УДК 511.33 DOI 10.17223/20710410/66/3

ПЕРИОДИЧЕСКИЕ МУЛЬТИПЛИКАТИВНЫЕ АРИФМЕТИЧЕСКИЕ ФУНКЦИИ

Е. В. Кайгородов

Горно-Алтайский государственный университет, г. Горно-Алтайск, Россия

E-mail: gazetaintegral@gmail.com

Вводятся понятия периодической мультипликативной функции, основного модуля такой функции, простейшей периодической мультипликативной функции. Изучаются основные свойства периодических мультипликативных функций, а также даётся их полное описание через характеры Дирихле. В частности, доказывается, что всякая отличная от единичной периодическая мультипликативная функция единственным образом представляется в виде произведения простейших периодических мультипликативных функций, причём основные модули таких функций представляют собой степени простых чисел, произведение которых есть каноническое разложение основного модуля исходной функции. На основании этого представления исследование периодических мультипликативных функций сводится к исследованию простейших периодических мультипликативных функций. Полученные результаты подводят к полному описанию периодических мультипликативных функций.

Ключевые слова: *арифметическая функция, периодическая мультипликативная функция, характер Дирихле, L-функция Дирихле.*

PERIODIC MULTIPLICATIVE ARITHMETIC FUNCTIONS

E. V. Kaigorodov

Gorno-Altaisk State University, Gorno-Altaisk, Russia

The notions of a periodic multiplicative function, the main modulus of such function, and the simplest periodic multiplicative function have been introduced. The basic properties of periodic multiplicative functions are studied, and a complete description of such functions through Dirichlet characters is given. In particular, it has been proven that any periodic multiplicative function other than unitary can be uniquely represented as a product of the simplest periodic multiplicative functions, and the principal modules of such functions are powers of prime numbers, the product of which is the canonical decomposition of the principal module of the original function. Based on this representation, the study of periodic multiplicative functions is reduced to the study of the simplest periodic multiplicative functions. The obtained results lead to a complete description of periodic multiplicative functions.

Keywords: *arithmetic function, periodic multiplicative function, Dirichlet character, Dirichlet L-function.*

Введение

Определение 1. Периодической мультипликативной функцией будем называть числовую функцию $f(n)$ натурального аргумента со следующими свойствами:

1) $f(n)$ отлична от тождественного нуля;
2) $f(n)$ мультипликативна, то есть $f(mn) = f(m)f(n)$ для любых взаимно простых натуральных чисел m и n;
3) $f(n)$ периодична, то есть найдётся такое натуральное число m, называемое периодом, что $f(n+m) = f(n)$ для любого n.

Пусть периодические мультипликативные функции $f(n)$ и $g(n)$ имеют период m. Нетрудно видеть, что в силу периодичности обеих функций они тождественно равны тогда и только тогда, когда их значения совпадают на некоторой полной системе вычетов по модулю m. Это значит, что любая периодическая мультипликативная функция однозначно определяется заданием своих значений на полной системе вычетов по модулю m.

Наименьший среди всех периодов обозначим буквой k и назовём основным модулем периодической мультипликативной функции $f(n)$. Чтобы указать, что число k является основным модулем функции $f(n)$, будем эту функцию записывать в виде $f(n,k)$. Эти и все другие обозначения, а также терминология в данной работе стандартны и заимствованы из [1].

Систематически изучать периодические мультипликативные функции начал, по-видимому, Г. Канольд, установивший в [2, 3] их простейшие свойства. Периодические арифметические функции привлекали внимание Т. М. Апостола — им посвящён § 27.10 фундаментального справочника коллектива авторов [4]. А. Конси и Т. Макгенри в [5] описали интересные примеры использования некоторых мультипликативных арифметических функций вместе с шифром Хилла в криптографии с открытым ключом.

В настоящее время изучение арифметических функций, их важнейших классов и свойств оправдано потребностями практики. На наш взгляд, именно актуальные проблемы криптографии побуждают сейчас специалистов заниматься вопросами описания конкретных классов функций и конструированием новых арифметических функций с определёнными свойствами, с использованием которых впоследствии, возможно, будут разработаны криптосистемы для постквантовой криптографии. Так, в декабре 2022 г. группа китайских ученых предложила способ взлома 2048-битного ключа криптосистемы RSA и допустила возможность реализации этого способа в будущем на квантовом компьютере с 372 физическими кубитами и глубиной квантовой схемы более 1000 [6]. Это обстоятельство даёт мощный толчок к ускорению теоретико-числовых исследований в области постквантовой криптографии. Крайне необходимо, чтобы такая система была построена и получила уверенное развитие к моменту квантового взлома.

Известно, что ключ дешифрования криптосистемы RSA определяется по функции Эйлера $\varphi(n)$, которая представляет собой классический пример мультипликативной арифметической функции в теории чисел. Свойства функции Эйлера позволили ей сыграть важную роль в построении названной криптосистемы. Эти факты наводят на мысль о вероятном создании в обозримом будущем криптосистем, в которых найдут применение новые арифметические функции с наперёд заданными свойствами, «заточенными» под специфику разрабатываемых квантовых алгоритмов шифрования. Задача поиска и изучения таких функций в некоторой мере смежна с проблемой описания конкретных классов арифметических (в частности, мультипликативных) функ-

ций. Понимание строения периодических мультипликативных арифметических функций может помочь в дальнейшем получить новые арифметические функции, пригодные для использования в постквантовых криптосистемах.

Следуя в основных чертах методу первой главы книги Н. Г. Чудакова [1], можно полностью описать строение периодических мультипликативных функций.

1. Основные свойства периодических мультипликативных функций

Теорема 1 [1, теорема 2]. Произведение конечного числа периодических мультипликативных функций есть также периодическая мультипликативная функция, основной модуль которой равен делителю наименьшего общего кратного основных модулей сомножителей, этот модуль равен произведению основных модулей сомножителей, если последние попарно взаимно просты.

Следующее простое утверждение по существу совпадает с теоремой 1 работы [3].

Теорема 2. Пусть имеем периодическую мультипликативную функцию $f(n,k)$. Существует характер Дирихле $\chi(n,k')$, где $k' \mid k$, такой, что $f(n,k) = \chi(n,k')$ для взаимно простых n и k.

Доказательство. Рассмотрим функцию $g(n) = f(n,k)\chi_0(n,k'')$, где k'' — произведение всех простых чисел, входящих в каноническое разложение k; $\chi_0(n,k'')$ — главный характер. Из теоремы 1 следует, что $g(n)$ — периодическая мультипликативная функция, причём её основной модуль k' делит наименьшее общее кратное чисел k и k'', равное k. Но если $p \nmid k$, то, как легко показать индукцией, $f(p^\alpha) = (f(p))^\alpha$: для $\alpha = 1$ это очевидно, а если это верно для данного α, то $(f(p))^{\alpha+1} = (f(p))^\alpha f(p) = f(p^\alpha)f(p+k) = f(p^{\alpha+1} + p^\alpha k) = f(p^{\alpha+1})$. Если же $p \mid k$, то $g(p^\alpha) = 0$. Значит, функция $g(n)$ вполне мультипликативна и является характером Дирихле. ■

Лемма 1. Если $(a,m) = 1$, n — натуральное число, то найдётся такое натуральное число x, что $(a + mx, n) = 1$.

Доказательство. Следует из теоремы Дирихле о простых числах в арифметической прогрессии. ■

Лемма 2. Пусть $A_i(x) = a_i + m_i x$, $d_i = (a_i, m_i)$; $(d_i, d_j) = 1$ при $i \neq j$, $i,j = 1,2,\ldots,\nu$. Тогда существует ν натуральных чисел $x_1, x_2, \ldots, x_\nu$, таких, что числа $A_1(x_1), A_2(x_2), \ldots, A_\nu(x_\nu)$ попарно взаимно просты.

Доказательство. Положим $a_i = a'_i d_i$, $m_i = m'_i d_i$, $A_i(x) = A'_i(x)d_i$. Тогда $A_i(x) = d_i(a'_i + m'_i x)$, причём $(a'_i, m'_i) = 1$. По лемме 1 найдётся такое натуральное число x_1, что $A'_1(x_1)$ взаимно просто с $d_1 d_2 \ldots d_\nu$. Далее, найдётся такое натуральное число x_2, что $A'_2(x_2)$ взаимно просто с $d_1 d_2 \ldots d_\nu A'_1(x_1)$, и т. д. Наконец, найдётся такое натуральное число x_ν, что $A'_\nu(x_\nu)$ взаимно просто с $d_1 d_2 \ldots d_\nu A'_1(x_1) A'_2(x_2) \ldots A'_{\nu-1}(x_{\nu-1})$. Очевидно, числа $x_1, x_2, \ldots, x_\nu$ — искомые. ■

Теорема 3. Пусть k — основной модуль периодической мультипликативной функции $f(n,k)$ и $k = k_1 k_2 \ldots k_\nu$, где все k_i попарно взаимно просты. Тогда существует единственная система периодических мультипликативных функций $f_1(n), f_2(n), \ldots, f_\nu(n)$, основные модули которых соответственно равны $k_1, k_2, \ldots, k_\nu$ и таковы, что $f(n) = f_1(n)f_2(n)\ldots f_\nu(n)$. При этом области значений функций $f_1(n)$, $f_2(n)$, …, $f_\nu(n)$ суть части области значений функции $f(n)$.

Доказательство. Пусть дано произвольное целое число $i \leqslant \nu$. Для каждого n определим (как в [1, теорема 3]) число n_i условиями

$$n_i \equiv n \pmod{k_i}, \quad n_i \equiv 1 \pmod{k_j} \text{ для всех } i \neq j. \tag{1}$$

Полагаем теперь $f_i(n) = f(n_i)$. Все n_i для данного n образуют один класс вычетов по модулю k, поэтому функция $f_i(n)$ определена однозначно. Ясно, что $f_i(1) = 1$, откуда следует, что функция $f_i(n)$ отлична от тождественного нуля.

Для произвольных взаимно простых чисел m и n имеем по определению m_i и n_i:

$$\begin{aligned} m_i &\equiv m \pmod{k_i}, \qquad m_i \equiv 1 \pmod{k_j}, \\ n_i &\equiv n \pmod{k_i}, \qquad n_i \equiv 1 \pmod{k_j}, \quad i \neq j. \end{aligned} \tag{2}$$

Перемножая сравнения, получаем $m_i n_i \equiv mn \pmod{k_i}$, $m_i n_i \equiv 1 \pmod{k_j}$, $i \neq j$. Отсюда имеем $f_i(mn) = f(m_i n_i) = f(m_i) f(n_i) = f_i(m) f_i(n)$, если числа m_i и n_i взаимно просты. Однако их можно такими выбрать. Действительно, если $(m_i, n_i) = d > 1$, то $(d, k) = 1$, так как в противном случае существовало бы такое простое число p, что $p \mid d$, $p \mid k$ и $p \mid k_i$ — потому что в силу (2) $p \not| k_j$ при $i \neq j$ и, наконец, $p \mid m_i$, $p \mid n_i$, откуда $p \mid m$ и $p \mid n$.

Из взаимной простоты чисел d и k по лемме 2 следует существование таких натуральных чисел x и y, что $(m_i + kx, n_i + ky) = 1$, поскольку $((m_i, k), (n_i, k)) = (d, k) = 1$.

Мультипликативность функции $f_i(n)$ доказана. Периодичность доказывается так же, как в [1, теорема 3].

Полагая $i = 1, 2, \ldots, \nu$, получим ν функций $f_1(n), f_2(n), \ldots, f_\nu(n)$. Покажем, что $f(n) = f_1(n) \cdot f_2(n) \cdot \ldots \cdot f_\nu(n)$. Это можно сделать по аналогии с [1, теорема 3], если доказать, что для данного n числа $n_1, n_2, \ldots, n_\nu$ можно выбрать попарно взаимно простыми. Положим для этого $K_i = k/k_i$. Рассмотрим арифметические прогрессии $n_i + kx$, где $i = 1, 2, \ldots, \nu$, и обозначим (n_i, k) через d_i. Имеем $(n_i, k_i) = d_i$, так как $(n_i, K_i) = 1$ в силу (1). Но $(k_i, k_j) = 1$ при $i \neq j$, а $d_i \mid k_i$, поэтому $(d_i, d_j) = 1$. Остаётся применить лемму 2.

Конец доказательства переносится сюда из [1] без изменений. ■

Теорема 3 показывает, что всякая отличная от единичной периодическая мультипликативная функция единственным образом представляется произведением вида

$$f(n, p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_\nu^{\alpha_\nu}) = f(n, p_1^{\alpha_1}) f(n, p_2^{\alpha_2}) \ldots f(n, p_\nu^{\alpha_\nu}).$$

2. Строение периодических мультипликативных функций

Изучим строение простейших периодических мультипликативных функций, то есть функций вида $f(n) = f(n, p^\alpha)$. Будем считать, что $\alpha \geqslant 1$ (иначе получается единичная функция). Примем обозначения: $\chi(n, p^\beta)$, $\beta \leqslant \alpha$, — характер Дирихле, соответствующий периодической мультипликативной функции $f(n, p^\alpha)$ в силу теоремы 2; $a_\nu = f(p^\nu)$, $\nu = 1, 2, \ldots$

Теорема 4. При $\nu \geqslant \alpha$ справедливо равенство $a_\nu = a_\alpha$. Если при этом характер $\chi(n)$ неглавный, то $a_\alpha = 0$.

Доказательство. Так как p^α — период функции $f(n)$, то при $\nu \geqslant \alpha$ получаем $a_\nu = f(p^\nu) = f(p^\alpha) = a_\alpha$. Пусть теперь характер $\chi(n, p^\beta)$ неглавный, тогда существует такое c, что $\chi(c) \neq 0$ и $\chi(c) \neq 1$. Для этого c будем иметь $\chi(c) a_\alpha = f(cp^\alpha) = f(p^\alpha) = a_\alpha$, откуда $a_\alpha = 0$. ■

Теорема 5. Пусть

$$f(n) = \begin{cases} \chi(n, p^\gamma), & \text{если } p \nmid n, \\ a_\nu, & \text{если } n = p^\nu, \end{cases}$$

причём $a_\beta \neq a_{\beta+1} = a_{\beta+2} = \ldots$ и $a_\beta = 0$, если характер $\chi(n)$ неглавный. Тогда $f(n)$ есть периодическая мультипликативная функция основного модуля p^α, где $\alpha = \beta + \gamma$.

Доказательство. Мультипликативность $f(n)$ очевидна. Непосредственной проверкой легко установить, что $p^{\beta+\gamma}$ есть период $f(n)$. Допустим теперь, что $p^{\beta+\gamma-1}$ — тоже период $f(n)$. Тогда если $\gamma = 1$, то $a_{\beta+1} = f(p^{\beta+1}) = f(p^\beta) = a_\beta$, что противоречит определению функции $f(n)$. Если $\gamma > 1$, то характер $\chi(n)$ неглавный, то есть $a_\beta = 0$. Возьмём число n, для которого $\chi(n) \neq \chi(n + p^{\gamma-1})$, очевидно, $p \nmid n$. Мы допустили, что $p^{\beta+\gamma-1}$ — период $f(n)$, поэтому

$$a_\beta \chi(n + p^{\gamma-1}) = f(p^\beta(n + p^{\gamma-1})) = f(np^\beta) = a_\beta \chi(n),$$

откуда $a_\beta = 0$, поскольку $\chi(n) \neq \chi(n + p^{\gamma-1})$. Снова пришли к противоречию. ■

Теоремы 1–5 полностью описывают строение периодических мультипликативных функций через характеры Дирихле.

Теперь можно установить связь между функциями

$$L(s, f) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$$

и классическими L-функциями Дирихле.

Пусть k — основной модуль периодической мультипликативной функции $f(n)$, а $\chi(n)$ — характер Дирихле, соответствующий функции $f(n)$ в силу теоремы 2. При $\operatorname{Re} s > 1$ имеем

$$L(s, f) = \prod_p \left(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \ldots\right) =$$

$$= \prod_{p \nmid k} \left(1 + \frac{\chi(p)}{p^s} + \frac{\chi(p^2)}{p^{2s}} + \ldots\right) \prod_{p \mid k} \left(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \ldots\right) =$$

$$= L(s, \chi) \prod_{p \mid k} \left(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \ldots\right).$$

Пусть $p^\alpha \mid k$. По теореме 3 запишем $f(n, k) = f_1(n, p^\alpha) f_2(n, k/p^\alpha)$. Значит,

$$f(p^\nu) = f_1(p^\nu) f_2(p^\nu) = a_\nu \chi_2(p^\nu) = a_\nu (\chi_2(p))^\nu = a_\alpha (\chi_2(p))^\nu$$

при $\nu \geqslant \alpha$. Поэтому

$$\sum_{\nu=0}^{\infty} \frac{(f(p))^\nu}{p^{\nu s}} = \sum_{\nu=0}^{\alpha-1} a_\nu \left(\frac{\chi_2(p)}{p^s}\right)^\nu + a_\alpha \sum_{\nu=\alpha}^{\infty} \left(\frac{\chi_2(p)}{p^s}\right)^\nu$$

является рациональной функцией (и даже многочленом, если окажется $a_\alpha = 0$) от p^{-s}. Таким образом, $L(s, f) = L(s, \chi) F(s)$, где χ — соответствующий f характер; $F(s)$ — произведение рациональных функций (и даже многочленов, если характер χ первообразный) от p^{-s} по всем p, делящим основной модуль периодической мультипликативной функции $f(n)$. Легко видеть, что в случае непервообразного характера $\chi(n)$ полюсы функции $F(s)$ гасятся тривиальными нулями $L(s, \chi)$, лежащими на прямой $\operatorname{Re} s = 0$.

Заключение

В работе полностью описано строение периодических мультипликативных арифметических функций через характеры Дирихле. Для решения этой задачи использованы методы теории характеров, предложенные советским математиком Н. Г. Чудаковым. Применение этих методов к изучению периодических мультипликативных арифметических функций дало вполне удовлетворительный результат, что говорит об их универсальности и потенциальной возможности распространения на смежные проблемы аналитической и мультипликативной теории чисел.

ЛИТЕРАТУРА

1. *Чудаков Н. Г.* Введение в теорию L-функций Дирихле. М.: ОГИЗ, 1947. 202 с.
2. *Kanold H. J.* Über periodische multiplikative zahlentheoretische Funktionen // Math. Ann. 1961. V. 144. P. 135–141. (in German)
3. *Kanold H. J.* Über periodische zahlentheoretische Funktionen // Math. Ann. 1962. V. 147. P. 269–274. (in German)
4. *Frank W. O., Daniel W. L., Ronald F. B., and Charles W. C.* NIST Handbook of Mathematical Functions. 1st. ed. Cambridge: Cambridge University Press, 2010. 966 p.
5. *Conci A. and MacHenry T.* Cryptography and multiplicative arithmetic functions // 2015 IEEE Intern. Conf. on Industrial Technology (ICIT). Seville, Spain, 2015. P. 1515–1519.
6. *Yan B., Tan Z., Wei S., et al.* Factoring Integers with Sublinear Resources on a Superconducting Quantum Processor. `https://arxiv.org/abs/2212.12372`. 2022.

REFERENCES

1. *Chudakov N. G.* Vvedenie v teoriyu L-funktsiy Dirikhle [Introduction to the theory of Dirichlet L-functions]. Moscow, OGIZ Publ., 1947. 202 p. (in Russian)
2. *Kanold H. J.* Über periodische multiplikative zahlentheoretische Funktionen. Math. Ann., 1961, vol. 144, pp. 135–141.
3. *Kanold H. J.* Über periodische zahlentheoretische Funktionen. Math. Ann., 1962, vol. 147, pp. 269–274.
4. *Frank W. O., Daniel W. L., Ronald F. B., and Charles W. C.* NIST Handbook of Mathematical Functions, 1st. ed. Cambridge, Cambridge University Press, 2010. 966 p.
5. *Conci A. and MacHenry T.* Cryptography and multiplicative arithmetic functions. 2015 IEEE Intern. Conf. on Industrial Technology (ICIT), Seville, Spain, 2015, pp. 1515–1519.
6. *Yan B., Tan Z., Wei S., et al.* Factoring Integers with Sublinear Resources on a Superconducting Quantum Processor. `https://arxiv.org/abs/2212.12372`, 2022.