ЖУРНАЛ ВЫЧИСЛИТЕЛЬНОЙ МАТЕМАТИКИ И МАТЕМАТИЧЕСКОЙ ФИЗИКИ, 2022, том 62, № 9, с. 1447–1457

ОБЩИЕ ЧИСЛЕННЫЕ МЕТОДЫ

УДК 519.16

О ЧИСЛЕ РЕШЕНИЙ ДИОФАНТОВА УРАВНЕНИЯ И ПРОБЛЕМЕ ФРОБЕНИУСА[1)]

© 2022 г. Э. Н. Гордеев[1,*], В. К. Леонтьев[2,**]

[1] 105005 Москва, 2-я Бауманская ул., 5, стр. 1, МГТУ им. Н.Э. Баумана, Россия

[2] 119133 Москва, ул. Вавилова, 40, ВЦ РАН ФИЦ ИУ РАН, Россия

*e-mail: werhorn@yandex.ru

**e-mail: vkleontiev@yandex.ru

Поступила в редакцию 10.09.2021 г.
Переработанный вариант 28.02.2022 г.
Принята к публикации 11.04.2022 г.

Рассматриваются вопросы, касающиеся разрешимости и числа решений линейного диофантова уравнения. Наряду с общим случаем внимание уделяется комбинаторным характеристикам числа решений и среднего числа решений уравнений специального вида. Один тип уравнения представляет разбиения натурального числа на натуральные слагаемые. Другой тип – это линейные уравнения с двумя переменными, обычно исследуемые в связи с проблемой Фробениуса. Основное внимание уделено трем аспектам. Первый касается исследования наличия и числа решений диофантова уравнения при параметризации задачи по правым частям. Даются формулы и оценки для подсчета этого числа как в общем, так и в частных случаях. Второй аспект посвящен задаче о разбиении. Третий касается известной проблемы Фробениуса. Библ. 31.

Ключевые слова: диофантово уравнение, разбиения, проблема Фробениуса, булевы уравнения, число Фробениуса.

DOI: 10.31857/S0044466922090046

1. ВВЕДЕНИЕ

Линейные диофантовы уравнения и неравенства являются стандартным объектом для различного рода математических моделей, относящихся к целочисленной оптимизации, защите информации, теории чисел, геометрии и т.д.

Это уравнение имеет вид

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

где компоненты n-мерного вектора $\mathbf{x} = (x_1,\ldots,x_n)$, а также коэффициенты $b, a_1, \ldots, a_n$ – неотрицательные целые числа.

Вопросы разрешимости этого уравнения, нахождения решения и числа всех решений этого уравнения – частные случаи известной в области исследования операций и комбинаторной оптимизации задачи целочисленного линейного программирования. Эта задача или ее обобщения и сужения занимают ключевое место среди задач дискретной оптимизации, как это показано, например, в [1]. То, что задача о рюкзаке и задача целочисленного линейного программирования в общем случае являются NP-полными, было установлено в числе первых результатов подобных исследований (см., например, [1], [2]). Кроме того, в классической публикации [2] можно найти многочисленные примеры известных задач, которые к ним сводятся, и, наоборот, задача целочисленного линейного программирования (или ее булев вариант) сводится к той или иной прикладной проблеме.

С другой стороны, дифантово уравнение и его частные случаи – предмет исследования в таких областях, как алгебра, теория чисел, криптография и др. Примерами здесь могут служить работы [3]–[6].

[1)]Работа выполнена при финансовой поддержке РФФИ (код проекта 20-01-00645).

Данная статья в одной из своих частей является продолжением исследований авторов, опубликованных в [7], [8], где речь шла про задачу о рюкзаке. Ключевую роль в получении результатов там сыграл аппарат производящих функций (см. [9]), который используется и в настоящей статье. Как видно, в частности, из подробной монографии [10], где приводится обширный обзор результатов, связанных с задачей о рюкзаке, данный подход позволил в [7] и [8] получить ряд новых свойств и соотношений, касающихся числа решений этой задачи и множества ее решений.

С прикладной точки зрения, изучаемая проблематика затрагивалась авторами данной статьи в [11] и [12] в связи с криптографическими объектами: аннигиляторами и алгебраической иммунностью. Одно из ключевых утверждений публикации [11], посвященной аннигиляторам и алгебраической иммунности, базируется на анализе совместимости системы уравнений и сводится к нахождению комбинаторной характеристики (аналога ранга) матрицы.

Исследования в той же области, но другими методами проводились, например, в [13] и [14].

В данной статье уделено внимание линейному диофантову уравнению специального вида, связанного с проблемой Фробениуса.

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

Множество A называется примитивным, если НОД$(a_1, ..., a_k) = 1$.

Для случая частного случая $k = 2$ известен следующий результат (см. [15], [16]).

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

Добавляя образующие, из этой теоремы легко вывести общий результат для любого k.

Теорема 1. *Если множество A примитивное, то найдется* $N(a_1, ..., a_k)$ *такое, что* $t \in \langle A \rangle$ *при любом натуральном* $t \geq N(a_1, ..., a_k)$.

В большинстве публикаций на эту тему именно $N(a_1, ..., a_k)$ называется числом Фробениуса (см., например, [17]). Однако заметим, что есть и разночтения в терминологии. В некоторых источниках, например в [3], числом Фробениуса называют величину $N(a_1, ..., a_k) - 1$, т.е. максимальное $t \notin \langle A \rangle$.

Мы в нашем тексте будем придерживаться первого варианта.

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

Задача нахождения числа $N(a_1, ..., a_k)$ известна как диофантова проблема Фробениуса (ПФ). Нахождение же всего множества C(A) обычно называется расширенной проблемой Фробениуса (РПФ).

ПФ и РПФ – популярная тематика исследований алгебраистов, специалистов в теории чисел, криптографов, а в последние десятилетия она привлекает внимание специалистов в области защиты информации (см., например, [3]–[5]).

В [5] опубликован достаточно подробный обзор основных результатов по этим проблемам, полученных до 2005 г.

Как было уже сказано выше, ПФ и РПФ для $k = 2$ были решены еще в 1884 г. (см. [15], [16]). Для произвольного случая изучались асимптотика и оценки числа Фробениуса, например, в [18], [19].

Алгоритм решения РПФ при $k = 3$ получен в [20], оценена сложность алгоритма.

Формула решения ПФ при $k > 2$ не была получена, уже при $k = 3$ в [21] доказаны утверждения, объясняющие принципиальные затруднения, связанные с этой проблемой.

Точные формулы имеются лишь для частных случаев. Различные частные случаи для $k = 3$ изучаются во многих работах, например, в статьях [22] и [23]. В [22] наряду с собственными результатами дается и обзор некоторых аспектов состояния проблемы на 2017 г.

Существуют и специфические постановки, которые выглядят как обобщение ПФ. В качестве примера можно привести [24].

С алгебраической точки зрения можно наложить определенные ограничения на полугруппу $\langle A \rangle$ и решать ПФ для полученного частного случая, как это делается в статьях [25]–[27].

Проблема исследовалась и с алгоритмической точки зрения. Например, в [28] представлен теоретико-графовый алгоритм определения $N(a_1, ..., a_k)$ со сложностью $O(a_1(k + \log a_1))$. Здесь

ПФ сведена к поиску определенного вида наибольшего кратчайшего пути в орграфе с a_1 вершинами и с ka_1 дугами, где из каждой вершины исходит k дуг весов $a_1, \ldots, a_k$ соответственно.

В [29] для РПФ и ПФ предложена редукция множества A к собственному подмножеству, снижающая сложность задачи в ряде случаев. Алгоритмы не дают аналитической формулы для числа Фробениуса.

Верхние оценки для числа Фробениуса тоже представляют прикладной интерес, как это, например, указано в учебнике по криптографическим методам защиты информации [3]. В [3], [4] и [5] приведены примеры результатов на эту тему.

Настоящая работа является продолжением исследований о разрешимости и нахождению числа решений линейных дифантовых уравнений, систем таких уравнений, неравенств и систем неравенств.

Данная статья в одной из своих частей является продолжением исследований авторов, опубликованных в [7], [8], где речь шла про задачу о рюкзаке, и непосредственным продолжением работы [30].

Статья состоит из введения, трех разделов и заключения. В разд. 2 исследуются линейное диофантово уравнение общего вида и один частный случай. Разд. 3 посвящен проблеме разбиения. В разд. 4 исследуются задачи, связанные с двухмерной проблемой Фробениуса.

2. О ЧИСЛЕ РЕШЕНИЙ ДИОФАНТОВА БУЛЕВА УРАВНЕНИЯ

Обозначим через $t_b(a_1,\ldots,a_n)$ число решений уравнения (1). Ясно, например, что положительность этого числа влечет за собой 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:

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

Если на $x_1, x_2, \ldots, x_k$ нет никаких ограничений, то число решений уравнения – это число разбиений n на натуральные слагаемые. Этот факт формально может быть выражен в терминах преобразования вектора $\mathbf{x} = (x_1, \ldots, x_k)$ в вектор $\mathbf{y} = (y_1, \ldots, y_n)$, где y_r, $r = 1, \ldots, n$, – это число координат вектора $\mathbf{x}$, равных натуральному r.

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

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

Пусть $L(x_1, \ldots, x_n)$ – линейная форма:

$$L(x_1,\ldots,x_n) = \sum_{i=1}^{n} a_i x_i. \tag{2}$$

Для случая булевых переменных через $L^*(x_1, \ldots, x_n)$ обозначим множество значений этой формы. Тогда вопрос о разрешимости уравнения (1) эквивалентен вопросу о принадлежности числа b этому множеству.

Рассмотрим производящую функцию последовательности $\{t_b(a_1,\ldots,a_n)\}$:

$$F_{a_1,\ldots,a_n}(z) = \sum_{b=0}^{\infty} z^b t_b(a_1,\ldots,a_n). \tag{3}$$

Для нее известно соотношение

$$F_{a_1,\ldots,a_n}(z) = \sum_{b=0}^{\infty} z^b t_b(a_1,\ldots,a_n) = \prod_{k=1}^{n} \frac{1}{1-z^{a_k}}. \tag{4}$$

Оно является простым следствием определения, представленного соотношением (3). Действительно, из (3) следует

$$F_{a_1,\dots,a_n}(z)=\sum_{b=0}^{\infty}z^b t_b(a_1,\dots,a_n)=\sum_{\{x_1,\dots,x_n\}}z^{a_1x_1+\dots+a_nx_n}=\prod_{i=1}^{n}\sum_{x_i=0}^{\infty}z^{a_ix_i}=\prod_{k=1}^{n}\frac{1}{1-z^{a_k}}.$$

Утверждение 1. *Справедливо соотношение*

$$t_b(a_1,\dots,a_n)=\frac{1}{2\pi i}\oint\limits_{|u|=\rho}\frac{F_{a_1,\dots,a_n}(z)}{z^{b+1}}dz,\quad \rho<1.$$

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

Пример 1. Если все $a_i=1$, $i=1,\dots,n$, то $F_{1,\dots,1}(z)=(1-z)^{-n}$ и $t_b(1,\dots,1)=(-1)^bC_b^{-n}=C_b^{n+b-1}=C_{n-1}^{n+b-1}$.

Это хорошо известная формула для числа разбиений натурального b в сумму не более n слагаемых.

Пример 2. Если $n=2$, то поведение функции $t_b(a_1,a_2)$ в значительной мере определяется упомянутой выше теоремой Сильвестра (см., например, [14], [15]).

Согласно ей при условии взаимной простоты $(a_1,a_2)=1$ уравнение разрешимо, если $b>a_1a_2$, и эта граница достижима. Таким образом, если $t_b(a_1,\dots,a_n)>0$ для всех $b\geq b_0$ и $t_b(a_1,\dots,a_n)=0$ для $b=b_0-1$, то значение числа Фробениуса равно b_0.

Для случая булевых переменных формула (4) имеет вид

$$F_{a_1,\dots,a_n}(z)=\sum_{b=0}^{\infty}z^b t_b(a_1,\dots,a_n)=\prod_{k=1}^{n}(1+z^{a_k}). \tag{5}$$

Из (5) следует выражение для $t_b\,(a_1,\dots,a_n)$:

$$t_b(a_1,\dots,a_n)=\frac{1}{2\pi i}\oint\limits_{|u|=\rho}\frac{(1+u^{a_1})\dots(1+u^{a_n})}{u^{b+1}}du,\quad \rho<1.$$

Пусть теперь $x_1\in A_1,\dots,\ x_n\in A_n$, где $A_1,\dots,A_n$ – произвольные подмножества натурального ряда.

Тогда производящая функция $t_b\,(A_1,\dots,A_n)$ для числа решений уравнения (1) с такой структурой множества аргументов имеет вид:

$$F_{A_1,\dots,A_n}(z)=\sum_{b=0}^{\infty}z^b t_b\,(A_1,\dots,A_n). \tag{6}$$

И она может быть представлена следующим образом.

Пусть

$$F_k(z)=\sum_{x\in A_k}z^x \tag{7}$$

есть производящая функция для множества A_k.

Непосредственно из (6) и (7) получаем

Утверждение 2. *Справедлива формула*

$$F_{A_1,\dots,A_n}(z)=F_1(z)F_2(z)\dots F_n(z).$$

Пример 3. Пусть $A_k=\{0,1,2\}, k=1,\dots,n$. Тогда $F_k(z)=\sum_{x\in A_k}z^x=1+z+z^2$.

Отсюда следует $F_{A_1,\dots,A_n}(z)=\prod_{i=1}^{n}(1+z^{a_i}+z^{2a_i})$.

Определение 1. Среднее число решений уравнения (1) – это величина вида

$$\overline{t_b}=\frac{1}{b^n}\sum_{a_1,\dots,a_n}t_b(a_1,\dots,a_n). \tag{8}$$

Перейдем теперь к рассмотрению величины $\overline{t}_b$.

Заметим, что ни один коэффициент в разрешимом уравнении не может превосходить b. Поэтому он может принимать значения от 1 до b. Кроме того, мы предполагаем, что в уравнении ровно n слагаемых. Таким образом, при равномерном распределении значений b величина $\overline{t}_b$ – это среднее число представлений правой части уравнения линейной формой $\sum_{i=1}^{n} a_i x_i$.

Пусть

$$F_n(z) = \sum_{i=1}^{n} \frac{1}{(1-z^{a_i})}. \tag{9}$$

Лемма 1. *Справедливо соотношение*

$$F_n(z) = n + \sum_{i=1}^{n} A_i z^i, \tag{10}$$

где A_i – это число делителей числа i в множестве $\{a_1,\ldots,a_n\}$.

Доказательство. Из (9) следует

$$F_n(z) = n + \sum_{r_1=1}^{\infty} z^{r_1 a_1} + \sum_{r_2=1}^{\infty} z^{r_2 a_2} + \ldots + \sum_{r_n=1}^{\infty} z^{r_n a_n}. \tag{11}$$

Найдем коэффициент при z^N в (11). Вхождение z^N в s-ю сумму означает, что $N = ra_s$ для какого-то r. Поэтому $N \equiv 0 \pmod{a_s}$, что и доказывает утверждение леммы.

Теорема 2. *Справедлива формула*

$$\overline{t}_b = \frac{1}{b^n} \operatorname*{Coef}_u \left\{ \frac{1}{u^{n+1}} \left(b + \sum_{r=1}^{\infty} \frac{u^r}{(1-u)^r} \right)^n \right\}. \tag{12}$$

Доказательство. По определению и из (8) имеем

$$\overline{t}_b = \frac{1}{b^n} \sum_{\{a_1,\ldots,a_n\}} t_b(a_1,\ldots,a_n) = \frac{1}{b^n} \sum_{\{a_1,\ldots,a_n\}} \operatorname*{Coef}_u \left\{ \frac{1}{u^{b+1}} \prod_{i=1}^{n} \frac{1}{1-u^{a_i}} \right\} = \frac{1}{b^n} \operatorname*{Coef}_u \left\{ \frac{1}{u^{b+1}} \prod_{i=1}^{n} \sum_{a_i=1}^{b} \frac{1}{1-u^{a_i}} \right\}.$$

Теперь используем предыдущую лемму и получаем соотношение

$$\overline{t}_b = \frac{1}{b^n} \operatorname*{Coef}_u \left\{ \frac{1}{u^{b+1}} \left(b + \sum_{r=1}^{\infty} \tau(r) u^r \right)^n \right\}, \tag{13}$$

где $\tau(r)$ – число делителей r.

Производящая функция для числа делителей изучалась во многих работах (см., например, [6]). Для нее известно следующее соотношение:

$$\sum_{r=1}^{\infty} \tau(r) u^r = \sum_{r=1}^{\infty} \frac{u^r}{1-u^r}. \tag{14}$$

Подставляем (14) в (13) и получаем (12).

Это завершает доказательство теоремы.

Следствие 1. Справедливо соотношение

$$\overline{t}_b(a_1,\ldots,a_n) = \frac{1}{2\pi i} \oint_{|u|=\rho} \frac{\left(b + \sum_{r=1}^{\infty} \frac{u^r}{(1-u)^r} \right)^n}{u^{b+1}} du, \quad \rho < 1. \tag{15}$$

3. ЗАДАЧА О РАЗБИЕНИИ

Рассмотрим задачу о разбиении – нахождении числа разбиений P_n для фиксированного n, что эквивалентно нахождению числа решений диофантова уравнения

$$n = \sum_{i=1}^{k} x_i = \sum_{r=1}^{n} r y_r. \tag{16}$$

Если на свойства разбиения нет ограничений, то в качестве вектора $\mathbf{y}$ может быть выбран любой вектор, удовлетворяющий (14).

Найдем методом коэффициентов выражение производящей функции для числа разбиений:

$$P_n(z) = \sum_{n=1}^{\infty} P_n z^n. \tag{17}$$

Из (16) и (17) следует

$$\begin{aligned} P_n &= \sum_{\{y_1,\ldots,y_n\}} \operatorname*{Coef}_u \left\{ \frac{u^{\sum_{r=1}^{n} r y_r}}{u^{n+1}} \right\} = \operatorname*{Coef}_u \left\{ \frac{1}{u^{n+1}} \sum_{\{y_1,\ldots,y_n\}} u^{\sum_{r=1}^{n} r y_r} \right\} = \\ &= \operatorname*{Coef}_u \left\{ \frac{1}{u^{n+1}} \sum_{y_1=0}^{\infty} u^{y_1} \sum_{y_2=0}^{\infty} u^{y_2} \ldots \sum_{y_n=0}^{\infty} u^{y_n} \right\} = \operatorname*{Coef}_u \left\{ \frac{1}{u^{n+1}} \prod_{k=1}^{\infty} \frac{1}{1-u^k} \right\}. \end{aligned} \tag{18}$$

Отсюда и следует выражение для производящей функции

$$P_n(u) = \sum_{n=1}^{\infty} P_n u^n = \prod_{k=1}^{\infty} \frac{1}{1-u^k}. \tag{19}$$

Мы привели классическое выражение для производящей функции числа разбиений.

Если все x_i различны, то на языке $\{y_i\}$ это будет означать, что $y_i \le 1$, $i = 1, \ldots, n$.

Пусть теперь P_n^0 – число разбиений n на различные слагаемые и $P_n^0(z) = \sum_{n=1}^{\infty} P_n^0 z^n$ – производящая функция для него. Тогда аналогично предыдущему рассуждению, имеем

$$P_n^0 = \operatorname*{Coef}_u \left\{ \frac{\prod_{i=1}^{n} \sum_{y_i=0}^{1} u^{i y_i}}{u^{n+1}} \right\} = \operatorname*{Coef}_u \left\{ \frac{\prod_{i=1}^{\infty} (1+u^i)}{u^{n+1}} \right\}.$$

Отсюда следует

$$P_n^0(z) = \sum_{n=1}^{\infty} P_n^0 z^n = \prod_{k=1}^{\infty} (1+z^k).$$

Теорема 3. *Число разбиений на нечетные слагаемые равно числу разбиений на различные слагаемые.*

Доказательство. Если все x_i нечетные, то на языке $\{y_i\}$ это будет означать, что $y_{2r} = 0$, $r = 1, \ldots, [n/2]$.

Пусть теперь P_n^r – число разбиений n на нечетные слагаемые и $P_n^r(z) = \sum_{n=1}^{\infty} P_n^r z^n$ – производящая функция для него.

Для краткости обозначим через $v(z)$ выражение

$$v(z) = \frac{1}{(1-z)(1-z^3)(1-z^5)\ldots} = (1-z^2)(1-z^4)(1-z^6)\ldots = \frac{1}{\prod_{k=1}^{\infty}(1-z^{2k+1})},$$

а через $u(z)$ выражение $\prod_{k=1}^{\infty}(1+z^k)$.

Далее заметим, что

$$u(z)(1-z)(1-z^2)(1-z^3)\ldots = (1-z^2)(1-z^4)(1-z^6)\ldots = \prod_{r=1}^{\infty}(1-z^{2r}).$$

Но это означает, что

$$\frac{\prod\limits_{r=1}^{\infty}(1-z^{2r})}{\prod\limits_{r=1}^{\infty}(1-z^{r})} = \frac{1}{\prod\limits_{r=0}^{\infty}(1-z^{2r+1})} = u(z).$$

Тогда из (18) следует

$$P_n^r(z) = \sum_{n=1}^{\infty} P_n^r z^n = \frac{1}{\prod\limits_{k=1}^{\infty}(1-z^{2k+1})}. \tag{20}$$

Но в этом случае из (20) мы имеем равенство

$$P_n^0(z)\prod_{k=1}^{\infty}(1-z^k) = \prod_{k=1}^{\infty}(1-z^{2k}).$$

Но тогда из этого равенства получаем

$$P_n^0(z) = \frac{\prod\limits_{k=1}^{\infty}(1-z^{2k})}{\prod\limits_{k=1}^{\infty}(1-z^{k})} = \frac{1}{\prod\limits_{k=1}^{\infty}(1-z^{2k+1})} = P_n^r(z).$$

Этим завершается доказательство утверждения.

Таким образом, мы здесь привели новое доказательство известного факта из теории разбиений (см., например, [31]).

4. О ПРОБЛЕМЕ ФРОБЕНИУСА

Рассмотрим диофантово уравнение (21) с двумя переменными. Введенные ниже обозначения будут использованы всюду в дальнейшем тексте.

$$ax + by = n. \tag{21}$$

Здесь все числа натуральные. Как известно, эти уравнения разрешимы для всех n, начиная с некоторого – границы разрешимости: $n_0(a, b, c)$ или $n_0(a, b)$. По теореме Сильвестра для взаимно простых a и b:

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

В [30] используя метод производящих функций, получена формула для числа решений $t_n(a,b)$ уравнения (21) при условии $(a, b) = 1$, из которой следует не только результат Сильвестра, но и формула для x_0 и y_0, на которых “лежит” граница разрешимости.

Теорема 4. *Если* $(a, b) = 1$, *то*

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

где $x_0(n)$ *и* $y_0(n)$ *– минимальные решения сравнений*: $ax \equiv n (\mathrm{mod}\, b)$ *и* $by \equiv n (\mathrm{mod}\, a)$.

Следствие 2. При взаимно простых a и b из неравенства $n > ab - (a + b)$ следует неравенство $t_n(a,b) > 0$.

Доказательство. Так $x_0 \le b-1$ и $y_0 \le a-1$, то

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

Но по условию $n > ab-(a+b)$. Отсюда и следует неравенство $t_n(a,b) > 0$.

А это известная формула Сильвестра для двухмерного 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 $ax \equiv n(\mathrm{mod}\, b)$ и $by \equiv n(\mathrm{mod}\, a)$при взаимно простых a и b имеют единственные минимальные решения, представимые в виде:

$$x_0(n) = (na^{\varphi(b)-1})_{\mathrm{mod}\, b} \quad \text{и} \quad y_0(n) = (nb^{\varphi(a)-1})_{\mathrm{mod}\, a}.$$

Отсюда и получается другое выражение для формулы, задающей число решений уравнения (21):

$$t_n(a,b) = \frac{n}{ab} - \frac{(na^{\varphi(b)-1})_{\mathrm{mod}\, b}a + (nb^{\varphi(a)-1})_{\mathrm{mod}\, a}b}{ab} + 1. \tag{23}$$

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

При $n = 12$ из (017) следует $t_{12}(4,7) = \frac{12}{28} - \frac{x_0(n)4 + y_0(n)7}{28} + 1$. Сравнения $4x \equiv 12(\mathrm{mod}\, 7)$ и $7y \equiv 12(\mathrm{mod}\, 4)$ 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 и соответствует решению (3, 0).

При $n = 13$ из (017) следует $t_{13}(4,7) = \frac{13}{28} - \frac{x_0(n)4 + y_0(n)7}{28} + 1$. Сравнения $4x \equiv 13(\mathrm{mod}\, 7)$ и $7y \equiv 13(\mathrm{mod}\, 4)$ 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 и соответствует тому факту, что решений у уравнения нет.

При $n = 32$ из (017) следует $t_{32}(4,7) = \frac{32}{28} - \frac{x_0(n)4 + y_0(n)7}{28} + 1$. Сравнения $4x \equiv 32(\mathrm{mod}\, 7)$ и $7y \equiv 32(\mathrm{mod}\, 4)$ 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 и соответствует двум решениям: (8, 0) и (1, 4).

Следствие 3. Справедлива формула

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

Доказательство. Рассмотрим функцию

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

Заметим, что $L_{n+ab}(a,b) = L_n(a,b)$. Имеем периодическую функцию с периодом ab.

Из этого факта и (23) следует (24).

Рассмотрим теперь вопрос о "среднем числе" решений уравнения (21).

Очевидно, что $a, b \le n$. Если параметры a и b равномерно распределены в квадрате nxn, то в качестве "среднего числа" решений можно взять следующую величину:

$$\overline{t_n} = \frac{1}{n^2}\sum_{a,b=0}^{n} t_n(a,b). \tag{25}$$

Величина $\overline{t_n}$ представляет определенный интерес, так как уравнение (21) может вовсе не иметь решений (например, если $(a,b) \not| n$), быть разрешимым для всех n (если $(a,b) = 1$, $n \ge (a-1)(b-1) - 1$ или находиться в любом из "промежуточных" случаев.

Пусть все параметры распределены независимо.

Лемма 2. *Пусть* $V = \{v_1,\ldots,v_k\}$ *— произвольное подмножество натуральных чисел. Тогда имеет место формула*:

$$Q_V(z) = \sum_{i=1}^{n} \frac{1}{1-z^{v_i}} = \sum_{N=0}^{\infty} B_N z^N, \tag{26}$$

где B_N *— число делителей числа* N, *лежащих в множестве* V *и* $B_0 = k$.

Равенство (26) обосновывается следующим.

Во-первых, по определению справедливо равенство

$$Q_V(z) = \sum_{r=0}^{\infty} z^{rv_1} + \sum_{r=0}^{\infty} z^{rv_2} + \ldots + \sum_{r=0}^{\infty} z^{rv_k}. \tag{27}$$

Во-вторых, B_N равно числу вхождений z^N в (27). В-третьих, вхождение z^N в s-ю сумму в (27) эквивалентно тому, что $N = rv_s$ для некоторого r. Поэтому $N \equiv 0_{\mathrm{mod}\, v_s}$. Из этого и вытекает утверждение леммы.

Пример 5. Если $V = \{2,4\}$, то

$$Q_V(z) = \sum\nolimits_{r=0}^{\infty} z^{r2} + \sum\nolimits_{r=0}^{\infty} z^{r4} = \sum\nolimits_{N=0}^{\infty} B_N z^N,$$

тогда из леммы мы получаем, что

$$B_N = \begin{cases} 0, & \text{если} \quad N \equiv 1_{\mathrm{mod}\,2}, \\ 1, & \text{если} \quad N \equiv 0_{\mathrm{mod}\,2}, \quad N \not\equiv 0_{\mathrm{mod}\,4}. \\ 2, & \text{если} \quad N \equiv 0_{\mathrm{mod}\,4}, \end{cases}$$

В качестве следствия из этой леммы можно получить соотношение

$$B_N = \tau(N)$$

при $N > 0$.

Пусть

$$Q_n(z) = \sum_{i=1}^{n} \frac{1}{1-z^i} = \sum_{N=0}^{\infty} B_N z^N, \quad J_n = \{1,2,\ldots n\}, \quad D_N = \{d : d/N\}.$$

Тогда из леммы следует, что

$$B_N = D_N.$$

Но это означает, что

$$B_N = \tau(N) \quad \text{при} \quad N > 0. \tag{28}$$

Из (26) и (28) следует соотношение

$$Q_V(z) = \sum_{N=0}^{\infty} B_N z^N = N + \sum_{N=1}^{\infty} \tau(N) z^N. \tag{29}$$

Теорема 5. *Справедливо соотношение*

$$\overline{t}_n = \frac{2\tau(n)}{n} + \frac{1}{n^2} \sum_{r=1}^{n} \tau(r)\tau(n-r), \tag{30}$$

где $\tau(0) = n$.

Доказательство. Согласно введенным 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

$$t_n(a,b) = \frac{1}{2\pi i} \oint_{|u|=\rho} \frac{1}{z^{n+1}(1-z^a)(1-z^b)}\, dz, \quad \rho < 1. \tag{31}$$

Подставляем (31) в (25) и получаем соотношение

$$\overline{t}_n = \frac{1}{n^2}\frac{1}{2\pi i}\oint\limits_{|u|=\rho}\frac{1}{z^{n+1}}\sum_{a,b\le n}\frac{1}{(1-z^a)(1-z^b)}dz, \quad \rho < 1. \tag{32}$$

Далее обращаем внимание на то, что

$$\sum_{a,b\le n}\frac{1}{(1-z^a)(1-z^b)} = \sum_{a=1}^{n}\frac{1}{(1-z^a)}\sum_{b=1}^{n}\frac{1}{(1-z^b)} = Q_n^2(z). \tag{33}$$

Из (28), (31) и (32) следует, что

$$\overline{t}_n = \frac{1}{n^2}\operatorname*{Coef}_z\left\{Q_n^2(z)\right\} = \frac{1}{n^2}\sum_{r=0}^{n}B_rB_{n-r} = \frac{1}{n^2}\operatorname*{Coef}_z\left\{\frac{1}{z^{n+1}}\left(n+\sum_{r=1}^{n}\tau(r)z^r\right)^2\right\}. \tag{34}$$

Но тогда из (26), (29) и (34) вытекает утверждение теоремы.

Следствие 4. Справедливо неравенство $\overline{t}_n \le \log^2 n$.

Доказательство. Применяем неравенство Коши к (34), учитывая (28), и получаем

$$\sum_{r=0}^{n}B_rB_{n-r} \le \left(\sum_{r=0}^{n}B_r^2\right)^{1/2}\left(\sum_{r=0}^{n}B_{n-r}^2\right)^{1/2}. \tag{35}$$

Так как

$$\left(\sum_{r=0}^{n}B_r^2\right)^{1/2} = \left(\sum_{r=0}^{n}B_{n-r}^2\right)^{1/2},$$

то из (28) следует

$$\sum_{r=0}^{n}B_rB_{n-r} \le \sum_{r=0}^{n}B_r^2 \le \sum_{r=0}^{n}\tau^2(r) \le \left(\sum_{r=0}^{n}\tau(r)\right)^2. \tag{36}$$

Известно, что

$$\sum_{r=0}^{n}\tau(r) \le \sum_{r=1}^{n}\left[\frac{n}{r}\right]. \tag{37}$$

Из (36) и (37) следует соотношение

$$\sum_{r=0}^{n}B_rB_{n-r} \le n^2\log^2 n.$$

Из этого соотношения и (34) получаем требуемое неравенство

$$\overline{t}_n \le \log^2 n.$$

Следствие доказано.

5. ЗАКЛЮЧЕНИЕ

В работе были рассмотрены комбинаторные аспекты задач, связанных с разбиением целых чисел на слагаемые. Это хорошо известная и исследованная область. Мы попытались взглянуть на поднятую проблематику сквозь призму получения формул и оценок для числа решений диофантовых уравнений специального типа.

Это позволило не только достаточно естественно вывести уже известные результаты, но и получить новые, что для такой хорошо известной и изученной проблемы представляется полезным и интересным.

В каждом из трех основных разделов работы главные результаты (их четыре) названы теоремами. Прикладные области, где они могут быть использованы, обсуждены частично во введении, где дан краткий экскурс по возможным постановкам задач и полученным результатам.

СПИСОК ЛИТЕРАТУРЫ

1. *Пападимитриу Х., Стайглиц С.* Комбинаторная оптимизация. М.: Мир, 1989.
2. *Гэри М., Джонсон Д.* Вычислительные машины и труднорешаемые задачи. М.: Мир, 1982.
3. *Фомичев В.М., Мельников Д.А.* Криптографические методы защиты информации. М.: Юрайт, 2017.
4. *Erdös P., Graham R.L.* On a linear diophantine problem of Frobenius // Acta Arith. 1972. V. 21. P. 399–408.
5. *Alfonsin J.R.* The Diophantine Frobenius Problem. Oxford: Oxford University Press, 2005.
6. *Харди Х., Райт Э.М.* Введение в теорию чисел. Oxford: Oxford University Press, 1975.
7. *Леонтьев В.К., Гордеев Э.Н.* Производящие функции в задаче о ранце // Докл. АН. 2018. Т. 481. № 5. С. 478–480. https://doi.org/10.31857/S086956520002139-5
8. *Леонтьев В.К., Гордеев Э.Н.* О некоторых комбинаторных свойствах задачи о рюкзаке // Ж. вычисл. матем. и матем. физ. 2019. Т. 59. № 8. С. 1439–1447. https://doi.org/10.1134/S0044466919080076
9. *Егорычев Г.П.* Интегральное представление и вычисление комбинаторных сумм. Новосибирск: Наука, 1977.
10. *Kellerer H., Pferschy U., Pisinger D.* Knapsack problems. Berlin: Springer, 2004.
11. *Леонтьев В.К., Гордеев Э.Н.* Об алгебраической иммунности систем кодирования // Вопросы кибербезопасности. 2019. № 1. С. 59–89. https://doi.org/10.21681/2311-3456-2019-1-59-68
12. *Гордеев Э.Н., Леонтьев В.К., Медведев Н.В.* О свойствах булевых полиномов, актуальных для криптосистем // Вопросы кибербезопасности. 2017. № 3. С. 63–69. https://doi.org/10.21681/2311-3456-2017-3-63-69
13. *Мазуров И.Д., Хачай М.Ю.* Комитеты систем линейных неравенств // АиТ. 2004. № 2. С. 43–54. https://doi.org/10.1023/B:AURC.0000014716.77510.61
14. *Береснев В.Л.* Эффективный алгоритм решения задачи минимизации полиномов от булевых переменных, обладающих свойством связности // Дискретн. анализ и исслед. операций. Сер. 2. 2005. Т. 12. № 1. С. 3–11.
15. *Sylvester J.J.* Problem 7382// The Educational Times, and Journal of the College of Preceptors, New Ser., 36(266) (1883), 177 Solution by W.J. Curran Sharp, ibid., 36(271) (1883), 315 Republished as [15].
16. *Sylvester J.J.* Problem 7382, in: W. J. C. Miller (Ed.), Mathematical questions, with their solutions, from The Educational Times, vol. 41, page 21. London: Francis Hodgson, 1884.
17. *Арнольд В.И.* Экспериментальное наблюдение математических фактов. М: Из-во МЦНМО, 2006.
18. *Arnold V.I.* Arithmetical Turbulence of Selfsimilar Fluctuations Statistics of Large Frobenius numbers of Additive Semigroups of Integer// Moscow Mathematical Journal. 2007. V. 7. № 2. P. 173–193.
19. *Арнольд В.И.* Слабые асимптотики числа решений диофантовых задач // Функциональный анализ и его приложения. 1999. Т. 33. № 4. С. 65–66.
20. *Фомичёв В.А.* Опенка экспонента некоторых графов с помощью чисел Фробениуса для трех аргументов // Прикладная дискретная матем. 2014. Т. 24. № 2. С. 88–96.
21. *Curtis F.* On formulas for the Frobenius number of a numerical semigroup // Math. Scand. 1990. V. 67. P. 190–192.
22. *Amitabha Tripathi*. Formulae for the Frobenius number in three Variables // J. of Number Theory. 2017. V. 170. P. 368–389.
23. *Савельев В.П., Шевченко В.Н.* Задача Фробениуса для трех чисел // Международные научные чтения (памяти Келдыша М.В.): Сб. статей. Международной научно-практической конференции (Москва, 16.11.2019 г.). М.: ЕФИР, 2019. С. 10–15.
24. *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. P. 623–647.
25. *Rosales J.C., Branco M.B., Torrao D.* The Frobenius problem for Thabit numerical semigroups // J. Number Theory. 2015. V. 155. P. 85–99.
26. *Rosales J.C., Branco M.B., Torrao D.* The Frobenius problem for repunit numerical semigroups // Ramanujan J. 2016. V. 40. P. 323–334.
27. *Rosales J.C., Branco M.B., Torrao D.* The Frobenius problem for Mersenne numerical semigroups // Math. Z. 2017. V. 286. P. 741–749.
28. *Nijenhuis M.* A minimal-path algorithm for the “money changing problem” // The American Mathematical Monthly. 1979. V. 86. P. 832–835.
29. *Фомичёв В.А.* Эквивалентные но Фробениусу примитивные множества чисел // Прикладная дискретная матем. 2014. Т. 23. № 1. С. 20–26.
30. *Леонтьев В.К.* О проблеме Фробениуса // Дискретный анализ и исследование операций. 2022. Т. 29. № 2. С. 24–37.
31. *Эндрюс Г.* Теория разбиений. М.: Наука, 1982.