than βq; hence $R_{l,1}^{(s)}(N)$ is the number of all those $w_l^{(s)}$ which do not exceed N.

In paper [1] I. M. Vinogradov, using his well-known method of trigonometric sums, proves the uniformity of the distribution of primes with respect to the modulus; the same result is obtained in [2] by elementary methods. In [3] the uniformity of the distribution with respect to a prime modulus of primes with a given value of Legendre Symbol is shown by elementary methods. In [4], the result of [1] is extended, by investigating the corresponding trigonometric sums, to the case of products of the same number of different prime factors. The present paper contains further results in this domain; we investigate problems connected with the distribution with respect to a prime modulus of the products of a given number of different primes with a given value of a character. The investigations are based upon the papers of Vinogradov, especially paper [4]. The arguments which already appear in Vinogradov's paper are here replaced by shorter ones.

LEMMA. *Let $0 < c \leqslant \frac{1}{6}$, $0 < \sigma \leqslant \frac{1}{3}$ and $0 < \gamma \leqslant 1-\sigma$. Let P be a product of primes different from q and not exceeding N^{σ}. Then if*

$$D = r^{\frac{\log r}{\log(1+c)}+n},$$

the divisors d of number P which do not exceed N can be distributed into $< D$ classes on condition that for all d which belong to a given class the value $\chi(d)$ is constant. For every class there exists a φ such that the numbers d from that class satisfy the inequality $\varphi < d \leqslant \varphi^{1+c}$. For some of the classes $\varphi \leqslant N^{\gamma}$. For all the remaining classes there exist a positive integer B and two increasing sequences of positive numbers x and y such that all x belong to a certain interval $\varphi_0 < x \leqslant \varphi_0^{1+c}$, which, in turn, is contained in the interval $N^{\gamma} < x \leqslant N^{\gamma+\sigma+c}$, and all the numbers d of the class under consideration, each of them taken B times, and only those numbers, can be obtained if we take the numbers xy with $(x, y) = 1$ from among all the products xy.

Proof. Let τ be the greatest integer satisfying the condition

$$2^{(1+c)^{\tau-1}} \leqslant N^{\sigma}.$$

Taking twice the logarithm of both sides of the last inequality we get

$$\tau < \frac{\log r}{\log(1+c)} - 3.$$

We put $b = [r]$ and consider all the non-increasing sequences $t_1, \ldots, t_b$, which can be obtained by selecting each t_j from among the numbers $\tau, \ldots, 1, 0$. The number of all such sequences will be smaller than

$$r^{\frac{\log r}{\log(1+c)}-2}.$$

We put

$$\varphi_j = 2^{(1+c)^{t_j-1}}, \quad F_j = \varphi_j^{1+c} \quad \text{if} \quad t_j > 0;$$
$$\varphi_j = 1, \quad F_j = 1 \quad \text{if} \quad t_j = 0.$$

Each d that does not exceed N is a product of $\leqslant b$ prime factors. Arranging all prime factors of the number d in a decreasing order, and (if their number h, is smaller than b) putting

$$p_{h+1} = \ldots = p_b = 1,$$

we represent d in the form

$$d = p_1 p_2 \ldots p_b.$$

Among the sequences $t_1, \ldots, t_b$ there is exactly one sequence which satisfies the conditions

$$\varphi_j < p_j \leqslant F_j \quad \text{if} \quad t_j > 0,$$
$$\varphi_j = p_j = F_j \quad \text{if} \quad t_j = 0,$$

and we shall say that the number d under consideration is connected with the sequence

$$(1) \qquad t_1, \ldots, t_b.$$

Putting $\varphi = \varphi_1 \ldots \varphi_b$ we have

$$\varphi < d \leqslant \varphi^{1+c}.$$

Let us consider the values d which are connected with sequence (1) with the condition

$$\varphi_1 \ldots \varphi_b \leqslant N^{\gamma}.$$

Let us split the values d into n classes, defined by the condition $\operatorname{ind} d \equiv s \pmod{n}$. Now we assume that $\varphi > N^{\gamma}$. Let us consider the class of all those d which are connected with the sequence $t_1, \ldots, t_b$. Let us denote by ζ the smallest integer satisfying the condition $\varphi_1 \ldots \varphi_\zeta > N^{\gamma}$. Then we have $\varphi_1 \ldots \varphi_{\zeta-1} \leqslant N^{\gamma}$, $\varphi_\zeta \leqslant N^{\sigma}$, $N^{\gamma} < \varphi_1 \ldots \varphi_\zeta \leqslant N^{\gamma+\sigma}$. Let $\varphi_{\zeta-k_1+1}, \ldots, \varphi_b, \ldots, \varphi_{\zeta+k_2}$ be all the values φ_j equal to φ_ζ. Then putting $d' = p_1 \ldots p_{\zeta-k_1}$, $d'' = p_{\zeta-k_1+1} \ldots p_{\zeta+k_2}$, $d''' = p_{\zeta+k_2+1} \ldots p_b$ we split the values d from the class considered into n^3 classes; for each value d from one of these new classes $\chi(d')$, $\chi(d'')$, $\chi(d''')$ will have the same value. For each new class, the values d'' will be split into $\leqslant r^n$ classes, each of them will consist of the numbers $d'd''d'''$ with the condition that among the prime factors of d'' there are μ_0 factors with index $\equiv 0 \pmod{n}$ where μ_0 is a given number, μ_1 factors with index $\equiv 1 \pmod{n}$ and so on, finally, μ_{n-1} factors with index $\equiv n-1 \pmod{n}$. Obviously, $\mu_0 + \mu_1 + \ldots + \mu_{n-1} = k_1 + k_2$.

Each of the numbers μ_i $(i = 0, 1, \ldots, n-1)$ will then be split into two integer terms $\lambda_1^{(i)}$ and $\lambda_2^{(i)}$ such that the following conditions are satisfied:

$$\lambda_1^{(0)}+\lambda_1^{(1)}+\ldots+\lambda_1^{(n-1)} = k_1;$$
$$\lambda_2^{(0)}+\lambda_2^{(1)}+\ldots+\lambda_2^{(n-1)} = k_2.$$

Let ξ and η run, independently of each other, over the following sets: ξ — over the products of k_1 different primes p_ζ which are connectep with φ_ζ, among which there are exactly $\lambda_1^{(0)}$ primes with indices $\equiv 0 \pmod n$, $\lambda_1^{(1)}$ primes with indices $\equiv 1 \pmod n, \ldots$, and $\lambda_1^{(n-1)}$ primes with indices $\equiv (n-1) \pmod n$; η — over the products of k_2 different primes p_ζ which are connected with φ_ζ, and among which there are exactly $\lambda_2^{(0)}$ primes with indices $\equiv 0 \pmod n$, $\lambda_2^{(1)}$ primes with indices $\equiv 1 \pmod n, \ldots$, and $\lambda_2^{(n-1)}$ primes with indices $\equiv n-1 \pmod n$.

For $(\xi, \eta) = 1$ and only in this case the product $\xi\eta$ will coincide with one of the numbers d'', and the same value d'' appears among all the products $\xi\eta$ exactly B times, where

$$B = \binom{\mu_0}{\lambda_1^{(0)}}\binom{\mu_1}{\lambda_1^{(1)}}\cdots\binom{\mu_{n-1}}{\lambda_1^{(n-1)}}.$$

But the numbers d of the chosen class, each of them taken B times, can be obtained by putting $x = d'\xi$, $y = \eta d'''$ and choosing from all xy only those which satisfy the condition $(x, y) = 1$. We easily obtain

$$(\varphi_1 \ldots \varphi_\zeta)^{1+c} \leqslant N^{\gamma+\sigma+c}.$$

Putting $\varphi_0 = \varphi_1 \ldots \varphi_\zeta$ we get $\varphi_0 < x \leqslant \varphi_0^{1+c}$. Moreover, the last interval is contained in the interval $N^\gamma < x \leqslant N^{\gamma+\sigma+c}$. To complete the proof of the lemma it suffices to notice that

$$n^3 r^{\frac{\log r}{\log(1+c)}-2} r^n < D.$$

THEOREM 1. *Let* $\sqrt{N} \leqslant \tau \leqslant N\exp(-r^{\varepsilon_0})$, $\alpha = a/q+\Theta/q\tau$, $(a, q) = 1$, $\exp(r^{\varepsilon_0}) \leqslant q \leqslant \tau$, $\Delta = \sqrt{1/q+q/N}$, $f = \Delta^{-1}$. *Let* K *be a positive integer with* $K \ll f^2$ *and*

$$S = \sum_{k=1}^{K}\Big|\sum_{w_l^{(s)} \leqslant N} \exp(2\pi i a k w_l^{(s)})\Big|.$$

Then we have

$$S \ll KN(\Delta^{1-\varepsilon'}+N^{-0.2+\varepsilon'}).$$

Proof. Let δ run over the set of products consisting of n_1 different prime factors which are not equal q and do not exceed $N^{0.2}$. Let z_h run over the set of products consisting of h different prime factors which are different from q and do not exceed $N^{0.2}$. By the lemma, all the values of δ which do not exceed N can be split into $< D$ classes and for each class there exists a number φ for which all the values δ of that class satisfy the relations:

$$\varphi < \delta \leqslant \varphi^{1+c}; \quad \chi(\delta) = \exp\left(2\pi i \frac{ts_0}{n}\right),$$

where s_0 is one of the numbers $0, 1, \ldots, n-1$. All the values of z_h can be split into n classes; for each of them the value of the character is constant and equal to $\chi(z_h) = \exp\left(2\pi i \frac{ts_1}{n}\right)$, where s_1 is one of the numbers $0, 1, \ldots, n-1$.

We shall denote by $z_h^{(s_1)}$ the value z_h, which belongs to the class for which

$$\chi(z_h) = \exp\left(2\pi i \frac{ts_1}{n}\right).$$

Let us consider the sum

$$S_h = \sum_{k=1}^{K}\Big|\sum \sum_{\delta z_h^{(s_1)} \leqslant N} \exp(2\pi i a k \delta z_h^{(s_1)})\Big|,$$

where δ runs over the set of values δ from an arbitrary class. At first we shall consider the class with $\varphi > N^{0.4}$. Let us put $\gamma = 0.4$, $\sigma = 0.2$ and apply the lemma. Then there exist a positive integer B and two increasing sequences of positive integers x and y such that all the values of x satisfy the condition

$$N^{0.4} < x \leqslant N^{0.6+c},$$

and all the values δ of the class considered, each of them taken B times, and only those values, can be obtained if from among all the products xy we take only such that $(x, y) = 1$. Thus,

$$S_h \ll \sum_{k=1}^{K}\Big|\sum_{x}\sum_{y}\sum_{z_h^{(s_1)}} \exp(2\pi i a k x y z_h^{(s_1)})\Big|,$$

where the summation is extended over the domain for which $xyz_h^{(s_1)} \leqslant N$ and $(x, y) = 1$. The next part of our considerations, which leads directly to the evaluation

$$S_h \ll KN(\Delta^{1-\varepsilon'}+N^{-0.2+\varepsilon'}),$$

does not differ from the corresponding considerations in the proof of Theorem 1 in paper [4]. We shall therefore omit it here. Let us now consider the case $\varphi \leqslant N^{0.4}$. The most difficult case is $\varphi \leqslant N^{0.2}$, and we shall consider only this case. We shall evaluate the sum S_h for $h = 1, 2, 3, 4$ (for $h = 0$, by the fact that $\varphi \leqslant N^{0.2}$, we have $S_h \ll KN^{0.2+c}$ and for $h > 4$ we have $S_h = 0$).

Let D be the product of all primes different from q and not exceeding $N^{0.2}$. Let Q be the product of all primes which are different from q and satisfy the condition $N^{0.2} < p \leqslant N$. For $s' = 1, 2, 3, 4$, putting

(2)
$$\sum_{\delta}\sum_{\substack{y_1|Q \\ \delta y_1\ldots y_{s'}\leqslant N, \\ \chi(y_1\ldots y_{s'})=\exp(2\pi i t s_1/n)}}\ldots\sum_{y_{s'}|Q}\exp(2\pi i a k\delta y_1\ldots y_{s'}) = W_{s'}$$

we get

$$W_{s'} = \sum_{\delta}\sum_{d_1|D}\sum_{\substack{m_1>0 \\ \delta d_1m_1\ldots d_{s'}m_{s'}\leqslant N, \\ \chi(d_1m_1\ldots d_{s'}m_{s'})=\exp(2\pi i t s_1/n)}}\ldots\sum_{d_{s'}|D}\sum_{m_{s'}>0}\mu(d_1)\ldots\mu(d_{s'})\exp(2\pi i a k\delta d_1m_1\ldots d_{s'}m_{s'}).$$

Among all the products $y_1, \ldots, y_{s'}$ of the left-hand side of (2) for a given δ, the number $z_h^{(s_1)}$ either appears $(s')^h$ times or does not appear at all. We put

$$S_h^{(s_1)} = \sum\sum_{\delta z_h^{(s_1)}\leqslant N}\exp(2\pi i a k\delta z_h^{(s_1)}).$$

Since among all the products $y_1y_2\ldots y_{s'}$ (for a given δ) there may be one which is equal to 1, and $\ll N^{0.8}\delta^{-1}$ of products which are divisible by the square of a prime divisor of the number Q, we obtain from (2):

(3)
$$s'S_1^{(s_1)} + (s')^2S_2^{(s_1)} + (s')^3S_3^{(s_1)} + (s')^4S_4^{(s_1)} = W_{s'} + O(N^{0.8+c}).$$

Putting $s' = 1, 2, 3, 4$, we get a system of four linear equations with four unknowns, whose determinant is different from zero. Thus, for some constants a_{ij} $(i = 1, 2, 3, 4,\ j = 1, 2, 3, 4)$ we find

$$S_i^{(s_1)} = a_{i1}W_1 + a_{i2}W_2 + a_{i3}W_3 + a_{i4}W_4 + O(N^{0.8+c}),$$

where $i = 1, 2, 3, 4$.

Now it is obvious that the problem is reduced to the evaluation of the sum

$$\sum_{k=1}^{K}|W_{s'}|,$$

where $s' = 1, 2, 3, 4$. We shall restrict our considerations to the case $s' = 4$ (the considerations in the remaining cases are the same). We split this sum into n^7 parts: for each of the parts $\chi(d_j), \chi(m_j)$ $(j = 1, 2, 3, 4)$ will assume a constant value. We shall consider only the part

$$\sum_{k=1}^{K}\Big|\sum_{\delta}\sum_{\substack{d_1|D \\ \delta d_1m_1\ldots d_4m_4\leqslant N}}^{\circ}\sum_{m_1>0}^{\circ}\ldots\sum_{d_4|D}^{\circ}\sum_{m_4>0}^{\circ}\exp(2\pi i a k\delta d_1m_1\ldots d_4m_4)\Big|,$$

where the summation is extended over the values δ of the chosen class, over the values d_j $(j = 1, 2, 3, 4)$ with the conditions $\chi(d_j) = 1$, and over the values m_j with the conditions $\chi(m_1) = \exp(2\pi i t s_1/n)$, $\chi(m_j) = 1$ $(j = 2, 3, 4)$. The remaining $n^7 - 1$ parts can be considered in a similar way. For each $j = 1, 2, 3, 4$ all the values d_j are distributed among $< D$ classes (by the lemma), and the values m_j $(j = 1, 2, 3, 4)$ are distributed among $\ll r$ classes with the conditions of the form

$$M_j < m_j \leqslant M_j', \quad 2M_j \leqslant M_j' < 4M_j.$$

Let

$$T = \sum_{k=1}^{K}\Big|\sum_{\delta}\sum_{\substack{d_1 \\ \delta d_1\ldots d_4m_1\ldots m_4\leqslant N}}^{\circ}\ldots\sum_{d_4}^{\circ}\sum_{m_1}^{\circ}\ldots\sum_{m_4}^{\circ}\exp(2\pi i a k\delta d_1\ldots d_4m_1\ldots m_4)\Big|,$$

where $\chi(d_j) = 1$ $(j = 1, 2, 3, 4)$, $\chi(m_1) = \exp(2\pi i t s_1/n)$, $\chi(m_j) = 1$ $(j = 2, 3, 4)$, and the summation is extended over the values δ from the chosen class, over the values d_1, d_2, d_3, d_4 with certain conditions of the form $\varphi^{(1)} < d_1 \leqslant F^{(1)}$, $\varphi^{(2)} < d_2 \leqslant F^{(2)}$, $\varphi^{(3)} < d_3 \leqslant F^{(3)}$, $\varphi^{(4)} < d_4 \leqslant F^{(4)}$, where $F^{(j)} = (\varphi^{(j)})^{1+c}$ $(j = 1, 2, 3, 4)$, and over four classes of values m_1, m_2, m_3, m_4 with conditions of the form

$$M_1 < m_1 \leqslant M_1', \quad M_2 < m_2 \leqslant M_2', \quad M_3 < m_3 \leqslant M_3', \quad M_4 < m_4 \leqslant M_4'.$$

Further considerations, which lead directly to the evaluation

$$T \ll KN(\Delta^{1-s'} + N^{-0.2+s'}),$$

are exactly the same as the corresponding considerations in the proof of Theorem 1 in paper [4]. We shall therefore omit them here. The theorem is proved.

THEOREM 2. *Let* $\sqrt{N} \leqslant \tau \leqslant N\exp(-r^{s_0})$, $\alpha = a/q + \Theta/q\tau$, $(a, q) = 1$, $\exp(r^{s_0}) \leqslant q \leqslant \tau$. *Let the symbol* $Z_{l,\beta}^{(s)}(N)$ *denote the number of those values* $w_l^{(s)}$ *which do not exceed* N *and satisfy the relation* $\{\alpha w_l^{(s)}\} < \beta$. *Then we have*

$$Z_{l,\beta}^{(s)}(N) = \beta Z_{l,1}^{(s)}(N) + O(N\Delta_1), \quad \textit{where } \Delta_1 = (1/q + q/N)^{0.5-s_1} + N^{-0.2+s_1}.$$

Proof. This theorem easily follows from Theorem 1 by the use of well-known methods (see, for instance, [1] and [4]).

THEOREM 3. *Let q be a prime number satisfying the condition* $\exp(r^{\varepsilon_0}) \leqslant q \leqslant N\exp(-r^{\varepsilon_0})$. *Then we have*

$$R_{l,\beta}^{(s)}(N) = \beta R_{l,1}^{(s)}(N) + O(N\Delta_1),$$

where

$$\Delta_1 = (1/q+q/N)^{0.5-\varepsilon_1} + N^{-0,2+\varepsilon_1}.$$

Proof. If we put $a = 1$, $\Theta = 0$, $\tau = N\exp(-r^{\varepsilon_0})$ in Theorem 2, we obtain the equality

$$Z_{l,\beta}^{(s)}(N) = R_{l,\beta}^{(s)}(N).$$

The theorem is proved. In the case $\chi(a) = \left(\frac{a}{q}\right)$, $l = 1$ we obtain the result of paper [3].

References

[1] I. M. Vinogradov (И. М. Виноградов), *Метод тригонометрических сумм в теории чисел*, (in Russian) Trudy Mat. Inst. Steklov. 23 (1947), pp. 1-109.

[2] — *Элементарное доказательство одной теоремы теории чисел*, (in Russian) Izv. Akad. Nauk SSSR, Ser. Mat., 17 (1953), pp. 3-12.

[3] — *Распределение по простому модулю простых чисел с заданным значением символа Лежандра*, (in Russian) Izw. Akad. Nauk SSSR, Ser. Mat., 18 (1954), pp. 105-112.

[4] — *О распределении произведений простых чисел и значений функции Мёбиуса*, (in Russian) Izw. Akad. Nauk SSSR, Ser. Mat., 12 (1948), pp. 341-350.

Reçu par la Rédaction le 30. 4. 1960

ACTA ARITHMETICA
VI (1961)

On the representation of integers by binary forms

by

D. J. LEWIS* (Notre Dame, Ind.) and K. MAHLER (Manchester)

Let $F(x, y)$ be a binary form of degree $n \geqslant 3$ with integral coefficients of height a and with non-zero discriminant, and let m be an integer distinct from zero. H. Davenport and K. F. Roth, in 1955, proved a general theorem on Diophantine equations of which the following result is a particular case.

The equation $F(x, y) = m$ *cannot have more than*

$$(4a)^{2n^2}|m|^3 + \exp(643n^2)$$

integral solutions x, y.

This result is of great interest because it gives an explicit upper bound for the number of solutions. The proof depends on the deep ideas which Roth introduced into the Thue-Siegel theory of the approximations of algebraic numbers.

We establish in this paper a better upper bound for the number of solutions of $F(x, y) = m$. Our proof does not depend on Roth's method, but uses instead the p-adic generalization of the Thue-Siegel theorem discovered by one of us in 1932. We consider only primitive solutions x, y, i. e. solutions where x and y are relatively prime; but this is not an essential restriction.

Already in the original paper M_2 of 1933, it was proved that the equation $F(x, y) = m$ has not more than

$$c^{t+1}$$

solutions where $c > 0$ is a constant independent of m, and t denotes the number of distinct prime factors of m. Since $c^{t+1} = O(|m|^{\varepsilon})$ for every $\varepsilon > 0$, this estimate is better than that by Davenport and Roth for all sufficiently large $|m|$; but it does not show the dependance on the coefficients and the degree of $F(x, y)$ of the number of solutions.

* National Science Foundation Fellow.