Math-Net.Ru

Общероссийский математический портал

В. К. Леонтьев, Об одном диофантовом уравнении, *Матем. заметки*, 2016, том 100, выпуск 3, 388–398

DOI: <https://doi.org/10.4213/mzm8943>

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: 35.173.219.12

26 апреля 2023 г., 15:06:08

Об одном диофантовом уравнении

В. К. Леонтьев

Рассматривается линейное диофантово уравнение с дополнительными ограничениями на неизвестные. Получены условия разрешимости.

Библиография: 8 названий.

Ключевые слова: диофантово уравнение, гамильтонов цикл, производящая функция.

DOI: 10.4213/mzm8943

1. Введение. Линейное диофантово уравнение

$$\sum_{i=1}^n a_i x_i = b$$

с натуральными параметрами a_i , b разрешимо в натуральных числах x_i , если a_i не имеют общего делителя $d > 1$ и b достаточно велико [1]–[3]. Для $n = 2$ границей разрешимости является число $b = b(a_1, a_2) = (a_1 - 1)(a_2 - 1)$. Это теорема Сильвестра.

Мы рассматриваем уравнение

$$a_1 x_1 + a_2 x_2 = b \tag{1}$$

с дополнительным условием

$$(x_1, m) = (x_2, n) = 1. \tag{2}$$

Здесь m, n – некоторые натуральные числа и (u, v) – наибольший общий делитель чисел u и v .

Условие (2) связано со следующей задачей из теории графов. Задана торическая (m, n) -решетка. Требуется определить: есть ли в ней гамильтонов цикл? Условия существования такого цикла найдены в работе [4] и состоят в разрешимости следующей системы в натуральных числах:

$$\begin{cases} x + y = (m, n), \\ (x, m) = (y, n) = 1. \end{cases} \tag{3}$$

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (грант № 14-00-00641).

Ряд любопытных фактов, связанных с уравнением (3), приведен в работе [5]. Ясно, что рассматриваемая нами система

$$ax + by = M, \quad (x, m) = (y, n) = 1, \quad (4)$$

содержит условия “гамильтоновости” (3) и потому представляет и некоторый общий интерес. Некоторые факты, связанные с разрешимостью уравнения “гамильтоновости” (3), приведены в работе [6]. Мы используем метод производящих функций и метод Харди–Литтлвуда для доказательства следующего утверждения о разрешимости системе (4): если $(am, bn) = 1$, то система (4) разрешима для $M > M_0$ и $M_0 = M_0(a, b, m, n)$.

Это утверждение и представляет основной результат настоящей работы. Если $(am, bn) > 1$, то система (4) может не иметь решений. Краткое содержание этой работы представлено в [7].

2. Метод Харди–Литтлвуда. Пусть $I_N(Z)$ – производящая функция последовательности $\{a_n\}$ натуральных чисел, взаимно-простых с N , т. е.

$$I_N(Z) = \sum_{(r, N)=1} Z^r. \quad (5)$$

Если $J_M(a, b, m, n)$ – число решений системы (4), то справедливо следующее утверждение.

ЛЕММА 1. *Имеет место равенство*

$$\sum_{M=0}^{\infty} J_M(a, b, m, n) Z^M = I_m(Z^a) I_n(Z^b). \quad (6)$$

ДОКАЗАТЕЛЬСТВО. По определению

$$\sum_{M=0}^{\infty} J_M(a, b, m, n) z^M = \sum_{\substack{(x, m)=1 \\ (y, n)=1}} Z^{ax+by} = \sum_{(x, m)=1} Z^{ax} \sum_{(y, n)=1} Z^{by} = I_m(Z^a) I_n(Z^b).$$

Нам потребуется следующее представление для производящей функции $I_N(Z)$ [4]. Пусть $N = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ – каноническое разложение числа N в произведение степеней простых чисел.

ЛЕММА 2. *Справедлива формула*

$$I_N(Z) = \sum_{d|N} \frac{\mu(d)}{1 - z^d}. \quad (7)$$

Здесь $\mu(d)$ – классическая теоретико-числовая функция Мёбиуса и суммирование в (7) ведется по всем делителям числа N . Эта формула приведена в работе [2] и является прямым следствием метода включения-исключения.

Следующее утверждение устанавливает связь между числом $J_M(a, b, m, n)$ решений системы (4) и числом $t_M(a, b)$ – решений классического уравнения

$$ax + by = M \quad (8)$$

в натуральных числах.

ЛЕММА 3. *Справедливо соотношение*

$$J_M(a, b, m, n) = \sum_{u|m, v|n} \mu(u)\mu(v)t_M(au, bv). \quad (9)$$

ДОКАЗАТЕЛЬСТВО. Из (6), используя формулу Коши, получаем

$$J_M(a, b, m, n) = \frac{1}{2\pi i} \oint_{|z|=\rho} \frac{I_m(Z^a)I_n(Z^b)}{Z^{M+1}} dZ, \quad (10)$$

где $\rho < 1$. Из (10), используя формулу (7), выводим

$$J_M(a, b, m, n) = \frac{1}{2\pi i} \oint_{|z|=\rho} \sum_{u|m, v|n} \frac{\mu(u)\mu(v)}{(1 - Z^{au})(1 - Z^{bv})Z^{M+1}} dZ. \quad (11)$$

Так как

$$t_M(au, bv) = \frac{1}{2\pi i} \oint_{|z|=\rho} \frac{dz}{(1 - Z^{au})(1 - Z^{bv})Z^{M+1}}, \quad (12)$$

то из (10) и (12) получаем (9).

Если P – произведение всех простых множителей числа m , а Q – произведение всех простых множителей числа n , то формулу (9) можно переписать следующим образом:

$$J_M(a, b, m, n) = \sum_{u|P, v|Q} \mu(u)\mu(v)t_M(au, bv). \quad (13)$$

Обратимся теперь к вычислению интеграла (12).

Пусть Z_k – множество всех корней степени k из единицы.

ЛЕММА 4. *Справедливо равенство*

$$\begin{aligned} & \frac{1}{2\pi i} \oint_{|z|=\rho} \frac{dz}{(1 - Z^{au})(1 - Z^{bv})Z^{M+1}} \\ &= \frac{M}{abuv} \sum_{\alpha \in Z_{au} \cap Z_{bv}} \frac{1}{\alpha^M} + \frac{au + bv}{2} \sum_{\alpha \in Z_{au} \cap Z_{bv}} \frac{1}{\alpha^M} \\ & \quad - \frac{1}{au} \sum_{\alpha \in Z_{au} \setminus Z_{bv}} \frac{\alpha^{-M}}{\alpha^{bv} - 1} - \frac{1}{bv} \sum_{\alpha \in Z_{bv} \setminus Z_{au}} \frac{\alpha^{-M}}{\alpha^{au} - 1}, \end{aligned} \quad (14)$$

где $\rho < 1$.

ДОКАЗАТЕЛЬСТВО. Рассмотрим следующую функцию:

$$f(z) = \frac{z^{-(M+1)}}{(Z^{au} - 1)(Z^{bv} - 1)}.$$

Интеграл (12) равен вычету в нуле функции $f(z)$. Все конечные ненулевые особые точки $f(z)$ – это корни из единицы или элементы множества $Z_{au} \cup Z_{bv}$. Вычет $f(z)$ в бесконечности равен нулю. Поэтому по основной теореме о вычетах справедлива формула

$$\operatorname{res}_{z=0} f(z) = - \sum_{\alpha \in Z_{au} \cup Z_{bv}} \operatorname{res} f(z). \quad (15)$$

Все особые точки $f(z)$ из $Z_{au} \cup Z_{bv}$ – это полюса порядка один и два. Вычеты в полюсах первого порядка вычисляются по стандартным формулам. Если положить

$$u(z) = z^{-(M+1)}, \quad v(z) = (Z^{au} - 1)(Z^{bv} - 1),$$

то для простого полюса имеем выражение

$$\begin{aligned} \operatorname{res}_{z=\alpha} f(z) &= \frac{u(\alpha)}{v'(\alpha)} = \frac{\alpha^{-M}}{au(\alpha^{bv} - 1)} \quad \text{при } \alpha \in Z_{au} \setminus Z_{bv}, \\ \operatorname{res}_{z=\alpha} f(z) &= \frac{u(\alpha)}{v'(\alpha)} = \frac{\alpha^{-M}}{bv(\alpha^{au} - 1)} \quad \text{при } \alpha \in Z_{bv} \setminus Z_{au}. \end{aligned} \quad (16)$$

Для вычисления вычетов в полюсах порядка два мы используем следующее техническое утверждение, приведенное в [6].

Пусть $f(z) = \varphi(z)/\lambda(z)$, где $\varphi(z)$ и $\lambda(z)$ – регулярные в окрестности ненулевой точки $z = \alpha$ функции и α – нуль кратности два функции $\lambda(z)$. Тогда справедлива формула

$$\operatorname{res}_{z=\alpha} f(z) = \frac{2[3\varphi'(\alpha)\lambda''(\alpha) - \varphi(\alpha)\lambda^{(3)}(\alpha)]}{3[\lambda''(\alpha)]^2}. \quad (17)$$

Мы используем эту формулу для $\varphi(z) = Z^{-(M+1)}$ и $\lambda(z) = (Z^{au} - 1)(Z^{bv} - 1)$ и $\alpha \in Z_{au} \cap Z_{bv}$. Простые вычисления приводят к следующим формулам:

$$\varphi'(\alpha) = -(M+1)\alpha^{-M-2}, \quad \lambda''(\alpha) = \frac{2abuv}{\alpha^2}, \quad \lambda^{(3)}(\alpha) = \frac{3}{\alpha^3}(abuv)(au + bv - 2), \quad (18)$$

и к следующему выражению:

$$\operatorname{res}_{z=\alpha} f(z) = -\frac{\alpha^{-M}}{abuv} \left(M + \frac{au + bv}{2} \right). \quad (19)$$

Используя теперь формулы (15), (16) и (19), получаем (14).

Полученную формулу (14) можно использовать для получения основного выражения для числа $J_M(a, b, m, n)$ – решений системы (4).

Пусть δ_M^r – предикат делимости

$$\delta_M^r = \begin{cases} 1, & \text{если } r \mid M, \\ 0, & \text{если } r \nmid M. \end{cases} \quad (20)$$

и $S_n(a, b)$ – следующая сумма Дедекинда [8]:

$$S_n(a, b) = \sum_{\alpha \in Z_b \setminus Z_a} \frac{1}{\alpha^n(\alpha^a - 1)}. \quad (21)$$

ТЕОРЕМА 1. *Справедлива формула*

$$\begin{aligned} J_M(a, b, m, n) &= \sum_{u \mid P, v \mid Q} \frac{\mu(u)\mu(v)}{[au, bv]} \delta_M^{(au, bv)} + \frac{1}{2} \sum \frac{\mu(u)\mu(v)(au + bv)}{[au, bv]} \delta_M^{(au, bv)} \\ &\quad - \frac{1}{a} \sum_{u \mid P, v \mid Q} \frac{\mu(u)\mu(v)}{u} S_M(bv, au) - \frac{1}{b} \sum_{u \mid P, v \mid Q} \frac{\mu(u)\mu(v)}{v} S_M(au, bv). \end{aligned} \quad (22)$$

Здесь (A, B) и $[A, B]$ – наибольший общий делитель и наименьшее общее кратное чисел A и B .

ДОКАЗАТЕЛЬСТВО. Подставляя в формулу (13) выражение для $t_M(au, bv)$, получаем

$$\begin{aligned}
 J_M(a, b, m, n) &= \sum_{u|P, v|Q} \mu(u)\mu(v)t_M(au, bv) \\
 &= \sum_{u|P, v|Q} \mu(u) \frac{M}{abuv} \sum_{\alpha \in Z_{au} \cap Z_{bv}} \frac{1}{\alpha^M} \\
 &\quad + \sum_{u|P, v|Q} \mu(u)\mu(v) \frac{au + bv}{2v} \sum_{\alpha \in Z_{au} \cap Z_{bv}} \frac{1}{\alpha^M} \\
 &\quad - \sum_{u|P, v|Q} \frac{\mu(u)\mu(v)}{au} \sum_{\alpha \in Z_{au} \setminus Z_{bv}} \frac{\alpha^{-M}}{\alpha^{bv} - 1} \\
 &\quad - \sum_{u|P, v|Q} \frac{\mu(u)\mu(v)}{bv} \sum_{\alpha \in Z_{bv} \setminus Z_{au}} \frac{\alpha^{-M}}{\alpha^{au} - 1}. \tag{23}
 \end{aligned}$$

Дальнейшие вычисления связаны со следующим хорошо известным тождеством:

$$\sum_{\alpha \in Z_r} \alpha^k = \sum_{\alpha \in Z_r} \frac{1}{\alpha^k} = \begin{cases} r, & \text{при } r \mid k, \\ 0, & \text{при } r \nmid k. \end{cases} \tag{24}$$

Так как $Z_{au} \cap Z_{bv} = \{\alpha : \alpha^{(au, bv)} - 1 = 0\}$, то

$$\sum_{\alpha \in Z_{au} \cap Z_{bv}} \frac{1}{\alpha^M} = \begin{cases} (au, bv), & \text{если } (au, bv) \mid M, \\ 0, & \text{если } (au, bv) \nmid M. \end{cases}$$

Поэтому

$$\begin{aligned}
 &\sum_{u|P, v|Q} \mu(u)\mu(v) \frac{M}{abuv} \sum_{\alpha \in Z_{au} \cap Z_{bv}} \frac{1}{\alpha^M} \\
 &= \frac{M}{ab} \sum_{u|P, v|Q} \mu(u)\mu(v) \frac{(au, bv)}{au \cdot bv} \delta_M^{(au, bv)} = \frac{M}{ab} \sum_{u|P, v|Q} \frac{\mu(u)\mu(v)}{[au, bv]} \delta_M^{(au, bv)},
 \end{aligned}$$

так как $(au, bv)[au, bv] = aubv$.

Аналогично

$$\begin{aligned}
 &\frac{1}{2} \sum_{u|P, v|Q} \mu(u)\mu(v) \frac{au + bv}{abuv} \sum_{\alpha \in Z_{au} \cap Z_{bv}} \frac{1}{\alpha^M} \\
 &= \frac{1}{2} \sum_{u|P, v|Q} \mu(u)\mu(v) \frac{(au + bv)(au, bv)}{abuv} \delta_M^{(au, bv)} \\
 &= \frac{1}{2} \sum_{u|P, v|Q} \frac{\mu(u)\mu(v)(au + bv)}{[au, bv]} \delta_M^{(au, bv)}.
 \end{aligned}$$

Далее

$$\sum_{u|P,v|Q} \frac{\mu(u)\mu(v)}{au} \sum_{\alpha \in Z_{au} \setminus Z_{bv}} \frac{\alpha^{-M}}{\alpha^{bv} - 1} = \frac{1}{a} \sum_{u|P,v|Q} \frac{\mu(u)\mu(v)}{u} S_M(bv, au),$$

$$\sum_{u|P,v|Q} \frac{\mu(u)\mu(v)}{bv} \sum_{\alpha \in Z_{bv} \setminus Z_{au}} \frac{\alpha^{-M}}{\alpha^{au} - 1} = \frac{1}{b} \sum_{u|P,v|Q} \frac{\mu(u)\mu(v)}{v} S_M(au, bv).$$

Формула (22) дает уже достаточно много информации о поведении функции $J_M(a, b, m, n)$, так как все слагаемые, кроме первого, “слабо” зависят от M и можно предположить, что основной вклад в сумму (22) вносит первое слагаемое.

Следующие утверждения служат для оценки первых двух слагаемых в формуле (22).

ЛЕММА 5. Если $(am, bn) = 1$, то

$$\text{а) } M \sum_{u|P,v|Q} \frac{\mu(u)\mu(v)}{[au, bv]} \delta_M^{(au, bv)} = \frac{M}{ab} \frac{\varphi(P)}{P} \frac{\varphi(Q)}{Q}, \quad (25)$$

$$\text{б) } 0 \leq \frac{1}{2} \sum_{u|P,v|Q} \frac{\mu(u)\mu(v)(au + bv)}{[au, bv]} \delta_M^{(au, bv)} \leq \frac{1}{2} \left[\frac{\varphi(Q)}{bQ} + \frac{\varphi(P)}{aP} \right]. \quad (26)$$

Здесь $\varphi(N)$ – функция Эйлера или число чисел $< N$ и взаимно-простых с N .

ДОКАЗАТЕЛЬСТВО. а) Из $(am, bn) = 1$ следует, что $(au, bv) = 1$, и поэтому имеем $\delta_M^{(au, bv)} = 1$. Далее

$$\begin{aligned} & M \sum_{u|P,v|Q} \frac{\mu(u)\mu(v)}{[au, bv]} \delta_M^{(au, bv)} \\ &= M \sum_{u|P,v|Q} \frac{\mu(u)\mu(v)}{au \cdot bv} = M \frac{1}{ab} \sum_{u|P} \frac{\mu(u)}{u} \sum_{v|Q} \frac{\mu(v)}{v} = \frac{M}{ab} \frac{\varphi(P)}{P} \frac{\varphi(Q)}{Q} \end{aligned}$$

в силу известной формулы

$$\varphi(N) = N \sum_{d|N} \frac{\mu(d)}{d}. \quad (27)$$

б) По определению из $(au, bv) = 1$ получаем

$$\begin{aligned} & \frac{1}{2} \sum_{u|P,v|Q} \frac{\mu(u)\mu(v)(au + bv)}{[au, bv]} \delta_M^{(au, bv)} \\ &= \frac{1}{2} \sum_{u|P,v|Q} \frac{\mu(u)\mu(v)}{au \cdot bv} (au + bv) \\ &= \frac{1}{2ab} \sum_{u|P,v|Q} \frac{\mu(u)\mu(v)}{uv} (au) + \frac{1}{2ab} \sum_{u|P,v|Q} \frac{\mu(u)\mu(v)}{uv} (bv) \\ &= \frac{1}{2b} \sum_{u|P,v|Q} \frac{\mu(u)\mu(v)}{v} + \frac{1}{2a} \sum_{u|P,v|Q} \frac{\mu(u)\mu(v)}{u} \\ &= \frac{1}{2b} \sum_{v|Q} \frac{\mu(v)}{v} \sum_{u|P} \mu(u) + \frac{1}{2a} \sum_{u|P} \frac{\mu(u)}{u} \sum_{v|Q} \mu(v). \end{aligned}$$

Так как

$$\sum_{d|N} \mu(d) = \begin{cases} 1, & \text{если } N = 1, \\ 0, & \text{если } N > 1, \end{cases} \quad (28)$$

то из (27), (28) получаем

$$0 \leq \frac{1}{2} \sum_{u|P, v|Q} \frac{\mu(u)\mu(v)(au+bv)}{[au, bv]} \delta_M^{(au, bv)} \leq \frac{1}{2} \left[\frac{\varphi(Q)}{bQ} + \frac{\varphi(P)}{aP} \right].$$

3. Суммы Дедекинда. В выражение (22) для числа решений $J_M(a, b, m, n)$ входят суммы вида $S_n(a, b)$

$$S_n(a, b) = \sum_{\alpha \in Z_b \setminus Z_a} \frac{1}{\alpha^n (\alpha^a - 1)}, \quad (29)$$

которые носят название сумм Дедекинда [8]. Суммирование в (29) ведется по всем корням степени b из единицы, не являющихся корнями степени a из единицы. В этом разделе производится оценка таких сумм.

Пусть K_0 – минимальное неотрицательное решение сравнения

$$ax + n \equiv 0 \pmod{b}. \quad (30)$$

ЛЕММА 6. *Справедливо соотношение*

$$S_n(a, b) = \begin{cases} 0, & \text{если } (a, b) \nmid n, \\ \frac{b}{2} + \frac{(a, b)}{2} - K_0 \cdot (a, b), & \text{если } K_0 \geq 1, \\ -\frac{b}{2} + \frac{(a, b)}{2}, & \text{если } K_0 = 0. \end{cases} \quad (31)$$

ДОКАЗАТЕЛЬСТВО. Ясно, что из $\alpha \in Z_b$, следует $\alpha^{-1} \in Z_b$, и поэтому замена $\alpha \rightarrow \alpha^{-1}$ не меняет сумму $S_n(a, b)$. Отсюда следует равенство

$$S_n(a, b) = \sum_{\alpha \in Z_b \setminus Z_a} \frac{\alpha^{n+a}}{1 - \alpha^a}.$$

Вычисление сумм Дедекинда часто ведется по следующей схеме. Рассматривается следующая функция $S(y)$ при $|y| < 1$:

$$S(y) = \sum_{\alpha \in Z_b} \frac{\alpha^{n+a}}{1 - (\alpha y)^a} - \sum_{\alpha \in Z_b \cap Z_a} \frac{\alpha^{n+a}}{1 - (\alpha y)^a}. \quad (32)$$

Ясно, что

$$\sum_{\alpha \in Z_b \setminus Z_a} \frac{\alpha^{n+a}}{1 - (\alpha y)^a} = S(y),$$

и поэтому

$$S_n(a, b) = \lim_{y \rightarrow 1} S(y).$$

Далее каждая из сумм в (32)

$$S_2(y) = \sum_{\alpha \in Z_b} \frac{\alpha^{n+a}}{1 - (\alpha y)^a}, \quad S_1(y) = \sum_{\alpha \in Z_{(a,b)}} \frac{\alpha^{n+a}}{1 - (\alpha y)^a}$$

вычисляется по отдельности.

а) По определению

$$S_1(y) = \sum_{\alpha \in Z_{(a,b)}} \frac{\alpha^{n+a}}{1 - (\alpha y)^a} = \sum_{\alpha \in Z_{(a,b)}} \alpha^{n+a} \sum_{k=0}^{\infty} (\alpha y)^{ka} = \sum_{k=0}^{\infty} y^{ka} \sum_{\alpha \in Z_{(a,b)}} \alpha^{a(k+1)+n}.$$

Так как $\alpha \in Z_{(a,b)}$, то $\alpha^a = 1$ и потому

$$S_1(y) = \sum_{k=0}^{\infty} y^{ka} \sum_{\alpha \in Z_{(a,b)}} \alpha^n.$$

Из (24) теперь получаем, используя (20),

$$S_1(y) = \delta_n^{(a,b)} \frac{(a,b)}{1 - y^a}. \quad (33)$$

б) Пусть теперь

$$S_2(y) = \sum_{\alpha \in Z_b} \frac{\alpha^{n+a}}{1 - (\alpha y)^a}.$$

Аналогично предыдущей выкладке получаем

$$S_2(y) = \sum_{k=0}^{\infty} y^{ka} \sum_{\alpha \in Z_b} \alpha^{a(k+1)+n}.$$

Далее

$$S_2(y) = \frac{1}{y^a} \sum_{k=0}^{\infty} y^{a(k+1)} \sum_{\alpha \in Z_b} \alpha^{a(k+1)+n} = \frac{1}{y^a} \sum_{k=1}^{\infty} y^{ak} \sum_{\alpha \in Z_b} \alpha^{ak+n}. \quad (34)$$

Внутренняя сумма в (34) в силу (24) отлична от нуля лишь для тех значений K , которые удовлетворяют условию

$$ak + n \equiv 0 \pmod{b}.$$

Все такие K образуют последовательность

$$K = K_0 + t \frac{b}{(a,b)}, \quad t = 0, 1, \dots,$$

и поэтому

$$S_2(y) = \frac{b}{y^a} \sum_t y^{a(K_0 + tb/(a,b))}. \quad (35)$$

Суммирование в (35) начинается с $t = 0$, если $K_0 \geq 1$, и с $t = 1$, если $K_0 = 0$.

В первом случае

$$S_2(y) = \frac{b}{y^a} y^{aK_0} \sum_{t=0}^{\infty} y^{t[a,b]} = by^{a(K_0-1)} \frac{1}{1-y^{[a,b]}}. \quad (36)$$

Во втором случае

$$S_2(y) = \frac{b}{y^a} \frac{y^{[a,b]}}{1-y^{[a,b]}}. \quad (37)$$

Напомним теперь, что

$$S_n(a, b) = \lim_{y \rightarrow 1} [S_2(y) - S_1(y)]. \quad (38)$$

Перед вычислением предела в (38) отметим, что $\delta_n^{(a,b)} = 1$, так как из условия

$$ak + n \equiv 0 \pmod{b}$$

следует, что n делится на (a, b) . В противном случае $S_n(a, b) = 0$. Далее, если $K_0 \geq 1$, то

$$S_n(a, b) = \lim_{y \rightarrow 1} \left[by^{a(K_0-1)} \frac{1}{1-y^{[a,b]}} - \frac{y^{(a,b)}}{1-y^a} \right]. \quad (39)$$

Положим $r = a(K_0 - 1)$ и рассмотрим разность

$$S_2(y) - S_1(y) = \frac{by^r(1-y^a) - (a, b)[1-y^{[a,b]}]}{(1-y^a)(1-y^{[a,b]})}. \quad (40)$$

Для вычисления предела в (39) воспользуемся следующими разложениями в ряд при $y = 1 + \Theta$ с точностью до $o(\Theta^3)$:

$$\begin{aligned} y^r(1-y^a) &= -\Theta a - \Theta^2 \binom{a}{2} - \Theta^2 ar, \\ 1-y^{[a,b]} &= -\Theta[a, b] - \Theta^2 \binom{[a,b]}{2}, \\ (1-y^a)(1-y^{[a,b]}) &= \Theta^2 a[a, b]. \end{aligned} \quad (41)$$

Отсюда получаем с учетом тождества $(a, b)[a, b] = ab$

$$\lim_{y \rightarrow 1} [S_2(y) - S_1(y)] = \frac{b}{2} + \frac{(a, b)}{2} - K_0(a, b). \quad (42)$$

Если же $K_0 = 0$, то

$$S_2(y) - S_1(y) = \frac{by^{[a,b]}(1-y^a) - (a, b)y^a[1-y^{[a,b]}]}{y^a(1-y^{[a,b]})(1-y^a)}. \quad (43)$$

Используя те же самые аргументы, что и раньше, из (43) получаем

$$\lim_{y \rightarrow 1} [S_2(y) - S_1(y)] = -\frac{b}{2} + \frac{(a, b)}{2}. \quad (44)$$

Из (42) и (44) получаем (31).

ПРИМЕРЫ. 1) Если $a = 1$, $b = 2$, то $Z_b \setminus Z_a = \{-1\}$ и сравнение

$$x + n \equiv 0 \pmod{2}$$

имеет минимальные решения $K_0 = 1$, если $n \equiv 1 \pmod{2}$ и $K_0 = 0$ при $n \equiv 0 \pmod{2}$. Поэтому

$$\begin{aligned} S_n(1, 2) &= \frac{b}{2} + \frac{(a, b)}{2} - 1 \cdot (a, b) = 1 + \frac{1}{2} - 1 = \frac{1}{2} \quad \text{при } n \equiv 1 \pmod{2}, \\ S_n(1, 2) &= -\frac{2}{2} + \frac{1}{2} = -\frac{1}{2} \quad \text{при } n \equiv 0 \pmod{2}. \end{aligned}$$

Эти формулы соответствуют очевидному ответу

$$S_n(1, 2) = \sum_{\alpha \in Z_2 \setminus Z_1} \frac{1}{\alpha^n(\alpha^a - 1)} = \frac{(-1)^{n+1}}{2}.$$

4. Оценки $J_M(a, b, m, n)$. Мы используем лемму 6 для оценки третьей и четвертой суммы в формуле (22).

СЛЕДСТВИЕ 1. Если $(am, bn) = 1$, то

$$\begin{aligned} \left| \frac{1}{a} \sum_{u|P, v|Q} \frac{\mu(u)\mu(v)}{u} S_M(bv, au) \right| &\leq \frac{1}{2} \tau(P)\tau(Q), \\ \left| \frac{1}{b} \sum_{u|P, v|Q} \frac{\mu(u)\mu(v)}{v} S_M(au, bv) \right| &\leq \frac{1}{2} \tau(P)\tau(Q), \end{aligned} \quad (45)$$

где $\tau(N)$ – число делителей числа N .

ДОКАЗАТЕЛЬСТВО. Так как

$$S_M(bv, au) = \sum_{\alpha \in Z_{au} \setminus Z_{bv}} \frac{1}{\alpha^M(\alpha^{bv} - 1)} \quad (46)$$

и из $(am, bn) = 1$ следует, что $(a, b) = 1$, то можно использовать формулу (26), из которой следует, что

$$|S_n(a, b)| < \frac{b}{2}.$$

Поэтому из (43) вытекает $|S_M(bv, au)| \leq au/2$, $|S_M(au, bv)| \leq bv/2$. Отсюда получаем

$$\left| \frac{1}{a} \sum_{u|P, v|Q} \frac{\mu(u)\mu(v)}{u} S_M(bv, au) \right| \leq \frac{\tau(P)\tau(Q)}{2}.$$

Аналогично доказывается вторая из оценок (45).

Из оценок леммы 5 и неравенств (45) следует основное утверждение этой работы.

ТЕОРЕМА 2. Если $(am, bn) = 1$, то система (4) разрешима при

$$M > \frac{abPQ\tau(P)\tau(Q)}{\varphi(P)\varphi(Q)}.$$

ДОКАЗАТЕЛЬСТВО. Используя теорему 1, лемму 5 и оценки (45) получаем неравенство

$$J_M(am, bn) > \frac{M}{ab} \frac{\varphi(P)}{P} \frac{\varphi(Q)}{Q} - \tau(P)\tau(Q). \quad (47)$$

Из (47) вытекает утверждение теоремы 2.

Используя предыдущие аргументы получаем также следующее утверждение.

ТЕОРЕМА 3. Если $(am, bn) = 1$ и $M \rightarrow \infty$, то

$$J_M(am, bn) \sim \frac{M}{ab} \frac{\varphi(P)\varphi(Q)}{PQ}. \quad (48)$$

Здесь P, Q – произведение всех простых делителей чисел m и n соответственно.

Отметим также, что условие $(am, bn) = 1$ является лишь достаточным для разрешимости системы

$$\begin{cases} ax + by = M, \\ (m, x) = (n, y) = 1. \end{cases} \quad (49)$$

Если это условие не выполнено, то система (49), вообще говоря, не разрешима, что показывает следующий простой пример

$$\begin{cases} 2x + 3y = 3M, \\ (x, 3) = (y, r) = 1. \end{cases} \quad (50)$$

Система (50) не имеет решений ни для каких $M > 0$ и r . Ясно, что в этом случае: $(am, bn) = (\delta, 3r) > 3$.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

- [1] И. Д. Кан, Б. С. Стечкин, И. В. Шарков, “К проблеме Фробениуса трех аргументов”, *Матем. заметки*, **62:4** (1997), 626–629.
- [2] J. J. Sylvester, “Mathematical questions with their solutions”, *Educational Times*, **41** (1884), 171–178.
- [3] M. Beck, R. Diaz, S. Robins, “The Frobenius problem, rational polytopes and Fourier–Dedekind sums”, *J. Number Theory*, **96:1** (2002), 1–21.
- [4] А. А. Евдокимов, “Нумерация подмножеств конечного множества”, *Методы дискретного анализа*, **34** (1980), 8–26.
- [5] W. T. Trotter Jr., P. Erdős, “When the Cartesian product of directed cycles is Hamiltonian”, *J. Graph Theory*, **2:2** (1978), 137–142.
- [6] В. К. Леонтьев, “Гамильтоновы циклы в торической решетке”, *ДАН*, **395:5** (2004), 590–591.
- [7] В. К. Леонтьев, “Об аналогах проблемы Фробениуса”, *ДАН*, **444:6** (2012), 605.
- [8] J. M. Gessel, “Generation function and generalized Dedekind sums”, *Electron. J. Comb.*, **4:2** (1997), R11.

В. К. Леонтьев

Вычислительный центр им. А. А. Дородницына,

Федеральный исследовательский центр

«Информатика и управление»

Российской академии наук, г. Москва

E-mail: vkleontiev@yandex.ru

Поступило

30.11.2010

Исправленный вариант

28.04.2016