Math-Net.Ru

Общероссийский математический портал

В. К. Леонтьев, О некоторых комбинаторных задачах теоретико-числового содержания, *Матем. заметки*, 2009, том 86, выпуск 3, 402–407

DOI: <https://doi.org/10.4213/mzm4737>

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: 34.227.88.159

26 апреля 2023 г., 15:37:37

О некоторых комбинаторных задачах теоретико-числового содержания

В. К. Леонтьев

Приводятся несколько выражений для производящих функций, возникающих при решении комбинаторных проблем, связанных с теорией графов и теорией кодирования.

Библиография: 6 названий.

В статье рассматривается ряд комбинаторных задач теоретико-числового содержания, возникающих при изучении отдельных проблем теории графов и теории корректирующих кодов [1], [2]. Мы находим простые выражения для целого ряда производящих функций и выводим из них следствия, нужные для решения исходных задач.

Пусть F_q – конечное поле из q элементов и $F_q[x]$ – кольцо полиномов над полем F_q . Далее мы будем рассматривать только нормированные полиномы из $F_q[x]$.

Функция Мёбиуса $\mu(g)$, заданная на элементах кольца $F_q[x]$, определяется каноническим способом

$$\mu(g) = \begin{cases} 1 & \text{при } g = 1, \\ (-1)^r & \text{при } g = v_1 v_2 \cdots v_r, \\ 0, & \text{если } g \text{ делится на квадрат.} \end{cases} \quad (1)$$

Здесь v_i – неприводимые полиномы факториального кольца $F_q[x]$. Функция Мёбиуса (1) является прямым аналогом классической теоретико-числовой функции Мёбиуса, определенной в кольце целых чисел.

Рассмотрим следующую производящую функцию:

$$F_q(z) = \sum_{g \in F_q[x]} \mu(g) z^{\deg g}. \quad (2)$$

ТЕОРЕМА 1. *Справедливо соотношение*

$$F_q(z) = 1 - qz. \quad (3)$$

ДОКАЗАТЕЛЬСТВО. Используя факториальность кольца $F_q[x]$, рассмотрим представление $g(x) = \prod_{i=1}^{\infty} v_i^{\alpha_i}$, где v_i – неприводимые полиномы из $F_q[x]$. Из (2) и

представления для $g(x)$ получаем

$$\begin{aligned} F_q(z) &= \sum_{\{\alpha_1 \alpha_2 \dots\}} \mu(v_1^{\alpha_1} v_2^{\alpha_2} \dots) z^{\alpha_1 \deg v_1 + \alpha_2 \deg v_2 + \dots} \\ &= \sum_{\alpha_1=0}^1 \mu(v_1^{\alpha_1}) z^{\alpha_1 \deg v_1} \sum_{\alpha_2=0}^1 \mu(v_2^{\alpha_2}) z^{\alpha_2 \deg v_2} \dots \end{aligned} \quad (4)$$

Для получения последнего выражения мы использовали мультипликативность функции Мёбиуса. Продолжая вычисления (4), получаем

$$F_q(z) = (1 - z^{\deg v_1})(1 - z^{\deg v_2}) \dots = \prod_{i=1}^{\infty} (1 - z^{\deg v_i}). \quad (5)$$

Используя теперь классическое соотношение [3]

$$\frac{1}{1 - qz} = \prod_{k=1}^{\infty} \left(\frac{1}{1 - z^k} \right)^{I_k}, \quad (6)$$

где I_k — число неприводимых нормированных полиномов степени k , из (5) и (6) выводим (3).

СЛЕДСТВИЕ 1 [4]. Пусть

$$L_s = \sum_{\deg g=s} \mu(g). \quad (7)$$

Тогда

$$L_s = \begin{cases} -q & \text{при } s = 1, \\ 0 & \text{при } s \geq 2. \end{cases} \quad (8)$$

Ранее формула (8) была доказана в работе [1] для $s \leq 6$.

Приводимое выше следствие было анонсировано в [4]. Задача оценки функции L_s связана с теорией циклических равновесных кодов.

Пусть $\tau(g)$ — число делителей полинома $g(x) \in F_q[x]$. Рассмотрим следующую производящую функцию:

$$\Phi_q(z) = \sum_{g \in F_q[x]} \tau(g) z^{\deg g}. \quad (9)$$

ТЕОРЕМА 2. Справедливо соотношение

$$\Phi_q(z) = (1 - qz)^{-2}. \quad (10)$$

ДОКАЗАТЕЛЬСТВО. Опять используя аргументы, приведенные выше, и мультипликативность функции $\tau(g)$, легко получить следующее представление:

$$\Phi_q(z) = \prod_{i=1}^{\infty} \sum_{\alpha_i=0}^{\infty} \tau(v_i^{\alpha_i}) z^{\alpha_i \deg v_i}. \quad (11)$$

Так как $\tau(v^\alpha) = \alpha + 1$ для неприводимого полинома v и

$$\sum_{\alpha=0}^{\infty} (\alpha + 1) z^{\alpha \deg v} = (1 - z^{\deg v})^{-2}, \quad (12)$$

опять используя формулу (6), мы выводим (10).

СЛЕДСТВИЕ 2. Пусть $\bar{\tau}_s$ – среднее число делителей у полинома степени s из $F_q[x]$, т.е.

$$\bar{\tau}_s = \frac{1}{q^s} \sum_{\deg g=s} \tau(g).$$

Тогда

$$\bar{\tau}_s = s + 1. \quad (13)$$

ДОКАЗАТЕЛЬСТВО. Из (9) имеем

$$\Phi_q(z) = \sum_{g \in F_q[x]} \tau(g) z^{\deg g} = \sum_s \sum_{\deg g=s} \tau(g) z^{\deg g} = \sum z^s \sum_{\deg g=s} \tau(g) = \sum_{s=0}^{\infty} z^s q^s \bar{\tau}_s.$$

Теперь формула (13) получается сравнением коэффициентов при z^s .

ЗАМЕЧАНИЕ. Любопытно отметить, что среднее число делителей у полинома степени s из кольца $F_q[x]$ не зависит от q .

П. Эрдёшу принадлежит задача о существовании гамильтонового цикла в торической $(m \times n)$ -решетке или, что то же самое, в графе $I_m \times I_n$, где граф I_k – это гамильтонов цикл длины k ([2], [5]). В работе [6] было получено комбинаторное решение этой задачи, которое состоит в следующем.

ТЕОРЕМА 3. Граф $I_m \times I_n$ является гамильтоновым, если и только если диофантово уравнение

$$\begin{cases} x + y = (m, n), \\ (x, m) = 1, & (y, n) = 1 \end{cases} \quad (14)$$

разрешимо в натуральных числах.

Приведенные ниже производящие функции Дирихле являются частью метода Харди–Литтлвуда, примененного для нахождения числа решений уравнения (14).

Пусть $m_1, m_2, \dots, m_k$ – произвольные натуральные числа и

$$P_i = \prod_{p|m_i} p, \quad P = [P_1, P_2, \dots, P_k]. \quad (15)$$

Таким образом P_i – это произведение всех простых делителей числа m_i , а P – наименьшее общее кратное этих произведений.

ТЕОРЕМА 4. Справедливо тождество

$$\sum_{d_1|m_1, \dots, d_k|m_k} \frac{\mu(d_1) \dots \mu(d_k)}{[d_1, d_2, \dots, d_k]^s} = \prod_{p|P} \left(1 - \frac{1}{p^s}\right). \quad (16)$$

Произведение в правой части (16) берется по всем простым делителям числа $P = [P_1, \dots, P_k]$.

ДОКАЗАТЕЛЬСТВО. Для сокращения записи рассмотрим сначала случай $k = 2$. Пусть $P = [P_1, P_2] = r_1 r_2 \dots r_M$. Каждый бесквадратный делитель числа d_i ($i = 1, 2$) мы будем задавать с помощью двоичного набора длины M : $\alpha_1 \alpha_2 \dots \alpha_M$, т.е. такой

делитель имеет запись $r_1^{\alpha_1} r_2^{\alpha_2} \dots r_M^{\alpha_M}$. При этом, исходя из определения функции Мёбиуса, можно записать следующие соотношения:

$$\mu(d_1) = (-1)^{\sum_{i=1}^M \alpha_i}, \quad \mu(d_2) = (-1)^{\sum_{i=1}^M \beta_i}, \quad [d_1, d_2] = r_1^{\max(\alpha_1, \beta_1)} \dots r_M^{\max(\alpha_M, \beta_M)}. \quad (17)$$

Отсюда следует

$$\sum_{d_1 | m_1, d_2 | m_2} \frac{\mu(d_1) \mu(d_2)}{[d_1, d_2]^s} = \sum_{\substack{(\alpha_1 \dots \alpha_M) \\ (\beta_1 \dots \beta_M)}} \frac{(-1)^{\sum_{i=1}^M \alpha_i} (-1)^{\sum_{i=1}^M \beta_i}}{r_1^{s \max(\alpha_1, \beta_1)} \dots r_M^{s \max(\alpha_M, \beta_M)}}. \quad (18)$$

Если простой сомножитель r_i входит в оба числа m_1 и m_2 , то

$$\sum_{\{\alpha_i, \beta_i\}} \frac{(-1)^{\alpha_i + \beta_i}}{r_i^{s \max(\alpha_i, \beta_i)}} = 1 - \frac{1}{r_i^s} - \frac{1}{r_i^s} + \frac{1}{r_i^s} = 1 - \frac{1}{r_i^s}, \quad (19)$$

так как в этом случае α_i и β_i принимают все возможные значения из нулей и единиц. Если же r_i делит лишь одно из чисел m_1 или m_2 , то

$$\sum_{\{\alpha_i, \beta_i\}} \frac{(-1)^{\alpha_i + \beta_i}}{r_i^{s \max(\alpha_i, \beta_i)}} = 1 - \frac{1}{r_i^s}. \quad (20)$$

Учитывая эти соотношения, из (18)–(20) получаем

$$\sum_{d_1 | m_1, d_2 | m_2} \frac{\mu(d_1) \mu(d_2)}{[d_1, d_2]^s} = \sum_{\{\alpha_i, \beta_i\}} \frac{(-1)^{\alpha_1 + \beta_1}}{r_1^{s \max(\alpha_1, \beta_1)}} \dots \sum_{\{\alpha_M, \beta_M\}} \frac{(-1)^{\alpha_M + \beta_M}}{r_M^{s \max(\alpha_M, \beta_M)}} = \prod_{i=1}^M \left(1 - \frac{1}{r_i^s}\right),$$

что совпадает с (16).

В случае произвольного k доказательство следует той же схеме. Имеем, учитывая прежние обозначения при $P = r_1 r_2 \dots r_M$,

$$\sum_{d_1 | m_1, \dots, d_k | m_k} \frac{\mu(d_1) \dots \mu(d_k)}{[d_1, \dots, d_k]^s} = \sum_{\{\alpha_1^1, \dots, \alpha_1^k\}} \frac{(-1)^{\alpha_1^1 + \dots + \alpha_1^k}}{r_1^{s \max(\alpha_1^1, \dots, \alpha_1^k)}} \dots \sum_{\{\alpha_M^1, \dots, \alpha_M^k\}} \frac{(-1)^{\alpha_M^1 + \dots + \alpha_M^k}}{r_M^{s \max(\alpha_M^1, \dots, \alpha_M^k)}}. \quad (21)$$

Рассмотрим отдельную сумму в (21). Пусть $a_t = (\alpha_t^1 \dots \alpha_t^k)$ и $\|a_t\|$ – число единиц в двоичном наборе a_t . Тогда

$$\sum_{\{\alpha_t^1, \dots, \alpha_t^k\}} \frac{(-1)^{\alpha_t^1 + \dots + \alpha_t^k}}{r_t^{s \max(\alpha_t^1, \dots, \alpha_t^k)}} = \sum_{\|a_t\|=0} + \sum_{\|a_t\|=1} + \dots. \quad (22)$$

Если простое число r_t входит ровно в l сомножителей m_i (например, в $m_1, \dots, m_l$), то

$$\begin{aligned} \sum_{\{\alpha_t^1, \dots, \alpha_t^k\}} \frac{(-1)^{\sum_{i=1}^k \alpha_t^i}}{r_t^{s \max(\alpha_t^1, \dots, \alpha_t^k)}} &= 1 - \frac{\binom{l}{1}}{r_t^s} + \frac{\binom{l}{2}}{r_t^s} \dots + (-1)^l \frac{\binom{l}{l}}{r_t^s} \\ &= 1 - \frac{1}{r_t^s} \left[\binom{l}{1} - \binom{l}{2} + \dots + (-1)^l \binom{l}{l} \right] = 1 - \frac{1}{r_t^s}. \end{aligned} \quad (23)$$

Теперь утверждение теоремы 3 следует из (21) и (23).

Пусть $(v_1, v_2, \dots, v_k)$ – наибольший общий делитель чисел $v_1, \dots, v_k$. Рассмотрим сумму, аналогичную (16),

$$S_1 = \sum_{v_1 | m_1, \dots, v_k | m_k} \frac{\mu(v_1) \dots \mu(v_k)}{(v_1, v_2, \dots, v_k)^s}. \quad (24)$$

Используя предыдущие обозначения, т.е.

$$P_i = \prod_{p | m_i} p, \quad i = 1, \dots, k,$$

сформулируем следующее утверждение.

ТЕОРЕМА 5. *Справедливо соотношение*

$$S_1 = \prod_{p | P} \left(1 - \frac{1}{p^s}\right), \quad (25)$$

если $P_1 = P_2 = \dots = P$, и $S_1 = 0$ во всех остальных случаях.

ДОКАЗАТЕЛЬСТВО. Будем использовать все обозначения из доказательства предыдущей теоремы и очевидное равенство

$$(u, v) = r_1^{\min(\alpha_1, \beta_1)} \dots r_M^{\min(\alpha_M, \beta_M)}.$$

Рассмотрим сумму

$$R = \sum_{\{\alpha_t^1, \dots, \alpha_t^k\}} \frac{(-1)^{\alpha_t^1 + \alpha_t^2 + \dots + \alpha_t^k}}{r_t^{s \min(\alpha_t^1, \dots, \alpha_t^k)}}.$$

Если простое число r_t входит во все сомножители r_i , то для набора $(\alpha_t^1, \dots, \alpha_t^k)$ возможны все 2^k значений. Отсюда следует

$$R = 1 - \binom{t}{1} + \binom{t}{2} - \dots + (-1)^t \binom{t}{t} \frac{1}{r_t^s} = (-1)^t \left(\frac{1}{r_t^s} - 1 \right).$$

Если же r_t не входит хотя бы в один из сомножителей m_i , то $\min(\alpha_t^1, \dots, \alpha_t^k) = 0$ и

$$R = \sum_{\{\alpha_t^1, \dots, \alpha_t^k\}} (-1)^{\alpha_t^1 + \dots + \alpha_t^k} = 0,$$

что и доказывает формулу (25).

Заметим, что формула (16) является многомерным обобщением классической формулы, связанной с функцией Эйлера $\varphi(n)$

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

и переходит в нее при $k = 1$ и $s = 1$.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

- [1] O. Moreno, Z. Zhang, P. V. Kumar, V. A. Zinoviev, “New constructions of optimal cyclically permutable constant weight codes”, *IEEE Trans. Inform. Theory*, **41**:2 (1995), 448–455.
- [2] W. T. Trotter, P. Erdős, “When the Cartesian product of directed cycles is Hamiltonian”, *J. Graph Theory*, **2**:2 (1978), 137–142.
- [3] Р. Лидл, Г. Нидеррайт, *Конечные поля*, Т. 1, 2, Мир, М., 1988.
- [4] В. К. Леонтьев, “О некоторых задачах, связанных в полиномами над конечным полем”, *Труды IV Международной научной конференции “Дискретные модели в теории управляющих систем”*, МГУ, М., 2000, 60–61.
- [5] В. К. Леонтьев, “Гамильтоновы циклы в торической решетке”, *Докл. РАН*, **395**:5 (2004), 590–591.
- [6] А. А. Евдокимов, “Нумерация подмножеств конечного множества”, *Методы дискретн. анализа*, **34** (1980), 8–26.

В. К. Леонтьев

Вычислительный центр им. А. А. Дородницына РАН

Поступило

07.04.2008

Исправленный вариант

14.01.2009