

O. M. Fomenko

О распределении по простому модулю простых чисел с заданным значением символа Лежандра

Czechoslovak Mathematical Journal, Vol. 11 (1961), No. 1, 143–149

Persistent URL: <http://dml.cz/dmlcz/100448>

Terms of use:

© Institute of Mathematics AS CR, 1961

Institute of Mathematics of the Czech Academy of Sciences provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.



This document has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* <http://dml.cz>

О РАСПРЕДЕЛЕНИИ ПО ПРОСТОМУ МОДУЛЮ ПРОСТЫХ ЧИСЕЛ
С ЗАДАННЫМ ЗНАЧЕНИЕМ СИМВОЛА ЛЕЖАНДРА

О. М. ФОМЕНКО, Краснодар, СССР

(Поступило в редакцию 12/II 1960 г.)

В статье исследуется вопрос о распределении простых чисел, для которых при данном простом модуле $q > 0$ и данном β , $0 < \beta \leq 1$, символ Лежандра (p/q) принимает предписанное значение, и наименьший неотрицательный вычет, которых $(\text{mod } q)$ меньше чем βq . Статья примыкает к работам Виноградова [1] и [2] и расширяет справедливость некоторых его результатов или их уточняет.

Обозначения. Буквою N обозначаем число с условием $N > c_0$, где c_0 достаточно велико; полагаем $r = \ln N$. Буквою θ обозначаем число с условием $-1 \leq \theta \leq 1$; c — положительное постоянное число; ε — произвольно малое положительное постоянное число. При $B > 0$ обозначение $A \ll B$ показывает, что $|A| \leq c|B|$. При вещественном x символ $\{x\}$ обозначает дробную часть числа x ; q — простое число; s — одно из чисел $1, -1$; $p^{(s)}$ пробегает простые числа с заданным значением символа Лежандра $(p^{(s)}/q) = s$; β — число с условием $0 < \beta \leq 1$; $\pi_{s,\beta}(N)$ — число тех $p^{(s)}$, не превосходящих N , наименьшие неотрицательные вычеты которых по $\text{mod } q$ меньше βq ; следовательно, $\pi_{s,1}(N)$ — число всех $p^{(s)}$, не превосходящих N ; $\mu(d)$ — функция Мебиуса.

В работе [1] И. М. Виноградов доказал элементарным методом равномерность распределения по простому модулю простых чисел с заданным значением символа Лежандра. В работе [2] И. М. Виноградов, используя свой известный метод тригонометрических сумм, доказал равномерность распределения простых чисел по модулю. Используя план этого доказательства мы в настоящей работе оцениваем тригонометрические суммы по простым числам с заданным значением символа Лежандра по простому модулю и отсюда выводим результат работы [1] с лучшим остаточным членом.

Лемма. Пусть $0 < c \leq \frac{1}{6}$; $0 < \sigma \leq \frac{1}{3}$; $0 \leq \gamma \leq 1 - \sigma$; P -произведение простых чисел, не равных q и не превосходящих N^σ . Тогда, полагая

$$D = r^{\ln r / \ln(1+c)},$$

делители d числа P , не превосходящие N , можно распределить среди $< D$ сово-

купностей с условием, что для чисел d , принадлежащих одной совокупности, символ (d/q) , а также функция $\mu(d)$ сохраняют неизменные значения. Для каждой совокупности существует свое ϕ с условием, что принадлежащие этой совокупности значения d удовлетворяют неравенствам

$$\phi < d \leq \phi^{1+c}.$$

Для некоторых совокупностей будет $\phi \leq N^\gamma$; для каждой из остальных совокупностей существует целое положительное B и 2 возрастающие последовательности целых положительных чисел x и y такие, что все x лежат в некотором интервале $\phi_0 < x \leq \phi_0^{1+c}$, полностью лежащем в интервале $N^\gamma < x \leq N^{\gamma+\sigma+c}$, причем все числа d рассматриваемой совокупности, взятые каждое B раз, и только эти числа, получим, если из всех произведений xy выберем лишь удовлетворяющие условию $(x, y) = 1$.

Доказательство. Пусть τ — наибольшее целое с условием

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

Дважды логарифмируя обе части неравенства, получаем

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

Полагая $b = [r]$, рассмотрим все невозрастающие ряды t_1, \dots, t_b , которые получим, выбирая каждое t_j среди чисел $\tau, \dots, 1, 0$. Число всех таких рядов будет

$$< r^{(\ln r / \ln(1+c)) - 2}.$$

Полагаем

$$\begin{aligned} \phi_j &= 2^{(1+c)t_j-1}, \quad F_j = \phi_j^{1+c}, \quad \text{если } t_j > 0; \\ \phi_j &= 1, \quad F_j = 1, \quad \text{если } t_j = 0. \end{aligned}$$

Всякое d , не превосходящее N , является произведением $\leq b$ простых сомножителей. Располагая простые сомножители числа d в порядке убывания и, если их число h меньше b , полагая $p_{h+1} = \dots = p_b = 1$, представим d в форме $d = p_1 p_2 \dots p_b$. Среди рядов t_1, \dots, t_b найдемся единственный ряд с условиями

$$\phi_j < p_j \leq F_j, \quad \text{если } t_j > 0; \quad \phi_j = p_j = F_j, \quad \text{если } t_j = 0,$$

и мы будем говорить, что рассматриваемое d связано с этим рядом

$$(1) \quad t_1, \dots, t_b.$$

Полагая $\phi = \phi_1 \dots \phi_b$, будем иметь $\phi < d \leq \phi^{1+c}$. Рассмотрим значения d , связанные с последовательностями (1) с условием $\phi_1 \dots \phi_b \leq N^\gamma$. Разобьем d на 2 класса; в один из них войдут значения d с условием $(d/q) = 1$, в другой — значения d с условием $(d/q) = -1$. Предположим теперь, что $\phi > N^\gamma$. Рассмотрим совокупность всех d , связанных с данным рядом t_1, \dots, t_b . Обозначим буквою β наименьшее целое число с условием $\phi_1 \dots \phi_\beta > N^\gamma$. Тогда имеем

$$\phi_1 \dots \phi_{\beta-1} \leq N^\gamma, \quad \phi_\beta \leq N^\sigma, \quad N^\gamma < \phi_1 \dots \phi_\beta \leq N^{\gamma+\sigma}.$$

Пусть $\phi_{\beta-k_1+1}, \dots, \phi_\beta, \dots, \phi_{\beta+k_2}$ — все значения ϕ_j , равные ϕ_β . Тогда, полагая

$$d' = p_1 \dots p_{\beta-k_1}, \quad d'' = p_{\beta-k_1+1} \dots p_\beta \dots p_{\beta+k_2}, \quad d''' = p_{\beta+k_2+1} \dots p_b,$$

мы значения d рассматриваемой совокупности разобьём на 8 совокупностей. Для значений d , принадлежащих одной из этих новых совокупностей символы

$$(d'|q), \quad (d''|q), \quad (d'''|q)$$

сохраняют неизменные значения. Для каждой новой совокупности значения d'' разобьём на $\leq r$ классов, относя к одному и тому же классу значения d'' с одним и тем же числом квадратичных невычетов по mod q среди простых сомножителей. В соответствии с этим каждая новая совокупность разобьётся на $\leq r$ классов. В каждый класс войдут числа d', d'', d''' совокупности с условием, что среди простых сомножителей d'' имеется заданное число μ квадратичных невычетов по mod q . Очевидно, должно быть $\mu \leq k_1 + k_2$.

Число μ можно разбить на 2 целочисленных слагаемых λ_1 и λ_2 с условием $\lambda_1 \leq k_1, \lambda_2 \leq k_2$. Пусть ξ и η независимо друг от друга пробегают: ξ — произведения k_1 различных простых p_β , связанных с ϕ_β , среди которых имеется ровно λ_1 квадратичных невычетов; η — произведения k_2 различных простых p_β , связанных с ϕ_β , среди которых имеется ровно λ_2 квадратичных невычетов. При $(\xi, \eta) = 1$ и только в этом случае произведение $\xi\eta$ совпадает с одним из d'' , причём одно и то же d'' встретится среди всех произведений $\xi\eta$ ровно

$$B = C_\mu^{\lambda_1} C_{k_1+k_2-\mu}^{k_1-\lambda_1} \text{ раз.}$$

Числа же d выбранного класса, каждое B раз, получим, если полагая $x = d'\xi, y = \eta d'''$, мы из всех $xу$ выберем лишь удовлетворяющие условию $(x, y) = 1$. Без труда получаем

$$(\phi_1 \dots \phi_\beta)^{1+c} \leq N^{\gamma+\sigma+c}.$$

Положив $\phi_0 = \phi_1 \dots \phi_\beta$, имеем $\phi_0 < x \leq \phi_0^{1+c}$. При этом последний интервал полностью лежит в интервале $N^\gamma < x \leq N^{\gamma+\sigma+c}$.

Заметив, что

$$8r \cdot r^{(\ln r / \ln(1+c)) - 2} < D,$$

убеждаемся в справедливости леммы. Настоящая лемма есть уточнение леммы 2 работы [1].

Теорема 1. Пусть

$$\sqrt{N} \leq \tau \leq Ne^{-r\epsilon_0}; \quad \alpha = \frac{a}{q} + \frac{\theta}{q\tau}; \quad (a, q) = 1;$$

$$e^{r\epsilon_0} \leq q \leq \tau; \quad \Delta = \sqrt{\frac{1}{q} + \frac{q}{N}}; \quad f = \Delta^{-1}; \quad K\text{-целое, } 0 < K \ll f^2;$$

$$S = \sum_{k=1}^K \left| \sum_{p^{(s)} \leq N} e^{2\pi i \alpha k p^{(s)}} \right|. \quad \text{Тогда имеем } S \ll KN(\Delta^{1-\epsilon'} + N^{-0,2+\epsilon'}).$$

Доказательство. Пусть

$$2 \leq H \leq N^{\frac{1}{2}}; \quad P = \prod_{\substack{p \leq H \\ p \neq q}} p; \quad Q = \prod_{\substack{H < p \leq N \\ p \neq q}} p;$$

s_0 — наибольшее целое с условием $H^{s_0} < N$. При s' , имеющем одно из значений $s' = 1, \dots, s_0$, полагая

$$(2) \quad \sum_{y_1 | Q} \dots \sum_{y_{s'} | Q} e^{2\pi i a k y_1 \dots y_{s'}} = W_{s'}, \quad y_1 \dots y_{s'} \leq N, \quad (y_1 \dots y_{s'} / q) = s,$$

имеем

$$W_{s'} = \sum_{d_1 | P} \sum_{m_1 > 0} \dots \sum_{d_{s'} | P} \sum_{m_{s'} > 0} \mu(d_1) \dots \mu(d_{s'}) e^{2\pi i a k d_1 m_1 \dots d_{s'} m_{s'}}.$$

$$d_1 m_1 \dots d_{s'} m_{s'} \leq N, \quad (d_1 m_1 \dots d_{s'} m_{s'} / q) = s.$$

Пусть j -натуральное число и $D_j^{(s)}$ — произведение j различных простых чисел, удовлетворяющее условию $(D_j^{(s)} / q) = s$. Полагаем

$$S_j^{(s)} = \sum_{D_j^{(s)} | Q} e^{2\pi i a k D_j^{(s)}}.$$

Среди произведений $y_1 \dots y_{s'}$, стоящих в показателях степеней левой части (2), данное $D_j^{(s)}$ встречается $(s')^j$ раз, так как каждый его простой сомножитель может входить в $y_1, y_2, \dots, y_{s'}$. Так как среди произведений $y_1 \dots y_{s'}$ имеется, может быть, одно равное 1, и $\ll NH^{-1}$ произведений, делящихся на квадрат целого, превосходящего 1, то из (2) следует

$$(3) \quad s' S_1^{(s)} + (s')^2 S_2^{(s)} + \dots + (s')^{s_0} S_{s_0}^{(s)} = W_{s'} + O(NH^{-1}).$$

Положим $H = N^{0,2}$; тогда $s_0 = 4$. Полагая в (3) $s' = 1, 2, 3, 4$, получим систему четырех линейных уравнений с четырьмя неизвестными $S_1^{(s)}, S_2^{(s)}, S_3^{(s)}, S_4^{(s)}$. Определитель системы $\neq 0$. Отсюда ввиду

$$S = \sum_{k=1}^K |S_1^{(s)}| + O(K\sqrt{N})$$

находим

$$S \ll \sum_{k=1}^K |W_1| + \sum_{k=1}^K |W_2| + \sum_{k=1}^K |W_3| + \sum_{k=1}^K |W_4| + KN^{0,8}.$$

Ограничимся оценкой четвертого слагаемого (первые три оцениваются аналогично). Разбиваем это слагаемое на 2^{11} частей: для каждой части $\mu(d_j), (d_j/q), (m_j/q)$ ($j = 1, \dots, 4$) сохраняют неизменные значения. Рассмотрим лишь часть

$$\sum_{k=1}^K \left| \sum_{d_1 | P} \sum_{m_1 > 0} \dots \sum_{d_4 | P} \sum_{m_4 > 0} e^{2\pi i a k d_1 m_1 \dots d_4 m_4} \right|, \quad d_1 m_1 \dots d_4 m_4 \leq N,$$

где суммирование распространяется на значения d_j ($j = 1, \dots, 4$) с условиями $\mu(d_j) = 1, (d_j/q) = 1$ и значения m_j с условиями $(m_1/q) = s, (m_j/q) = 1$ ($j = 2, \dots, 4$). Остальные $2^{11} - 1$ частей рассматриваются аналогично.

Значения d_j ($j = 1, \dots, 4$) распределяются среди $< D$ совокупностей (по лемме, причем $\sigma = 0,2$), а значения m_j ($j = 1, \dots, 4$) распределяются среди $\ll r$ совокупностей с условием вида $M_j < m_j \leq M'_j$, $M'_j \leq 2M_j$. Пусть

$$T = \sum_{k=1}^K \left| \sum_{d_1=0}^{\infty} \sum_{d_2=0}^{\infty} \sum_{d_3=0}^{\infty} \sum_{d_4=0}^{\infty} \sum_{m_1=0}^{\infty} \sum_{m_2=0}^{\infty} \sum_{m_3=0}^{\infty} \sum_{m_4=0}^{\infty} e^{2\pi i \alpha k d_1 d_2 d_3 d_4 m_1 m_2 m_3 m_4} \right|, \quad d_1 d_2 d_3 d_4 m_1 m_2 m_3 m_4 \leq N,$$

где

$$\begin{aligned} \mu(d_j) &= 1, \quad (d_j/q) = 1 \quad (j = 1, 2, 3, 4), \\ (m_1/q) &= s, \quad (m_j/q) = 1 \quad (j = 2, 3, 4), \end{aligned}$$

причем суммирование распространяется на какие-либо четыре совокупности значений d_1, d_2, d_3, d_4 , определяемые неравенствами $\phi^{(1)} < d_1 \leq F^{(1)}$; $\phi^{(2)} < d_2 \leq F^{(2)}$; $\phi^{(3)} < d_3 \leq F^{(3)}$; $\phi^{(4)} < d_4 \leq F^{(4)}$; $F^{(j)} = (\phi^{(j)})^{1+c}$, и четыре совокупности значений m_1, m_2, m_3, m_4 , определяемые неравенствами

$$\begin{aligned} M_1 < m_1 \leq M'_1; \quad M_2 < m_2 \leq M'_2; \\ M_3 < m_3 \leq M'_3; \quad M_4 < m_4 \leq M'_4. \end{aligned}$$

Дальнейшая часть доказательства совершенно аналогична окончанию доказательства теоремы 3 гл. 9 работы [2].

Теорема 2. Пусть

$$\begin{aligned} \sqrt{N} \leq \tau \leq Ne^{-r^{\epsilon_0}}; \quad \alpha - \text{вещественное, } \alpha = a/q + \Theta/q\tau; \quad (a, q) = 1; \\ e^{r^{\epsilon_0}} \leq q \leq \tau; \quad 0 < \beta \leq 1; \quad H^{(s)} \text{ обозначает число простых чисел } p^{(s)} \text{ с условиями} \\ p^{(s)} \leq N, \{ap^{(s)}\} < \beta. \text{ Тогда} \end{aligned}$$

$$H^{(s)} = \beta\pi_{s,1}(N) + O(N\gamma); \quad \gamma = (1/q + q/N)^{0,5-\epsilon} + N^{-0,2+\epsilon}.$$

Доказательство. Эта теорема легко выводится из теоремы 1 с помощью приёмов, изложенных в гл. 11 работы [2].

Теорема 3. Пусть q — простое число с условием

$$e^{r^{\epsilon_0}} \leq q \leq Ne^{-r^{\epsilon_0}}.$$

Тогда имеем

$$\pi_{s,\beta}^{\mathbb{F}}(N) = \beta\pi_{s,1}(N) + O(N\gamma); \quad \gamma = (1/q + q/N)^{0,5-\epsilon} + N^{-0,2+\epsilon}.$$

Доказательство. Положив в теореме 2 $a = 1$, $\Theta = 0$, $\tau = Ne^{-r^{\epsilon_0}}$, приходим к равенству $H^{(s)} = \pi_{s,\beta}(N)$. Теорема доказана.

Теорема 3 с несколько худшим остаточным членом

$$(O(N^{1+\epsilon}(\sqrt{1/q + q/N} + N^{-\frac{1}{2}})))$$

получена в работе [1].

Литература

- [1] *И. М. Виноградов*: Распределение по простому модулю простых чисел с заданным значением символа Лежандра. Изв. АН СССР, серия матем., № 2, т. 18, 1954, 105—112.
 [2] *И. М. Виноградов*: Метод тригонометрических сумм в теории чисел. Труды Матем. ин-та АН СССР, т. 23, 1947, 1—111.

Résumé

SUR LA RÉPARTITION DU MODULE PREMIER DES NOMBRES
 PREMIERS A VALEUR DU SYMBOLE DE LEGENDRE DONNÉE

O. M. FOMENKO. Krasnodar (URSS)

Soient p et q deux nombres premiers, ε , ε_0 , ε' des nombres positifs aussi petits qu'on veut, $0 < \beta \leq 1$ une constante réelle fixée, et $|\vartheta| \leq 1$; désignons par (p/q) le symbole de Legendre. Soit ensuite N un nombre positif suffisamment grand et $r = \ln N$, $s = 1$ ou -1 . Par $p^{(s)}$ nous désignons le nombre premier pour lequel $(p^{(s)}/q) = s$. Soit enfin $\pi_{s,\beta}(N)$ le nombre de nombres premiers $p^{(s)}$ ne dépassant pas N et dont les plus petits restes non-négatifs mod q sont plus petits que βq .

Théorème 1. *Soit*

$$\sqrt{N} \leq \tau \leq Ne^{-r\varepsilon_0}, \alpha = a/q + \vartheta/q\tau, (a, q) = 1, e^{r\varepsilon_0} \leq q \leq \tau,$$

$$\Delta = \sqrt{1/q + q/N}, f = \Delta^{-1};$$

soit ensuite K un entier, $0 < K \ll f^2$ et

$$S = \sum_{k=1}^K \left| \sum_{p^{(s)} \leq N} e^{2\pi i \alpha k p^{(s)}} \right|.$$

Alors

$$(1) \quad S \ll KN(\Delta^{1-\varepsilon'} + N^{-0,2+\varepsilon'}).$$

Théorème 2. *Soit $\sqrt{N} \leq \tau \leq Ne^{-r\varepsilon_0}$, soit α réel*

$$\alpha = a/q + \vartheta/q\tau, (a, q) = 1, e^{r\varepsilon_0} \leq q \leq \tau, 0 < \beta \leq 1$$

soit enfin $H^{(s)} = \sum_{p^{(s)} \leq N} 1, \{\alpha p^{(s)}\} < \beta$. Alors

$$(2) \quad H^{(s)} = \beta \pi_{s,1}(N) + O(N\gamma),$$

où

$$\gamma = (1/q + q/N)^{\frac{1}{2}-\varepsilon} + N^{-\frac{1}{s}+\varepsilon}.$$

Théorème 3. Soit q un nombre premier, $e^{\varepsilon_0} \leq q \leq Ne^{-r\varepsilon_0}$. Alors

$$(3) \quad \pi_{s,\beta}(N) = \beta\pi_{s,1}(N) + O(N\gamma),$$

où

$$\gamma = (1/q + q/N)^{\frac{1}{2}-\varepsilon} + N^{-\frac{1}{5}+\varepsilon}.$$

Les théorèmes 1 et 2 généralisent les résultats de I. M. VINOGRADOV (voir [2], chap. 9, théorème 3, et chap. 11, théorème 1) qui a obtenu les mêmes relations (1)

et (2) pour les sommes $S = \sum_{k=1}^K \left| \sum_{p \leq N} e^{2\pi i \alpha k p} \right|$ où $H = \sum_{p \leq N, \{\alpha p\} < \beta} 1$, resp.

La relation (3) avec une estimation moins précise du reste, savoir

$$\pi_{s,\beta}(N) = \beta\pi_{s,1}(N) + O(N\gamma')$$

où

$$\gamma' = (1/q + q/N)^{\frac{1}{2}} N^{\varepsilon} + N^{-\frac{1}{5}+\varepsilon}$$

a été également trouvée par Vinogradov dans son travail [1].