Вісник Харківського національного університету імені В.Н. Каразіна
Серія "Математика, прикладна математика і механіка"
УДК 511 № 875, 2009, с.69–79

Функция Кармайкла на бесквадратных числах

А.В. Лелеченко
Одесский национальный университет им. И.И. Мечникова, Одесса, Украина
andrew.lelechenko@gmail.com

Используя методы вероятностной теории чисел, мы находим распределения значений некоторых арифметических функций на бесквадратных числах, поведение которых тесно связано с поведением функций Эйлера и Кармайкла.

Лелеченко А.В., **Функція Кармайкла на безквадратних числах**. Використовуючи методи ймовірнісної теорії чисел, ми знаходимо розподіли значень деяких арифметичних функцій на безквадратних числах, поведінка яких тісно пов'язана з поведінкою функцій Ейлера та Кармайкла.

A.V.Lelechenko, **Carmichael function on the square-free numbers**. Using methods of the probabilistic number theory, we find the distributions of values on the square-free numbers of some arithmetical functions. The behavior of these functions is closely related to that of the Euler and Carmichael functions.

2000 Mathematics Subject Classification: 11A25.

1. Введение

1.1. Объекты исследования

Обозначим через $\phi(n)$ *функцию Эйлера*, определяемую как количество обратимых элементов в кольце вычетов по модулю n. Тогда $\phi(p^k) = p^{k-1}(p-1)$ и

$$\phi\Big(\prod_i p_i^{k_i}\Big) = \prod_i \phi(p_i^{k_i}) = \prod_i p_i^{k_i-1}(p_i-1).$$

Обозначим через $\lambda(n)$ *функцию Кармайкла*, которая ставит в соответствие натуральному n наибольший из порядков элементов $\mathbb{Z}_n^*$. Тогда

$$\lambda(p^k) = \begin{cases} \phi(2) = 1, & p = 2, k = 1, \\ \phi(4) = 2, & p = 2, k = 2, \\ \phi(p^k)/2, & p = 2, k \geq 3, \\ \phi(p^k), & p \geq 3. \end{cases}$$

Из теорем о порядках элементов в группах следует, что

$$\lambda\Big(\prod_i p_i^{k_i}\Big) = \operatorname*{lcm}_i \lambda(p_i^{k_i}),$$

где $\operatorname{lcm}_i \alpha_i$ обозначает наименьшее общее кратное всех элементов множества $\{\alpha_i\}$. Отметим, что множества простых делителей $\phi(n)$ и $\lambda(n)$ совпадают.

Наконец, введем $\xi(n) = \phi(n)/\lambda(n)$. Из $\lambda(p^k) \mid \phi(p^k)$ и $\operatorname{lcm}_i \alpha_i \mid \prod_i \alpha_i$ следует, что $\lambda(n) \mid \phi(n)$, а значит $\xi(n)$ — целочисленная функция. Этот факт также следует из теоретико-групповой интерпретации: порядок любого элемента группы всегда делит порядок группы нацело.

Особенно ясное строение приобретают эти функции, если ограничить рассмотрение только бесквадратными n. Напомним, что натуральное n называется *бесквадратным*, если из $p \mid n$ следует $p^2 \nmid n$. Отсюда всякое бесквадратное число может быть записано как $\prod_i p_i$, где все p_i различны. Удобно использовать $\mu^2(n)$ как индикатор бесквадратности, где μ — функция Мёбиуса. Итак, для бесквадратных n получим

$$\begin{aligned} \phi(n) &= \phi\Big(\prod_i p_i\Big) = \prod_i \phi(p_i) = \prod_i (p_i - 1), \\ \lambda(n) &= \lambda\Big(\prod_i p_i\Big) = \operatorname*{lcm}_i \lambda(p_i) = \operatorname*{lcm}_i (p_i - 1). \end{aligned}$$

Здесь, аналогично введенному ранее обозначению $\operatorname{lcm}_i \alpha_i$, $\gcd_i \alpha_i$ обозначает наибольший общий делитель всех элементов множества $\{\alpha_i\}$. Понятно, что за исключением случая $n = p_1 p_2$ соотношение $\xi(n) = \gcd_i(p_i - 1)$ будет выполняться не всегда.

Функция $\lambda(n)$ была введена Р. Д. Кармайклом [3] в начале XX века, однако долгое время не привлекала внимания исследователей. Толчком к изучению стало открытие ее приложений в ряде разделов математики, в частности — в криптографии. Это произошло в конце 80-х — начале 90-х годов и с тех пор количество публикаций о функции Кармайкла дискретно растет.

1.2. Элементарные свойства

Равенство $\phi(n) = \lambda(n)$ (т. е. $\xi(n) = 1$) эквивалентно утверждению о том, что группа $\mathbb{Z}_n^*$ является циклической, а значит $n = 2, 4, p^k, 2p^k$, где $p \neq 2$, $k \in$ $\in \mathbb{N}$. При всех прочих значениях $n = \prod_i p_i^{k_i}$ значение $\lambda(n)$ представляет собой наименьшее общее кратное двух или более четных чисел, а значит $\prod_i \lambda(p_i^{k_i})$ и тем более $\phi(n) = \prod_i \phi(p_i^{k_i})$ делятся на $2\lambda(n)$ и, значит, величина $\xi(n)$ четна. Очевидно также, что для таких значений n значение $\phi(n)$ делится на 4, а $\lambda(n)$ — четно.

Обобщим предыдущее рассуждение: если $p \mid \xi(n)$, $p > 2$, то степень множителя p в каноническом разложении $\phi(n)$ должна быть строго больше его степени в каноническом разложении $\lambda(n)$. Поскольку $\phi(n)$ может отличаться от $\prod_i \lambda(p_i^{k_i})$ только на степень 2, то в множестве $\{\lambda(p_i^{k_i})\}$ найдутся по крайней мере два элемента, делящиеся на p (а значит $p \mid \lambda(n)$). Но это тем более верно для множества, составленного из $\phi(p_i^{k_i})$, поэтому $p^2 \mid \prod_i \phi(p_i^{k_i}) = \phi(n)$. Обратное неверно: из $p^2 \mid \phi(n)$ не обязательно следует, что $p \mid \xi(n)$. Например, $9 \mid \phi(19)$, но $\xi(19) = 1$.

Это свойство объясняет важность изучения $\xi(n)$, ибо поведение этой функции дает нам информацию и о поведении функции Кармайкла, и о поведении функции Эйлера одновременно.

Отсюда можно вывести грубую оценку: наибольший простой делитель q числа $\xi(n)$ не превосходит $\sqrt{\phi(n)} < \sqrt{n}$. В [1] элементарными методами получена лучшая оценка: для всех $n \geq 276$ выполняется $q \leq \frac{\sqrt{3n+1}-2}{6}$.

Отметим также, что большое количество результатов об асимптотическом росте и арифметических свойствах $\lambda(n)$ и $\xi(n)$ приводится в работах [1], [2] и [5].

1.3. Обозначения

Как обычно, p и q с индексами или без них будут обозначать простые числа; x — возрастающий параметр. Символы Ландау o, O и $\sim$, символы Виноградова $\gg$, $\ll$ и $\asymp$ будут рассматриваться при $x \to \infty$. Всюду под символом log подразумевается натуральный логарифм и используются сокращения: $x_1 = \log x$ и $x_k = \log x_{k-1}$. Введем функции $P(n)$, равную наибольшему простому делителю n, и $\Omega(n)$, равную числу простых делителей n с учетом их кратности. Функцию $\pi(x)$ положим равной количеству простых чисел, не превосходящих x, а функция $\pi(x, k, l)$ будет равна количеству простых чисел, не превосходящих x и сравнимых с l по модулю k.

2. Свойства $P(\xi(n))$

2.1. Цель настоящей работы

Недавно в работе [1] изучались арифметические свойства функций $\phi(n)$, $\lambda(n)$, $\xi(n)$. Основной результат работы этих авторов связан с распределением значений функции $P(\xi(n))$. Они доказали, что при любой убывающей к 0 функции $\epsilon(x)$ такой, что $\epsilon(x)x_2$ возрастает к $+\infty$, почти для всех n выполнено неравенство

$$\epsilon(n) \log\log n \leq P(\xi(n)) \leq \frac{(\log\log n)^2}{\epsilon(n) \log\log\log n}.$$

В работе [7] был использован аппарат вероятностной теории чисел для изучения локального поведения функций $P(\xi(n))$.

В настоящей работе мы, используя идеи [7] и [8], доказываем следующие утверждения:

Теорема 1. *Введем функцию двух переменных Y и n, определяемую как*

$$E_Y(n) := \#\{q > Y \mid q^2 \mid \phi(n)\}$$

и зафиксируем некоторое действительное b. Тогда для $Y = Y(x) = bx_2^2/x_3$ имеем

$$\lim_{x\to\infty} \frac{1}{x}\#\{n \le x \mid E_Y(n) = k, \mu^2(n) = 1\} = \frac{6}{\pi^2}\frac{\lambda^k}{k!}e^{-\lambda},$$

где $k = 0, 1, 2\ldots$, $\lambda = 1/2b$.

Теорема 2. *Пусть $\gamma(n)$ обозначает такое наибольшее простое q, что $q^2 \mid \phi(n)$. Зафиксируем некоторые $0 < c_1 < c_2 < +\infty$. Тогда для каждого простого $q \in [c_1x_2^2/x_3, c_2x_2^2/x_3]$ равномерно*

$$\frac{1}{x}\#\{n \le x \mid \gamma(n) = q, \mu^2(n) = 1\} = (1 + o(1))\frac{6}{\pi^2}\frac{x_2^2}{2q^2}e^{-\lambda_q},$$

где $\lambda_q = \frac{x_2^2}{2qx_3}$.

Из теоремы 2 и очевидного факта о том, что для бесквадратных n значения $\gamma(n)$ и $P(\xi(n))$ совпадают, вытекает основной результат работы.

Следствие 1

$$\frac{1}{x}\#\{n \le x \mid P(\xi(n)) = q, \mu^2(n) = 1\} = (1 + o(1))\frac{6}{\pi^2}\frac{x_2^2}{2q^2}e^{-\lambda_q}.$$

Перечисленные результаты можно трактовать и с теоретико-вероятностной позиции. Например, теорема 1 говорит о том, что

$$\lim_{x\to\infty} P\{E_Y(n) = k, \mu^2(n) = 1\} = \frac{6}{\pi^2}\frac{\lambda^k}{k!}e^{-\lambda},$$

(Здесь возникла коллизия обозначений: $P\{A\}$ — вероятность события A, а $P(n)$ — арифметическая функция наибольшего простого делителя.)

2.2. Вспомогательные утверждения

Леммы 1 и 2, а также следствие 2 суть классические результаты (см. напр. [11] и [12]).

Лемма 1 (преобразование Абеля) *Пусть задана произвольная последовательность комплексных чисел $\{a_k \in \mathbb{C}\}$ и непрерывно дифференцируемая функция $g\colon [t, +\infty] \mapsto \mathbb{C}$. Тогда*

$$\sum_{t\le k\le T} a_k g(k) = A(T)g(T) - \int_t^T A(x)g'(x)\,dx,$$

где $A(x) = \sum_{t\le k\le x} a_k$. *Если к тому же ряд* $\sum_{k=t}^{\infty} a_k g(k)$ *сходится и при этом* $A(T)g(T) \to 0$ *при* $T \to \infty$, *то*

$$\sum_{k=t}^{\infty} a_k g(k) = -\int_t^{\infty} A(x)g'(x)\,dx.$$

Следствие 2 (суммирование степеней простых чисел)

$$\sum_{p>x} p^{-k} \ll x^{1-k}x_1^{-1}, \qquad k > 1.$$

Лемма 2 (плостность бесквадратных чисел)

$$\sum_{n\le x} \mu^2(n) = \frac{6}{\pi^2}x + O(x^{1/2}).$$

Лемма 3 *Пусть* $z_1, z_2, \ldots, z_M$ — *последовательность из 0 и 1, и пусть* $T = \sum_{i=1}^{M} z_i$. *Тогда для каждого* $r = 1, \ldots, M$ *выполнено*

$$\sum_{\substack{i_1,i_2,\ldots,i_r \\ \alpha\ne\beta\to i_\alpha\ne i_\beta}} z_{i_1}\ldots z_{i_r} = T(T-1)\ldots(T-r+1).$$

Доказательство. Справедливость леммы очевидно вытекает из комбинаторного тождества

$$\sum_{i_1<i_2<\ldots<i_r} z_{i_1}\ldots z_{i_r} = \binom{T}{r}.$$

Введем функцию $U(x, D) := \#\{n \le x \mid D \mid \phi(n)\}$, обозначающую число таких не превосходящих x натуральных n, что заданное число D делит $\phi(n)$.

Лемма 4 *Пусть* $D = (p_1\ldots p_t)^2$, $p_1 < \ldots < p_t$ — *простые числа,* $x_2^{\delta} \le p_j \le x_2^L$, $0 < \delta < 1/2$, L — *фиксированное число. Тогда*

$$U(x, D) = \frac{x}{2^t}\cdot\frac{x_2^{2t}}{D}\left(1 + O\left(x_2^{-\delta}\right)\right).$$

Доказательство. См. [6].

Лемма 5 *Пусть* $l = \pm 1$. *Тогда равномерно по* $k < x$ *выполняется*

$$\sum_{\substack{p\equiv l \pmod k \\ p\le x}} \frac{1}{p} = (1 + o(1))\frac{x_2}{\phi(k)}.$$

Доказательство. См. [9, лемма 6.3] или [10, теорема 1].

2.3. Доказательство теоремы 1

Ниже мы докажем, пользуясь асимптотическими оценками плотностей элементов с определенными свойствами тот факт, что в условиях теоремы выполнено

$$\lim_{x\to\infty}\frac{1}{x}\#\{n\le x \mid E_Y(n)=k\}=\frac{\lambda^k}{k!}e^{-\lambda}.$$

Отсюда и из леммы 2 будет следовать утверждение теоремы.

Мы построим близкую к $E_Y(n)$ функцию более простой природы и оценим ее факториальные моменты. Мы увидим, что они совпадают с факториальными моментами распределения Пуассона, откуда и будет следовать утверждение теоремы.

Пусть $z=x_2^2$. Тогда, применяя лемму 4,

$$\sum_{n\le x}E_z(n) \;=\; \sum_{n\le x}\sum_{\substack{q>z\\ q^2\mid\phi(n)}}1=\sum_{x^{1/2}\ge q>z}U(x,q^2)\ll xx_2^2\sum_{x^{1/2}\ge q>x_2^2}q^{-2}.$$

Последняя величина по следствию 2 асимптотически меньше $xx_2^2\frac{x_2^{-2}}{x_3}=$ $=xx_3^{-1}=o(x)$. Введя новую функцию

$$\Delta_Y(n):=\#\big\{q\in[Y,z]\;\big|\;q^2\mid\phi(n)\big\},$$

видим, что если для некоторого n значения $\Delta_Y(n)$ и $E_Y(n)$ различны, то $E_z(n)>0$. Отсюда

$$\frac{1}{x}\#\{n\le x\mid\Delta_Y(n)\ne E_Y(n)\}\le\frac{1}{x}\sum_{n\le x}E_z(n)\to 0\qquad(x\to\infty).$$

Пусть $q\in[Y,z]$. Для простых $p_1<p_2$ определим функцию, являющуюся индикатором делимости p_1-1 и p_2-1 на q:

$$f_q(p_1,p_2):=\begin{cases}1, & \text{если } q\mid(p_1-1), q\mid(p_2-1),\\ 0, & \text{в остальных случаях.}\end{cases}$$

Тогда из $f_q(p_1,p_2)=1$ следует $q^2\mid\phi(p_1p_2)$. Далее, положим

$$\kappa_q(n):=\sum_{\substack{p_1p_2\mid n\\ p_1<p_2}}f_q(p_1,p_2),$$

т. е. это количество упорядоченных пар (p_1,p_2) простых чисел, делящих n, для которых $p_1\equiv p_2\equiv 1\pmod q$. Наконец, просуммируем $\kappa_q(n)$ по некоторому отрезку значений q:

$$\Delta_Y^*(n):=\sum_{q\in[Y,z]}\kappa_q(n).$$

Теперь мы хотим показать, что

$$\frac{1}{x}\#\{n \le x \mid \Delta_Y^*(n) \ne \Delta_Y(n)\} \to 0.$$

Действительно, если $\Delta_Y(n) \ne \Delta_Y^*(n)$, то существует по крайней мере одно $q \in$ $\in [Y, z]$, что либо $\kappa_q(n) \ge 2$, либо $\kappa_q(n) = 0$, но в то же время $q^2 \mid \phi(n)$.

Вклад целых $n \le x$ для второй ситуации есть $o(x)$: по лемме 5 для фиксированного q их не более, чем

$$\sum_{n\le x} \sum_{\substack{p\mid n \\ p\equiv 1 \pmod{q^2}}} 1 \le \sum_{\substack{p\le x \\ q^2\mid p-1}} \frac{x}{p} \sim x x_2 q^{-2}.$$

Если же просуммировать последнее выражение по $q \in [Y, z]$, то получится (аналогично вышеприведенным выкладкам для $\sum_{n\le x} E_z(n)$) выражение, действительно равное $o(x)$.

Наконец, покажем, что и ситуация $\kappa_q(n) \ge 2$ асимптотически редка. Поскольку при $\kappa_q(n) \ge 2$ верно $\kappa_q(n) \le \kappa_q(n)\big(\kappa_q(n) - 1\big)$, то перемножая суммы почленно, получим

$$\kappa_q(n) \le \Big(\sum_{\substack{p_1p_2\mid n \\ p_1<p_2}} f_q(p_1,p_2)\Big)\Big(\sum_{\substack{p_1p_2\mid n \\ p_1<p_2}} f_q(p_1,p_2) - 1\Big) =$$

$$= \sum_{\substack{p_1p_2\mid n \\ p_1'p_2'\mid n}} f_q(p_1,p_2) f_q(p_1',p_2') - \sum_{\substack{p_1p_2\mid n \\ p_1<p_2}} f_q(p_1,p_2) = \sum_{\substack{\operatorname{lcm}(p_1p_2,p_1'p_2')\mid n \\ (p_1,p_2)\ne(p_1',p_2')}} f_q(p_1,p_2) f_q(p_1',p_2').$$

Отсюда запишем, для краткости опуская далее условия $p_1 < p_2$ и $p_1' < p_2'$,

$$\sum_{\substack{n\le x \\ \kappa_q(n)\ge 2}} \kappa_q(n) \le \sum_{n\le x} \sum_{\substack{\operatorname{lcm}(p_1p_2,p_1'p_2')\mid n \\ (p_1,p_2)\ne(p_1',p_2')}} f_q(p_1,p_2) f_q(p_1',p_2'). \qquad (*)$$

Правая часть $(*)$ меньше, чем

$$x \sum_{m=3}^{4} \sum_{\substack{p_1\dots p_m\le x \\ p_j\equiv 1 \pmod{q}}} \frac{1}{p_1\dots p_m} \ll x \sum_{m=3}^{4} \left(\frac{x_2}{q}\right)^m \ll \frac{x x_2^3}{q^3}.$$

(Для получения первой оценки мы применили лемму 5.) В силу следствия 2 имеем

$$\sum_{Y<q} q^{-3} \ll \frac{Y^{-2}}{\log Y} \ll \frac{x_3^2}{x_2^4 x_3} = x_2^{-4} x_3,$$

а значит

$$\sum_{Y\le q\le z} \sum_{\substack{n\le x \\ \kappa_q(n)\ge 2}} \kappa_q(n) \ll \frac{x x_3}{x_2} = o(x). \qquad (**)$$

Этим и завершается доказательство того, что $\frac{1}{x}\#\{n \le x \mid \Delta_Y^*(n) \ne \Delta_Y(n)\} \to$ $\to 0$.

Пусть

$$\tau_l(n) = \Delta_Y^*(n)\big(\Delta_Y^*(n)-1\big)\dots\big(\Delta_Y^*(n)-l+1\big),$$

где $l = 0,1,2\dots$ В таком случае $\frac{1}{x}\sum_{n\le x}\tau_l(n)$ по определению есть l-й факториальный момент функции $\Delta_Y^*(n)$.

Применяя лемму 3 к определению $\tau_l(n)$, получим

$$\tau_l(n) = \sum_{\substack{p_1^{(k)}p_2^{(k)}\mid n\\ q_k\in[Y,z]\\ k=1,\dots,l}} \prod_{j=1}^{l} f_{q_j}(p_1^{(j)},p_2^{(j)}),$$

Пусть $\tau_l(n) = \tau_l^{(1)}(n)+\tau_l^{(2)}(n)$, где $\tau_l^{(1)}(n)$ — сумма по всем тем слагаемым, для которых из $i \ne j$ следует $q_i \ne q_j$ и $\{p_1^{(i)},p_2^{(i)}\}\cap\{p_1^{(j)},p_2^{(j)}\} = \varnothing$. К $\tau_l^{(2)}(n)$ отнесем все остальные слагаемые. Тогда

$$\begin{aligned}\sum\nolimits_2 \;&:=\; \sum_{n\le x}\tau_l^{(2)}(n) \ll \sum_{n\le x}\sum_{q}\sum_{\substack{p_1^{(i)}p_2^{(i)}\mid n\\ i=1,2}} f_q(p_1^{(1)},p_2^{(1)})f_q(p_1^{(2)},p_2^{(2)}) +\\ &+\; \sum_{n\le x}\sum_{q_1\ne q_2}\sum_{\substack{p_1^{(i)}p_2^{(i)}\mid n\\ i=1,2}}^{*} f_{q_1}(p_1^{(1)},p_2^{(1)})f_{q_2}(p_1^{(2)},p_2^{(2)}) =: \sum\nolimits_{21}+\sum\nolimits_{22}.\end{aligned}$$

Здесь $q,q_1,q_2\in[Y,z]$, а звездочка над $\sum_{22}^*$ указывает на то, что

$$2 \le \Omega(\operatorname{lcm}(p_1^{(1)}p_2^{(1)},p_1^{(2)}p_2^{(2)})) \le 3.$$

В силу $(**)$ имеем оценку

$$\sum\nolimits_{21} = o(x).$$

Далее, меняя порядок суммирования, имеем

$$\begin{aligned}\sum\nolimits_{22} \;&\ll\; \sum_{q_1\ne q_2}\sum_{\substack{p_1^{(k)},p_2^{(k)}\\ k=1,2}}^{*} f_{q_1}(p_1^{(1)},p_2^{(1)})f_{q_2}(p_1^{(2)},p_2^{(2)})\cdot\frac{x}{\operatorname{lcm}(p_1^{(1)}p_2^{(1)},p_1^{(2)}p_2^{(2)})} \ll\\ &\ll\; x\sum_{q_1\ne q_2}\frac{1}{q_1^2q_2^2}\sum_{j=2}^{3}x_2^j \ll \frac{x}{x_2}\Big(\sum_{Y\le q\le z}\frac{x_2^2}{q^2}\Big)^2.\end{aligned}$$

А в силу леммы 1

$$\frac{x}{x_2}\Big(\sum_{Y\le q\le z}\frac{x_2^2}{q^2}\Big)^2 \ll \frac{x}{x_2}\left(\frac{x_2^2}{Y\log Y}\right)^2 = o(x),$$

ибо $\frac{x_2^2}{Y\log Y} \ll x_3$.

Отсюда вся $\sum_2 = o(x)$. Остается оценить $\tau_l^{(1)}$. Запишем по лемме 4, что

$$\sum\nolimits_1 := \sum_{n\le x}\tau_l^{(1)}(n) = \sum_{\substack{q_1<\ldots<q_l\\ q_j\in[Y,z]}} U(x,q_1^2\ldots q_l^2) = \frac{x}{2^l}\sum_{\substack{q_1<\ldots<q_l\\ q_j\in[Y,z]}}\frac{x_2^{2l}}{q_1^2\ldots q_l^2} + O\left(\frac{x}{x_2^\delta}\right) = \\ = \frac{x}{2^l l!}\Big(\sum_{q\in[Y,z]}\frac{x_2^2}{q^2}\Big)^l + O\left(\frac{x}{x_2^\delta}\right).$$

Здесь множитель $l!$ появляется в знаменателе правой части, т. к. там уже не учитывается упорядоченность q_i по возрастанию. Далее, в силу леммы 1

$$\sum_{Y<q<z} q^{-2} = \frac{\pi(z-1)-\pi(Y)}{z^2} + \int_{Y+1}^{z-1} 2\pi(u)u^{-3}\,du \sim 2\int_Y^z \frac{du}{u^2\log u} \sim \\ \sim [\text{в силу } 2x_3 = \log z \sim \log Y] \sim x_3^{-1}\int_Y^z u^{-2}\,du = x_3^{-1}u^{-1}\Big|_z^Y \sim \frac{1}{bx_2^2}.$$

поэтому

$$\frac{1}{x}\sum\nolimits_1 = \frac{1}{2^l l!}\Big(\frac{x_2^2}{bx_2^2}\Big)^l + o(1) = \frac{1}{(2b)^l l!} + o(1).$$

Обозначим, как и в условии теоремы, $\lambda := 1/2b$.

Теперь, принимая во внимание теорему Frechet—Shohat (см. [4]) и то, что $\frac{\lambda^l}{l!}$ являются факториальными моментами распределения Пуассона, мы получаем

$$\lim_{x\to\infty}\frac{1}{x}\#\{n\le x \mid E_Y(n) = k\} = \lim_{x\to\infty}\frac{1}{x}\#\{n\le x \mid \Delta_Y^*(n) = k\} = \frac{\lambda^k}{k!}e^{-\lambda}.$$

Действительно, характеристическая функция распределения Пуассона $\phi(t) = e^{\lambda(e^{it}-1)}$ регулярна во всей комплексной плоскости, а значит моменты однозначно определяют значения вероятностей.

2.4. Доказательство теоремы 2

Пусть $q \in [c_1x_2^2/x_3, c_2x_2^2/x_3]$ — простое число, где $0 < c_1 < c_2$.

Введем $\mathfrak{M}_q$, состоящее из чисел вида $m = p_1p_2$, где p_1 и p_2 — различные простые, причем $q \mid (p_1-1)$ и $q \mid (p_2-1)$. Для некоторого x обозначим через $E_{q,\epsilon}$ множество тех $m \in \mathfrak{M}_q$, для которых $P(m) = \max\{p_1,p_2\} \le x^\epsilon$.

Пусть $N_{q,x} := \big\{n \;\big|\; n\le x, \mu^2(n) = 1, q^2 \mid \phi(n)\big\}$. Тогда

$$\#N_{q,x} \asymp U(x,q^2) = \frac{xx_2^2}{2q^2} \asymp \frac{xx_3^2}{x_2^2}.$$

Множество $N_{q,x}$ состоит из чисел, делящихся на $m = p_1p_2 \in \mathfrak{M}_q$.

Для фиксированного $\omega \in E_{q,\epsilon}$ введем $N_{q,x}^{(\omega)} := \{n\omega \le x \mid \mu^2(n\omega) = 1\}$. Очевидно, что для любого ω верно вложение $N_{q,x}^{(\omega)} \subset N_{q,x}$. Тогда рассмотрим множество

$$N^* := N_{q,x} \setminus \bigcup_{\omega \in E_{q,\epsilon}} N_{q,x}^{(\omega)}.$$

Мы хотим показать, что $\#N^* = o(\#N_{q,x})$. В силу сказанного выше о составе $N_{q,x}$ остается получить оценку для чисел из него, обладающих простым делителем, превосходящим x^ϵ. Но совершенно очевидно, что

$$\frac{x}{x^\epsilon} \ll o(\#N_{q,x}).$$

Далее, в процессе доказательства теоремы 1 была введена функция $\kappa_q(n)$ и доказано, что

$$\#\{n \le x \mid \kappa_q(n) \ge 2\} \ll \frac{xx_2^3}{q^3} \ll \frac{xx_3^3}{x_2^3}.$$

Ясно, что если $\omega_1 \ne \omega_2$ и $n \in N_{q,x}^{(\omega_1)} \cap N_{q,x}^{(\omega_2)}$, то $\kappa_q(n) \ge 2$. Поэтому

$$\sum_{\substack{\omega_1 \ne \omega_2 \\ \omega_1, \omega_2 \in E_{q,\epsilon}}} \#(N_{q,x}^{(\omega_1)} \cap N_{q,x}^{(\omega_2)}) = o(\#N_{q,x}).$$

Пусть $\omega \in E_{q,\epsilon}$ и пусть $q_1 \ne q$. Если $q_1^2 \mid \phi(n)$, то, очевидно, $q_1^2 \mid \phi(n\omega)$. Оценим количество $K(q_1)$ всех тех $n\omega \le x$, для которых $\mu^2(n\omega) = 1$, $q_1^2 \mid \mid \phi(n\omega)$, но $q_1^2 \nmid \phi(n)$. Пользуясь установленными выше фактами о N^* и $N_{q,x}^{(\omega_1)} \cap N_{q,x}^{(\omega_2)}$, имеем

$$K(q_1) \ll q_1^{-2} \#N_{q,x}.$$

Теперь, суммируя по $q_1 \in (q, x_2^2)$, мы получим, что общее количество тех $n\omega$, для которых $\mu^2(n\omega) = 1$,$q_1^2 \mid \phi(n\omega)$ и $q_1^2 \nmid \phi(n)$ хотя бы для одного из $q_1 \in \in (q, x_2^2)$ не больше, чем $o(\#N_{q,x})$. Действительно,

$$\sum_{q < q_1 < x_2^2} q_1^{-2} \ll \frac{\pi(x_2^2)}{q^2} = o(1).$$

По определению, ненулевое значение $E_q(n)$ как раз говорит о наличии $q_1 > > q$, такого, что $q_1^2 \mid \phi(n)$, а значит $q_1^2 \mid \phi(n\omega)$. Поэтому, используя результат теоремы 1, получим оценку искомой величины в виде

$$\#\{n \le x \mid \gamma(n) = q, \mu^2(n) = 1\} = \sum_{\substack{n \le x \\ q^2 \mid \phi(n) \\ \mu^2(n) = 1 \\ E_q(n) = 0}} 1 = \sum_{\omega \in E_{q,\epsilon}} \sum_{\substack{n \le x/\omega \\ \mu^2(n) = 1 \\ E_q(n) = 0}} 1 + o(\#N_{q,x}) =$$

$$= \sum_{\omega \in E_{q,\epsilon}} \#\{n \le x/\omega \mid \mu^2(n) = 1, E_q(n) = 0\} + o(x) = \sum_{\omega \in E_{q,\epsilon}} \frac{6}{\pi^2} \frac{x}{\omega} e^{-\lambda_q} + o(x),$$

где $\lambda_q = \frac{x_2^2}{2qx_3}$. Наконец, применяя лемму 5,

$$\sum_{\omega\in E_{q,\epsilon}} \frac{1}{\omega} = \sum_{\substack{p_1p_2\le x^\epsilon \\ p_1<p_2 \\ q|(p_1-1) \\ q|(p_2-1)}} \frac{1}{p_1p_2} = \frac{1}{2} \sum_{\substack{p_1\le x^\epsilon \\ q|(p_1-1)}} \frac{1}{p_1} \sum_{\substack{p_2\le x^\epsilon/p_1 \\ q|(p_2-1)}} \frac{1}{p_2} = (1+o(1))\frac{x_2^2}{2q^2}.$$

Подставив это в выражение для $\#\{n \le x \mid \gamma(n) = q, \mu^2(n) = 1\}$, сразу получим утверждение теоремы.

ЛИТЕРАТУРА

1. Banks W. D., Luca F., Shparlinski I. E. Arithmetic properties of $\phi(n)/\lambda(n)$ and the structure of the multiplicative group modulo n. // Comm. Math. Helv.,— 2006.— **81.**— С. 1–22.
2. Cameron P. J., Preece D. A. Notes on primitive lambda-roots. — http://www.maths.qmw.ac.uk/∼pjc/csgnotes/lambda.pdf.
3. Carmichael R. D. Note on a new number theory function. // Bull. Amer. Math. Soc.,— 1909–10.— **16.**— С. 232–238.
4. Elliot P. D. T. A. Probabilistic number theory.— New-York: Springer, 1973.— 476 с.
5. Erdős P., Pomerance C., Schmutz E. Carmichael's lambda function. // Acta Arith.,— 1991.— **58.**— С. 363–385.
6. Kátai I. On the prime power divisors of iterates of $\phi(n)$ and $\sigma(n)$.— Preprint, E. Lorand University, Budapest, 2007.
7. Kátai I. Some results on the Carmichael's and on the Euler's ϕ function. // Acta Math. Hungar., (to appear).
8. De Koninck J. M., Kátai I. On the distribution of subsets of primes in the prime factorization of integers. // Acta Arith.,— 1995.— **72.**— С. 169–200.
9. Norton K. K. On the number of restricted prime factors of an integer I. // Illinois J. Math.,— 1976.— **20.**— С. 681–705.
10. Pomerance C. On the distribution of amicable numbers. // J. Reine Angew. Math.,— 1977.— **293/294.**— С. 217–222.
11. Карацуба А. А. Основы аналитической теории чисел.— М.: УРСС, 2004.— 184 с.
12. Прахар К. Распределение простых чисел.— М.: Мир, 1967.— 512 с.

Статья получена: 25.06.2009; окончательный вариант: 25.10.2009; принята: 15.11.2009.