Math-Net.Ru

Общероссийский математический портал

М. А. Королёв, О среднем числе степенных вычетов по составному модулю, *Изв. РАН. Сер. матем.*, 2010, том 74, выпуск 6, 127–156

DOI: <https://doi.org/10.4213/im4110>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением <http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 3.85.7.115

26 апреля 2023 г., 09:29:26

УДК 511

М. А. Королёв

О среднем числе степенных вычетов по составному модулю

Изучается поведение величин $a_n(q)$ и $b_n(q)$, обозначающих количество вычетов степени n в соответственно приведенной и полной системах вычетов по составному модулю q , где $n \geq 2$ – произвольное фиксированное число. В частности, доказываются асимптотические формулы для сумматорных функций $A_n(x)$ и $B_n(x)$ этих величин.

Библиография: 15 наименований.

Ключевые слова: степенные вычеты, среднее число степенных вычетов, задача Лемера–Ландау.

§ 1. Введение

Прежде всего, дадим несколько определений, необходимых для дальнейшего.

ОПРЕДЕЛЕНИЕ 1. Пусть q и n – целые числа, $q \geq 2$, $n \geq 2$. *Вычетом степени n по модулю q* будем называть всякое целое число, сравнимое по модулю q с одним из чисел ряда $0, 1, 2^n, 3^n, 4^n, \dots$. Вычеты второй степени будем называть *квадратичными вычетами*, третьей степени – *кубическими*, четвертой степени – *биквадратичными*.

ОПРЕДЕЛЕНИЕ 2. Через $a_n(q)$ и $b_n(q)$ будем обозначать количества различных вычетов степени n в соответственно приведенной и полной системах вычетов по модулю q . Положим также $a_n(1) = b_n(1) = 1$ при любом n .

ПРИМЕР 1. Пусть $n = 3$, $q = 12$. Из сравнений

$$\begin{array}{ll} 0^3 \equiv 0 \pmod{12}, & 6^3 \equiv 0 \pmod{12}, \\ 1^3 \equiv 1 \pmod{12}, & 7^3 \equiv 7 \pmod{12}, \\ 2^3 \equiv 8 \pmod{12}, & 8^3 \equiv 8 \pmod{12}, \\ 3^3 \equiv 3 \pmod{12}, & 9^3 \equiv 9 \pmod{12}, \\ 4^3 \equiv 4 \pmod{12}, & 10^3 \equiv 4 \pmod{12}, \\ 5^3 \equiv 5 \pmod{12}, & 11^3 \equiv 11 \pmod{12} \end{array}$$

следует, что кубическими вычетами по модулю 12 служат числа 0, 1, 3, 4, 5, 7, 8, 9 и 11, из которых приведенной системе вычетов принадлежат числа 1, 5, 7 и 11. Таким образом, $a_3(12) = 4$, $b_3(12) = 9$.

Настоящая статья посвящена изучению величин $a_n(q)$ и $b_n(q)$ и, в частности, поведения сумм

$$A_n(x) = \sum_{q \leq x} a_n(q), \quad B_n(x) = \sum_{q \leq x} b_n(q)$$

при неограниченном возрастании x в случае, когда $n \geq 2$ – произвольное фиксированное число.

Задача нахождения асимптотик величин $A_n(x)$, $B_n(x)$ оказывается очень похожей на задачу Лемера–Ландау (см. [1]–[7], а также [8, с. 641–669]) об определении количества чисел, не превосходящих заданной границы, все простые делители p которых принадлежат фиксированному набору арифметических прогрессий по заданному модулю n :

$$p \equiv l_1 \pmod{n}, \quad \dots, \quad p \equiv l_k \pmod{n}. \quad (1)$$

Здесь $1 \leq k \leq \varphi(n)$, $1 \leq l_1 < \dots < l_k < n$, $(l_\nu, n) = 1$, $\nu = 1, \dots, k$. Если обозначить множество таких чисел через $D = D(n; l_1, \dots, l_k)$ и определить при $\operatorname{Re} s > 1$ производящую функцию $\Phi(s)$ равенством

$$\Phi(s) = 1 + \sum_{n \in D} n^{-s},$$

то можно показать, что $\Phi(s)$ представляется в полуплоскости $\operatorname{Re} s > 1$ производением

$$(\zeta(s))^\delta \prod_{\substack{\chi \bmod n \\ \chi \neq \chi_0}} (L(s, \chi))^{\delta(\chi)} h(s), \quad (2)$$

в котором χ пробегает неглавные характеры Дирихле по модулю n , функция $h(s)$ аналитична при $\operatorname{Re} s > 1/2$, а $\delta(\chi)$ – числа (вообще говоря, комплексные), определяемые равенством

$$\delta(\chi) = \frac{1}{\varphi(n)} \sum_{\nu=1}^k \bar{\chi}(l_\nu),$$

причем $\delta = \delta(\chi_0) = k/\varphi(n)$. Следствием (2) является асимптотическая формула Ландау

$$\sum_{\substack{n \in D \\ n \leq x}} 1 = \frac{x}{(\ln x)^{1-\delta}} \left(\sum_{m=0}^M \frac{D_m}{\Gamma(\delta - m)} \frac{1}{(\ln x)^m} + O\left(\frac{1}{(\ln x)^{M+1}}\right) \right),$$

в которой M – произвольное фиксированное число, $D_0, D_1, \dots$ – некоторые константы, зависящие от n и набора $l_1, \dots, l_k$; постоянная в знаке O зависит от M .

Полагая для $\operatorname{Re} s > 2$

$$F_n(s) = \sum_{q=1}^{\infty} \frac{a_n(q)}{q^s}, \quad G_n(s) = \sum_{q=1}^{\infty} \frac{b_n(q)}{q^s}, \quad (3)$$

в настоящей статье мы показываем, что каждая из этих производящих функций имеет вид

$$(\zeta(s-1))^{\gamma(n)} \prod_{\substack{\chi \bmod n \\ \chi \neq \chi_0}} (L(s-1, \chi))^{\gamma(n; \chi)} h(s), \quad (4)$$

где $h(s)$ аналитична в полуплоскости $\operatorname{Re} s > 3/2$, а числа $\gamma(n; \chi)$ и $\gamma(n)$ определяются равенствами

$$\gamma(n; \chi) = \frac{1}{\varphi(n)} \sum_{\substack{k=1 \\ (k, n)=1}}^n \frac{\overline{\chi}(k)}{(k-1, n)}, \quad \gamma(n) = \gamma(n; \chi_0) = \frac{1}{\varphi(n)} \sum_{\substack{k=1 \\ (k, n)=1}}^n \frac{1}{(k-1, n)}. \quad (5)$$

Здесь $\varphi(n)$ – функция Эйлера, а через (a, b) обозначен наибольший общий делитель целых чисел a и b , причем $(a, 0) = a$.

Неожиданной особенностью рассматриваемой задачи оказывается то обстоятельство, что для любого комплексного характера χ по модулю n число $\gamma(n; \chi)$ является вещественным.

Пользуясь представлением (4), каждую из функций $F_n(s)$ и $G_n(s)$ можно продолжить в некоторую область с границей, проходящей левее прямой $\operatorname{Re} s = 2$. Выбирая затем подходящий замкнутый контур, лежащий целиком внутри этой области, с помощью метода комплексного интегрирования мы заключаем, что имеет место следующая

ТЕОРЕМА 1. *При любом фиксированном $M \geq 0$ и $x \rightarrow +\infty$ справедливы асимптотические формулы*

$$A_n(x) = \frac{x^2}{(\ln x)^{1-\gamma}} \left(\sum_{m=0}^M \frac{A_m}{\Gamma(\gamma-m)} \frac{1}{(\ln x)^m} + O\left(\frac{1}{(\ln x)^{M+1}}\right) \right), \quad (6)$$

$$B_n(x) = \frac{x^2}{(\ln x)^{1-\gamma}} \left(\sum_{m=0}^M \frac{B_m}{\Gamma(\gamma-m)} \frac{1}{(\ln x)^m} + O\left(\frac{1}{(\ln x)^{M+1}}\right) \right), \quad (7)$$

где $\gamma = \gamma(n)$, $A_0, A_1, \dots, B_0, B_1, \dots$ – константы, зависящие от n , а постоянные в знаках O зависят от M .

Из формул (5)–(7) следует, например, что “в среднем” натуральные числа оказываются вычетами пятой степени чаще, чем кубическими, а кубическими вычетами – чаще, чем квадратичными. Сказанное следует понимать в том смысле, что при достаточно большом x выполняются неравенства

$$A_2(x) < A_3(x) < A_5(x), \quad B_2(x) < B_3(x) < B_5(x). \quad (8)$$

Действительно, полагая $n = 2, 3, 5$ в равенствах (5), получим

$$\gamma(2) = \frac{1}{2}, \quad \gamma(3) = \frac{1}{2} \left(\frac{1}{3} + 1 \right) = \frac{2}{3}, \quad \gamma(5) = \frac{1}{4} \left(\frac{1}{5} + 1 + 1 + 1 \right) = \frac{4}{5}.$$

Таким образом, при подходящих положительных постоянных C_n , $n = 2, 3, 5$, из теоремы 1 получаем соотношения

$$A_2(x) \sim \frac{C_2 x^2}{\sqrt{\ln x}}, \quad A_3(x) \sim \frac{C_3 x^2}{\sqrt[3]{\ln x}}, \quad A_5(x) \sim \frac{C_5 x^2}{\sqrt[5]{\ln x}}$$

(аналогично для $B_n(x)$), следствиями которых будут неравенства (8).

В статье также изучаются числа $\gamma(n)$, определенные равенством (5) и входящие в показатель степени $\ln x$ в формулах (6) и (7).

Заметим, что число $\delta = k/\varphi(n)$, играющее в задаче Лемера–Ландау ту же роль, что и число $\gamma(n)$ в рассматриваемой задаче, допускает очевидную интерпретацию. Именно, δ есть отношение числа прогрессий (1), среди которых находятся все простые делители чисел множества D , к общему числу всех арифметических прогрессий по модулю n , первый член которых взаимно прост с модулем. Однако числа $\gamma(n)$ такой наглядной интерпретации, по-видимому, не допускают.

Продолжая вычисление значений $\gamma(n)$ по формулам (5), получим следующую таблицу:

n	$\gamma(n)$	n	$\gamma(n)$	n	$\gamma(n)$	n	$\gamma(n)$
2	$\frac{1}{2}$	10	$\frac{2}{5}$	18	$\frac{17}{54}$	26	$\frac{6}{13}$
3	$\frac{2}{3}$	11	$\frac{10}{11}$	19	$\frac{18}{19}$	27	$\frac{152}{243}$
4	$\frac{3}{8}$	12	$\frac{1}{4}$	20	$\frac{3}{10}$	28	$\frac{3}{14}$
5	$\frac{4}{5}$	13	$\frac{12}{13}$	21	$\frac{4}{7}$	29	$\frac{28}{29}$
6	$\frac{1}{3}$	14	$\frac{3}{7}$	22	$\frac{5}{11}$	30	$\frac{4}{15}$
7	$\frac{6}{7}$	15	$\frac{8}{15}$	23	$\frac{22}{23}$	31	$\frac{30}{31}$
8	$\frac{11}{32}$	16	$\frac{43}{128}$	24	$\frac{11}{48}$	32	$\frac{171}{512}$
9	$\frac{17}{27}$	17	$\frac{16}{17}$	25	$\frac{99}{125}$	33	$\frac{20}{33}$

Из нее видно, что последовательность $\gamma(n)$ ведет себя достаточно нерегулярно. Например, в случае, когда n – простое число, величины $\gamma(n)$ близки к единице, а в случае, когда n пробегает степени двойки, значения $\gamma(n)$ с ростом n приближаются к $1/3$. В свете сказанного естественно поставить вопрос о среднем значении $\gamma(n)$, т. е. о пределе при $x \rightarrow +\infty$ величины

$$\frac{1}{x} \sum_{2 \leq n \leq x} \gamma(n).$$

Имеет место следующая

ТЕОРЕМА 2. *При $x \rightarrow +\infty$ справедлива асимптотическая формула*

$$\sum_{2 \leq n \leq x} \gamma(n) = Cx + O((\ln x)(\ln \ln x)^2),$$

где

$$C = \prod_p \left(1 - \frac{p}{p^3 - 1} \right) = 0.5759599 \dots$$

Наконец, теорема 2 устанавливает еще одну закономерность, отраженную в таблице, и дает способ вычисления $\gamma(n)$ для случая, когда известно каноническое разложение числа n на простые сомножители.

ТЕОРЕМА 3. *Функция $\gamma(n)$ мультипликативна. Если n – степень простого числа p , то*

$$\gamma(n) = 1 - \frac{p}{p^2 - 1} \left(1 - \frac{1}{n^2} \right).$$

В частности, при $p = 2, 3, 5, 7$ справедливы равенства

$$\gamma(n) = \frac{n^2 + 2}{3n^2}, \quad \gamma(n) = \frac{5n^2 + 3}{8n^2}, \quad \gamma(n) = \frac{19n^2 + 5}{24n^2}, \quad \gamma(n) = \frac{41n^2 + 7}{48n^2}.$$

Далее, для простого p , натурального $n > 1$ и неотрицательного целого числа a запись $p^a \| n$ означает, что n делится на p^a , но не делится на p^{a+1} . В частности, для $a = 0$ эта запись означает взаимную простоту чисел n и p . Через $\mu(n)$, $\tau(n)$ и $\nu(n)$ обозначены стандартные теоретико-числовые функции: функция Мёбиуса, число делителей n и число различных простых сомножителей, входящих в каноническое разложение n . Наконец, через $\theta, \theta_1, \dots$ обозначены комплексные числа, не превосходящие по абсолютной величине единицы и в разных соотношениях, вообще говоря, разные. Все прочие обозначения вводятся по ходу изложения.

§ 2. Явные формулы для $a_n(q)$ и $b_n(q)$

В настоящем параграфе доказывается мультипликативность функций $a_n(q)$ и $b_n(q)$ при фиксированном n и приводятся формулы для этих величин в случае, когда q – степень простого числа.

ЛЕММА 1. *При фиксированном n функции $a_n(q)$ и $b_n(q)$ мультипликативны по q .*

ДОКАЗАТЕЛЬСТВО. Пусть $q = q_1 q_2$, где $(q_1, q_2) = 1$, $q_1 > 1$, $q_2 > 1$. Рассмотрим все остатки v , которые получаются при делении на q чисел $v_1 q_2^n + v_2 q_1^n$, где v_1 и v_2 пробегает вычеты степени n соответственно по модулям q_1 и q_2 , причем $1 \leq v_1 \leq q_1$, $1 \leq v_2 \leq q_2$. Число таких остатков совпадает с числом пар v_1, v_2 и равно $b_n(q_1) b_n(q_2)$. Все эти остатки различны по модулю q , так как из сравнений

$$v \equiv v_1 q_2^n + v_2 q_1^n \equiv v' \equiv v'_1 q_2^n + v'_2 q_1^n \pmod{q}$$

следует, что $v_1 \equiv v'_1 \pmod{q_1}$, $v_2 \equiv v'_2 \pmod{q_2}$, т. е. $v_1 = v'_1$, $v_2 = v'_2$, $v = v'$.

Выбирая числа u_1 и u_2 так, чтобы выполнялись сравнения

$$v_1 \equiv u_1^n \pmod{q_1}, \quad v_2 \equiv u_2^n \pmod{q_2},$$

закключаем, что каждое из чисел v есть вычет степени n по модулю q :

$$v \equiv v_1 q_2^n + v_2 q_1^n \equiv (u_1 q_2)^n + (u_2 q_1)^n \equiv (u_1 q_2 + u_2 q_1)^n \pmod{q}.$$

Покажем теперь, что каждый вычет w по модулю q сравним с одним из остатков v . Действительно, если $w \equiv u^n \pmod{q}$, то, определяя числа u_1 и u_2 из условий

$$u \equiv u_1 q_2 \pmod{q_1}, \quad u - u_1 q_2 = u_2 q_1,$$

будем иметь

$$u = u_1 q_2 + u_2 q_1, \\ w \equiv (u_1 q_2 + u_2 q_1)^n \equiv u_1^n q_2^n + u_2^n q_1^n \equiv v_1 q_2^n + v_2 q_1^n \pmod{q},$$

где v_1, v_2 – вычеты степени n по модулям q_1 и q_2 соответственно, $v_s \equiv u_s^n \pmod{q_s}$, $1 \leq v_s \leq q_s$, $s = 1, 2$. Таким образом, число остатков v равно $b_n(q)$, т. е. $b_n(q) = b_n(q_1)b_n(q_2)$.

Мультипликативность $a_n(q)$ доказывается аналогично с той лишь разницей, что в приведенных выше рассуждениях следует рассматривать лишь вычеты, взаимно простые с модулем.

ОПРЕДЕЛЕНИЕ 3. Для целых чисел $n \geq 2$, $q \geq 2$ через $e_n(q)$ обозначим *число решений сравнения*

$$x^n \equiv 1 \pmod{q}. \quad (9)$$

В случае $q = 1$ положим $e_n(q) = 1$.

ЗАМЕЧАНИЕ 1. Величина $e_n(q)$ совпадает с числом решений любого сравнения $x^n \equiv v \pmod{q}$, где v – вычет степени n по модулю q , взаимно простой с модулем. Поскольку величина $e(f, q)$, равная числу решений сравнения

$$f(x) = a_n x^n + \dots + a_1 x + a_0 \equiv 0 \pmod{q},$$

для заданного многочлена f является мультипликативной функцией q , то и $e_n(q)$ при фиксированном n мультипликативна по q .

ЛЕММА 2. Пусть $q = p^k$, где p – простое, $k \geq 1$ – целое числа, и пусть $n \geq 2$. Тогда справедливы равенства

$$a_n(q) = \frac{\varphi(p^k)}{e_n(p^k)}, \quad b_n(q) = \frac{\varphi(p^k)}{e_n(p^k)} + \frac{\varphi(p^{k-n})}{e_n(p^{k-n})} + \dots + \frac{\varphi(p^{k-mn})}{e_n(p^{k-mn})} + 1,$$

где m – наибольшее целое число с условием $k - mn \geq 1$.

ДОКАЗАТЕЛЬСТВО. Все числа полной системы вычетов по модулю q разобьем на классы, относя к классу с номером s , $0 \leq s \leq k$, числа, кратные p^s , но не кратные p^{s+1} , т. е. числа вида $x p^s$, $(x, p) = 1$. Пусть $k - sn \geq 1$. Подсчитаем, сколько различных остатков образуется при делении на q n -х степеней чисел s -го класса. Их будет столько же, сколько существует различных остатков от деления на $q_1 = p^{k-sn}$ n -степеней чисел приведенной системы вычетов по модулю q_1 .

Пусть r – искомое количество остатков, и пусть $x_1, \dots, x_r$ – некоторые числа, n -е степени которых различны по модулю q_1 . Обозначим через $v_1, \dots, v_c$ все решения сравнения $x^n \equiv 1 \pmod{q_1}$, $c = e_n(q_1)$. Каждый из $\varphi(q_1)$ вычетов, взаимно простых с q_1 , при возведении в степень n сравним лишь с одним из чисел x_i^n , $1 \leq i \leq r$. Все числа $x_i v_1, \dots, x_i v_c$ при возведении в степень n дают один и тот же остаток. Следовательно, все числа приведенной системы вычетов по модулю q_1 распределятся по r группам, каждая из которых состоит из c элементов. Таким образом, $cr = \varphi(q_1)$, откуда имеем

$$r = \frac{\varphi(q_1)}{e_n(q_1)}. \quad (10)$$

Если $sn \geq k$, то все числа s -го класса после возведения в степень становятся кратными q , т. е. дают при делении на q один и тот же остаток – нулевой.

Суммируя величины (10) по всем классам, начиная с нулевого, придем к искомой формуле для $b_n(q)$. Поскольку вычеты, взаимно простые с q , получаются при возведении в n -ю степень чисел нулевого класса, то

$$a_n(q) = \frac{\varphi(q)}{e_n(q)}.$$

ЛЕММА 3. Пусть $q = p^k$, где p – простое, $k \geq 1$ – целое числа. Тогда $e_n(q) = (2n, \varphi(q))$, если n четное, $p = 2$, $k \geq 3$, и $e_n(q) = (n, \varphi(q))$ в остальных случаях.

ДОКАЗАТЕЛЬСТВО. В каждом из случаев $q = 2, 4, p^k$, $p \geq 3$, $k \geq 1$, зафиксируем произвольный первообразный корень g по модулю q и перепишем сравнение (9) в виде

$$n\gamma \equiv 0 \pmod{\varphi(q)},$$

где γ – индекс x по основанию g . Число решений последнего сравнения равно $(n, \varphi(q))$.

В случае $q = 2^k$, $k \geq 3$, все числа x приведенной системы вычетов запишем в виде

$$x \equiv (-1)^{\gamma_0} 5^\gamma \pmod{q},$$

где (γ_0, γ) – система индексов по модулю q , $0 \leq \gamma_0 \leq 1$, $1 \leq \gamma \leq \varphi(q)/2 = 2^{k-2}$. Тогда сравнение (9) эквивалентно системе

$$n\gamma_0 \equiv 0 \pmod{2}, \quad n\gamma_1 \equiv 0 \pmod{\frac{1}{2}\varphi(q)}.$$

В случае нечетного n эта система имеет единственное решение $\gamma_0 = 0$, $\gamma_1 = \varphi(q)/2$, так что число ее решений совпадает с $(n, \varphi(q))$. Если n – четное число, то первое сравнение системы имеет два решения, а второе – $(n, \varphi(q)/2)$ решений. Общее же число систем индексов (γ_0, γ_1) , удовлетворяющих системе, составит $2(n, \varphi(q)/2) = (2n, \varphi(q))$.

(По поводу доказательств формул лемм 2, 3 см. [9].)

ПРИМЕР 2. Пусть $n = 3$. Полагая $q = p^k$, где p – простое число, при $p \neq 3$ получим

$$e_3(q) = (3, p^{k-1}(p-1)) = (3, p-1) = \begin{cases} 3, & \text{если } p \equiv 1 \pmod{3}, \\ 1, & \text{если } p \equiv 2 \pmod{3}. \end{cases}$$

Если $p = 3$, то

$$e_3(q) = (3, 2 \cdot 3^{k-1}) = (3, 3^{k-1}) = \begin{cases} 1, & \text{если } k = 1, \\ 3, & \text{если } k \geq 2. \end{cases}$$

В частности, $e_3(3) = e_3(4) = 1$, откуда имеем

$$\begin{aligned} a_3(12) &= a_3(4) a_3(3) = \varphi(4) \varphi(3) = 2 \cdot 2 = 4, \\ b_3(12) &= b_3(4) b_3(3) = (\varphi(4) + 1)(\varphi(3) + 1) = 3 \cdot 3 = 9. \end{aligned}$$

§ 3. Производящие функции последовательностей $a_n(q)$ и $b_n(q)$

В настоящем параграфе изучаются свойства производящих функций $F_n(s)$ и $G_n(s)$ последовательностей $a_n(q)$ и $b_n(q)$, определенных в полуплоскости $\operatorname{Re} s > 2$ равенствами (3).

Зафиксируем целое число $n \geq 2$ и выясним, какие значения принимает величина $e_n(q)$, когда q пробегает степени одного и того же простого числа p . Для этого рассмотрим несколько случаев.

Случай 1: p не делит n . Согласно лемме 3 имеем

$$e_n(p^m) = (n, p^{m-1}(p-1)) = (n, p-1).$$

Несложно заметить, что если числа d, d' принадлежат одной арифметической прогрессии с разностью n , то значения $(n, d-1)$ и $(n, d'-1)$ совпадают. Если выбрать число k с условиями $1 \leq k < n$, $(n, k) = 1$, то для всех простых чисел p из арифметической прогрессии $p \equiv k \pmod{n}$ величины $e_n(p^m)$ имеют одно и то же значение $\delta = (n, k-1)$. Поскольку n фиксировано, то все такие числа δ содержатся среди делителей n . Обозначим через $c_\delta(n)$ количество чисел k в приведенной системе вычетов по модулю n , удовлетворяющих условию $(n, k-1) = \delta$. Если при некотором δ оказывается $c_\delta(n) > 0$, то это означает, что существует в точности $c_\delta(n)$ арифметических прогрессий по модулю n , обладающих следующим свойством: для всех простых чисел p , принадлежащих этим прогрессиям, имеют место равенства

$$e_n(p) = e_n(p^2) = e_n(p^3) = \dots = \delta.$$

Случай 2: p делит n , $p > 2$. Пусть a – наибольшая степень p , делящая n . Тогда, полагая $\delta = (n, p-1)$, будем иметь

$$e_n(p^m) = (n, p^{m-1}(p-1)) = (n, p-1)(p^a, p^{m-1}) = \delta p^c,$$

где c – меньшее из чисел a и $m-1$.

Случай 3: p делит n , $p = 2$. Если a – наибольшая степень двойки, делящая n , то $e_n(2) = (n, 1) = 1$, $e_n(4) = (n, 2) = 2$ и при $m \geq 3$

$$e_n(2^m) = (2n, 2^{m-1}) = (2^{a+1}, 2^{m-1}) = 2^c,$$

где c – меньшее из чисел $a+1$, $m-1$. Эта же формула справедлива и в случаях $m = 1$, $m = 2$.

Из мультипликативности $a_n(q)$ и $b_n(q)$ следует, что в области $\operatorname{Re} s > 2$ функции $F_n(s)$ и $G_n(s)$ разлагаются в эйлеровы произведения вида

$$F_n(s) = \prod_p F_{n,p}(s), \quad G_n(s) = \prod_p G_{n,p}(s),$$

где

$$F_{n,p}(s) = 1 + \sum_{m=1}^{\infty} \frac{a_n(p^m)}{p^{ms}}, \quad G_{n,p}(s) = 1 + \sum_{m=1}^{\infty} \frac{b_n(p^m)}{p^{ms}}.$$

ЛЕММА 4. Пусть p – простое, $a \geq 0$ – целое числа, $p^a \parallel n$, и пусть $\delta_p = (n, p-1)$. Если $p = 2$, $a \geq 1$, то

$$F_{n,p}(s) = 1 + \frac{2^{(a+1)s}(2^s - 2) + 1}{2^{(a+1)s}(2^s - 2)(2^s - 1)},$$

$$G_{n,p}(s) = 1 + \frac{2^{(a+1)s}(2^s - 2)(2 \cdot 2^{ns} - 1) + 2^{ns}}{2^{(a+1)s}(2^s - 2)(2^{ns} - 1)(2^s - 1)}.$$

Во всех остальных случаях имеем

$$F_{n,p}(s) = 1 + \frac{p-1}{\delta_p} \frac{p^{as}(p^s - p) + p-1}{p^{as}(p^s - 1)(p^s - p)},$$

$$G_{n,p}(s) = 1 + \frac{p^{as}(p^s - p)\{p^{ns}(p-1 + \delta_p) - \delta_p\} + p^{ns}(p-1)^2}{\delta_p p^{as}(p^s - 1)(p^s - p)(p^{ns} - 1)}.$$

В частности, для $a = 0$ имеем

$$F_{n,p}(s) = \left(1 - \frac{1}{\delta_p p^{s-1}}\right)^{-1} f_{n,p}(s), \quad G_{n,p}(s) = \left(1 - \frac{1}{\delta_p p^{s-1}}\right)^{-1} g_{n,p}(s),$$

где

$$\begin{aligned} f_{n,p}(s) &= 1 + \frac{(\delta_p - 1)p - \delta_p p^{s-1} + 1}{\delta_p^2 p^s (p^{s-1} - 1)}, \\ g_{n,p}(s) &= 1 + \frac{(\delta_p - 1)p - \delta_p p^{s-1} + 1}{\delta_p^2 p^s (p^{s-1} - 1)} \\ &\quad + \left(1 - \frac{1}{\delta_p p^{s-1}}\right) \left(\frac{1}{p^s - 1} + \frac{p - 1}{\delta_p (p^s - p)(p^{ns} - 1)}\right). \end{aligned}$$

ДОКАЗАТЕЛЬСТВО. Пусть сначала $p = 2$, $a \geq 1$. Поскольку $e_n(2^m) = 2^{m-1}$ при $1 \leq m \leq a + 1$ и $e_n(2^m) = 2^{a+1}$ при $m \geq a + 2$, то

$$\begin{aligned} F_{n,2}(s) &= 1 + \sum_{m=1}^{a+1} \frac{\varphi(2^m)}{2^{m-1}} 2^{-ms} + \sum_{m=a+2}^{\infty} \frac{\varphi(2^m)}{2^{a+1}} 2^{-ms} \\ &= 1 + \sum_{m=1}^{a+1} 2^{-ms} + 2^{-(a+2)} \sum_{m=a+2}^{\infty} 2^{-m(s-1)} \\ &= 1 + \frac{2^{(a+1)s} - 1}{2^{(a+1)s}(2^s - 1)} + \frac{1}{2^{(a+1)s}(2^s - 2)} = 1 + \frac{2^{(a+1)s}(2^s - 2) + 1}{2^{(a+1)s}(2^s - 2)(2^s - 1)}. \end{aligned}$$

В оставшихся случаях ($p = 2$, $a = 0$ либо $p \geq 3$, $a \geq 0$) $e_n(p^m) = \delta_p p^{m-1}$ при $1 \leq m \leq a$ и $e_n(p^m) = \delta_p p^a$ при $m \geq a + 1$. Следовательно,

$$\begin{aligned} F_{n,p}(s) &= 1 + \frac{1}{\delta_p} \sum_{m=1}^a \frac{\varphi(p^m)}{p^{m-1}} p^{-ms} + \frac{1}{\delta_p} \sum_{m=a+1}^{\infty} \frac{\varphi(p^m)}{p^a} p^{-ms} \\ &= 1 + \frac{p-1}{\delta_p} \sum_{m=1}^a p^{-ms} + \frac{p-1}{\delta_p} \sum_{m=a+1}^{\infty} p^{-m(s-1)} \\ &= 1 + \frac{p-1}{\delta_p} \left(\frac{1 - p^{-as}}{p^s - 1} + \frac{p^{-as}}{p^s - p} \right) = 1 + \frac{p-1}{\delta_p} \frac{p^{as}(p^s - p) + p - 1}{p^{as}(p^s - 1)(p^s - p)}. \end{aligned}$$

Чтобы просуммировать ряд для $G_{n,p}(s)$, заметим, что число слагаемых в формуле леммы 2 для $b_n(p)$ равно $\left[\frac{m-1}{n}\right] + 2$ и имеет одно и то же значение $k + 2$ для $m = kn + 1, kn + 2, \dots, (k + 1)n$. Таким образом,

$$\begin{aligned} G_{n,p}(s) &= 1 + \sum_{k=0}^{\infty} \sum_{m=kn+1}^{(k+1)n} p^{-ms} \left(\frac{\varphi(p^m)}{e_n(p^m)} + \frac{\varphi(p^{m-n})}{e_n(p^{m-n})} + \dots + \frac{\varphi(p^{m-kn})}{e_n(p^{m-kn})} + 1 \right) \\ &= 1 + \frac{1}{p^s - 1} + \sum_{k=0}^{\infty} \sum_{m=kn+1}^{\infty} p^{-ms} \frac{\varphi(p^{m-kn})}{e_n(p^{m-kn})} \\ &= 1 + \frac{1}{p^s - 1} + \sum_{k=0}^{\infty} \sum_{\mu=1}^{\infty} p^{-(kn+\mu)s} \frac{\varphi(p^{\mu})}{e_n(p^{\mu})} \end{aligned}$$

$$= 1 + \frac{1}{p^s - 1} + \sum_{k=0}^{\infty} p^{-kns} \sum_{\mu=1}^{\infty} p^{-\mu s} \frac{\varphi(p^\mu)}{e_n(p^\mu)} = 1 + \frac{1}{p^s - 1} + \frac{p^{ns}}{p^{ns} - 1} (F_{n,p}(s) - 1).$$

Теперь утверждение леммы следует из полученных выше формул для $F_{n,p}(s)$.

ЛЕММА 5. Пусть k, δ – натуральные числа, $(k, n) = 1$, и пусть при $\operatorname{Re} s > 1$

$$\Pi(s) = \Pi_{n,k,\delta}(s) = \prod_{p \equiv k \pmod{n}} \left(1 - \frac{1}{\delta} p^{-s}\right)^{-1}. \quad (11)$$

Тогда при тех же s справедливо тождество

$$\begin{aligned} \Pi(s) &= \prod_{\chi \bmod n} \{L(s, \chi)\}^{\frac{\bar{\chi}(k)}{\delta \varphi(n)}} \\ &\times \exp \left\{ \sum_{m=2}^{\infty} \frac{1}{m \delta^m} \sum_{p \equiv k \pmod{n}} p^{-ms} - \sum_{m=2}^{\infty} \frac{1}{m \delta} \sum_{p^m \equiv k \pmod{n}} p^{-ms} \right\}. \end{aligned}$$

ДОКАЗАТЕЛЬСТВО. Логарифмируя обе части равенства (11) и пользуясь тем, что сумма

$$\frac{1}{\varphi(n)} \sum_{\chi \bmod n} \chi(q) \bar{\chi}(k)$$

равна единице, если $q \equiv k \pmod{n}$, и равна нулю в противном случае, находим

$$\begin{aligned} \ln \Pi(s) &= \sum_{m=1}^{\infty} \frac{1}{m \delta^m} \sum_{p \equiv k \pmod{n}} p^{-ms} = \frac{1}{\varphi(n)} \sum_{\chi \bmod n} \bar{\chi}(k) \sum_{m=1}^{\infty} \frac{1}{m \delta^m} \sum_p \chi(p) p^{-ms} \\ &= \frac{1}{\varphi(n)} \sum_{\chi \bmod n} \bar{\chi}(k) \left(\sum_p \sum_{m=1}^{\infty} \frac{\chi(p^m)}{m \delta} p^{-ms} \right. \\ &\quad \left. + \sum_p \sum_{m=1}^{\infty} \frac{1}{m} \left(\frac{\chi(p)}{\delta^m} - \frac{\chi(p^m)}{\delta} \right) p^{-ms} \right) \\ &= \frac{1}{\delta \varphi(n)} \sum_{\chi \bmod n} \bar{\chi}(k) \ln L(s, \chi) + \sum_{m=2}^{\infty} \frac{1}{m \delta^m} \sum_{p \equiv k \pmod{n}} p^{-ms} \\ &\quad - \sum_{m=2}^{\infty} \frac{1}{m \delta} \sum_{p^m \equiv k \pmod{n}} p^{-ms}. \end{aligned}$$

ЛЕММА 6. При $\operatorname{Re} s > 2$ справедливы равенства

$$\begin{aligned} F_n(s) &= (\zeta(s-1))^{\gamma(n)} \prod_{\substack{\chi \bmod n \\ \chi \neq \chi_0}} (L(s-1, \chi))^{\gamma(n; \chi)} f(s), \\ G_n(s) &= (\zeta(s-1))^{\gamma(n)} \prod_{\substack{\chi \bmod n \\ \chi \neq \chi_0}} (L(s-1, \chi))^{\gamma(n; \chi)} g(s), \end{aligned}$$

где величины $\gamma(n)$, $\gamma(n; \chi)$ определены в (5), функции $f(s)$ и $g(s)$ аналитичны в полуплоскости $\operatorname{Re} s > 3/2$ и удовлетворяют в полосе $3/2 < \operatorname{Re} s = \sigma \leq 5/2$ неравенствам

$$|f(s)| < e^4 \tau^2(n) \left(\sigma - \frac{3}{2} \right)^{-2}, \quad |g(s)| < e^8 \tau^2(n) \left(\sigma - \frac{3}{2} \right)^{-7}.$$

ДОКАЗАТЕЛЬСТВО. Обозначим через $f_1(s)$, $g_1(s)$, $f_2(s)$, $g_2(s)$ произведения

$$\prod_{p^a \parallel n, a > 0} F_{n,p}(s), \quad \prod_{p^a \parallel n, a > 0} G_{n,p}(s), \quad \prod_{p \nmid n} f_{n,p}(s), \quad \prod_{p \nmid n} g_{n,p}(s)$$

соответственно. Разбивая множество простых чисел, не делящих n , на $\varphi(n)$ арифметических прогрессий вида $p \equiv k \pmod{n}$, $(k, n) = 1$, получим

$$F_n(s) = f_1(s) f_2(s) H(s), \quad G_n(s) = g_1(s) g_2(s) H(s),$$

где

$$H(s) = \prod_{p \nmid n} \left(1 - \frac{1}{\delta_p p^{s-1}} \right) = \prod_{\substack{k=1 \\ (k,n)=1}}^n \prod_{p \equiv k \pmod{n}} \left(1 - \frac{1}{(n, k-1) p^{s-1}} \right)^{-1}.$$

Функция $H(s)$ с помощью леммы 5 преобразуется к виду

$$\prod_{\substack{k=1 \\ (k,n)=1}}^n \prod_{\chi \bmod n} (L(s-1, \chi))^{\frac{\overline{\chi}(k)}{\varphi(n)(n, k-1)}} h(s),$$

где

$$h(s) = \exp \left\{ \sum_{\substack{k=1 \\ (k,n)=1}}^n \sum_{m=2}^{\infty} \left(\frac{(n, k-1)^{-m}}{m} \sum_{p \equiv k \pmod{n}} p^{-m(s-1)} - \frac{(n, k-1)^{-1}}{m} \sum_{p^m \equiv k \pmod{n}} p^{-m(s-1)} \right) \right\}.$$

Замечая теперь, что

$$L(s, \chi_0) = \zeta(s) \prod_{p|n} (1 - p^{-s}),$$

получим равенства из условия леммы, в которых

$$f(s) = \left(\prod_{p|n} (1 - p^{-(s-1)}) \right)^{\gamma(n)} f_1(s) f_2(s) h(s),$$

$$g(s) = \left(\prod_{p|n} (1 - p^{-(s-1)}) \right)^{\gamma(n)} g_1(s) g_2(s) h(s).$$

Нетрудно видеть, что бесконечные ряды в выражении для $h(s)$, а также бесконечные произведения $f_2(s)$ и $g_2(s)$ сходятся абсолютно в полуплоскости

$\operatorname{Re} s > 3/2$. Следовательно, функции $f(s)$ и $g(s)$ аналитичны в этой области. Оценим теперь их абсолютные значения в полосе $3/2 < \operatorname{Re} s = \sigma \leq 5/2$. Прежде всего, из очевидных неравенств $0 < \gamma(n) < 1$ заключаем, что

$$\left| \prod_{p|n} (1 - p^{1-s})^{\gamma(n)} \right| < \prod_{p|n} \left(1 + \frac{1}{\sqrt{p}} \right) < 2^{\nu(n)} \leq \tau(n).$$

Далее,

$$\begin{aligned} |h(s)| &\leq \exp \left\{ \sum_{\substack{k=1 \\ (k,n)=1}}^n \sum_{m=2}^{\infty} \left(\frac{(n, k-1)^{-m}}{m} \sum_{p \equiv k \pmod{n}} p^{-m(\sigma-1)} \right. \right. \\ &\quad \left. \left. + \frac{(n, k-1)^{-1}}{m} \sum_{p^m \equiv k \pmod{n}} p^{-m(\sigma-1)} \right) \right\} \\ &\leq \exp \left\{ 2 \sum_{m=2}^{\infty} \frac{1}{m} \sum_p p^{-m(\sigma-1)} \right\} \\ &= \exp \left\{ 2 \sum_{\mu=1}^{\infty} \frac{1}{2\mu} \sum_p p^{-2\mu(\sigma-1)} + 2 \sum_{\mu=1}^{\infty} \frac{1}{2\mu+1} \sum_p p^{-(2\mu+1)(\sigma-1)} \right\} \\ &\leq \exp \left\{ - \sum_p \ln(1 - p^{-2(\sigma-1)}) + \frac{2}{3} \sum_p \sum_{\mu=1}^{\infty} p^{-(2\mu+1)/2} \right\} \\ &< \exp \{ \ln \zeta(2\sigma - 2) + 2 \} = e^2 \zeta(2\sigma - 2) < \frac{3}{2} e^2 \left(\sigma - \frac{3}{2} \right)^{-1}. \end{aligned}$$

Оценим теперь сомножители произведений $f_1(s)$ и $g_1(s)$. Пусть $p^a \| n$, $a \geq 1$. В случае $p = 2$ будем иметь

$$\begin{aligned} \left| 1 + \frac{2^{-(a+1)s}}{2^s - 2} \right| &\leq 1 + \frac{1}{2^{2\sigma}(2\sigma - 2)} \leq 1 + \frac{1}{8(2\sqrt{2} - 2)} = \frac{\sqrt{2} + 17}{16}, \\ |F_{n,p}(s)| &= \left| 1 + \frac{1}{2^s - 1} \left(1 + \frac{2^{-(a+1)s}}{2^s - 2} \right) \right| \leq 1 + \frac{1}{2^\sigma - 1} \frac{\sqrt{2} + 17}{16} < 2, \\ |G_{n,p}(s)| &= \left| 1 + \frac{1}{2^s - 1} \left(1 + \frac{1}{1 - 2^{-ns}} \left(1 + \frac{2^{-(a+1)s}}{2^s - 2} \right) \right) \right| \\ &\leq 1 + \frac{1}{2\sqrt{2} - 1} \left(1 + \frac{1}{1 - \frac{1}{8}} \frac{\sqrt{2} + 17}{16} \right) < 2.3. \end{aligned}$$

Далее, при $p \geq 3$ получаем

$$\begin{aligned} \left| \frac{p-1}{p^{as}(p^s - p)} \right| &< \frac{p}{p^\sigma(p^\sigma - p)} \leq \frac{1}{p(p - \sqrt{p})} \leq \frac{3 + \sqrt{3}}{18}, \\ |F_{n,p}(s)| &= \left| 1 + \frac{1}{\delta_p} \frac{p-1}{p^s - p} \left(1 + \frac{p-1}{p^{as}(p^s - p)} \right) \right| \leq 1 + \frac{p}{p\sqrt{p} - 1} \left(1 + \frac{3 + \sqrt{3}}{18} \right) \\ &\leq 1 + \frac{3}{3\sqrt{3} - 1} \frac{21 + \sqrt{3}}{18} < 2, \end{aligned}$$

$$\begin{aligned}
|G_{n,p}(s)| &= \left| 1 + \frac{1}{(p^s - 1)(1 - p^{-ns})} \left(\frac{p-1}{\delta_p} + 1 - \frac{1}{p^{ns}} + \frac{p-1}{\delta_p} \frac{p-1}{p^{as}(p^s - p)} \right) \right| \\
&\leq 1 + \frac{1}{(p\sqrt{p} - 1)(1 - p^{-3})} \left(p + \frac{1}{p^3} + p \frac{3 + \sqrt{3}}{18} \right) \\
&\leq 1 + \frac{1}{(\sqrt{p} - p^{-1})(1 - p^{-3})} \left(1 + \frac{1}{p^4} + \frac{3 + \sqrt{3}}{18} \right) \\
&\leq 1 + \frac{\frac{21 + \sqrt{3}}{18} + \frac{1}{81}}{(\sqrt{3} - \frac{1}{3})(1 - \frac{1}{27})} < 2.
\end{aligned}$$

Таким образом, всюду в полуплоскости $\operatorname{Re} s > 3/2$ справедливы неравенства

$$|f_1(s)| \leq \prod_{p^a \| n} 2 \leq 2^{\nu(n)} \leq \tau(n), \quad |g_1(s)| \leq 2.3 \prod_{p^a \| n, p > 2} 2 \leq 2.3\tau(n).$$

Переходя к произведениям $f_2(s)$ и $g_2(s)$, находим

$$|f_{n,p}(s)| = \left| 1 - \frac{1}{\delta_p p^s} \left(1 - \frac{\delta_p - 1}{\delta_p} \frac{p-1}{p^{s-1} - 1} \right) \right| \leq 1 + \frac{1}{\delta_p p^\sigma} \left(1 + \frac{\delta_p - 1}{\delta_p} \frac{p-1}{p^{\sigma-1} - 1} \right).$$

В случае $\delta_p = 1$, очевидно, имеем

$$|f_{n,p}(s)| \leq 1 + \frac{1}{p^\sigma} < 1 + p^{-(\sigma-0.5)} < (1 - p^{-(\sigma-0.5)})^{-1}.$$

Если $\delta_p \geq 2$, то

$$|f_{n,p}(s)| \leq 1 + \frac{1}{2p^\sigma} \left(1 + \frac{p-1}{p^{\sigma-1} - 1} \right).$$

При $2 \leq \sigma \leq 5/2$ последнее выражение не превосходит величины

$$1 + \frac{1}{2p^\sigma} \left(1 + \frac{p-1}{p-1} \right) = 1 + \frac{1}{p^\sigma} < (1 - p^{-(\sigma-0.5)})^{-1},$$

а при $3/2 < \sigma \leq 2$ — величины

$$1 + \frac{1}{2p^\sigma} \left(1 + \frac{p-1}{\sqrt{p}-1} \right) = 1 + \left(\frac{1}{2} + \frac{1}{\sqrt{p}} \right) p^{-(\sigma-0.5)}.$$

Таким образом,

$$|f_{n,p}(s)| \leq \begin{cases} \left(\frac{1}{2} + \frac{1}{\sqrt{p}} \right) (1 - p^{-(\sigma-0.5)})^{-1}, & \text{если } p = 2, 3, \\ (1 - p^{-(\sigma-0.5)})^{-1}, & \text{если } p \geq 5, \end{cases}$$

и, следовательно,

$$|f_2(s)| \leq \left(\frac{1}{2} + \frac{1}{\sqrt{2}} \right) \left(\frac{1}{2} + \frac{1}{\sqrt{3}} \right) \prod_p (1 - p^{-(\sigma-0.5)})^{-1} < \frac{3}{2} \zeta \left(\sigma - \frac{1}{2} \right) < 3 \left(\sigma - \frac{3}{2} \right)^{-1}.$$

Наконец,

$$|g_{n,p}(s)| \leq |f_{n,p}(s)| + |h_{n,p}(s)|,$$

где

$$\begin{aligned}
 |h_{n,p}(s)| &= \left| \left(1 - \frac{1}{\delta_p p^{s-1}} \right) \left(\frac{1}{p^s - 1} + \frac{p-1}{\delta_p (p^s - p)(p^{ns} - 1)} \right) \right| \\
 &\leq \left(1 + \frac{1}{\sqrt{p}} \right) \left(\frac{1}{1 + p^{-\sigma}} + \frac{p-1}{p^{2\sigma} - 1} \frac{1}{1 - p^{1-\sigma}} \right) \frac{1}{p^\sigma} \\
 &\leq \left(1 + \frac{1}{\sqrt{p}} \right) \left(\frac{1}{1 - \frac{1}{p\sqrt{p}}} + \frac{p-1}{p^3 - 1} \frac{1}{1 - \frac{1}{\sqrt{p}}} \right) \frac{1}{p^\sigma} \\
 &< \frac{1 + \frac{1}{\sqrt{p}}}{1 - \frac{1}{\sqrt{p}}} \left(1 + \frac{1}{p^2 + p + 1} \right) \frac{1}{p^\sigma} < \frac{8}{7} (3 + 2\sqrt{2}) \frac{1}{p^\sigma},
 \end{aligned}$$

так что

$$\begin{aligned}
 |g_{n,p}(s)| &\leq 1 + \left(\frac{1}{2} + \frac{1}{\sqrt{p}} + \frac{8}{7} \frac{3 + 2\sqrt{2}}{\sqrt{p}} \right) p^{-(\sigma-0.5)} \\
 &< 1 + 6p^{-(\sigma-0.5)} < (1 - p^{-(\sigma-0.5)})^{-6}, \\
 |g_2(s)| &< \prod_p (1 - p^{-(\sigma-0.5)})^{-6} = \zeta^6 \left(\sigma - \frac{1}{2} \right) < 64 \left(\sigma - \frac{3}{2} \right)^{-6}.
 \end{aligned}$$

Собирая полученные оценки вместе, находим

$$\begin{aligned}
 |f(s)| &\leq \tau(n) \frac{3}{2} e^2 \left(\sigma - \frac{3}{2} \right)^{-1} \tau(n) 3 \left(\sigma - \frac{3}{2} \right)^{-1} < e^4 \tau^2(n) \left(\sigma - \frac{3}{2} \right)^{-2}, \\
 |g(s)| &\leq \tau(n) \frac{3}{2} e^2 \left(\sigma - \frac{3}{2} \right)^{-1} 2.3 \tau(n) 64 \left(\sigma - \frac{3}{2} \right)^{-6} < e^8 \tau^2(n) \left(\sigma - \frac{3}{2} \right)^{-7}.
 \end{aligned}$$

ЛЕММА 7. Пусть p – простое число, k, r, s – целые числа, причем $k \geq 1$, $0 \leq r \leq k-1$, $1 \leq s < p^{k-r}$, $(s, p) = 1$. Тогда биномиальный коэффициент $\binom{p^k}{sp^r}$ делится на p^{k-r} .

ДОКАЗАТЕЛЬСТВО. Пусть α_1, α_2 , и α_3 – показатели, с которыми p входит в разложение чисел $(p^k)!$, $(sp^r)!$ и $(p^k - sp^r)!$. Определяя целое число ν из условий $p^{\nu-1} < s < p^\nu$, будем иметь

$$\begin{aligned}
 \alpha_1 &= p^{k-1} + p^{k-2} + \dots + p + 1, \\
 \alpha_2 &= \sum_{t \geq 1} \left[\frac{sp^r}{p^t} \right] = s(p^{r-1} + p^{r-2} + \dots + p + 1) + \sum_{t=1}^{\nu-1} [sp^{-t}], \\
 \alpha_3 &= \sum_{t \geq 1} \left[\frac{p^k - sp^r}{p^t} \right] = (p^{k-1} - sp^{r-1}) + \dots + (p^{k-r} - s) + \sum_{t=1}^{k-r-1} [p^{k-r-t} - sp^{-t}] \\
 &= (p^{k-1} + \dots + p^{k-r}) - s(p^{r-1} + p^{r-2} + \dots + 1) \\
 &\quad + \sum_{t=1}^{k-r-1} [p^{k-r-t} - [sp^{-t}] - \{sp^{-t}\}].
 \end{aligned}$$

Пользуясь тем, что все дробные доли $\{sp^{-t}\}$ отличны от нуля, заключаем, что последняя сумма имеет вид

$$\sum_{t=1}^{k-r-1} (p^{k-r-t} - [sp^{-t}] - 1) = p^{k-r-1} + \dots + p + 1 - \sum_{t=1}^{k-r-1} [sp^{-t}] - (k-r-1).$$

Поскольку $\nu \leq k-r$ и при $t \geq \nu$ величины $[sp^{-t}]$ тождественно равны нулю, окончательно находим

$$\alpha_3 = (p^{k-1} + \dots + p + 1) - s(p^{r-1} + \dots + p + 1) - \sum_{t=1}^{\nu-1} [sp^{-t}] - (k-r).$$

Следовательно, показатель, с которым p входит в каноническое разложение биномиального коэффициента, имеет вид

$$\begin{aligned} \alpha_1 - (\alpha_2 + \alpha_3) &= (p^{k-1} + \dots + p + 1) - s(p^{r-1} + \dots + p + 1) - \sum_{t=1}^{\nu-1} [sp^{-t}] \\ &\quad - (p^{k-1} + \dots + p + 1) + s(p^{r-1} + \dots + p + 1) + \sum_{t=1}^{\nu-1} [sp^{-t}] + k - r = k - r. \end{aligned}$$

ЛЕММА 8. Пусть p – простое, x – целое числа. Тогда для произвольных натуральных чисел α, β выполняется сравнение

$$(1 + xp^\alpha)^{p^\beta} \equiv 1 \pmod{p^{\alpha+\beta}}.$$

ДОКАЗАТЕЛЬСТВО. Пусть k – произвольное число с условием $1 \leq k \leq p^\beta$, и пусть $k = sp^\gamma$, где $(s, p) = 1$, $0 \leq \gamma \leq \beta$. Согласно лемме 7 произведение $p^{k\alpha} \binom{p^\beta}{k}$ делится на p^δ , где $\delta = k\alpha + \beta - \gamma$. Учитывая теперь, что

$$\delta = (\alpha + \beta) + (sp^\gamma - 1)\alpha - \gamma \geq (\alpha + \beta) + p^\gamma - \gamma - 1 \geq \alpha + \beta,$$

находим

$$\begin{aligned} p^{k\alpha} \binom{p^\beta}{k} &\equiv 0 \pmod{p^{\alpha+\beta}}, \\ (1 + xp^\alpha)^{p^\beta} &\equiv 1 + \sum_{k=1}^{p^\beta} x^k p^{k\alpha} \binom{p^\beta}{k} \equiv 1 \pmod{p^{\alpha+\beta}}. \end{aligned}$$

ЛЕММА 9. Пусть p – простое число, a, α, β – целые числа, $(a, p) = 1$, $\alpha \geq 1$, $\beta \geq 1$, $q = p^{\alpha+\beta}$, и пусть χ – произвольный характер по модулю q . Тогда сумма

$$S = \sum_{x=1}^{p^\beta} \chi(ap^\alpha x + 1)$$

равна одному из чисел 0 или p^β .

ДОКАЗАТЕЛЬСТВО. Если χ – главный характер, то утверждение леммы очевидно. Поэтому далее считаем $\chi \neq \chi_0$. Пусть $p \geq 3$, g – первообразный корень по модулю q , и пусть при $(n, p) = 1$

$$\chi(n) = \chi_c(n) = \exp\left\{2\pi i \frac{c\gamma}{\varphi(q)}\right\},$$

где γ – индекс n по основанию g , а c – некоторое число с условием $1 \leq c \leq \varphi(q)$. Согласно лемме 8 каждое из чисел $ap^\alpha x + 1$, $x = 1, \dots, p^\beta$, удовлетворяет сравнению

$$(ap^\alpha x + 1)^{p^\beta} \equiv 1 \pmod{p^{\alpha+\beta}}.$$

Значит, индексы $\gamma = \gamma(x)$ этих чисел удовлетворяют сравнению

$$\gamma p^\beta \equiv 0 \pmod{p^{\alpha+\beta-1}(p-1)}$$

и, следовательно, делятся на $p^{\alpha-1}(p-1)$. Однако среди индексов γ по модулю q , образующих полную систему вычетов по модулю $\varphi(q) = p^{\alpha+\beta-1}(p-1)$, кратными $p^{\alpha-1}(p-1)$ будут числа $tp^{\alpha-1}(p-1)$, $t = 1, 2, \dots, p^\beta$, и только они. Следовательно,

$$S = \sum_{x=1}^{p^\beta} \exp\left\{2\pi i \frac{c\gamma(x)}{\varphi(q)}\right\} = \sum_{t=1}^{p^\beta} \exp\left\{2\pi i \frac{ctp^{\alpha-1}(p-1)}{p^{\alpha+\beta-1}(p-1)}\right\} = \sum_{t=1}^{p^\beta} \exp\left\{2\pi i \frac{ct}{p^\beta}\right\}.$$

Последняя сумма равна p^β либо 0 в зависимости от того, делится ли число c на p^β или не делится.

Пусть теперь $p = 2$. Если $\alpha = 1$, то исходная сумма, очевидно, имеет вид

$$\sum_{x=1}^{q/2} \chi(2x+1) = \sum_{x=1}^q \chi(x) = 0.$$

В случае $\alpha \geq 2$ для нечетного n имеем

$$\chi(n) = \chi_{c_0, c}(n) = (-1)^{c_0 \gamma_0} \exp\left\{2\pi i \frac{c\gamma}{2^{\alpha+\beta-2}}\right\},$$

где γ_0 , γ – система индексов числа n по модулю $2^{\alpha+\beta}$ (так что $n \equiv (-1)^{\gamma_0} 5^\gamma$), а c_0 , c – некоторые целые числа соответственно с условием $0 \leq c_0 \leq 1$, $1 \leq c \leq 2^{\alpha+\beta-2}$. Пользуясь леммой 8, несложно заключить, что $\gamma = \gamma(x)$ принимает значения из множества чисел вида $t \cdot 2^{\alpha-2}$, $t = 1, 2, \dots, 2^\beta$, когда x пробегает последовательность $1, 2, \dots, 2^\beta$. Далее, при $\alpha \geq 2$ числа $2^\alpha ax + 1$ сравнимы с единицей по модулю 4. Поскольку с единицей по модулю 4 сравнимы лишь числа $(-1)^{05^\gamma}$, $\gamma = 1, 2, \dots, 2^{\alpha+\beta-2}$, то из сказанного следует, что системы индексов чисел $2^\alpha ax + 1$, $x = 1, 2, \dots, 2^\beta$, образуют множество пар $(0, t \cdot 2^{\alpha-2})$, $t = 1, 2, \dots, 2^\beta$. Следовательно,

$$S = \sum_{t=1}^{2^\beta} (-1)^{c_0 \cdot 0} \exp\left\{2\pi i \frac{ct \cdot 2^{\alpha-2}}{2^{\alpha+\beta-2}}\right\} = \sum_{t=1}^{2^\beta} \exp\left\{2\pi i \frac{ct}{2^\beta}\right\},$$

откуда следует утверждение леммы.

ЛЕММА 10. Если $n = ab$, где $(a, b) = 1$, $a > 1$, $b > 1$, χ – характер по модулю n , $\chi = \chi_1 \chi_2$, где χ_1 и χ_2 – характеры по модулю a и b соответственно, то

$$\gamma(n; \chi) = \gamma(a; \chi_1) \gamma(b; \chi_2).$$

ДОКАЗАТЕЛЬСТВО. Поскольку при любом $r \geq 0$ справедливо равенство $(r, n) = (r, a)(r, b)$, то

$$\gamma(n; \chi) = \sum_{\substack{k=1 \\ (k, n)=1}}^n \frac{\bar{\chi}_1(k) \bar{\chi}_2(k)}{(k-1, a)(k-1, b)}.$$

Далее, представляя k в виде $k = ak_2 + bk_1$, где k_1 и k_2 пробегает приведенные системы вычетов по модулям a и b соответственно, будем иметь

$$\begin{aligned} \gamma(n; \chi) &= \sum_{\substack{k_1=1 \\ (k_1, a)=1}}^a \sum_{\substack{k_2=1 \\ (k_2, b)=1}}^b \frac{\bar{\chi}_1(ak_2 + bk_1) \bar{\chi}_2(ak_2 + bk_1)}{(ak_2 + bk_1 - 1, a)(ak_2 + bk_1 - 1, b)} \\ &= \sum_{\substack{k_1=1 \\ (k_1, a)=1}}^a \sum_{\substack{k_2=1 \\ (k_2, b)=1}}^b \frac{\bar{\chi}_1(bk_1) \bar{\chi}_2(ak_2)}{(bk_1 - 1, a)(ak_2 - 1, b)} \\ &= \sum_{\substack{k_1=1 \\ (k_1, a)=1}}^a \sum_{\substack{k_2=1 \\ (k_2, b)=1}}^b \frac{\bar{\chi}_1(k_1) \bar{\chi}_2(k_2)}{(k_1 - 1, a)(k_2 - 1, b)} = \gamma(a; \chi_1) \gamma(b; \chi_2). \end{aligned}$$

СЛЕДСТВИЕ 1. Если положить $\gamma(1) = 1$, то функция $\gamma(n)$ мультипликативна по n .

ЛЕММА 11. Для любого комплексного характера χ по модулю n величина $\gamma(n; \chi)$ есть вещественное число.

ДОКАЗАТЕЛЬСТВО. В силу леммы 10 утверждение достаточно проверить для случая, когда n есть степень простого числа. Группируя вместе слагаемые, отвечающие одному и тому же значению $\delta = (k-1, n)$, получим

$$\gamma(n; \chi) = \sum_{\delta|n} \frac{1}{\delta} \bar{S}_\delta, \quad S_\delta = \sum_{\substack{k=1 \\ (k, n)=1, (k-1, n)=\delta}}^n \chi(k).$$

Пользуясь известным свойством функции Мёбиуса, будем иметь

$$\begin{aligned} S_\delta &= \sum_{\substack{k=1 \\ (k+1, n)=1, (k, n)=\delta}}^n \chi(k+1) = \sum_{\substack{k=1 \\ (k, n)=\delta}}^n \chi(k+1) = \sum_{\substack{s=1 \\ k=s\delta, (s, n/\delta)=1}}^{n/\delta} \chi(k+1) \\ &= \sum_{s=1}^{n/\delta} \chi(s\delta + 1) \sum_{d|(s, n/\delta)} \mu(d) = \sum_{d|(n/\delta)} \mu(d) \sum_{\substack{s=1 \\ s \equiv 0 \pmod{d}}}^{n/\delta} \chi(s\delta + 1) \\ &= \sum_{d|(n/\delta)} \mu(d) \sum_{x=1}^{n/(d\delta)} \chi(xd\delta + 1). \end{aligned}$$

Согласно лемме 9 каждая из внутренних сумм есть вещественное число. Таким образом, каждая из сумм S_δ , а вместе с ними и каждая из величин $\gamma(n; \chi)$ будет вещественным числом.

ЛЕММА 12. Пусть χ пробегает неглавные характеры по модулю n . Тогда существуют положительные постоянные c_1 и c_2 , зависящие от n и такие, что в области

$$\operatorname{Re} s \geq 1 - \frac{c_1}{\ln(|t| + 2)}$$

для каждой из функций $L(s, \chi)$ справедливы оценки

$$|L(s, \chi)| \leq c_2 \ln(|t| + 2), \quad |L(s, \chi)|^{-1} \leq c_2 \ln(|t| + 2).$$

При этом постоянную c_1 можно считать настолько малой, а постоянную c_2 – настолько большой, что в области

$$\operatorname{Re} s \geq 1 - \frac{c_1}{\ln(|t| + 2)}, \quad |t| \geq \frac{1}{2},$$

будет выполняться также оценка $|\zeta(s)| \leq c_2 \ln(|t| + 2)$.

ДОКАЗАТЕЛЬСТВО. Выберем абсолютные постоянные κ_1 и κ_2 так, чтобы ни одна из функций $L(s, \chi)$ не имела нулей в области

$$\operatorname{Re} s > 1 - \frac{\kappa_1}{\ln(n(|t| + 2))}, \quad -\infty < t < +\infty, \quad (12)$$

если χ – комплексный характер, или в области

$$\operatorname{Re} s > 1 - \frac{\kappa_1}{\ln(n(|t| + 2))}, \quad t \neq 0, \quad s > 1 - \frac{\kappa_2}{\sqrt{n} \ln^4 n}, \quad t = 0, \quad (13)$$

если χ – вещественный характер (см., например, [10, с. 139–145]). Полагая

$$\kappa_3 = \frac{\min(\kappa_1, \kappa_2)}{3\sqrt{n} \ln^4 n},$$

несложно убедиться в том, что ни одна из функций $L(s, \chi)$ не обращается в нуль в области

$$\operatorname{Re} s > 1 - \frac{\kappa_3}{\ln(|t| + 2)}.$$

Повторяя рассуждения, с помощью которых доказываются леммы 1, 3 из книги [11, гл. 3, п. 9], можно доказать существование постоянных κ_4 и κ_5 , $0 < \kappa_4 \leq \kappa_3/2$, зависящих от n и таких, что в области

$$\operatorname{Re} s > 1 - \frac{\kappa_4}{\ln(|t| + 2)}$$

справедливы неравенства

$$|L(s, \chi)| \leq \kappa_5 \ln(|t| + 2), \quad \left| \frac{L'(s, \chi)}{L(s, \chi)} \right| \leq \kappa_5 \ln(|t| + 2).$$

Используя последнюю оценку и рассуждения из [11, гл. 3, п. 11], заключаем, что в области

$$\operatorname{Re} s > 1 - \frac{\kappa_6}{\ln(|t| + 2)},$$

где $0 < \kappa_6 \leq \kappa_4/4$, имеет место оценка $|L(s, \chi)|^{-1} \leq \kappa_7 \ln(|t| + 2)$. Наконец, в некоторой области

$$\operatorname{Re} s \geq 1 - \frac{\kappa_8}{\ln(|t| + 2)}, \quad |t| \geq \frac{1}{2},$$

дзета-функция удовлетворяет неравенству $|\zeta(s)| \leq \kappa_9 \ln(|t| + 2)$, где κ_8 и κ_9 – абсолютные постоянные (см., например, [10, с. 72]). Полагая теперь $c_1 = \min(\kappa_6, \kappa_8)$, $c_2 = \min(\kappa_5, \kappa_7, \kappa_9)$, получим утверждение леммы.

ЛЕММА 13. *Определим функции $u(s)$ и $v(s)$ соотношениями*

$$u(s) = (s-1)\zeta(s), \quad v(s) = (u(s))^{\gamma(n)} = e^{\gamma(n) \ln u(s)},$$

причем в последнем равенстве возьмем ту ветвь функции $\ln z$, что принимает положительные значения при $z > 1$. Тогда $u(s)$ и $v(s)$ аналитичны в круге $|s-1| \leq 1$ и всюду в этом круге справедливы оценки

$$|u(s)| < 6, \quad |v(s)| < 6, \quad |\zeta(s)| < 6|s-1|^{-1}.$$

ДОКАЗАТЕЛЬСТВО. Полагая $s = 1 + (3/2)e^{i\varphi}$ в равенстве

$$u(s) = (s+1) \left(\frac{1}{2} + s(s-1) \int_1^\infty \frac{\sigma(x)}{x^{s+2}} dx \right), \quad \sigma(x) = \int_0^x \left(\frac{1}{2} - \{y\} \right) dy,$$

и учитывая оценку $0 \leq \sigma(u) \leq 1/8$, будем иметь

$$|u(s)| < \frac{7}{2} \left(\frac{1}{2} + \frac{15}{4} \int_1^\infty \frac{dx}{8x^{3/2}} \right) < 6.$$

Поскольку $u(s)$ – целая функция, последнее неравенство остается справедливым и в круге $|s-1| \leq 1$. Следовательно,

$$|\zeta(s)| = |u(s)| |s-1|^{-1} < 6|s-1|^{-1}.$$

Далее, из свойств $\zeta(s)$ следует, что $u(s)$ не имеет нулей в круге $|s-1| \leq 1$. Поэтому функция $v(s)$ аналитична в этом круге и удовлетворяет в нем неравенствам

$$|v(s)| \leq |u(s)|^{\gamma(n)} < 6^{\gamma(n)} < 6.$$

ЛЕММА 14. *Определим функции $\alpha(s)$, $\beta(s)$, $A(s)$ и $B(s)$ соотношениями*

$$\begin{aligned} F_n(s) &= (\zeta(s-1))^{\gamma(n)} \alpha(s), & G_n(s) &= (\zeta(s-1))^{\gamma(n)} \beta(s), \\ A(s) &= \frac{v(s-1)}{s} \alpha(s), & B(s) &= \frac{v(s-1)}{s} \beta(s), \end{aligned}$$

где $v(s)$ – функция из условия леммы 13. Пусть, далее, $T_0 = T_0(n)$ настолько велико, что при $T \geq T_0$ справедливо неравенство $\delta = c_1(\ln T)^{-1}/2 < 1/4$, где c_1 – постоянная леммы 12. Тогда:

1) функции $F_n(s)$ и $G_n(s)$ аналитически продолжаются в область

$$2 - \delta \leq \operatorname{Re} s \leq 2 + \frac{1}{4}, \quad |\operatorname{Im} s| \leq T; \quad (14)$$

2) всюду в прямоугольнике (14) выполняются оценки

$$|\alpha(s)| < (\ln T)^{n-1}, \quad |\beta(s)| < (\ln T)^{n-1};$$

3) в окрестности точки $s = 2$ имеют место разложения

$$A(s) = \sum_{m=0}^{\infty} A_m(s-2)^m, \quad B(s) = \sum_{m=0}^{\infty} B_m(s-2)^m, \quad (15)$$

где $A_0 = \alpha(2)/2$, $B_0 = \beta(2)/2$, и при $m \geq 1$ выполняются неравенства $|A_m|, |B_m| \leq cr^{-m}$, c и r – некоторые положительные постоянные, зависящие лишь от n ; оба ряда (15) сходятся абсолютно и равномерно в круге $|s-2| \leq r/2$, и всюду в этом круге разность между каждой из функций $A(s)$, $B(s)$ и суммой первых N слагаемых соответствующего ряда не превосходит по модулю $2c|(s-2)/r|^N$.

ДОКАЗАТЕЛЬСТВО. Согласно лемме 12 ни одна из функций $L(s, \chi)$ не имеет нулей в области (14). Следовательно, $F_n(s)$ и $G_n(s)$ аналитически продолжают-ся в эту область с помощью формул леммы 6. Пользуясь тем, что числа $\gamma(n; \chi)$ вещественные, из неравенств $|\gamma(n; \chi)| \leq \gamma(n) < 1$ и леммы 12 заключаем, что

$$\begin{aligned} \left| \prod_{\substack{\chi \bmod n \\ \chi \neq \chi_0}} (L(s-1, \chi))^{\gamma(n; \chi)} \right| &\leq \prod_{\substack{\chi \bmod n \\ \chi \neq \chi_0}} |L(s-1, \chi)|^{\gamma(n; \chi)} \leq \prod_{\substack{\chi \bmod n \\ \chi \neq \chi_0}} (2c_2 \ln T)^{\gamma(n)} \\ &= (2c_2 \ln T)^{\gamma(n)(\varphi(n)-1)} < (2c_2 \ln T)^{n-2}. \end{aligned}$$

Отсюда и из леммы 6 получаем оценки

$$\begin{aligned} |\alpha(s)| &\leq (2c_2 \ln T)^{n-2} e^4 \tau^2(n) \left(\frac{7}{4} - \frac{3}{2} \right)^{-2} < (\ln T)^{n-1}, \\ |\beta(s)| &\leq (2c_2 \ln T)^{n-2} e^8 \tau^2(n) \left(\frac{7}{4} - \frac{3}{2} \right)^{-7} < (\ln T)^{n-1}. \end{aligned}$$

Пусть абсолютные постоянные κ_1 и κ_2 таковы, что ни одна из функций $L(s, \chi)$ не имеет нулей в области (12), если χ – комплексный характер, либо в области (13), если χ – вещественный характер. Положим

$$r = r(n) = \frac{1}{2} \min \left(\frac{\kappa_1}{\ln 3n}, \frac{\kappa_2}{\sqrt{n} \ln^4 n}, \frac{1}{2} \right).$$

Поскольку круг $|s-1| \leq r$ лежит в области, свободной от нулей функций $L(s, \chi)$, можно подобрать постоянную $\kappa_1 > 1$, зависящую лишь от n и такую, что каждая из функций $L(s, \chi)$ удовлетворяет в круге $|s-1| \leq r$ неравенствам $\kappa_1^{-1} < |L(s, \chi)| < \kappa_1$. Следовательно, для таких s будут справедливы и оценки

$$\begin{aligned} \left| \prod_{\substack{\chi \bmod n \\ \chi \neq \chi_0}} (L(s-1, \chi))^{\gamma(n; \chi)} \right| &\leq \prod_{\substack{\chi \bmod n \\ \chi \neq \chi_0}} |L(s-1, \chi)|^{\gamma(n; \chi)} \leq \prod_{\substack{\chi \bmod n \\ \chi \neq \chi_0}} \kappa_1^{\gamma(n)} \\ &= \kappa_1^{\gamma(n)(\varphi(n)-1)} = \kappa_2, \\ |\beta(s)| &\leq \kappa_2 e^8 \tau^2(n) \left(\frac{7}{4} - \frac{3}{2} \right)^{-7} = \kappa_3, \quad |\alpha(s)| \leq \kappa_2 e^4 \tau^2(n) \left(\frac{7}{4} - \frac{3}{2} \right)^{-2} < \kappa_3. \end{aligned}$$

Кроме того, функции $A(s)$ и $B(s)$ аналитичны в круге $|s - 2| \leq r$ и разлагаются в ряды Тейлора по степеням $(s - 2)$, причем первые коэффициенты таких разложений соответственно имеют вид

$$A_0 = \frac{1}{2} v(1)\alpha(2) = \frac{1}{2} \alpha(2), \quad B_0 = \frac{1}{2} v(1)\beta(2) = \frac{1}{2} \beta(2).$$

Из формулы Коши для коэффициентов A_m , B_m , $m \geq 1$, этих разложений с помощью неравенств леммы 13 получаем оценки

$$|A_m| = \left| \frac{1}{2\pi i} \int_{|s-2|=r} \frac{v(s-1)\alpha(s)}{s(s-2)^{m+1}} ds \right| < \frac{1}{2\pi} \int_0^{2\pi} \frac{4 \cdot 6\kappa_3}{7r^m} d\varphi < 4\kappa_3 r^{-m},$$

$$|B_m| < 4\kappa_3 r^{-m}.$$

Следовательно, при любом s с условием $|s - 2| \leq r/2$ и любом $N \geq 0$ имеют место неравенства

$$\left| A(s) - \sum_{m=0}^{N-1} A_m(s-2)^m \right| \leq \sum_{m=N}^{\infty} |A_m| |s-2|^m < 4\kappa_3 \sum_{m=N}^{\infty} \left| \frac{s-2}{r} \right|^m$$

$$\leq 4\kappa_3 \left| \frac{s-2}{r} \right|^N \sum_{m=N}^{\infty} 2^{-m} = 8\kappa_3 \left| \frac{s-2}{r} \right|^N$$

(аналогично для $B(s)$). Для завершения доказательства остается положить $c = 4\kappa_3$.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 1. Пусть x – полуцелое число, $b = 2 + (\ln x)^{-1} < 2 + 1/4$, $2 \leq T \leq x^{c_1/2} < x$, где c_1 – постоянная из леммы 12. Будем предполагать число T настолько большим, чтобы величина $\delta = c_1(\ln T)^{-1}/4$ была меньше $r/2$, где $r = r(n)$ – постоянная из леммы 14. Положим, наконец, $a = 2 - \delta$.

Рассмотрим интеграл от функции $F_n(s)x^s/s$ по контуру Γ , проходимому против часовой стрелки и состоящему из отрезков, последовательно соединяющих точки $a - i \cdot 0$, $a - iT$, $b - iT$, $b + iT$, $a + iT$, $a + i \cdot 0$, а также из верхнего и нижнего краев разреза, проведенного от точки a до точки 2. В силу леммы 14 подынтегральная функция аналитична внутри Γ . Следовательно,

$$\frac{1}{2\pi i} \int_{b-iT}^{b+iT} F_n(s) \frac{x^s}{s} ds = - \sum_{k=1}^6 I_k, \quad (16)$$

где через I_1 , I_6 обозначены интегралы по верхней и нижней сторонам Γ , через I_3 , I_4 – интегралы по верхнему и нижнему краям разреза, а через I_2 и I_5 – интегралы по вертикальным отрезкам $[a + iT, a + i \cdot 0]$ и $[a - i \cdot 0, a - iT]$ соответственно.

Из известного равенства

$$\frac{1}{2\pi i} \int_{b-iT}^{b+iT} \frac{\alpha^s}{s} ds = \begin{cases} 1 + \theta \frac{\alpha^b}{T} (\ln \alpha)^{-1}, & \text{если } \alpha > 1, \\ \theta \frac{\alpha^b}{T} |\ln \alpha|^{-1}, & \text{если } 0 < \alpha < 1, \end{cases}$$

несложно заключить, что левая часть (16) имеет вид

$$\sum_{q=1}^{\infty} a_n(q) \frac{1}{2\pi i} \int_{b-iT}^{b+iT} \left(\frac{x}{q} \right)^s \frac{ds}{s} = \sum_{q \leq x} a_n(q) + \theta R(x),$$

где

$$\begin{aligned} R(x) &= \frac{x^2}{T} \sum_{q=1}^{\infty} q^{1-b} \left| \ln \frac{x}{q} \right|^{-1} \ll \frac{x^2}{T} \sum_{q=1}^{\infty} q^{1-b} + \frac{x^2}{T} \sum_{0.5x \leq q \leq 1.5x} \frac{x^{2-b}}{|q-x|} \\ &\ll \frac{x^2}{T} (\zeta(b-1) + \ln x) \ll \frac{x^2}{T} \ln x. \end{aligned}$$

Оценки интегралов I_1 , I_6 получаются с помощью лемм 12, 14, согласно которым

$$\begin{aligned} |I_1| &= \left| \int_{b+iT}^{a+iT} F_n(s) \frac{x^s}{s} ds \right| < \frac{x^b}{2\pi T} \int_a^b |F_n(\sigma + iT)| d\sigma \\ &\ll \frac{x^2}{T} \int_a^b |\zeta(\sigma - 1 + iT)|^{\gamma(n)} |\alpha(\sigma + iT)| d\sigma \ll \frac{x^2}{T} (\ln T)^{n-1+\gamma(n)} \ll \frac{x^2}{T} (\ln x)^n, \\ |I_6| &\ll \frac{x^2}{T} (\ln x)^n. \end{aligned}$$

Аналогично оцениваются интегралы I_2 и I_5 по вертикальным отрезкам. Отличие состоит лишь в том, что при $|t| \leq 1/2$ нужно воспользоваться неравенством из леммы 13, согласно которому

$$|\zeta(a-1+it)| = |\zeta(1-\delta+it)| < 6|\delta-it|^{-1} < 6\delta^{-1} = 24c_1^{-1} \ln(x^{c_1/2}) = 12 \ln x.$$

Таким образом, получим

$$\begin{aligned} |I_2| &= \left| \frac{1}{2\pi} \int_0^T (\zeta(a-1+it))^{\gamma(n)} \frac{\alpha(a+it)x^{a+it}}{a+it} dt \right| \\ &\ll x^a (\ln T)^{n-1} \left(\int_0^{1/2} (\ln x)^{\gamma(n)} dt + \int_{1/2}^T \ln T \frac{dt}{t} \right) \ll x^a (\ln x)^{n+1}, \\ |I_5| &\ll x^a (\ln x)^{n+1}. \end{aligned}$$

Следовательно, имеем

$$\sum_{q \leq x} a_n(q) = -(I_3 + I_4) + O\left(\frac{x^2}{T} (\ln x)^n\right) + O(x^a (\ln x)^{n+1}).$$

Далее, воспользовавшись обозначениями из леммы 14, вычислим сумму интегралов по краям разреза:

$$\begin{aligned} I_3 + I_4 &= \frac{1}{2\pi i} \left(\int_{a+i \cdot 0}^{2+i \cdot 0} + \int_{2-i \cdot 0}^{a-i \cdot 0} \right) (s-2)^{\gamma(n)} A(s) x^s ds \\ &= \frac{1}{2\pi i} \int_0^\delta ((-u+i \cdot 0)^{-\gamma(n)} + (-u-i \cdot 0)^{-\gamma(n)}) A(2-u) x^{2-u} du \\ &= \frac{x^2}{2\pi i} \int_0^\delta (e^{-\pi i \gamma(n)} u^{-\gamma(n)} - e^{\pi i \gamma(n)} u^{-\gamma(n)}) A(2-u) x^{-u} du \\ &= -\frac{x^2}{\pi} \sin(\pi \gamma(n)) \int_0^\delta u^{-\gamma(n)} A(2-u) x^{-u} du. \end{aligned}$$

Поскольку $\delta \leq r/2$, по лемме 14 функция $A(2-u)$ разлагается на отрезке $0 \leq u \leq \delta$ в ряд по степеням u , сходящийся абсолютно и равномерно. Из той же леммы заключаем, что при любом $N \geq 0$ справедливо равенство

$$I_3 + I_4 = -\frac{x^2}{\pi} \sin(\pi\gamma(n)) \int_0^\delta u^{-\gamma(n)} \left(\sum_{k=0}^N (-1)^k A_k u^k + \theta c \left(\frac{u}{r} \right)^{N+1} \right) x^{-u} du,$$

где $c = c(n)$. Далее, для целого $k \geq 0$ и γ с условием $0 < \gamma < 1$ имеем

$$\int_0^\delta u^{k-\gamma} x^{-u} du = \left(\int_0^\infty - \int_\delta^\infty \right) u^{k-\gamma} x^{-u} = \frac{\Gamma(k+1-\gamma) - j_k(\delta \ln x)}{(\ln x)^{k+1-\gamma}},$$

где

$$j_k(\lambda) = \int_\lambda^\infty v^{k-\gamma} e^{-v} dv.$$

Многократно интегрируя $j_k(\lambda)$ по частям, получим

$$\begin{aligned} j_k(\lambda) &= \lambda^{k-\gamma} e^{-\lambda} + (k-\gamma) j_{k-1}(\lambda) = \dots = \lambda^{-\gamma} e^{-\lambda} (\lambda^k + (k-\gamma) \lambda^{k-1} \\ &\quad + (k-\gamma)(k-\gamma-1) \lambda^{k-2} + \dots + (k-\gamma)(k-\gamma-1) \dots (2-\gamma) \lambda) \\ &\quad + (k-\gamma)(k-\gamma-1) \dots (2-\gamma)(1-\lambda) j_0(\lambda). \end{aligned}$$

Замечая теперь, что при $\lambda > 1$ справедливы оценки

$$\begin{aligned} j_0(\lambda) &= \int_\lambda^\infty u^{-\gamma} e^{-u} du \leq \lambda^{-\gamma} \int_\lambda^\infty e^{-u} du = \lambda^{-\gamma} e^{-\lambda}, \\ 0 < j_k(\lambda) &\leq \lambda^{-\gamma} e^{-\lambda} (\lambda^k + k \lambda^{k-1} + k(k-1) \lambda^{k-2} + \dots + k!) \\ &= k! e^{-\lambda} \lambda^{-\gamma} \left(\frac{\lambda^k}{k!} + \frac{\lambda^{k-1}}{(k-1)!} + \dots + \frac{\lambda}{1!} + 1 \right) \\ &\leq \lambda^{k-\gamma} k! e^{-\lambda} \left(\frac{1}{k!} + \frac{1}{(k-1)!} + \dots + \frac{1}{1!} + 1 \right) < e k! \lambda^{k-\gamma} e^{-\lambda}, \end{aligned}$$

и полагая $\gamma = \gamma(n)$, $\lambda = \delta \ln x$, будем иметь

$$\int_0^\delta u^{k-\gamma} x^{-u} du = \frac{\Gamma(k+1-\gamma)}{(\ln x)^{k+1-\gamma}} - \theta_1 e k! \frac{\delta^{k-\gamma} x^{-\delta}}{\ln x}.$$

Поскольку $\delta^{-\gamma} \ln^{-1} x < (\delta \ln x)^{-1} < 1$, то

$$\begin{aligned} I_3 + I_4 &= -\frac{x^2}{\pi} \sin(\pi\gamma(n)) \left(\sum_{k=0}^N (-1)^k A_k \int_0^\delta u^{k-\gamma} x^{-u} du \right. \\ &\quad \left. + \theta c r^{-(N+1)} \int_0^\delta u^{N+1-\gamma} x^{-u} du \right) \\ &= -\frac{x^2}{\pi} \sin(\pi\gamma(n)) \left(\sum_{k=0}^N (-1)^k \frac{A_k \Gamma(k+1-\gamma)}{(\ln x)^{k+1-\gamma}} + \theta_2 e N! x^{-\delta} \sum_{k=0}^N |A_k| \delta^k \right. \\ &\quad \left. + \theta c r^{-(N+1)} \frac{\Gamma(N+2-\gamma)}{(\ln x)^{N+2-\gamma}} \right). \end{aligned}$$

Наконец, замечая, что

$$\sum_{k=0}^N |A_k| \delta^k \leq c \sum_{k=0}^N r^{-k} \left(\frac{1}{2}r\right)^k < 2c, \quad \frac{1}{\pi} (-1)^k \sin(\pi\gamma) \Gamma(k+1-\gamma) = \frac{1}{\Gamma(\gamma-k)},$$

находим

$$\begin{aligned} I_3 + I_4 &= -\frac{x^2}{(\ln x)^{1-\gamma(n)}} \left(\sum_{k=0}^N \frac{A_k}{\Gamma(\gamma(n)-k)} \frac{1}{(\ln x)^k} + O\left(\frac{1}{(\ln x)^{N+1}}\right) \right) + O(x^{2-\delta}), \\ \sum_{q \leq x} a_n(q) &= \frac{x^2}{(\ln x)^{1-\gamma(n)}} \left(\sum_{k=0}^N \frac{A_k}{\Gamma(\gamma(n)-k)} \frac{1}{(\ln x)^k} + O\left(\frac{1}{(\ln x)^{N+1}}\right) \right) + O(x^{2-\delta}) \\ &\quad + O\left(\frac{x}{T} (\ln x)^n\right) + O(x^{2-\delta} (\ln x)^{n+1}), \end{aligned}$$

где постоянные в знаках O зависят от n и N . Полагая $T = e^{\sqrt{\ln x}}$, получаем утверждение теоремы. Если x не является полупростым числом, то теорема следует из формулы конечных приращений Лагранжа и доказанного выше.

Доказательство асимптотики для $B_n(x)$ проводится аналогично. Теорема доказана.

СЛЕДСТВИЕ 2. *Имеют место следующие асимптотические формулы:*

$$\begin{aligned} A_2(x) &= \frac{x^2}{\sqrt{\ln x}} (C_2 + O(\ln^{-1} x)), & A_3(x) &= \frac{x^2}{\sqrt[3]{\ln x}} (C_3 + O(\ln^{-1} x)), \\ A_4(x) &= \frac{x^2}{(\ln x)^{3/8}} (C_4 + O(\ln^{-1} x)), \end{aligned}$$

где

$$\begin{aligned} C_2 &= \frac{43}{80} \left\{ \frac{1}{\pi} \prod_p \left(1 - \frac{3}{4}p^{-2} - \frac{1}{4}p^{-3} \right) \right\}^{1/2} = 0.246\,272\dots, \\ C_3 &= \frac{17}{3} \left(\pi^2 \Gamma\left(\frac{2}{3}\right) \right)^{-1} \left\{ \frac{\pi}{4\sqrt{3}} \prod_{p \equiv 1 \pmod{6}} (1 - p^{-2})^{-2} \right. \\ &\quad \times \left. \left(1 - \frac{2}{3}p^{-2} - \frac{8}{27}p^{-3} - \frac{1}{27}p^{-4} \right) \right\}^{1/3} = 0.330\,511\dots, \\ C_4 &= \frac{171}{256} \left(\frac{\pi}{16} \right)^{1/8} \left(\Gamma\left(\frac{3}{8}\right) \right)^{-1} \left\{ \prod_{p \equiv 3 \pmod{4}} \left(1 - \frac{3}{4}p^{-2} - \frac{1}{4}p^{-3} \right) \right\}^{1/2} \\ &\quad \times \left\{ \prod_{p \equiv 1 \pmod{4}} (1 - p^{-2})^{1/2} \left(1 - \frac{5}{8}p^{-2} - \frac{5}{16}p^{-3} - \frac{15}{256}p^{-4} - \frac{1}{256}p^{-5} \right) \right\}^{1/4} \\ &= 0.212\,402\dots \end{aligned}$$

ЗАМЕЧАНИЕ 2. Пользуясь формулами из леммы 2, можно построить примеры модулей q , для которых число вычетов степени n будет мало по сравнению со средним значением. Пусть, например, $n = 2$, и пусть $q = p_1 \cdots p_k$, где $p_r -$

занумерованные в порядке возрастания подряд идущие нечетные простые числа. Тогда

$$a_2(q) = (p_1 - 1) \cdots (p_k - 1) \cdot 2^{-k} < q \cdot 2^{-k}.$$

Из асимптотического закона распределения простых чисел при $k \rightarrow +\infty$ находим

$$\ln q = \sum_{p \leq p_k} \ln p \sim p_k \sim k \ln k, \quad k \sim \frac{\ln q}{\ln \ln q}.$$

Следовательно, для любого фиксированного ε с условием $0 < \varepsilon < 1$ при $k \geq k_0(\varepsilon) > 1$ справедлива оценка

$$a_2(q) < q \cdot 2^{-(1-\varepsilon) \frac{\ln q}{\ln \ln q}}.$$

Подобным образом строятся примеры и для больших значений n .

ЗАМЕЧАНИЕ 3. Иное доказательство теоремы 1 получается с помощью итерационного метода Левина–Файнлейба (см. [12], а также [13, с. 379–393]). Первое слагаемое в правых частях формул (6) и (7) может быть найдено и с помощью общей теоремы Вирзинга [14]. Кроме того, после сдачи работы в печать автору стало известно о том, что частные случаи формул теоремы 1 ($n = 2$ и $n = 3$) с одним слагаемым в главном члене и без оценки остатка приведены в препринте [15].

§ 4. Свойства чисел $\gamma(n)$

Пусть δ – произвольный делитель n . Обозначим через $c_\delta(n)$ количество чисел k приведенной системы вычетов по модулю n , удовлетворяющих условию $(k - 1, n) = \delta$. Тогда из определения величин $\gamma(n)$ следует равенство

$$\gamma(n) = \frac{1}{\varphi(n)} \sum_{\delta|n} \frac{c_\delta(n)}{\delta}.$$

Для нахождения среднего значения чисел $\gamma(n)$ нам понадобится, в частности, явная формула для $c_\delta(n)$.

ЛЕММА 15. *Справедливо равенство*

$$c_\delta(n) = \varphi\left(\frac{n}{\delta}\right) \prod_{p|n, p \nmid \delta} \left(1 - \frac{1}{\varphi(p)}\right).$$

ДОКАЗАТЕЛЬСТВО. Имеем равенства

$$\begin{aligned} c_\delta(n) &= \sum_{(k,n)=1, (k-1,n)=\delta} 1 = \sum_{\substack{k=1 \\ k \equiv 1 \pmod{\delta}}}^n \left(\sum_{d|(k,n)} \mu(d) \right) \left(\sum_{d_1 | (\frac{k-1}{\delta}, \frac{n}{\delta})} \mu(d_1) \right) \\ &= \sum_{d|n} \mu(d) \sum_{\substack{k \equiv 1 \pmod{\delta} \\ k \equiv 0 \pmod{d}}} \sum_{d_1 | (\frac{k-1}{\delta}, \frac{n}{\delta})} \mu(d_1) = \sum_{d|n} \mu(d) \sum_{d_1 | \frac{n}{\delta}} \mu(d_1) \sum_{\substack{k \equiv 1 \pmod{d_1 \delta} \\ k \equiv 0 \pmod{d}}} 1. \end{aligned}$$

Из условий, которым удовлетворяют числа k во внутренней сумме, следует, что число d взаимно просто с произведением $d_1\delta$. Если это условие выполнено, то сравнения

$$k \equiv 1 \pmod{d_1\delta}, \quad k \equiv 0 \pmod{d}$$

эквивалентны некоторому сравнению $k \equiv k_0 \pmod{dd_1\delta}$. Поскольку числа d и $d_1\delta$ являются делителями n , то число решений последнего сравнения с условием $1 \leq k \leq n$ равно $n/(dd_1\delta)$. Таким образом,

$$c_\delta(n) = \frac{n}{\delta} \sum_{d|n, (d,\delta)=1} \frac{\mu(d)}{d} \sum_{d_1|\frac{n}{\delta}, (d,d_1)=1} \frac{\mu(d_1)}{d_1}.$$

Внутренняя сумма преобразуется к виду

$$\prod_{p|\frac{n}{\delta}, p \nmid d} \left(1 - \frac{1}{p}\right) = \prod_{p|\frac{n}{\delta}} \left(1 - \frac{1}{p}\right) \prod_{p|d} \left(1 - \frac{1}{p}\right)^{-1} = \frac{\delta}{n} \varphi\left(\frac{n}{\delta}\right) \frac{d}{\varphi(d)}.$$

Следовательно,

$$c_\delta(n) = \varphi\left(\frac{n}{\delta}\right) \sum_{d|n, (d,\delta)=1} \frac{\mu(d)}{\varphi(d)} = \varphi\left(\frac{n}{\delta}\right) \prod_{p|n, p \nmid \delta} \left(1 - \frac{1}{\varphi(p)}\right).$$

ЛЕММА 16. Пусть a, b – натуральные числа. Тогда при $x \rightarrow +\infty$ справедлива следующая асимптотическая формула:

$$\sum_{n \leq x} \frac{\varphi(an)}{\varphi(bn)} = \mathfrak{S}(a, b)x + \theta r(a, b),$$

где

$$\mathfrak{S}(a, b) = \frac{a}{b} \frac{\prod_{p|a} \left(1 - \frac{1}{p} + \frac{1}{p^2}\right) \prod_{p|b} \left(1 + \frac{1}{p}\right)}{\prod_{p|(a,b)} \left(1 + \frac{1}{p^3}\right)}, \quad r(a, b) = \frac{ab}{(\varphi(b))^2}.$$

ДОКАЗАТЕЛЬСТВО. Прежде всего, имеем

$$\frac{\varphi(an)}{\varphi(bn)} = \frac{a}{b} \frac{\prod_{p|an} \left(1 - \frac{1}{p}\right)}{\prod_{p|bn} \left(1 - \frac{1}{p}\right)} = \frac{a}{b} \frac{\prod_{p|a} \left(1 - \frac{1}{p}\right)}{\prod_{p|b} \left(1 - \frac{1}{p}\right)} \frac{\prod_{p|n, p \nmid a} \left(1 - \frac{1}{p}\right)}{\prod_{p|n, p \nmid b} \left(1 - \frac{1}{p}\right)}.$$

После сокращения в числителе последней дроби останутся лишь множители, отвечающие простым делителям (n, b) , не делящим a , а в знаменателе – множители, отвечающие простым делителям (n, a) , не делящим b . Следовательно, получаем

$$\begin{aligned} \frac{\varphi(an)}{\varphi(bn)} &= \frac{\varphi(a)}{\varphi(b)} \prod_{p|(n,b), p \nmid a} \left(1 - \frac{1}{p}\right) \prod_{p|(n,a), p \nmid b} \left(1 - \frac{1}{p}\right)^{-1} \\ &= \frac{\varphi(a)}{\varphi(b)} \prod_{p|(n,b), p \nmid a} \left(1 - \frac{1}{p}\right) \prod_{p|(n,a), p \nmid b} \left(1 + \frac{1}{\varphi(p)}\right) \\ &= \frac{\varphi(a)}{\varphi(b)} \sum_{d|(b,n), d \nmid a} \frac{\mu(d)}{d} \sum_{\delta|(a,n), \delta \nmid b} \frac{\mu^2(\delta)}{\varphi(\delta)}. \end{aligned}$$

Исходная сумма преобразуется к виду

$$\begin{aligned} \sum_{n \leq x} \frac{\varphi(an)}{\varphi(bn)} &= \frac{\varphi(a)}{\varphi(b)} \sum_{n \leq x} \sum_{\delta | (a,n), \delta \nmid b} \frac{\mu^2(\delta)}{\varphi(\delta)} \sum_{d | (b,n), d \nmid a} \frac{\mu(d)}{d} \\ &= \frac{\varphi(a)}{\varphi(b)} \sum_{\delta | a, (\delta, b)=1} \frac{\mu^2(\delta)}{\varphi(\delta)} \sum_{d | b, (d, a)=1} \frac{\mu(d)}{d} \sum_{\substack{n \leq x \\ (n, a) \equiv 0 \pmod{\delta} \\ (n, b) \equiv 0 \pmod{d}}} 1. \end{aligned}$$

Условия, которым подчинены числа n во внутренней сумме, эквивалентны условиям $n \equiv 0 \pmod{\delta}$, $n \equiv 0 \pmod{d}$, которые в силу равенства $(d, \delta) = 1$ можно заменить одним условием $n \equiv 0 \pmod{d\delta}$. Таким образом, находим

$$\begin{aligned} \sum_{n \leq x} \frac{\varphi(an)}{\varphi(bn)} &= \frac{\varphi(a)}{\varphi(b)} \sum_{\delta | a, (\delta, b)=1} \frac{\mu^2(\delta)}{\varphi(\delta)} \sum_{d | b, (d, a)=1} \frac{\mu(d)}{d} \left(\frac{x}{d\delta} + \theta \right) \\ &= \mathfrak{S}(a, b)x + \theta_1 r_1(a, b), \end{aligned}$$

где

$$\begin{aligned} \mathfrak{S}(a, b) &= \frac{\varphi(a)}{\varphi(b)} \sum_{\delta | a, (\delta, b)=1} \frac{\mu^2(\delta)}{\delta \varphi(\delta)} \sum_{d | b, (d, a)=1} \frac{\mu(d)}{d^2} \\ &= \frac{\varphi(a)}{\varphi(b)} \prod_{p | a, p \nmid b} \left(1 + \frac{1}{p(p-1)} \right) \prod_{p | b, p \nmid a} \left(1 - \frac{1}{p^2} \right) \\ &= \frac{a}{b} \frac{\prod_{p | a} \left(1 - \frac{1}{p} \right) \left(1 + \frac{1}{p(p-1)} \right) \prod_{p | b} \left(1 - \frac{1}{p^2} \right)}{\prod_{p | (a, b)} \left(1 + \frac{1}{p(p-1)} \right) \left(1 - \frac{1}{p^2} \right) \prod_{p | b} \left(1 - \frac{1}{p} \right)} \\ &= \frac{a}{b} \frac{\prod_{p | a} \left(1 - \frac{1}{p} + \frac{1}{p^2} \right) \prod_{p | b} \left(1 + \frac{1}{p} \right)}{\prod_{p | (a, b)} \left(1 + \frac{1}{p^3} \right)}, \\ r_1(a, b) &= \frac{\varphi(a)}{\varphi(b)} \sum_{\delta | a} \frac{\mu^2(\delta)}{\varphi(\delta)} \sum_{d | b} \frac{\mu^2(d)}{d} = \frac{\varphi(a)}{\varphi(b)} \frac{a}{\varphi(a)} \prod_{p | b} \left(1 + \frac{1}{p} \right) < \frac{a}{\varphi(b)} \frac{b}{\varphi(b)}. \end{aligned}$$

СЛЕДСТВИЕ 3. Если $(a, c) = 1$, то

$$\sum_{n \leq x} \frac{\varphi(an)}{\varphi(acn)} = \frac{x}{c} \prod_{p | c} \left(1 + \frac{1}{p} \right) + \theta \left(\frac{a}{\varphi(a)} \right)^2 \frac{c}{\varphi^2(c)}.$$

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 2. Согласно лемме 15 имеем

$$\begin{aligned} c_\delta(n) &= \varphi\left(\frac{n}{\delta}\right) \prod_{p | n, p \nmid \delta} \left(1 - \frac{1}{\varphi(p)} \right) = \varphi\left(\frac{n}{\delta}\right) \sum_{\substack{d | n \\ (d, \delta)=1}} \frac{\mu(d)}{\varphi(d)}, \\ \gamma(n) &= \frac{1}{\varphi(n)} \sum_{\delta | n} \frac{c_\delta(n)}{\delta} = \frac{1}{\varphi(n)} \sum_{\delta | n} \frac{1}{\delta} \varphi\left(\frac{n}{\delta}\right) \sum_{\substack{d | n \\ (d, \delta)=1}} \frac{\mu(d)}{\varphi(d)}. \end{aligned}$$

Следовательно,

$$\begin{aligned} \sum_{n \leq x} \gamma(n) &= \sum_{n \leq x} \frac{1}{\varphi(n)} \sum_{\delta | n} \frac{1}{\delta} \varphi\left(\frac{n}{\delta}\right) \sum_{\substack{d | n \\ (d, \delta) = 1}} \frac{\mu(d)}{\varphi(d)} = \sum_{\delta \leq x} \frac{1}{\delta} \sum_{\substack{d \leq x \\ (d, \delta) = 1}} \frac{\mu(d)}{\varphi(d)} \sum_{\substack{n \leq x \\ n \equiv 0 \pmod{d\delta}}} \frac{\varphi(n/\delta)}{\varphi(n)} \\ &= \sum_{\delta \leq x} \frac{1}{\delta} \sum_{\substack{d \leq x \\ (d, \delta) = 1}} \frac{\mu(d)}{\varphi(d)} \sum_{m \leq x/(d\delta)} \frac{\varphi(dm)}{\varphi(d\delta m)}. \end{aligned}$$

Чтобы вычислить внутреннюю сумму по m , воспользуемся леммой 16. Получим

$$\begin{aligned} \sum_{n \leq x} \gamma(n) &= \sum_{\delta \leq x} \frac{1}{\delta} \sum_{\substack{d \leq x \\ (d, \delta) = 1}} \frac{\mu(d)}{\varphi(d)} \left(\frac{x}{d\delta^2} \prod_{p | \delta} \left(1 + \frac{1}{p}\right) + \theta_1 \left(\frac{d}{\varphi(d)} \right)^2 \frac{\delta}{\varphi^2(\delta)} \right) \\ &= x \sum_{\delta \leq x} \frac{1}{\delta^3} \prod_{p | \delta} \left(1 + \frac{1}{p}\right) \sum_{\substack{d \leq x \\ (d, \delta) = 1}} \frac{\mu(d)}{d\varphi(d)} + \theta_2 \sum_{\delta \leq x} \frac{1}{\varphi^2(\delta)} \sum_{d \leq x} \left(\frac{d}{\varphi(d)} \right)^2 \frac{1}{\varphi(d)}. \end{aligned} \quad (17)$$

Из оценок

$$\frac{d}{\varphi(d)} \ll \ln \ln(d+3), \quad \sum_{n \leq x} \frac{1}{\varphi(n)} \ll \ln x$$

следует, что последнее слагаемое в (17) не превосходит по порядку $(\ln x)(\ln \ln x)^2$. Далее, замечая, что

$$\sum_{\substack{d \leq x \\ (d, \delta) = 1}} \frac{\mu(d)}{d\varphi(d)} = \sum_{\substack{d=1 \\ (d, \delta) = 1}}^{\infty} \frac{\mu(d)}{d\varphi(d)} + \left(\frac{\ln x}{x} \right) = \prod_{p \nmid \delta} \left(1 - \frac{1}{p(p-1)} \right) + \left(\frac{\ln x}{x} \right),$$

находим

$$\sum_{n \leq x} \gamma(n) = x \prod_p \left(1 - \frac{1}{p(p-1)} \right) \sum_{\delta \leq x} \frac{\lambda(\delta)}{\delta^3} + O((\ln x)(\ln \ln x)^2),$$

где

$$\lambda(\delta) = \prod_{p | \delta} \frac{1 + \frac{1}{p}}{1 - \frac{1}{p(p-1)}} = \prod_{p | \delta} \frac{p^2 - 1}{p^2 - p - 1}.$$

Поскольку функция $\lambda(\delta)$ мультипликативна, причем $\lambda(p^m) = \lambda(p)$ при любом $m \geq 1$, окончательно находим

$$\begin{aligned} \sum_{n \leq x} \gamma(n) &= x \prod_p \left(1 - \frac{1}{p(p-1)} \right) \left(\sum_{\delta=1}^{\infty} \frac{\lambda(\delta)}{\delta^3} + O(x^{-1}) \right) + O((\ln x)(\ln \ln x)^2) \\ &= Cx + O((\ln x)(\ln \ln x)^2), \end{aligned}$$

причем

$$\begin{aligned}
 C &= \prod_p \left(1 - \frac{1}{p(p-1)}\right) \sum_{\delta=1}^{\infty} \frac{\lambda(\delta)}{\delta^3} = \prod_p \left(1 - \frac{1}{p(p-1)}\right) \left(1 + \frac{\lambda(p)}{p^3} + \frac{\lambda(p)}{p^6} + \dots\right) \\
 &= \prod_p \left(1 - \frac{1}{p(p-1)}\right) \left(1 + \frac{\lambda(p)}{p^3 - 1}\right) \\
 &= \prod_p \frac{p^2 - p - 1}{p(p-1)} \left(1 + \frac{p+1}{(p^2 + p + 1)(p^2 - p - 2)}\right) \\
 &= \prod_p \frac{p^2 - p - 1}{p(p-1)} \frac{p^4 - p^2 - p}{(p^2 + p + 1)(p^2 - p - 2)} = \prod_p \frac{p^3 - p - 1}{p^3 - 1} = \prod_p \left(1 - \frac{p}{p^3 - 1}\right).
 \end{aligned}$$

Теорема доказана.

В заключение приведем несколько формул, позволяющих вычислять величину $\gamma(n)$, когда известно каноническое разложение n на простые сомножители.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 3. Первая часть утверждения теоремы представляет собой следствие леммы 10. Для доказательства второго утверждения подсчитаем количество чисел k из приведенной системы вычетов по модулю $n = p^m$, для которых величина $(k-1, n)$ имеет одно и то же значение p^s , $s \geq 0$.

Величина $(k-1, n)$ равна единице тогда и только тогда, когда k имеет вид $pt + r$, где $2 \leq r \leq p-1$, $t = 0, 1, 2, \dots, p^{m-1}-1$. Общее количество таких чисел в приведенной системе вычетов равно $p^{m-1}(p-2)$.

Если $k = pt + 1$, то $(k-1, n) = (pt, p^m) = p(t, p^{m-1})$. Однако в последовательности $t = 0, 1, 2, \dots, p^{m-1}-1$ имеется ровно $p^{m-s-1} - p^{m-s-2}$ чисел, делящихся на p^s , но не делящихся на p^{s+1} , $s = 0, 1, \dots, m-2$; единственным числом, делящимся на p^{m-1} , будет число 0. Следовательно,

$$\begin{aligned}
 \gamma(n) &= \frac{1}{\varphi(n)} \left(p^{m-1}(p-2) + \frac{1}{p} \sum_{s=0}^{m-2} \frac{p^{m-s-1} - p^{m-s-2}}{p^s} + \frac{1}{p^m} \right) \\
 &= \frac{1}{\varphi(n)} \left(p^m - 2p^{m-1} + (p^m - p^{m-1}) \frac{1 - p^2 p^{-2m}}{p^2 - 1} + \frac{1}{p^m} \right) \\
 &= 1 - \frac{p}{p^2 - 1} \left(1 - \frac{1}{n^2} \right).
 \end{aligned}$$

Теорема доказана.

СЛЕДСТВИЕ 4. Если n – бесквадратное число, то $\gamma(n) = \varphi(n)/n$.

Список литературы

1. D. N. Lehmer, “Asymptotic evaluation of certain totient sums”, *Amer. J. Math.*, **22**:4 (1900), 293–335.
2. E. Landau, “Bemerkungen zu Herrn D. N. Lehmer’s Abhandlung in Bd. 22 dieses Journals, S. 293–335”, *Amer. J. Math.*, **26**:3 (1904), 209–222.
3. E. Landau, “Über die Einteilung der positiven ganzen Zahlen in vier Klassen nach der Mindestzahl der zu ihrer additiven Zusammensetzung erforderlichen Quadrate”, *Archiv der Mathematik und Physik, Ser. 3*, **13** (1908), 305–312.

4. E. Landau, “Lösung des Lehmer’schen Problems”, *Amer. J. Math.*, **31**:1 (1909), 86–102.
5. Д. А. Райков, “О распределении чисел, простые делители которых принадлежат заданной арифметической прогрессии”, *Матем. сб.*, **4(46)**:3 (1938), 563–570.
6. P. Kuhn, “Über ein Problem in der Theorie der Primzahlen”, *Ark. Mat.*, **4**:1 (1960), 1–14.
7. Ш. Х. Тутушев, “Об одной задаче Ландау”, *Тр. Физического об-ва Республики Адыгея*, **2** (1997), 70–74; <http://fora.adygnet.ru/?1997>.
8. E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen*, Chelsea Publ., New York, 1974.
9. J. Chungang, “The number of k th power residues modulo m ”, *J. Nanjing Norm. Univ. Nat. Sci. Ed.*, **24**:1 (2001), 1–2.
10. А. А. Карацуба, *Основы аналитической теории чисел*, Наука, М., 1983; англ. пер.: A. Karatsuba, *Basic analytic number theory*, Springer-Verlag, Berlin, 1993.
11. Э. Ч. Титчмарш, *Теория дзета-функции Римана*, ИЛ, М., 1953; пер. с англ.: E. C. Titchmarsh, *The theory of the Riemann zeta-function*, Clarendon Press, Oxford, 1951.
12. Б. В. Левин, А. С. Файнлейб, “Применение некоторых интегральных уравнений к вопросам теории чисел”, *УМН*, **22**:3 (1967), 119–197; англ. пер.: B. V. Levin, A. S. Fainleib, “Application of some integral equations to problems of number theory”, *Russian Math. Survey*, **22**:3 (1967), 119–204.
13. А. Г. Постников, *Введение в аналитическую теорию чисел*, Наука, М., 1971; англ. пер.: A. G. Postnikov, *Introduction to analytic number theory*, Transl. Math. Monogr., **68**, Amer. Math. Soc., Providence, RI, 1971.
14. E. Wirsing, “Das asymptotische Verhalten von Summen über multiplikative Funktionen”, *Math. Ann.*, **143**:1 (1961), 75–102.
15. S. Finch, P. Sebah, *Squares and Cubes Modulo n* , arXiv:<http://arxiv.org/abs/math.NT/0604465v2>.

М. А. КОРОЛЁВ (M. A. KOROLEV)
Математический институт им. В. А. Стеклова РАН
E-mail: hardy_ramanujan@mail.ru

Поступило в редакцию
28.04.2009