

О ПРОБЛЕМЕ ФРОБЕНИУСА

В. К. Леонтьев

Вычислительный центр им. А. А. Дородницына ФИЦ ИУ РАН,
ул. Вавилова, 40, 119333 Москва, Россия
E-mail: vkleontiev@yandex.ru

Аннотация. Рассматривается классическая проблема Фробениуса (проблема монет Фробениуса). С помощью метода производящих функций находится выражение для числа решений диофантова уравнения. В качестве следствия из этого результата вытекает известная теорема Сильвестра. Кроме того, получено не только выражение для числа Фробениуса, но и формулы для тех значений переменных, на которых это число достигается. Проблематика данной работы тесно связана с задачами дискретной оптимизации, а также с криптографическими методами защиты информации. Табл. 1, библиогр. 25.

Ключевые слова: диофантово уравнение, проблема Фробениуса, теорема Сильвестра, производящая функция, метод коэффициентов.

Введение

Данная работа посвящена следующей задаче.

Пусть $A = \{a_1, \dots, a_k\}$, $k > 1$, — возрастающая последовательность натуральных чисел, $\langle A \rangle$ — аддитивная полугруппа, порождённая множеством A . Полугруппа $\langle A \rangle$ состоит из всех линейных комбинаций чисел a_1, \dots, a_k с целыми неотрицательными коэффициентами.

Множество A называется примитивным, если $\text{НОД}(a_1, \dots, a_k) = 1$

Для случая $k = 2$ известен следующий результат (см. [1–3]).

Теорема Сильвестра. *Порождённая взаимно простыми числами a и b полугруппа содержит все целые числа, начиная с $N(a, b) = (a - 1) \times (b - 1)$.*

Добавляя образующие, из этой теоремы легко вывести более общий результат.

Исследование выполнено при поддержке Российского фонда фундаментальных исследований (проект № 20–01–00645).

Теорема 1. Если множество A примитивное, то найдётся такое число $N(a_1, \dots, a_k)$, что $t \in \langle A \rangle$ при любом натуральном $t > N(a_1, \dots, a_k)$.

Это число $N(a_1, \dots, a_k)$ называется числом Фробениуса (см. [4]). Заметим, что есть разночтения в терминологии. В некоторых источниках, например в [5], числом Фробениуса называют величину $N(a_1, \dots, a_k) - 1$, т. е. максимальное $t \notin \langle A \rangle$. Мы здесь будем придерживаться первого варианта.

Пусть \mathbb{N} — множество всех натуральных чисел. Обозначим через $C(A)$ множество всех чисел t таких, что $t \notin \mathbb{N}/\langle A \rangle$.

Определение $N(a_1, \dots, a_k)$ известно как диофантова проблема Фробениуса (ПФ). Расширенная проблема Фробениуса (РПФ) — это определение множества $C(A)$.

Проблема Фробениуса и РПФ — очень популярная тематика исследований алгебраистов, специалистов в теории чисел, криптографов, а в последние десятилетия она привлекает внимание теоретиков в области защиты информации (см., например, [5–7]).

В [7] опубликован обзор результатов по этим проблемам до 2005 г. ПФ и РПФ для $k = 2$ решены ещё в 1884 г. в [1–3]. Для произвольного случая изучались асимптотика и оценки числа Фробениуса, например в [8, 9].

Алгоритм решения РПФ при $k = 3$ получен в [10], оценена сложность алгоритма.

Формула решения ПФ при $k > 2$ не была получена, уже при $k = 3$ доказано в [11], что не найдётся конечного числа полиномов, выражающих в общем случае число $N(a_1, a_2, a_3)$ с помощью разбиения области определения. Точные формулы имеются лишь для частных случаев.

Для случая $k = 3$ в [12] наряду с собственными результатами автор даёт и обзор некоторых аспектов состояния проблемы на 2017 г. Различные частные случаи для $k = 3$ изучаются, например, в статьях [12, 13]. Существуют и различные специфические постановки, которые выглядят как обобщение ПФ. В качестве примера можно привести [14]. С алгебраической точки зрения можно наложить определённые ограничения на подгруппу $\langle A \rangle$ и решать ПФ для полученного частного случая, как это делается в статьях [15–17].

Проблема исследовалась и с алгоритмической точки зрения. Например, в [18] представлен теоретико-графовый алгоритм определения числа $N(a_1, \dots, a_k)$ со сложностью $O(a_1(k + \log a_1))$. Здесь ПФ сведена к поиску определённого вида наибольшего кратчайшего пути в орграфе с a_1 вершинами и ka_1 дугами, где из каждой вершины исходит k дуг весов a_1, \dots, a_k соответственно.

В [19] для РПФ и ПФ предложена редукция множества A к собственному подмножеству, снижающая сложность задачи в ряде случаев. Алгоритмы не дают аналитической формулы для ПФ.

Верхние оценки для числа Фробениуса тоже представляют прикладной интерес, как это, например, указано в учебнике по криптографическим методам защиты информации [5]. В [5–7] приведены примеры результатов на эту тему.

Настоящая работа является продолжением исследований возможности применения аппарата производящих функций и метода коэффициентов (см. [20]) к решению вопроса о разрешимости и нахождению числа решений диофантовых уравнений, систем уравнений, неравенств и систем неравенств. В качестве примеров этих исследований можно привести работы [21, 22].

В разд. 1 приведены вспомогательные результаты и некоторые сведения о диофантовых уравнениях и проблеме Фробениуса, которые помогают проиллюстрировать основной результат, изложенный в разд. 2.

1. Диофантово уравнение и проблема Фробениуса

Диофантово уравнение имеет вид

$$\sum_{i=1}^k a_i x_i = n, \quad (1)$$

где n и a_i , $i = 1, \dots, k$, — целые числа, а $x = (x_1, \dots, x_k)$ — k -мерный целочисленный вектор.

Частные случаи уравнения общего вида получаются путём наложения некоторых ограничений на параметры и неизвестные или декларирования их определённых свойств.

Заметим также, что ни один коэффициент в разрешимом уравнении не может превосходить n . В противном случае слагаемое с этим коэффициентом является «фиктивным».

Обозначим через $t_n(a_1, \dots, a_k)$ число решений уравнения (1). Ясно, например, что положительность этого числа влечёт разрешимость уравнения.

Если на область определения переменных наложены ограничения, то, чем шире область определения, тем вероятнее разрешимость уравнения (1).

Заметим, что нахождение числа решений уравнения (1) тесно связано с известной задачей о разбиениях, т. е. с нахождением числа решений уравнения

$$x_1 + x_2 + \dots + x_k = n.$$

Если на n нет никаких ограничений, то число решений уравнения — это число разбиений n на натуральные слагаемые. Этот факт формально

может быть выражен в терминах преобразования $x = (x_1, \dots, x_k)$ в вектор $y = (y_1, \dots, y_n)$, где y_r , $r = 1, \dots, n$, — число координат вектора x , равных натуральному r .

Таким образом, нахождение числа разбиений P_n для фиксированного n эквивалентно нахождению числа решений диофантова уравнения

$$n = \sum_{i=1}^k x_i = \sum_{r=1}^n r y_r.$$

Пусть $L(x_1, \dots, x_k)$ — линейная форма

$$L(x_1, \dots, x_k) = \sum_{i=1}^k a_i x_i. \quad (2)$$

Для случая булевых переменных через $L^*(x_1, \dots, x_k)$ обозначим множество значений этой формы. Тогда вопрос о разрешимости эквивалентен вопросу о принадлежности n множеству $L^*(x_1, \dots, x_k)$.

Рассмотрим производящую функцию

$$F_{a_1, \dots, a_k}(z) = \sum_{n=0}^{\infty} z^n t_n(a_1, \dots, a_k) \quad (3)$$

последовательности $\{t_n(a_1, \dots, a_k)\}$. Для неё известна

Теорема 2. *Справедливо равенство*

$$F_{a_1, \dots, a_k}(z) = \sum_{n=0}^{\infty} z^n t_n(a_1, \dots, a_k) = \prod_{p=1}^k \frac{1}{1 - z^{a_p}}. \quad (4)$$

Доказательство. По определению имеем следующую цепочку равенств:

$$\begin{aligned} F_{a_1, \dots, a_k}(z) &= \sum_{n=0}^{\infty} z^n t_n(a_1, \dots, a_k) = \sum_{\{x_1, \dots, x_k\}} z^{a_1 x_1 + \dots + a_k x_k} \\ &= \prod_{i=1}^k \sum_{x_i=0}^{\infty} z^{a_i x_i} = \prod_{i=1}^k \frac{1}{1 - z^{a_i}}. \end{aligned}$$

Теорема 2 доказана.

Заметим, что доказанное выражение для производящей функции приведено, например, в книге Риордана [23].

Следствие 1. *Справедливо соотношение*

$$t_n(a_1 \dots a_k) = \frac{1}{2\pi i} \int_{|z|=\rho} \frac{F_{a_1, \dots, a_k}(z)}{z^{n+1}} dz, \quad \rho < 1.$$

Очевидно, что эти формулы позволяют найти $t_n(a_1, \dots, a_k)$ путём сравнения коэффициентов в левой и правой частях. Кроме того, с их помощью можно найти оценки для $t_n(a_1, \dots, a_k)$ и некоторые характеристики этой величины.

Пример 1. Если $a_i = 1$ для всех $i = 1, \dots, k$, то $F_{1, \dots, 1}(z) = (1 - z)^{-k}$ и $t_n(1, \dots, 1) = (-1)^n C_n^{-k} = C_n^{n+k-1} = C_{k-1}^{n+k-1}$. Это хорошо известная формула для числа разбиений натурального b в сумму не более n слагаемых.

Пример 2. Если $k = 2$, то поведение функции $t_n(a_1, a_2)$ в значительной мере определяется известной теоремой Сильвестра (см., например, [1–3]). Согласно ей при условии взаимной простоты $(a_1, a_2) = 1$ уравнение разрешимо, если $b > a_1 a_2$, и эта граница достижима.

Если $t_n(a_1, \dots, a_k) > 0$ для всех $n \geq n_0$ и $t_n(a_1, \dots, a_k) = 0$ для $n = n_0 - 1$, то значение числа Фробениуса равно n_0 .

Для случая булевых переменных формула (4) имеет вид

$$F_{a_1, \dots, a_k}(z) = \sum_{n=0}^{\infty} z^n t_n(a_1, \dots, a_k) = \prod_{p=1}^n (1 + z^{a_p}). \quad (5)$$

Из (5) следует выражение для $t_n(a_1, \dots, a_k)$:

$$t_n(a_1, \dots, a_k) = \frac{1}{2\pi i} \int_{|z|=p} \frac{(1 + u^{a_1}) \dots (1 + u^{a_k})}{u^{n+1}} du, \quad \rho < 1.$$

2. Число решений уравнения в двумерном случае и его связь с проблемой Фробениуса

Введённые ниже обозначения будут использованы всюду в дальнейшем тексте. Рассмотрим диофантово уравнение с двумя переменными

$$ax + by = n. \quad (6)$$

Здесь все числа натуральные. Как известно, такие уравнения разрешимы для всех n , начиная с некоторого числа Фробениуса $n_0(a, b)$. По теореме Сильвестра для взаимно простых a и b

$$n_0(a, b) = ab - (a + b).$$

Используя метод производящих функций, получим формулу для числа решений $t_n(a, b)$ уравнения (6) при условии $(a, b) = 1$, из которой будет следовать не только результат Сильвестра, но и формула для x_0 и y_0 , на которых «лежит» граница разрешимости.

Пусть ξ^a — множество всех корней степени a из единицы, а $\bar{\xi}^a$ — множество всех корней степени a из единицы за исключением единицы.

Лемма 1. *Справедлива формула*

$$t_n(a, b) = \frac{n}{ab} + \frac{a+b}{2ab} - \frac{1}{a} \sum_{\xi^{-a}} \frac{1}{\xi^n(\xi^b - 1)} - \frac{1}{b} \sum_{\xi^{-a}} \frac{1}{\xi^n(\xi^a - 1)}. \quad (7)$$

ДОКАЗАТЕЛЬСТВО. Согласно введённым обозначениям производящая функция для $t_n(a, b)$ выглядит следующим образом:

$$\sum_{n=0}^{\infty} t_n(a, b) z^n = \sum_{x, y} z^{ax+by}.$$

Далее, используя формулу Коши, получаем

$$t_n(a, b) = \frac{1}{2\pi i} \int_{|u|=\rho} \frac{1}{z^{n+1}(1-z^a)(1-z^b)} dz, \quad \rho < 1. \quad (8)$$

Если $f_n(z) = \frac{1}{z^{n+1}(1-z^a)(1-z^b)}$, то $t_n(a, b)$ равно вычету в нуле функции $f_n(z)$. Остальные особые точки следующие: $z_1 = \infty$, $z_2 = 1$, $z_a = \{z \neq 1 \mid z^a - 1 = 0\}$, $z_b = \{z \neq 1 \mid z^b - 1 = 0\}$.

Поскольку по условию a и b взаимно просты, то $z_a \cap z_b = \emptyset$. Так как сумма вычетов относительно всех особых точек функции $f_n(z)$ равна нулю и $\operatorname{res}_{z=z_1} f_n(z) = 0$ (это равенство нулю вычета в бесконечно удалённой точке подробно доказано, например, [24, с. 221]), получаем

$$\operatorname{res}_{z=0} f_n(z) = -\operatorname{res}_{z=1} f_n(z) - \sum_{z \in z_a} \operatorname{res} f_n(z) - \sum_{z \in z_b} \operatorname{res} f_n(z).$$

Заметим далее, что точка $z_2 = 1$ является полюсом порядка два, поэтому

$$\operatorname{res}_{z=z_2} f_n(z) = \frac{d}{dz} [f_n(z)(z-1)^2] = -\frac{a+b}{2ab} - \frac{n}{ab}. \quad (9)$$

Все точки из z_a являются простыми полюсами $f_n(z)$. Представим $f_n(z)$ в виде

$$f_n(z) = \frac{z^{-n-1}}{(1-z^a)(1-z^b)} = \frac{u(z)}{v(z)}$$

и воспользуемся известной формулой

$$\operatorname{res}_{\alpha \in z_a} f_n(z) = \frac{u(\alpha)}{v'(\alpha)} = \frac{1}{a\alpha^n(\alpha^b - 1)},$$

откуда следует, что

$$S_n(a, b) = \sum_{z \in z_a} \operatorname{res} f_n(z) = \frac{1}{a} \sum_{\substack{\alpha \neq 1, \\ \alpha^a = 1}} \frac{1}{\alpha^n(\alpha^b - 1)}. \quad (10)$$

Аналогично

$$S_n(b, a) = \sum_{z \in z_b} \operatorname{res} f_n(z) = \frac{1}{b} \sum_{\substack{\alpha \neq 1, \\ \alpha^a = 1}} \frac{1}{\alpha^n (\alpha^a - 1)}. \quad (11)$$

Из формул (9)–(11) следует утверждение леммы. Лемма 1 доказана.

Приведём простую и хорошо известную формулу.

Лемма 2. *Справедлива формула*

$$\sum_{\xi^a=1} \xi^m = \begin{cases} a, & \text{если } m \equiv 0 \pmod{a}, \\ 0, & \text{если } m \not\equiv 0 \pmod{a}. \end{cases} \quad (12)$$

Суммирование в левой части (12) ведётся по всем корням степени a из единицы.

Применить эту формулу к вычислению $S_n(a, b)$ мешает то обстоятельство, что $\alpha \neq 1$. Эта трудность преодолевается стандартным приёмом, заключающимся в рассмотрении следующей аналитической функции в области $|z| < 1$:

$$\Phi(z) = \sum_{\xi^a=1} \frac{1}{\xi^n (1 - (z\xi)^b)}, \quad (13)$$

которая связана с $S_n(a, b)$ так:

$$-aS_n(a, b) = \lim_{z \rightarrow 1} \left[\Phi(z) - \frac{1}{1 - z^b} \right]. \quad (14)$$

Рассмотрим сравнение

$$by \equiv n \pmod{a}, \quad (15)$$

где y пробегает всё множество неотрицательных целых чисел, а параметры a и b взаимно простые. Пусть $y_0(n)$ — минимальное решение сравнения (15). Тогда все решения этого сравнения заключены в последовательности $y = y_0(n) + at$, $t = 0, 1, 2, \dots$.

Пример 3. Если $a = 2$, $b = 3$, то $y_0(n) = \begin{cases} 0, & \text{если } n \equiv 0 \pmod{2}, \\ 1, & \text{если } n \equiv 1 \pmod{2}. \end{cases}$

Если $a = 5$, $b = 8$, то в табл. 1 приведены все значения $y_0(n)$ для различных значений $n \bmod 5$.

Таблица 1

$n \bmod 5$	0	1	2	3	4
$y_0(n)$	0	2	4	1	3

Мы готовы к нахождению $S_n(a, b)$.

Лемма 3. *Справедлива формула*

$$S_n(a, b) = \frac{y_0(n)}{a} - \frac{a-1}{2a}. \quad (16)$$

ДОКАЗАТЕЛЬСТВО. Преобразуем аналитическую функцию $\Phi(z)$, введённую выше:

$$\Phi(z) = \sum_{\xi^a=1} \frac{1}{\xi^n(1-(z\xi)^b)} = \sum_{\xi^a=1} \frac{1}{\xi^n} \sum_{y=0}^{\infty} (z\xi)^{by} = \sum_{y=0}^{\infty} (z)^{by} \sum_{\xi^a=1} \xi^{by-n}. \quad (17)$$

Заметим, что внутренняя сумма в (17) отлична от нуля лишь при условии $by \equiv n \pmod{a}$, поэтому, как было показано выше в лемме 2 и пояснениях к ней, выполняется равенство $y = y_0(n) + at$, $t = 0, 1, 2, \dots$. Отсюда следует, что

$$\Phi(z) = a \sum_{t=0}^{\infty} z^{b(y_0(n)+at)} = az^{by_0(n)} \frac{1}{1-z^{ab}},$$

Напомним, что функция $\Phi(z)$ связана с $S_n(a, b)$ равенством (14). Стало быть,

$$-aS_n(a, b) = \lim_{z \rightarrow 1} \left[az^{by_0(n)} \frac{1}{1-z^{ab}} - \frac{1}{1-z^b} \right]. \quad (18)$$

Найдём этот предел, используя правило Лопиталя. Пусть

$$\frac{u(z)}{v(z)} = az^{by_0(n)} \frac{1}{1-z^{ab}} - \frac{1}{1-z^b} = \frac{az^{by_0(n)} - az^{b+by_0(n)} - 1 + z^{ab}}{1-z^{ab} - z^b + z^{ab+b}}.$$

После дифференцирования и очевидных преобразований получаем

$$\frac{u''(z)}{v''(z)} = \frac{a - 2y_0(n) - 1}{2}. \quad (19)$$

Из 18 и 19 следует, что

$$S_n(a, b) = \frac{y_0(n)}{a} - \frac{a-1}{2a}. \quad (20)$$

Лемма 3 доказана.

Следствие 2. *Справедлива формула*

$$S_n(b, a) = \frac{x_0(n)}{b} - \frac{b-1}{2b}. \quad (21)$$

Основной результат работы может быть сформулирован в виде следующего утверждения.

Теорема 3. *Если $(a, b) = 1$, то*

$$t_n(a, b) = \frac{n}{ab} - \frac{x_0(n)a + y_0(n)b}{ab} + 1, \quad (22)$$

где $x_0(n)$ и $y_0(n)$ — минимальные решения сравнений $ax \equiv n \pmod{b}$ и $by \equiv n \pmod{a}$.

ДОКАЗАТЕЛЬСТВО прямо следует из формул (7), (8), (11), (20), (21).

Действительно, выше в лемме 1 с помощью метода производящих функций получена формула (7) для числа решений $t_n(a, b)$ уравнения (6) при условии $(a, b) = 1$. Для этого в явном виде была выписана производящая функция для $t_n(a, b)$, а затем с использованием формулы Коши задача была сведена к вычислению интеграла (8).

В ходе доказательства леммы 1 получены две ключевые формулы для сумм вычетов (10) и (11) в двух классах особых точек, которые в сумме и должны дать $t_n(a, b)$. Однако эти суммы найти напрямую, по-видимому, сложно. Проблему удалось обойти с помощью леммы 2, на основе которой была введена вспомогательная аналитическая функция (14). С использованием этой функции в лемме 3 и следствии 2 удалось найти сумму всех вычетов, к которым сводится интеграл (8).

Таким образом, утверждение (22) данной теоремы достигается простым суммированием выражений (20) и (21). Теорема 3 доказана.

Следствие 3. При взаимно простых a и b из неравенства $n > ab - (a + b)$ следует неравенство $t_n(a, b) > 0$.

ДОКАЗАТЕЛЬСТВО. Так как $x_0 \leq b - 1$ и $y_0 \leq a - 1$, то

$$t_n(a, b) = \frac{n}{ab} - \frac{x_0(n)a + y_0(n)b}{ab} + 1 \geq \frac{n - (ab - a - b)}{ab},$$

но по условию $n > ab - (a + b)$, откуда следует неравенство $t_n(a, b) > 0$. Следствие 3 доказано.

Следствием теоремы 3 является известная формула Сильвестра для двумерного числа Фробениуса.

Формулу (22) можно записать в более «строгой» форме. Пусть $\varphi(k)$ — функция Эйлера (число чисел, меньших k и взаимно простых с k). Тогда очевидно, что сравнения $ax \equiv n \pmod{b}$ и $by \equiv n \pmod{a}$ при взаимно простых a и b имеют единственные минимальные решения, представимые в виде

$$x_0(n) = na^{\varphi(b)-1} \pmod{b}, \quad y_0(n) = nb^{\varphi(a)-1} \pmod{a}.$$

Отсюда получаем другое выражение для формулы, задающей число решений уравнения (6):

$$t_n(a, b) = \frac{n}{ab} - \frac{a(na^{\varphi(b)-1} \pmod{b}) + b(nb^{\varphi(a)-1} \pmod{a})}{ab} + 1. \quad (23)$$

Заметим, что в [25, разд. 5.7] рассмотрены задачи, связанные с проблемой Фробениуса для двух переменных, и приведён ряд результатов. Однако

формулы (22) и (23) там отсутствуют, а их вывод из приведённых в книге утверждений является, по нашему мнению, нетривиальной задачей.

Пример 4. Рассмотрим уравнение $4x + 7y = n$.

При $n = 12$ из (22) следует, что $t_{12}(4, 7) = \frac{12}{28} - \frac{x_0(n)4 + y_0(n)7}{28} + 1$. Сравнения $4x \equiv 12 \pmod{7}$ и $7y \equiv 12 \pmod{4}$ имеют минимальные решения $x_0(n) = 3$ и $y_0(n) = 0$. Отсюда $t_{12}(4, 7) = \frac{12}{28} - \frac{12}{28} + 1 = 1$, что соответствует решению $(3, 0)$.

При $n = 13$ из (18) следует, что $t_{13}(4, 7) = \frac{13}{28} - \frac{x_0(n)4 + y_0(n)7}{28} + 1$. Сравнения $4x \equiv 13 \pmod{7}$ и $7y \equiv 13 \pmod{4}$ имеют минимальные решения $x_0(n) = 5$ и $y_0(n) = 3$. Отсюда $t_{13}(4, 7) = \frac{13}{28} - \frac{41}{28} + 1 = 0$, что соответствует тому факту, что решений у уравнения нет.

При $n = 32$ из (18) следует, что $t_{32}(4, 7) = \frac{32}{28} - \frac{x_0(n)4 + y_0(n)7}{28} + 1$. Сравнения $4x \equiv 32 \pmod{7}$ и $7y \equiv 32 \pmod{4}$ имеют минимальные решения $x_0(n) = 1$ и $y_0(n) = 0$. Отсюда $t_{32}(4, 7) = \frac{32}{28} - \frac{4}{28} + 1 = 2$, что соответствует двум решениям $(8, 0)$ и $(1, 4)$.

Следствие 4. Справедлива формула

$$t_{n+ab}(a, b) = t_n(a, b) + 1. \quad (24)$$

ДОКАЗАТЕЛЬСТВО. Рассмотрим функцию

$$L_n(a, b) = \frac{a(na^{\varphi(b)-1} \bmod b) + b(nb^{\varphi(a)-1} \bmod a)}{ab}.$$

Заметим, что $L_{n+ab}(a, b) = L_n(a, b)$. Имеем периодическую функцию с периодом ab . Отсюда и из (23) следует (24). Следствие 4 доказано.

ЛИТЕРАТУРА

1. **Sylvester J. J.** Problem 7382 // Educ. Times, J. Coll. Precept. 1883. V. 36, No. 266. P. 177.
2. **Curran Sharp W. J.** Problem 7382. Solution // Educ. Times, J. Coll. Precept. 1883. V. 36, No. 271. P. 315.
3. **Sylvester J. J.** Problem 7382 // Mathematical questions with their solutions: From the "Educational Times". V. 41. London: C. F. Hodgson, 1884. P. 21.
4. **Арнольд В. И.** Экспериментальное наблюдение математических фактов. М.: МЦНМО, 2006. 119 с.
5. **Фомичёв В. М., Мельников Д. А.** Криптографические методы защиты информации. М.: Юрайт, 2017.
6. **Erdős P., Graham R. L.** On a linear Diophantine problem of Frobenius // Acta Arithmetica. 1972. V. 21. P. 399–408.
7. **Alfonsín J. R.** The Diophantine Frobenius problem. London: Oxford Univ. Press, 2005.
8. **Arnold V. I.** Arithmetical turbulence of selfsimilar fluctuations statistics of large Frobenius numbers of additive semigroups of integer // Moscow Math. J. 2007. V. 7, No. 2. P. 173–193.

9. Арнольд В. И. Слабые асимптотики числа решений диофантовых задач // Функцион. анализ и его прил. 1999. Т. 33, № 4. С. 65–66.
10. Фомичёв В. М. Оценка экспонента некоторых графов с помощью чисел Фробениуса для трёх аргументов // Прикл. дискрет. математика. 2014. № 2. С. 88–96.
11. Curtis F. On formulas for the Frobenius number of a numerical semigroup // Math. Scand. 1990. V. 67. P. 190–192.
12. Tripathi A. Formulae for the Frobenius number in three variables // J. Number Theory. 2017. V. 170. P. 368–389.
13. Савельев В. П., Шевченко В. Н. Задача Фробениуса для трёх чисел // Сб. статей Междунар. науч.-практ. конф. М: ЕФИР, 2019. С. 10–15.
14. Song K. The Frobenius problem for numerical semigroups generated by the Thabit numbers of the first, second kind base b and the Cunningham numbers // Bull. Korean Math. Soc. 2020. V. 57, No. 3. P. 623–647.
15. Rosales J. C., Branco M. B., Torráo D. The Frobenius problem for Thabit numerical semigroups // J. Number Theory. 2015. V. 155. P. 85–99.
16. Rosales J. C., Branco M. B., Torráo D. The Frobenius problem for repunit numerical semigroups // Ramanujan J. 2016. V. 40. P. 323–334.
17. Rosales J. C., Branco M. B., Torráo D. The Frobenius problem for Mersenne numerical semigroups // Math. Z. 2017. V. 286. P. 741–749.
18. Nijenhuis M. A minimal-path algorithm for the “money changing problem” // Amer. Math. Mon. 1979. V. 86. P. 832–835.
19. Фомичёв В. М. Эквивалентные по Фробениусу примитивные множества чисел // Прикл. дискрет. математика. 2014. № 1. С. 20–26.
20. Егорычев Г. П. Интегральное представление и вычисление комбинаторных сумм. Новосибирск: Наука, 1977. 281 с.
21. Леонтьев В. К., Гордеев Э. Н. Производящие функции в задаче о ранце // Докл. Академии наук. 2018. Т. 481, № 5. С. 478–480.
22. Леонтьев В. К., Гордеев Э. Н. О некоторых комбинаторных свойствах задачи о рюкзаке // Журн. вычисл. математики и мат. физики. 2019. Т. 59, № 8. С. 1439–1447.
23. Риордан Дж. Введение в комбинаторный анализ. М.: Изд-во иностр. лит., 1963. 287 с.
24. Сидоров Ю. В., Федорюк М. В., Шабунин М. И. Лекции по теории функций комплексного переменного. М.: Наука, 1989. 480 с.
25. Харди Г. Г. Двенадцать лекций о Рамануджане. М.: Ин-т компьютер. иссл., 2002. 336 с.

Леонтьев Владимир Константинович

Статья поступила

6 декабря 2021 г.

После доработки —

19 января 2022 г.

Принята к публикации

21 января 2022 г.

ON THE FROBENIUS PROBLEM

V. K. Leontiev

Dorodnitsyn Computing Center,
40 Vavilov Street, 119333 Moscow, Russia
E-mail: vkleontiev@yandex.ru

Abstract. The classical Frobenius problem (the Frobenius coin problem) is considered. Using the method of generating functions, a formula is found for the number of solutions of the Diophantine equation associated with this problem. Special attention is paid to the case of two variables, which is considered to be investigated, but there are no rigorous proofs in some of its aspects. As a consequence of the result obtained in this work, both the well-known Sylvester theorem (expressions for the Frobenius number) and formulas for those values of variables on which this number is achieved follow. The problems of this work are closely related to algorithms for solving discrete optimization problems, as well as cryptographic methods in information security. Tab. 1, bibliogr. 25.

Keywords: Diophantine equation, Frobenius problem, Sylvester's theorem, generating function, coefficient method.

REFERENCES

1. **J. J. Sylvester**, Problem 7382, *Educ. Times, J. Coll. Precept.* **36** (266), 177 (1883).
2. **W. J. Curran Sharp**, Problem 7382. Solution, *Educ. Times, J. Coll. Precept.* **36** (271), 315 (1883).
3. **J. J. Sylvester**, Problem 7382, in *Mathematical Questions with Their Solutions: From the "Educational Times"*, Vol. 41 (C. F. Hodgson, London, 1884), p. 21.
4. **V. I. Arnol'd**, *Experimental Observations of Mathematical Facts* (MTsNMO, Moscow, 2006) [Russian].
5. **V. M. Fomichev** and **D. A. Mel'nikov**, *Cryptographic Methods of Information Security* (Yurayt, Moscow, 2017) [Russian].

This research is supported by the Russian Foundation for Basic Research (Project 20-01-00645).

English version: Journal of Applied and Industrial Mathematics **16** (2) (2022).

6. **P. Erdős** and **R. L. Graham**, On a linear Diophantine problem of Frobenius, *Acta Arithmetica* **21**, 399–408 (1972).
7. **J. R. Alfonsín**, The Diophantine Frobenius Problem (Oxford Univ. Press, London, 2005).
8. **V. I. Arnol'd**, Arithmetical turbulence of selfsimilar fluctuations statistics of large Frobenius numbers of additive semigroups of integer, *Moscow Math. J.* **7** (2), 173–193 (2007).
9. **V. I. Arnol'd**, Weak asymptotics for the numbers of solutions of Diophantine problems, *Funkts. Anal. Prilozh.* **33** (4), 65–66 (1999) [Russian] [*Funct. Anal. Appl.* **33** (4), 292–293 (1999)].
10. **V. M. Fomichev**, Estimates for exponent of some graphs by Frobenius's numbers of three arguments, *Prikl. Diskretn. Mat.*, No. 2, 88–96 (2014) [Russian].
11. **F. Curtis**, On formulas for the Frobenius number of a numerical semigroup, *Math. Scand.* **67**, 190–192 (1990).
12. **A. Tripathi**, Formulae for the Frobenius number in three variables, *J. Number Theory* **170**, 368–389 (2017).
13. **V. P. Savelyev** and **V. N. Shevchenko**, The Frobenius problem for three numbers, in *Proc. Int. Scientific Practice Conf.* (EFIR, Moscow, 2019), pp. 10–15 [Russian].
14. **K. Song**, The Frobenius problem for numerical semigroups generated by the Thabit numbers of the first, second kind base b and the Cunningham numbers, *Bull. Korean Math. Soc.* **57** (3), 623–647 (2020).
15. **J. C. Rosales**, **M. B. Branco**, and **D. Torrão**, The Frobenius problem for Thabit numerical semigroups, *J. Number Theory* **155**, 85–99 (2015).
16. **J. C. Rosales**, **M. B. Branco**, and **D. Torrão**, The Frobenius problem for repunit numerical semigroups, *Ramanujan J.* **40**, 323–334 (2016).
17. **J. C. Rosales**, **M. B. Branco**, and **D. Torrão**, The Frobenius problem for Mersenne numerical semigroups, *Math. Z.* **286**, 741–749 (2017).
18. **M. Nijenhuis**, A minimal-path algorithm for the “money changing problem”, *Amer. Math. Mon.* **86**, 832–835 (1979).
19. **V. M. Fomichev**, Primitive sets of numbers equivalent by Frobenius, *Prikl. Diskretn. Mat.*, No. 1, 20–26 (2014) [Russian].
20. **G. P. Egorychev**, *Integral Representation and Computing of Combinatorial Sums* (Nauka, Novosibirsk, 1977) [Russian].
21. **V. K. Leontyev** and **Eh. N. Gordeev**, Generating functions in the Knapsack problem, *Dokl. Akad. Nauk* **481** (5), 478–480 (2018) [Russian] [*Dokl. Math.* **98** (1), 364–366 (2018)].
22. **Eh. N. Gordeev** and **V. K. Leontyev**, On combinatorial properties of the Knapsack problem, *Zh. Vychisl. Mat. Mat. Fiz.* **59** (8), 1439–1447 (2019) [Russian] [*Comput. Math. Math. Phys.* **59** (8), 1380–1388 (2019)].
23. **J. Riordan**, *An Introduction to Combinatorial Analysis* (John Wiley Sons, New York, 1958; Izd. Inostr. Lit., Moscow, 1963 [Russian]).
24. **Yu. V. Sidorov**, **M. V. Fedoryuk**, and **M. I. Shabunin**, *Lectures on the Theory of Functions of a Complex Variable* (Nauka, Moscow, 1989) [Russian].

-
- 25. G. H. Hardy**, Ramanujan: Twelve Lectures on Subjects Suggested by His Life and Work (AMS, Providence, RI, 1999; Inst. Komp. Issled., Moscow, 2002 [Russian]).

Vladimir K. Leontiev

Received December 6, 2021

Revised January 19, 2022

Accepted January 21, 2022