ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Октябрь–декабрь 2023. Т. 30, № 4. С. 35–45

УДК 519.7 DOI 10.33048/daio.2023.30.775

О СООТНОШЕНИЯХ, СВЯЗАННЫХ С ФУНКЦИЕЙ ЭЙЛЕРА

В. К. Леонтьев[a], *Э. Н. Гордеев*[b]

Вычислительный центр им. А. А. Дородницына ФИЦ ИУ РАН,
ул. Вавилова, 40, 119333 Москва, Россия

E-mail: [a] vkleontiev@yandex.ru, [b] werhorn@yandex.ru

Аннотация. Исследуются свойства множества чисел, меньших и взаимно простых с n, с введённой на нём операцией умножения по модулю n (этот объект иногда называют группой Эйлера). Мощность такого множества — известная функция Эйлера $\varphi(n)$, которая является одной из классических функций теории чисел. Области её применения достаточно широкие и включают, например, различные разделы дискретной математики, а также имеют существенные приложения в криптографии. В работе рассматриваются различные комбинаторные задачи, возникающие при исследовании группы Эйлера и функции Эйлера. Выведены соотношения между теоретико-числовыми параметрами, связанными с группой Эйлера и функцией Эйлера. Полученные в работе комбинаторные соотношения могут быть использованы при решении прикладных комбинаторных проблем и в криптографии. Библиогр. 10.

Ключевые слова: делитель числа, функция Эйлера, группа Эйлера, числа Стирлинга, функция Мёбиуса, производящая функция.

Введение

Функция Эйлера $\varphi(n)$ — число натуральных чисел, меньших и взаимно простых с n — одна из классических функций теории чисел, встречающаяся в различных разделах дискретной математики.

Группой Эйлера называется мультипликативная группа взаимно простых с n вычетов по модулю n (см., например, [1]). Таким образом, группа Эйлера является коммутативной группой порядка $\varphi(n)$.

Функции Эйлера посвящены многочисленные работы известных математиков — Ферма, Эйлера, Гаусса, Лежандра, Якоби и др. (см., например, [2–4]). Группа Эйлера также привлекала внимание многих исследователей (см., например, [1, 4, 5]). Подобные исследования актуальны

в настоящее время как для прикладных проблем в дискретной математике (см., например, [1, 4]), так и в криптографии [3]. Функция Эйлера и её свойства до сих пор привлекают внимание исследователей [1, 6, 7].

Некоторые из приведённых здесь результатов были изложены нами ранее в работе [8].

В гл. 17 тома 3 классической справочной книги [9] сформулирован ряд задач и дан обзор некоторых комбинаторных соотношений в исследуемой нами области (с. 195–200). Таким образом, полученные в работе результаты дополняют и расширяют поднятую ранее проблематику.

1. Основная часть

Пусть n — натуральное число и

$$M_n = \{x \in \mathbb{N} \mid (x, n) = 1,\ x \leqslant n\}.$$

Таким образом, M_n — это множество натуральных чисел, не превосходящих n и взаимно простых с n ((a, b) — как обычно — это наибольший общий делитель чисел a и b). Множество M_n с операцией умножения по модулю n является группой $\mathcal{M}_n$, которая носит имя Эйлера. Число элементов $\varphi(n)$ группы $\mathcal{M}_n$ — это функция Эйлера.

Два классических выражения для функция $\varphi(n)$ хорошо известны:

$$\varphi(n) = n \sum_{d \,|\, n} \frac{\mu(d)}{d},$$

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

Здесь $\mu(d)$ — это функция Мёбиуса, определяемая следующим образом. Пусть $d = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_k^{\gamma_k}$ — каноническое представление натурального числа в виде произведения степеней простых чисел. Тогда

$$\mu(d) = \begin{cases} 1, & \text{если } d = 1, \\ 0, & \text{если } \gamma_i \geqslant 2 \text{ для некоторого } i, \\ (-1)^{\sum\limits_{i=1}^{k} \gamma_i} & \text{иначе.} \end{cases} \tag{1}$$

Ниже будут приведены доказательства нескольких соотношений, связанных со свойствами группы Эйлера $\mathcal{M}_n$.

Теорема 1. *Справедливо соотношение*

$$\mathbb{F}_n(z) = \sum_{(m,n)=1} z^m = \sum_{d \,|\, n} \frac{\mu(d)}{1 - z^d}. \tag{2}$$

Доказательство. Пусть ξ_p^m — предикат делимости натурального m на простое число p, т. е. $\xi_p^m = 1$, если p делит m, и $\xi_p^m = 0$ в противном случае. Тогда при $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ имеем

$$\sum_{(m,n)=1} z^m = \sum_{m=0}^{\infty} z^m \bigl(1 - \xi_{p_1}^m\bigr) \dots \bigl(1 - \xi_{p_k}^m\bigr).$$

Отсюда при $|z| < 1$ последовательно получаем

$$\mathbb{F}_n(z) = \sum_{m=0}^{\infty} z^m - \sum_i \sum_{m=0}^{\infty} z^m \xi_{p_i}^m + \sum_{i<j} \sum_{m=0}^{\infty} z^m \xi_{p_i}^m \xi_{p_j}^m - \dots.$$

Далее заметим, что

$$\sum_{m=0}^{\infty} z^m \xi_{p_i}^m = \sum_{r=0}^{\infty} z^{rp_i} = \frac{1}{1 - z^{p_i}},$$
$$\sum_{m=0}^{\infty} z^m \xi_{p_i}^m \xi_{p_j}^m = \sum_{r=0}^{\infty} z^{rp_ip_j} = \frac{1}{1 - z^{p_ip_j}}$$

и т. д., поэтому выполняется соотношение

$$\sum_{(m,n)=1} z^m = \sum_{m=0}^{\infty} z^m - \sum_{i=1}^{k} \sum_{r=0}^{\infty} z^{rp_i} + \sum_{1 \leqslant i < j \leqslant k} \sum_{r=0}^{\infty} z^{rp_ip_j} - \dots$$
$$= \frac{1}{1-z} - \sum_{p \,|\, n} \frac{1}{1 - z^p} + \sum_{\substack{p<q, \\ p \,|\, n,\, q \,|\, n}} \frac{1}{1 - z^{pq}} - \dots. \quad (3)$$

Выражение (2) можно получить из (3) с использованием свойства (1) функции Мёбиуса. Теорема 1 доказана.

Пусть $M_n = \{1, r_2, \dots, r_N\}$ — элементы группы Эйлера $\mathcal{M}_n$. Здесь $N = \varphi(n)$.

Теорема 2. *Справедлива формула*

$$\varphi_n(z) = \sum_{k=1}^{N} z^{r_k} = \sum_{d \,|\, n} \mu(d) \, \frac{1 - z^n}{1 - z^d}. \quad (4)$$

Доказательство. Пусть $N_n = \{m\}$ — все натуральные числа, взаимно простые с n. Тогда

$$m = x \cdot n + r_i$$

для некоторого натурального x и $r_i \in M_n$. Действительно, делим m на n и отмечаем, что $(n, r_i) = 1$. Отсюда

$$\sum_{(m,n)=1} z^m = \sum_{x,\, r_i} z^{xn+r_i} = \sum_x z^{xn} \sum_{i=1}^{N} z^{r_i} = \frac{1}{1-z^n} \sum_{i=1}^{N} z^{r_i}.$$

Из теоремы 1 получаем

$$\sum_{k=1}^{N} z^{r_k} = \sum_{d\,|\,n} \mu(d) \frac{1-z^n}{1-z^d}.$$

Теорема 2 доказана.

Следствие 1. *Имеет место равенство*

$$N = \varphi(n) = n \sum_{d\,|\,n} \frac{\mu(d)}{d}.$$

Доказательство. Переходя в формуле (4) к пределу при $z \to 1$, получаем

$$N = \varphi(n) = n \sum_{d\,|\,n} \frac{\mu(d)}{d}.$$

Следствие 1 доказано.

Следствие 2. *Имеет место равенство*

$$\varphi(n) = n \prod_{p\,|\,n} \Big(1 - \frac{1}{p}\Big).$$

Доказательство. В силу (1) каждый делитель d в формуле (2) имеет вид $d = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_k^{\gamma_k}$, где $\gamma_i \in \{0, 1\}$, $i = 1, 2, \dots, k$. Отсюда

$$\varphi(n) = n \sum_{\{\gamma_1,\dots,\gamma_k\}} \frac{(-1)^{\gamma_1+\gamma_2+\dots+\gamma_k}}{p_1^{\gamma_1} p_2^{\gamma_2} \dots p_k^{\gamma_k}}$$

$$= n \sum_{\gamma_1=0}^{1} \frac{(-1)^{\gamma_1}}{p_1^{\gamma_1}} \sum_{\gamma_2=0}^{1} \frac{(-1)^{\gamma_2}}{p_2^{\gamma_2}} \cdots \sum_{\gamma_k=0}^{1} \frac{(-1)^{\gamma_k}}{p_k^{\gamma_k}} = n \prod_{p\,|\,n} \Big(1 - \frac{1}{p}\Big).$$

Следствие 2 доказано.

Следствие 1 можно вывести из тождества Гаусса

$$\sum_{d\,|\,n} \varphi(n) = n$$

с помощью формулы обращения Мёбиуса. Вывод следствия 2 также известен. Однако формула (4) позволяет получить гораздо больше информации об элементах группы $\mathcal{M}_n$, чем приведённые следствия из неё. Действительно, с помощью (4) можно в «явном» виде получить любые значения симметрической функции от $(r_1, r_2, \ldots, r_N)$. Имеющиеся утверждения поясняют это замечание.

Следствие 3. *Справедлива формула*

$$\sum_{r\in M_n} r = \frac{n\varphi(n)}{2}. \tag{5}$$

Доказательство. Так как при $n = s \cdot d$ выполняется соотношение

$$\frac{1-z^n}{1-z^d} = 1 + z^d + z^{2d} + \cdots + z^{(s-1)d},$$

из (4) после дифференцирования получаем

$$\varphi_n'(z) = \sum_{k=1}^{N} r_k z^{r_k-1} = \sum_{d\,|\,n} \mu(d) \sum_{r=1}^{\frac{n}{d}-1} rdz^{rd-1}.$$

Отсюда при $z = 1$ имеем цепочку соотношений

$$\sum_{k=1}^{N} r_k = \sum_{d\,|\,n} d\mu(d)\binom{n/d}{2} = \frac{1}{2}\sum_{d\,|\,n} d\mu(d)\Big(\frac{n}{d}-1\Big)\frac{n}{d}$$
$$= \frac{n}{2}\sum_{d\,|\,n}\mu(d)\Big(\frac{n}{d}\Big) - \frac{n}{2}\sum_{d\,|\,n}\mu(d) = \frac{n}{2}\varphi(n).$$

Так как $\sum\limits_{d\,|\,n}\mu(d) = 0$, если $n \neq 1$, окончательно имеем

$$\sum_{r_k\in M_n} r_k = \frac{n}{2}\varphi(n).$$

Следствие 3 доказано.

Замечание. Формулу (5) можно получить без всяких вычислений, если заметить, что из того, что $a \in M_n$, вытекает, что $n - a \in M_n$, и отсюда

$$\sum_{a\in M_n} a = \sum_{a\in M_n} (n-a),$$

что и доказывает (5).

Аналогичные вычисления приводят к следующей формуле [3, 4].

Следствие 4. *Справедливо выражение*

$$\sum_{r\in M_n} r^2 = \frac{n^2}{3}\,\varphi(n) - \frac{\varphi(n)}{6}\,p_1p_2\dots p_k,$$

где $n = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$.

В общем случае, если

$$\varphi_n(z) = \sum_{r_m\in M_n} z^{r_m} = \sum_{a\in M_n} z^a,$$

то

$$\varphi_n^{(k)}(z) = \sum_{r_m\in M_n} r_m(r_m-1)\dots(r_m-k+1)z^{r_m-k} = \sum_{a\in M_n} a(a-1)\dots(a-k+1)z^{a-k}.$$

Так как

$$(a)_k = a(a-1)\dots(a-k+1) = \sum_{r=1}^{k} s(k,r)a^r,$$

где $s(k,r)$ — числа Стирлинга I рода (см. [2]), то

$$\varphi_n^{(k)}(z) = \sum_{a\in M_n} z^{a_m-k}\sum_{r=1}^{k} s(k,r)a^r = \sum_{r=1}^{k} s(k,r)\sum_{a\in M_n} a^r z^{a-k}.$$

Теорема 3. *Справедлива формула*

$$\Phi_n^{(k)}(1) = \sum_{r=1}^{k} s(k,r)\sum_{a\in M_n} a^r. \tag{6}$$

Если

$$S_n(r) = \sum_{a\in M_n} a^r,$$

то из (6) получаем формулу

$$\Phi_n^{(k)}(1) = \sum_{r=1}^{k} s(k,r)S_n(r),$$

которая позволяет последовательно вычислять $S_n(r)$ для $r = 0, 1, \dots$, исходя из значений $\Phi_n^{(k)}(1)$.

Пусть σ_k — k-й элементарный симметрический полином. Тогда, выражая элементарные симметрические полиномы через степенные функции $S_n(r)$, в силу классического соотношения (см., например, [10, § 52])

$$\prod_{x\in M_n}(z-x)=\sum_{k=1}^{\varphi(n)}(-1)^k z^k\sigma_k$$

можно «явно» вычислить элементы группы M_n.

Для множества $M=\{a_1,a_2,\dots,a_r\}$ введём обозначение

$$v\cdot M=\{va_1,va_2,\dots,va_r\}.$$

Пусть

$$M_n^t=\{a\in\mathbb{N}\mid (a,n)=t,\ a\leqslant n\}.$$

Тогда для M_n^t справедливо следующее представление.

Теорема 4. *Имеет место равенство при $t\mid n$.*

$$M_n^t=t\cdot M_{n/t}^1.$$

Доказательство вытекает из того, что при $(a,b)=t$ выполняется равенство $\left(\frac{a}{t},\frac{b}{t}\right)=1$. Теорема 4 доказана.

Примеры. 1. Если $t=2$ и $n=12$, то

$$M_{12}^2=2\cdot\{1,5,7,11\}=\{2,10,2,10\}=\{2,10\}.$$

Действительно, $\left|M_{12}^2\right|=\left|M_6^1\right|=|\{1,5\}|=2$, т. е. $M_6^1=\{1,5\}$, $M_{12}^2=2\cdot\{1,5\}=\{2,10\}$.

2. Если $t=4$ и $n=8$, то

$$M_8^4=4\cdot\{1,3,5,7\}=\{4,4,4,4\}=\{4\}.$$

Действительно, $M_8^4=4\cdot M_2^1=4\cdot\{1\}=\{4\}$.

В терминах производящих функций все приведённые выше рассуждения выглядят так. Пусть

$$F_n^t(z)=\sum_{(x,n)=t}z^x.$$

Теорема 5. *Справедливо соотношение*

$$F_{n,d}^t(z)=\sum_{d\,|\,\frac{n}{t}}\frac{\mu(d)}{1-z^{td}}.$$

Следствие 5. *Имеет место формула*

$$\sum_{a\in M_n^t}z^a=\sum_{d\,|\,\frac{n}{t}}\mu(d)\frac{1-z^n}{1-z^{td}}.$$

Следствие 6. *При $t\mid n$ справедливо равенство*

$$\left|M_n^t\right|=\varphi\left(\frac{n}{t}\right).$$

Пусть

$$F_n^t(z) = \sum_{x=1}^{n} z^{(n,x)}.$$

Утверждение 1. *Имеет место формула*

$$F_n^t(z) = \sum_{d \mid n} z^d \varphi\Big(\frac{n}{t}\Big).$$

Пусть $\varphi_n(a)$ — число меньших n и взаимно простых с числом a чисел, $\tau_p(n)$ — число простых делителей n, $M_p(n)$ — множество простых делителей числа n. Положим для краткости $k = \tau_p(n)$.

Теорема 6. *Имеет место соотношение*

$$\varphi_n(a) = n - \sum_{i=1}^{k} \Big[\frac{n}{p_i}\Big] + \sum_{1 \leqslant i < j \leqslant k} \Big[\frac{n}{p_i p_j}\Big] - \dots,$$

где $a = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$.

При этом заметим, что $\varphi_n(n) = \varphi(n)$ и $\varphi_n(a) = \frac{n}{a}\varphi(a)$, если $M_p(n) = M_p(a)$.

Далее приведём ещё три соотношения.

1) $\varphi(n^r) = n^{r-1}\varphi(n)$.

2) Пусть $M_p(a) \subseteq M_p(mn)$. Тогда

$$\varphi_{mn}(a) = mn - \sum_{p \mid a} \Big[\frac{mn}{p}\Big] + \sum_{pq \mid a} \Big[\frac{mn}{pq}\Big] - \dots$$

$$= mn - \sum_{p \mid a} \frac{mn}{p} + \sum_{pq \mid a} \frac{mn}{pq} - \dots = mn \prod_{p \mid a} \Big(1 - \frac{1}{p}\Big).$$

Отсюда

$$\varphi_{mn}(a) = \frac{mn}{a}\varphi(a).$$

3) Если $M_p(a) = M_p(mn)$, то $\varphi_{mn}(a) = \varphi(mn)$.

ЛИТЕРАТУРА

1. **Арнольд В. И.** Группы Эйлера и арифметика геометрических прогрессий. М.: МЦНМО, 2003. 44 с.
2. **Сачков В. Н.** Введение в комбинаторные методы дискретной математики. М.: МЦНМО, 2004.
3. **Алфёров А. П., Зубов А. Ю., Кузьмин А. С., Черёмушкин А. В.** Основы криптографии. М.: Гелиос АРВ, 2002. 480 с.

4. **Грэхем Р., Кнут Д., Паташник О.** Конкретная математика. Основание информатики. М.: Мир, 1998.
5. **Hardy G. H., Wright E. M.** An introduction to the theory of numbers. Oxford: Clarendon Press, 1979. 426 p.
6. **Shramm W.** The Fourier transform of functions of the greatest common divisor // INTEGERS: Electron. J. Comb. Number Theory. 2008. V. 8. Paper ID A50. 7 p.
7. **Coleman R.** Some remarks on Euler's totient function. Ithaca, NY: Cornell Univ., 2012. (Cornell Univ. Libr. e-Print Archive; arXiv:1207.4446).
8. **Леонтьев В. К.** Комбинаторика и информация. Ч. 1. Комбинаторный анализ. М.: МФТИ, 2015. 174 с.
9. **Бейтмен Г., Эрдейи А.** Высшие трансцендентные функции. Т. 3. М.: Наука, 1967. 296 с.
10. **Курош А. Г.** Курс высшей алгебры. М.: Наука, 1968. 431 с.

Леонтьев Владимир Константинович
Гордеев Эдуард Николаевич

Статья поступила
23 мая 2023 г.
После доработки —
2 августа 2023 г.
Принята к публикации
20 августа 2023 г.

DISKRETNYI ANALIZ I ISSLEDOVANIE OPERATSII
/DISCRETE ANALYSIS AND OPERATIONS RESEARCH/
October–December 2023. Vol. 30, No. 4. P. 35–45

UDC 519.7 DOI 10.33048/daio.2023.30.775

ON RELATIONS ASSOCIATED WITH THE EULER FUNCTION

V. K. Leontiev[a] and *E. N. Gordeev*[b]

Dorodnitsyn Computing Center RAS,
40 Vavilov Street, 119333 Moscow, Russia
E-mail: [a] vkleontiev@yandex.ru, [b] werhorn@yandex.ru

Abstract. The paper studies the properties of the set of numbers smaller than and coprime to n with the modulo n multiplication operation introduced on it (this object is sometimes called the Euler group). The cardinality of such a set is the well-known Euler function $\varphi(n)$, which is one of the classical functions in the number theory. The fields of its application are quite wide and include, for example, various branches of discrete mathematics, and it also has significant applications in cryptography. The paper considers various combinatorial problems arising in the study of the Euler group and the Euler function. Relations between theoretical and numerical parameters associated with the Euler group and Euler function are derived. The combinatorial relations obtained in the paper can be used when solving applied combinatorial problems and in cryptography. Bibliogr. 10.

Keywords: divisor, Euler function, Euler group, Stirling numbers, Möbius function, generating function.

REFERENCES

1. **V. I. Arnold,** *Euler Groups and Arithmetics of Geometric Progression* (MTsNMO, Moscow, 2003) [Russian].
2. **V. N. Sachkov,** *An Introduction to Combinatorial Methods of Discrete Mathematics* (MTsNMO, Moscow, 2004) [Russian].
3. **A. P. Alfyorov, A. Yu. Zubov, A. S. Kuzmin,** and **A. V. Cheryomushkin,** *Basics of Cryptography* (Gelios ARV, Moscow, 2002) [Russian].
4. **R. L. Graham, D. E. Knuth,** and **O. Patashnik,** *Concrete Mathematics: A Foundation for Computer Science* (Addison-Wesley, Reading, MA, 1994; Mir, Moscow, 1998 [Russian]).

English version: Journal of Applied and Industrial Mathematics **17** (4), 760–766 (2023), DOI 10.1134/S1990478923040075.

5. **G. H. Hardy** and **E. M. Wright,** *An Introduction to the Theory of Numbers* (Clarendon Press, Oxford, 1979).
6. **W. Shramm,** The Fourier transform of functions of the greatest common divisor, *INTEGERS: Electron. J. Comb. Number Theory* **8**, Paper ID A50 (2008).
7. **R. Coleman,** Some remarks on Euler's totient function (Cornell Univ., Ithaca, NY, 2012) (Cornell Univ. Libr. e-Print Archive, arXiv:1207.4446).
8. **V. K. Leontiev,** *Combinatorics and Information. Pt. 1. Combinatorial Analysis* (Mosk. Fiz. Tekh. Inst., Moscow, 2015) [Russian].
9. **H. Bateman** and **A. Erdélyi,** *Higher Transcendental Functions,* Vol. 3 (New York, McGraw-Hill Book Co., 1953; Nauka, Moscow, 1967 [Russian]).
10. **A. G. Kurosh,** *A Course in Higher Algebra* (Nauka, Moscow, 1968) [Russian].

Vladimir K. Leontiev
Eduard N. Gordeev

Received May 23, 2023
Revised August 2, 2023
Accepted August 20, 2023