

О ВЫЧИСЛИТЕЛЬНОЙ СЛОЖНОСТИ
ОРИГИНАЛЬНОЙ И РАСШИРЕННОЙ
ДИОФАНТОВОЙ ПРОБЛЕМЫ ФРОБЕНИУСА *)

В. М. Фомичёв^{1,2}

¹Финансовый университет при Правительстве РФ,
Ленинградский пр., 49, 125993 Москва, Россия

²Национальный исследовательский ядерный университет «МИФИ»,
Каширское шоссе, 31, 115409 Москва, Россия

E-mail: fomichev@nm.ru

Аннотация. Выведен закон нестационарной рекурсии, позволяющий для любого примитивного множества $A = \{a_1, \dots, a_k\}$, $k > 2$, построить алгоритм определения множества чисел $C(a_1, \dots, a_k)$, не содержащихся в аддитивной полугруппе, порождённой множеством A . В частности, получен новый алгоритм определения чисел Фробениуса $g(a_1, \dots, a_k)$. Оценена вычислительная сложность алгоритмов в битовых операциях. Предложена двухэтапная редукция исходного примитивного множества в эквивалентное примитивное множество, позволяющая улучшить оценки сложности в тех случаях, когда двухэтапная редукция приводит к существенному сокращению порядка исходного множества. Библиогр. 16.

Ключевые слова: число Фробениуса, примитивное множество, аддитивная полугруппа, сложность вычислений.

Основные обозначения

В статье используются следующие обозначения: $\log a = \log_2 a$;
 $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$, где \mathbb{N} — множество всех натуральных чисел;
 $a \mid b$ и $a \nmid b$ — a делит b и a не делит b соответственно, $a, b \in \mathbb{N}$;
 $\gcd(a_1, \dots, a_k)$ — наибольший общий делитель чисел $a_1, \dots, a_k \in \mathbb{N}$;
 $\text{lcm}(a_1, \dots, a_k)$ — наименьшее общее кратное чисел $a_1, \dots, a_k \in \mathbb{N}$;
 $bA = \{ba_1, \dots, ba_k\}$, $b \pm A = \{b \pm a_1, \dots, b \pm a_k\}$, $A/a = \{a_1/a, \dots, a_k/a\}$,
где $A = \{a_1, \dots, a_k\}$, $b \in \mathbb{N}_0$, $a \in \mathbb{N}$;
 $A^{(i)} = \{a_1, \dots, a_i\}$, $d_i = \gcd(a_1, \dots, a_i)$, $i = 1, \dots, k$;
 $\delta_i = d_{i-1}/d_i$, $i = 2, \dots, k$;

*) Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект 16-01-00226).

$g(A) = g(a_1, \dots, a_k)$ — число Фробениуса для аргументов a_1, \dots, a_k , если $d_k = 1$;

$\langle A \rangle$ — аддитивная полугруппа, порождённая множеством $A \subset \mathbb{N}$;

$C(A^{(i)}) = d_i \mathbb{N}_0 \setminus \langle A^{(i)} \rangle$, $z_i = \max C(A^{(i)})$, $\overline{\langle A^{(i)} \rangle} = \{a \in \langle A^{(i)} \rangle \mid a < z_i\}$, $i = 2, \dots, k$.

Введение

Пусть $A = \{a_1, \dots, a_k\}$ — возрастающая последовательность натуральных чисел, $k > 1$. Множество A называется *примитивным*, если $\gcd(a_1, \dots, a_k) = 1$.

Функция Фробениуса $g(a_1, \dots, a_k)$ определена на всех примитивных множествах $\{a_1, \dots, a_k\}$ при $a_1 > 1$ как наибольшее натуральное число $t \notin \langle a_1, \dots, a_k \rangle$, т. е. число, не представимое в виде линейной комбинации чисел a_1, \dots, a_k с неотрицательными целыми коэффициентами (далее рассматриваются только такие линейные комбинации чисел):

$$g(a_1, \dots, a_k) = \max\{t \in \mathbb{N} \mid t \neq c_1 a_1 + \dots + c_k a_k\}.$$

При $a_1 = 1$ полагают $g(1, a_2, \dots, a_k) = -1$.

По определению $C(A) = C(A^{(k)})$ — множество всех натуральных чисел, не представимых линейной комбинацией чисел a_1, \dots, a_k . Тогда число Фробениуса $g(A)$ равно $\max C(A)$. Задача определения $g(a_1, \dots, a_k)$ известна как *диофантова проблема Фробениуса* (ПФ). Задачу определения множества $C(A)$ назовём *расширенной проблемой Фробениуса* (РПФ).

Алгоритмы РПФ при $k > 2$ неизвестны, вместе с тем, активно изучался порядок множества $C(A)$ [15, гл. 5], а первые результаты были получены Сильвестром [16].

В случае $k = 2$ число Фробениуса и решение РПФ имеет вид

$$g(a_1, a_2) = a_1 a_2 - a_1 - a_2. \quad (1)$$

Известны несколько доказательств формулы (1) (см. [15, разд. 2.1]). Отметим предпочтительность использования при вычислениях компактной формулы: как правило, в этом случае соответствующий алгоритм требует незначительных ресурсов вычислительного устройства. Вместе с тем, доказано [10], что уже при $k = 3$ не существует конечного числа полиномов, позволяющих в общем случае выразить через них число Фробениуса $g(a_1, a_2, a_3)$ с помощью разбиения области определения. Это определяет более высокую продуктивность алгоритмического подхода к ПФ.

К настоящему времени диофантовой проблеме Фробениуса посвящено много работ (см. библиографию в [1–3, 15]), получены точные формулы для ряда частных случаев, а также нижние и верхние оценки числа $g(a_1, \dots, a_k)$ при различных k . Для некоторых случаев получены формулы «упрощения» задачи. Например, при $d_{k-1} > 1$ имеется следующее «упрощение» [9]:

$$g(a_1, \dots, a_k) = d_{k-1}g(a_1/d_{k-1}, \dots, a_{k-1}/d_{k-1}, a_k) + (d_{k-1} - 1)a_k. \quad (2)$$

Вместе с тем, общая формула при $k > 2$ не получена.

Более продуктивным стал алгоритмический подход к определению $g(a_1, \dots, a_k)$. Получен [15] ряд алгоритмов при $k = 3$. В [11, 12] был разработан алгоритм вычисления функции Фробениуса с помощью экспоненцирования квадратной неотрицательной M матрицы порядка a_k и определения её показателя примитивности (экспонента) с использованием соотношения

$$g(a_1, \dots, a_k) = \exp M - a_k.$$

Матрица M является матрицей смежности вершин сильно связанного орграфа с a_k вершинами, содержащего циклы длины a_1, \dots, a_k . Вычислительная сложность алгоритма в битовых операциях при фиксированном k оценивается в общем случае полиномом третьей степени относительно a_k . В [7] предложено улучшение этого алгоритма: сложность его оценивается полиномом второй степени, однако обоснование корректности алгоритма не представлено. Заметим, что для хранения степеней матрицы M требуется память порядка $(a_k)^2 \log_2 a_k$ битов. Алгоритм экспоненцирования матрицы не позволяет получить в явном виде аналитическую зависимость числа $g(a_1, \dots, a_k)$ от аргументов.

Алгоритм со сложностью $O(a_1(k + \log a_1))$ определения $g(a_1, \dots, a_k)$ на основе теоретико-графового подхода представлен в [14]. ПФ была сведена к поиску наибольшего из кратчайших путей определённого вида в орграфе Γ с a_1 вершинами и ka_1 дугами, в котором из каждой вершины исходит k дуг весов a_1, \dots, a_k соответственно. Для поиска кратчайших путей в орграфе использованы известные алгоритмы просмотра дуг графа и вычисления весов путей со сложностью порядка числа дуг [13]. В [6] улучшена оценка сложности алгоритма определения $g(a_1, \dots, a_k)$, она снижена до величины порядка $O(ka_1)$ операций.

В данной работе для $k \geq 3$ получены рекуррентные формулы, выражающие множество $C(A^{(i)})$ через $C(A^{(i-1)})$ и другие множества, определяемые числами a_1, \dots, a_i , $i = 3, \dots, k$. На основе формул построены

новые алгоритмы РПФ и ПФ, даны оценки их сложности в битовых операциях, величина которых определяется числами a_1, \dots, a_k и делителями d_2, \dots, d_k (для случая $k = 3$ соответствующие алгоритмы представлены в [5]). Предложена редукция РПФ и ПФ для множества A к РПФ и ПФ соответственно для собственного подмножества, приводящая в ряде случаев к существенному снижению сложности задачи. Проведено сравнение полученных оценок сложности ПФ с известными оценками.

1. Определяющие свойства примитивного множества чисел

Приведём необходимые свойства, некоторые из них известны.

Утверждение 1. 1. $a_i \mid a$ при $a \in d_{i-1}\mathbb{N}_0$ тогда и только тогда, когда $\delta_i a_i \mid a$, $i = 3, \dots, k$.

2. Пусть $A = (a_1, a_2)$ и $g(A) = a + b$, где $a, b \geq 0$. Тогда либо $a \in \overline{\langle A \rangle}$ и $b \in C(A)$, либо наоборот. Отсюда с учётом (1) следуют равенства $C(A) = \{g(A) - a \mid a \in \overline{\langle A \rangle}\}$ и $|C(A)| = |\overline{\langle A \rangle}| = (a_1 - 1)(a_2 - 1)/2$ [16].

3. Множество $A^{(i)}/d_i$ примитивное, $\langle A^{(i)} \rangle = d_i \langle A^{(i)}/d_i \rangle$, $i = 2, \dots, k$.

4. $\{z_i - a \mid a \in \overline{\langle A^{(i)} \rangle}\} \subseteq C(A^{(i)}) = d_i \{1, \dots, g(A^{(i)}/d_i)\} \setminus \overline{\langle A^{(i)} \rangle}$, $|C(A^{(i)})| \leq z_i/d_i$, где $z_i = d_i g(A^{(i)}/d_i)$, $i = 2, \dots, k$.

5. Если $a \in \langle A^{(i)} \rangle$ и $b \in C(A^{(i)})$, то $b - a \in C(A^{(i)})$ и не менее половины чисел множества $d_i \{1, \dots, g(A^{(i)}/d_i)\}$ принадлежат $C(A^{(i)})$, $i = 2, \dots, k$.

6. $g(a_1, \dots, a_k) \leq (a_1 - 1)(a_k - 1) - 1 < a_1 a_k$ [15, теорема 3.1.1].

7. $z_i \leq d_i(a_1/d_i - 1)(a_i/d_i - 1) - 1 < a_1 a_i/d_i$, $i = 2, \dots, k$.

ДОКАЗАТЕЛЬСТВО. 1. **ДОСТАТОЧНОСТЬ.** Если $\delta_i a_i \mid a$, то и $a_i \mid a$.

НЕОБХОДИМОСТЬ. Из определения чисел d_i , $i = 3, \dots, k$, следует, что $d_i = \gcd(a_i, d_{i-1})$, тогда $a_i = b d_i$, где $(b, d_{i-1}) = 1$. Так как $d_{i-1} = \delta_i d_i$, то $(b, \delta_i) = 1$ и $\text{lcm}(a_i, d_{i-1}) = b \delta_i d_i$. По условию $a_i \mid a$ и $d_{i-1} \mid a$, значит, $\text{lcm}(a_i, d_{i-1}) \mid a$, отсюда $a_i \delta_i \mid a$.

Свойства 3 и 4 следуют из принятых обозначений.

5. Если $b - a \notin C(A^{(i)})$, то получаем $b \in \langle A^{(i)} \rangle$; противоречие.

Свойство 7 следует из 4 и 6. Утверждение 1 доказано.

Множество $A = \{a_1, \dots, a_k\}$ назовём *приведённым*, если a_i не является линейной комбинацией чисел a_1, \dots, a_{i-1} , т. е. $a_i \in C(A^{(i-1)})$, $i = 2, \dots, k$. Неприведённое множество A содержит приведённые подмножества.

Определим индуктивно приведённое подмножество B множества A , которое назовём *A-базисом*: $a_1 \in B$; $a_2 \in B$ тогда и только тогда, когда a_2 не кратно a_1 ; пусть из $\{a_1, \dots, a_{i-1}\}$ в подмножество B включены числа

b_1, \dots, b_j , тогда $a_i \in B$ в том и только том случае, когда либо $d_i < d_{i-1}$, либо $d_i = d_{i-1}$ и $a_i \in C(b_1, \dots, b_j)$, $i = 3, \dots, k$.

Обозначим через $L(A)$ возрастающую последовательность таких номеров $i \in \{2, \dots, k\}$, что $a_i \in B$, т. е. $i \in L(A)$ тогда и только тогда, когда либо $d_i < d_{i-1}$, либо $d_i = d_{i-1}$ и $a_i \in C(a_1, \dots, a_{i-1})$, $\lambda_A = |L(A)|$. Обозначим через $M(A)$ множество всех номеров $i \in L(A)$ таких, что $d_i < d_{i-1}$, $\mu_A = |M(A)|$. Индексом примитивности упорядоченного примитивного множества $A = \{a_1, \dots, a_k\}$ (обозначается через p_A) называется наименьшее $p \in \mathbb{N}$, при котором $d_p = 1$. Отсюда $p_A \in M(A)$, $2 \leq p_A \leq k$ и $d_{p-1} > d_p = \dots = d_k = 1$ при $p_A = p$.

- Утверждение 2.** 1. $\langle B \rangle = \langle A \rangle$, $\gcd A = \gcd B$;
 2. $|B| \leq \min\{k, a_1/d\}$, где $d = \gcd A$, и оценка $|B|$ достижима;
 3. $0 \leq \mu_A \leq \min\{p_A - 1, \lambda_A, \log d_2\}$.

ДОКАЗАТЕЛЬСТВО. 1. По построению $B \subseteq A$, поэтому $\langle B \rangle \leq \langle A \rangle$ и $\gcd A \mid \gcd B$. Вместе с тем, каждое число множества $A \setminus B$ есть линейная комбинация чисел B , значит, $\langle A \rangle = \langle B \rangle$ и $\gcd A = \gcd B$, так как любой общий делитель B делит все числа из A .

2. Пусть $B = \{b_1, \dots, b_\theta\}$. Тогда по построению $\theta \leq k$. Покажем, что $\theta \leq a_1/d$. В системе $\{b_1 \bmod a_1, \dots, b_\theta \bmod a_1\}$ наименьших неотрицательных вычетов содержится не более a_1/d различных чисел. Если $\theta > a_1/d$, то $b_i \bmod a_1 = b_j \bmod a_1$ при некоторых i, j , где $1 \leq i < j \leq \theta$. Тогда $b_j = b_i + ra_1$ при некотором натуральном r , что противоречит приведённости множества B . Следовательно, $\theta \leq a_1/d$. При $a \in \mathbb{N}$ оценка $|B|$ достигается на множестве $A = \{da, d(a+1), \dots, d(2a-1)\}$.

3. По определению $\mu_A \leq \lambda_A$ и $\mu_A \leq p_A - 1$. Покажем, что $\mu_A \leq \log d_2$. В невозрастающей цепи чисел $d_2 \geq d_3 \geq \dots \geq d_k$ каждое следующее число делит предыдущее. Тогда μ_A не больше числа простых делителей в каноническом разложении числа d_2 с учётом их кратностей, значит, $\mu_A \leq \log d_2$. Если a_i кратно a_{i-1} , $i = 2, \dots, k$, то $a_1 = d_1 = d_2 = \dots = d_k$ и $\mu_A = 0$. Утверждение 2 доказано.

Следствие 1. Если множество A примитивное, то $g(A) = g(B)$, при этом $|B| \leq \min\{k, a_1\}$.

ДОКАЗАТЕЛЬСТВО. По условию $d = \gcd A = 1$, тогда по утверждению 2(1) имеем $\gcd B = 1$. Значит, множество B примитивно и в силу равенства $\langle B \rangle = \langle A \rangle$ выполнено: $g(A) = \max C(A) = \max C(B) = g(B)$.

При $d = 1$ из утверждения 2(2) получаем $|B| \leq \min\{k, a_1\}$. Следствие 1 доказано.

Таким образом, РПФ (ПФ) для примитивного множества A редуцируется к РПФ (ПФ) для A -базиса.

2. Точные формулы

Пусть $A = \{a_1, \dots, a_k\}$ — примитивное множество. Обозначим через $R(i)$ множество натуральных чисел r таких, что $r\delta_i a_i \in C(A^{(i-1)})$, $S^{(i-1)}(a_i)$ — подмножество множества $C(A^{(i-1)})$:

$$S^{(i-1)}(a_i) = \bigcup_{r \in R(i)} \{(r\delta_i a_i + b) \in C(A^{(i-1)}) \mid b \in \overline{\langle A^{(i-1)} \rangle}\}.$$

Лемма 1. При $i = 3, \dots, k$ имеем

1. $S^{(i-1)}(a_i) = C(A^{(i-1)}) \cap \langle A^{(i)} \rangle$;
2. $C(A^{(i-1)}) \setminus S^{(i-1)}(a_i) \neq \emptyset$.

ДОКАЗАТЕЛЬСТВО. 1. Пусть $a \in C(A^{(i-1)}) \cap \langle A^{(i)} \rangle$. Так как $a \in \langle A^{(i)} \rangle$, то $a = a' + ca_i$, где $a' \in \langle A^{(i-1)} \rangle$ и $a' < a$, при этом $c \in \mathbb{N}$, поскольку при $c = 0$ получаем противоречие: $a \in \langle A^{(i-1)} \rangle$. Тогда по утверждению 1(5) $(a - a') \in C(A^{(i-1)})$ и $a_i \mid (a - a')$. Отсюда в силу утверждения 1(1) $\delta_i a_i \mid (a - a')$. Следовательно, $a \in S^{(i-1)}(a_i)$.

Пусть $a \in S^{(i-1)}(a_i)$, тогда по определению $a \in C(A^{(i-1)})$ и найдётся число $b \in \overline{\langle A^{(i-1)} \rangle}$ такое, что $a = r\delta_i a_i + b$ при некотором натуральном r , где $r\delta_i a_i \in C(A^{(i-1)})$. Отсюда $a \in \langle A^{(i)} \rangle$, поэтому $a \in C(A^{(i-1)}) \cap \langle A^{(i)} \rangle$.

2. Поскольку A — приведённое множество, то $d_2 < a_1$. Следовательно, $d_2 \in C(A^{(i)})$, так как любой ненулевой элемент полугруппы $\langle A^{(i)} \rangle$ больше либо равен a_1 , $i = 2, \dots, k$. Тогда $C(A^{(i-1)}) \setminus \langle A^{(i)} \rangle \neq \emptyset$, $i = 3, \dots, k$, что с учётом леммы 1(1) исключает равенство $C(A^{(i-1)}) \setminus S^{(i-1)}(a_i) = \emptyset$. Лемма 1 доказана.

Определим функцию $q_i: \{0, \dots, \delta_i - 1\} \rightarrow \{0, d_i, \dots, (\delta_i - 1)d_i\}$ по правилу

$$q_i(r) = ra_i \bmod d_{i-1}, \quad i = 3, \dots, k.$$

Лемма 2. При $i = 3, \dots, k$ функция q_i является биекцией со свойством $q_i(0) = 0$.

ДОКАЗАТЕЛЬСТВО. По условию $\gcd(d_{i-1}, a_i) = d_i$. Следовательно, $\gcd(a_i/d_i, \delta_i) = 1$, и множество $\{ra_i \bmod d_{i-1}, r = 0, \dots, \delta_i - 1\}$ состоит из всех неотрицательных вычетов по модулю d_{i-1} , кратных d_i , $i = 3, \dots, k$. Значит, q_i — подстановка множества $\{0, d_i, \dots, (\delta_i - 1)d_i\}$, где $q_i(0) = 0$. Лемма 2 доказана.

Замечание 1. Если $d_i = d_{i-1}$, то q_i — подстановка степени 1.

Определим связь между множествами $C(A^{(2)}), C(A^{(3)}), \dots, C(A^{(k)})$. Введём следующие обозначения:

$$\begin{aligned} V_0^{(i)} &= U_0^{(i)} = \emptyset, \\ V_r^{(i)} &= \{q_i(r) + td_{i-1} \mid t = 0, \dots, m_r^i - 1\}, \\ U_r^{(i)} &= \{q_i(r) + td_{i-1} \mid t = m_r^i, \dots, m_r^i + z_{i-1}/d_{i-1}\}. \end{aligned}$$

Здесь $1 \leq r \leq \delta_i - 1$, $m_r^i = (ra_i - q_i(r))/d_{i-1}$.

Теорема 1. 1. $C(A^{(i)}) = \bigcup_{r=0}^{\delta_i-1} V_r^{(i)} \cup \{(C(A^{(i-1)}) \setminus S^{(i-1)}(a_i)) + ra_i\};$
 2. $z_i = \max\{C(A^{(i-1)}) \setminus S^{(i-1)}(a_i)\} + (\delta_i - 1)a_i$, $i = 3, \dots, k$.

ДОКАЗАТЕЛЬСТВО. По определению $C(A^{(i)}) = d_i\mathbb{N}_0 \setminus \langle A^{(i)} \rangle$, причём $C(A^{(i)}) \subseteq C(A^{(i-1)}) \subseteq d_i\mathbb{N}_0$ при $\delta_i = 1$. Следовательно,

$$C(A^{(i)}) = C(A^{(i-1)}) \setminus \langle A^{(i)} \rangle = C(A^{(i-1)}) \setminus (C(A^{(i-1)}) \cap \langle A^{(i)} \rangle).$$

Отсюда по лемме 1(1) при $\delta_i = 1$ имеем

$$C(A^{(i)}) = C(A^{(i-1)}) \setminus S^{(i-1)}(a_i), \quad z_i = \max\{C(A^{(i-1)}) \setminus S^{(i-1)}(a_i)\}.$$

Тем самым при $\delta_i = 1$ теорема доказана.

Пусть $\delta_i > 1$. Так как $d_i \mid d_{i-1}$, то выполнено разбиение

$$d_i\mathbb{N}_0 = \bigcup_{r=0}^{\delta_i-1} (rd_i + d_{i-1}\mathbb{N}_0), \quad (3)$$

где $rd_i + d_{i-1}\mathbb{N}_0$ — множество всех чисел из \mathbb{N}_0 , сравнимых с rd_i по модулю d_{i-1} , $r = 0, \dots, \delta_i - 1$.

По определению z_{i-1} есть наибольшее кратное d_{i-1} число, не принадлежащее $\langle A^{(i-1)} \rangle$. Тогда $\{z_{i-1} + td_{i-1} \mid t \in \mathbb{N}\} \subseteq \langle A^{(i-1)} \rangle$. Поскольку $q_i(r) = ra_i \bmod d_{i-1}$, то для $r = 0, \dots, \delta_i - 1$ имеем

$$\{z_{i-1} + td_{i-1} + ra_i \mid t \in \mathbb{N}\} \subseteq \langle A^{(i)} \rangle \cap \{q_i(r) + d_{i-1}\mathbb{N}_0\}.$$

Объединим эти включения по r , учитывая, что q_i — биекция (лемма 2):

$$\begin{aligned} &\bigcup_{r=0}^{\delta_i-1} \{z_{i-1} + td_{i-1} + ra_i \mid t \in \mathbb{N}\} \\ &\subseteq \langle A^{(i)} \rangle \cap (d_{i-1}\mathbb{N}_0 \cup (d_i + d_{i-1}\mathbb{N}_0) \cup \dots \cup ((\delta_i - 1)d_i + d_{i-1}\mathbb{N}_0)). \end{aligned}$$

Отсюда с учётом (3) и включения $\langle A^{(i)} \rangle \subseteq d_i \mathbb{N}_0$ получаем

$$\bigcup_{r=0}^{\delta_i-1} \{z_{i-1} + td_{i-1} + ra_i \mid t \in \mathbb{N}\} \subseteq \langle A^{(i)} \rangle.$$

Тогда по определению множества $C(A^{(i)})$ имеем

$$C(A^{(i)}) \subseteq d_i \mathbb{N}_0 \setminus \bigcup_{r=0}^{\delta_i-1} \{z_{i-1} + td_{i-1} + ra_i \mid t \in \mathbb{N}\},$$

откуда, учитывая, что $ra_i \in \langle A^{(i)} \rangle$, получаем

$$\begin{aligned} C(A^{(i)}) &\subseteq \bigcup_{r=0}^{\delta_i-1} \{q_i(r) + td_{i-1} \mid t = 0, \dots, (ra_i - q_i(r) + z_{i-1})/d_{i-1}\} \\ &= \bigcup_{r=0}^{\delta_i-1} (V_r^{(i)} \cup U_r^{(i)}). \end{aligned} \quad (4)$$

Пусть $r > 0$ и $b \in V_r^{(i)}$. Поскольку b не кратно d_{i-1} , то $b \notin \langle A^{(i-1)} \rangle$. Тогда или $b \in \langle A^{(i)} \rangle \setminus \langle A^{(i-1)} \rangle$, или $b \in C(A^{(i)})$. Пусть $b \in \langle A^{(i)} \rangle \setminus \langle A^{(i-1)} \rangle$, тогда $b = n_i a_i + a$, где $a \in \langle A^{(i-1)} \rangle$, $n_i a_i \equiv q_i(r) \pmod{d_{i-1}}$ и $n_i \geq r$, так как ra_i — наименьшее кратное a_i число в классе вычетов $q_i(r) + d_{i-1} \mathbb{N}_0$. Значит, $b \geq ra_i$, что противоречит определению множества $V_r^{(i)}$. Таким образом, $b \in C(A^{(i)})$ и $V_r^{(i)} \subseteq C(A^{(i)})$.

Пусть $r > 0$ и $b \in U_r^{(i)}$, тогда $b = td_{i-1} + ra_i$, где $t \in \{0, \dots, z_{i-1}/d_{i-1}\}$. Следовательно, $\{(C(A^{(i-1)}) \setminus S^{(i-1)}(a_i)) + ra_i\} \subseteq U_r^{(i)}$, где $b \in \langle A^{(i)} \rangle$ или $b \in C(A^{(i)})$. Опишем числа td_{i-1} , при которых $b \in C(A^{(i)})$. Число td_{i-1} принадлежит одному из следующих непересекающихся множеств: $\langle A^{(i-1)} \rangle$, или $C(A^{(i-1)}) \setminus S^{(i-1)}(a_i)$, или $S^{(i-1)}(a_i)$ при $S^{(i-1)}(a_i) \neq \emptyset$.

Если $td_{i-1} \in \langle A^{(i-1)} \rangle$, то $b \in \langle A^{(i)} \rangle$. Если $td_{i-1} \in S^{(i-1)}(a_i)$, то по лемме 1(1) получаем $td_{i-1} \in \langle A^{(i)} \rangle$, откуда следует, что $b \in \langle A^{(i)} \rangle$. Наконец, если $td_{i-1} \in C(A^{(i-1)}) \setminus S^{(i-1)}(a_i)$, то $b \in C(A^{(i)})$ или $b \in \langle A^{(i)} \rangle$. Во втором случае $td_{i-1} + ra_i = a + n_i a_i$ при некоторых $n_i \in \mathbb{N}$ и $a \in \langle A^{(i-1)} \rangle$ таких, что $n_i a_i \equiv ra_i \pmod{d_{i-1}}$. При $n_i = r$ имеем $td_{i-1} \in \langle A^{(i-1)} \rangle$; противоречие. Поэтому $n_i > r$, так как ra_i — наименьшее кратное a_i число в классе вычетов $q_i(r) + d_{i-1} \mathbb{N}_0$. Следовательно, $td_{i-1} = a + (n_i - r)a_i \in \langle A^{(i)} \rangle$ и $td_{i-1} \in S^{(i-1)}(a_i)$ по лемме 1(1), что противоречит условию. Значит, $b \in C(A^{(i)})$ тогда и только тогда, когда $td_{i-1} \in C(A^{(i-1)}) \setminus S^{(i-1)}(a_i)$. Отсюда и из (4) следуют равенства для $C(A^{(i)})$.

Так как $\max V_r^{(i)} \leq \min\{C(A^{(i-1)}) \setminus S^{(i-1)}(a_i) + ra_i\}$, $r = 1, \dots, \delta_i - 1$, в соответствии с теоремой 1(1) имеем

$$\begin{aligned} z_i &= \max C(A^{(i)}) = \max\{C(A^{(i-1)}) \setminus S^{(i-1)}(a_i) + ra_i\} \\ &= \max\{C(A^{(i-1)}) \setminus S^{(i-1)}(a_i)\} + \max\{0, a_i, \dots, (\delta_i - 1)a_i\}. \end{aligned}$$

В силу леммы 1(2) $C(A^{(i-1)}) \setminus S^{(i-1)}(a_i) \neq \emptyset$. Тогда

$$z_i = \max\{C(A^{(i-1)}) \setminus S^{(i-1)}(a_i)\} + (\delta_i - 1)a_i, \quad i = 3, \dots, k.$$

Теорема 1 доказана.

Следствие 2. При $i = 3, \dots, k$ имеем $z_i \leq z_{i-1} + (\delta_i - 1)a_i$, откуда следует оценка Брауэра [8]:

$$g(a_1, \dots, a_k) \leq a_1 a_2 / d_2 - a_1 - a_2 + \sum_{i=3}^k (\delta_i - 1)a_i.$$

В последней оценке числа $g(a_1, \dots, a_k)$ достигается равенство, если $S^{(i-1)}(a_i) = \emptyset$ для всех $i = 3, \dots, k$.

Следствие 3. Пусть $p_A = p$ и $d_j = d_{j+1} = \dots = d_m$ при некоторых j и m , где $1 < j < m \leq k$. Тогда имеем ряд включений

$$C(A^{(j)}) \supseteq C(A^{(j+1)}) \supseteq \dots \supseteq C(A^{(m)}), \quad (5)$$

а для числа Фробениуса $g(a_1, \dots, a_k)$ справедлива оценка

$$\begin{aligned} g(a_1, \dots, a_k) &\leq \max\{C(A^{(p-1)}) \setminus S^{(p-1)}(a_p)\} + (d_{p-1} - 1)a_p \\ &\leq (a_1 - 1)(a_p - 1) - 1 < a_1 a_p. \end{aligned}$$

ДОКАЗАТЕЛЬСТВО. В данных условиях $\delta_{j+1} = \delta_{j+2} = \dots = \delta_m$, тогда по теореме 1 выполнена цепочка (5). В частности, условия выполнены при $j = p$, $m = k$. Тогда из (5) следует, что

$$z_p \geq z_{p+1} \geq \dots \geq z_k = g(a_1, \dots, a_k),$$

где $z_p = \max\{C(A^{(p-1)}) \setminus S^{(p-1)}(a_p)\} + (d_{p-1} - 1)a_p$ по теореме 1. В силу утверждения 1(6) $z_p \leq (a_1 - 1)(a_p - 1) - 1 < a_1 a_p$. Следствие 3 доказано.

Следствие 4. Пусть множество $A = \{a_1, a_2, a_3\}$ примитивное и

$$\max\{(C(A^{(2)}) \setminus S^{(2)}(a_3))\} = b.$$

Тогда $g(a_1, a_2, a_3) = b + (d_2 - 1)a_3$ и

$$C(A) = \bigcup_{r=0}^{d_2-1} (V_r^{(3)} \cup \{(C(A^{(2)}) \setminus S^{(2)}(a_3)) + ra_3\}).$$

Пример 1 (достижимость оценки Брауэра). Рассмотрим множество чисел $A = \{30, 42, 70a, 105b\}$, которое примитивно при любых простых $a \neq 3$ и $b \neq 2$. Вычислим $d_2 = 6$, $d_3 = 2$, $d_4 = 1$, $\delta_3 = 3$ и $\delta_4 = 2$. Тогда $z_2 = 138$. При $3 \cdot 70a > 138$ выполнено $S^{(2)}(70a) = \emptyset$ и $z_3 = 138 + 140a$. При $2 \cdot 105b > 138 + 140a$ имеем $S^{(3)}(105b) = \emptyset$ и $g(30, 42, 70a, 105b) = z_4 = 138 + 140a + 105b$. Следовательно, оценка достижима, в частности, при выполнении системы условий $\{210a > 138, 210b > 138 + 140a\}$, например, при $a = 5$ и любом простом $b \geq 5$.

3. Редукция РПФ (ПФ) и сравнение оценок

В [4] показано, что для сокращения вычислений при решении РПФ и ПФ можно использовать отношения эквивалентности. Примитивные множества A и B называются *эквивалентными*, если $C(A) = C(B)$ (или, что равносильно, $\langle A \rangle = \langle B \rangle$). Тогда $g(A) = g(B)$ для эквивалентных множеств A и B .

В соответствии с утверждением 2(1) минимальным подмножеством, эквивалентным множеству A , является A -базис. При построении A -базиса необходимо проверять свойства $a_i \in C(A^{(i-1)})$, $i = 3, \dots, k$, а для этого необходимо решить РПФ для множества $A^{(i-1)}$. Следовательно, в худшем случае сложность построения A -базиса близка к сложности РПФ. Вместе с тем, несложно построить эквивалентное подмножество A' множества A , содержащее A -базис [4].

Удаление из исходного множества $A'' = \{a_1, \dots, a_k\}$ «лишних» чисел можно выполнить в два этапа с помощью поиска в нём линейных зависимостей частного вида. Обозначим через s_A число различных классов вычетов по модулю a_1 , элементы которых содержатся в A .

Алгоритм редукции множества A''

Этап 1. Поиск с помощью факторизации чисел a_2, \dots, a_k по модулю a_1 [4, разд. 2].

Из A'' удаляются все числа, кроме наименьших чисел всех фактор-классов по модулю a_1 , представленных в A . Полученное примитивное подмножество A' эквивалентно A'' и состоит из $s_{A''}$ чисел, где $s_{A''} \leq s_A$.

Пусть (без ограничения общности) $s_{A''} = s$, $A' = \{a_1, \dots, a_s\}$, $p_{A'} = \pi$.

ЭТАП 2. Удаление «больших» чисел из множества A' [4, разд. 3].

Пусть $d_i = \gcd(a_1, \dots, a_i)$, $i = 1, \dots, s$, где $a_1 > 2$. Определим отношение эквивалентности для чисел $i, j \in \{2, \dots, s\}$: $i \simeq j \Leftrightarrow d_i = d_j$. При $d_1 > d_2$ число классов эквивалентности равно μ , где $\mu = \mu_{A'} \leq s - 1$. Множество $M(A')$ определяет разбиение последовательности $\{a_2, \dots, a_s\}$ на μ отрезков длины $n_1, \dots, n_\mu \geq 1$, где каждый отрезок состоит из чисел с эквивалентными индексами, при этом $n_1 + \dots + n_\mu = s - 1$, $n_\mu = s - \pi + 1$.

Пусть I_1, \dots, I_μ — классы эквивалентных чисел: $I_\mu = \{\pi, \dots, s\}$, $I_r = \{j_{r-1} + 1, \dots, j_{r-1} + n_r\}$, $j_{r-1} = n_1 + \dots + n_{r-1}$, $1 \leq r < \mu$, $j_0 = 1$. Если $n_r > 1$, то из (5) получаем $z_{j_{r-1}+1} \geq z_{j_{r-1}+2} \geq \dots \geq z_{j_{r-1}+n_r}$, где по утверждению 1(7) $z_{j_{r-1}+1} \leq a_1 a_{j_{r-1}+1} / d_{j_{r-1}+1} - a_1 - a_{j_{r-1}+1}$, $r = 1, \dots, \mu$. Следовательно, если при $j \in \{j_{r-1} + 2, \dots, j_{r-1} + n_r\}$

$$a_j > a_1 a_{j_{r-1}+1} / d_{j_{r-1}+1} - a_1 - a_{j_{r-1}+1}, \quad (6)$$

то числа $a_j, \dots, a_{j_{r-1}+n_r}$ принадлежат полугруппе $\langle a_1, \dots, a_{j_{r-1}+1} \rangle$. После их удаления получаем подмножество A порядка l , которое эквивалентно A' , где $l \leq s \leq a_1$, $\max A \leq a_1 a_\pi - a_1 - a_\pi$.

Пример 2. Пусть $A'' = \{15, 25, 35, 40, 45, 54, 93, 913\}$. Факторизация чисел из A'' по модулю 15 даёт множество $\{0, 10, 5, 10, 0, 9, 3, 13\}$. Удаляя из A'' 40 и 45, получаем $A' = \{15, 25, 35, 54, 93, 913\}$.

Для A' вычисляем $d_2 = d_3 = 5$, $d_4 = d_5 = d_6 = 1$, тогда $\mu = 2$, $I_1 = \{2, 3\}$, $I_2 = \{4, 5, 6\}$. Классу I_1 соответствует граничное значение $5(3 \cdot 7 - 3 - 7) = 55$. Значит, из отрезка $\{25, 35\}$ числа не удаляются. Классу I_2 соответствует граничное значение $5 \cdot 54 - 15 - 54 = 741$. Значит, из отрезка $\{93, 913\}$ удаляется число 913, превышающее границу. Окончательно имеем $A'' \simeq A = \{15, 25, 35, 54, 93\}$.

4. Алгоритм РПФ и оценка сложности

Лемма 3. Пусть $A = \{a_1, \dots, a_l\}$, $\mu_A = \mu$, $p_A = p$, $\alpha \in \mathbb{N}$. Тогда

$$\sum_{i=2}^p a_i d_i^{-\alpha} < (p - \mu) a_p.$$

ДОКАЗАТЕЛЬСТВО. Рассмотрим функцию $\phi(x_2, x_3, \dots, x_p) = \sum_{i=2}^p a_i x_i$, где переменные x_2, x_3, \dots, x_p принимают положительные действительные значения. Положим $(x_2, x_3, \dots, x_p) \leq (y_2, y_3, \dots, y_p)$, если и только если $x_i \leq y_i$, $i = 2, \dots, p$. Тогда в данной области определения функция ϕ монотонна, так как $0 < a_1 < \dots < a_p$.

При $\mu_A = \mu$ множество $\{d_2, d_3, \dots, d_p\}$ разбивается на классы равных чисел I_1, \dots, I_μ , при этом порядки классов равны n_1, \dots, n_μ соответственно, где $I_\mu = \{d_p\}$, $I_r = \{d_{j_r+1}, d_{j_r+2}, \dots, d_{j_r+n_r}\}$, $j_1 = 1$, $j_{r+1} = 1 + n_1 + \dots + n_r$, $r = 1, \dots, \mu - 1$. Следовательно,

$$(d_2^{-\alpha}, d_3^{-\alpha}, \dots, d_p^{-\alpha}) \leq (b_2^{-\alpha}, b_3^{-\alpha}, \dots, b_p^{-\alpha}) \quad \text{при любом } \alpha \in \mathbb{N},$$

где $b_{1+r} = d_{j_r+1}$ при $r = 1, \dots, \mu$, $b_{\mu+2} = \dots = b_p = d_p = 1$. Отсюда

$$\begin{aligned} \sum_{i=2}^p a_i d_i^{-\alpha} &= \phi(d_2^{-\alpha}, d_3^{-\alpha}, \dots, d_p^{-\alpha}) \\ &\leq \phi(b_2^{-\alpha}, b_3^{-\alpha}, \dots, b_p^{-\alpha}) = \sum_{i=2}^{\mu+1} a_i b_i^{-\alpha} + \sum_{i=\mu+2}^p a_i b_i^{-\alpha}, \end{aligned}$$

где $\sum_{i=\mu+2}^p a_i b_i^{-\alpha} = \sum_{i=\mu+2}^p a_i \leq a_p(p - \mu - 1)$ при $\alpha \in \mathbb{N}$. По построению $b_{j-1}^{-\alpha} < b_j^{-\alpha}$ и $b_{j-1}^{-\alpha}$ делит $b_j^{-\alpha}$, $j = 3, \dots, \mu + 1$, следовательно, при $\alpha \in \mathbb{N}$ имеем

$$\sum_{i=2}^{\mu+1} a_i b_i^{-\alpha} \leq a_{\mu+1} \sum_{i=2}^{\mu+1} b_i^{-\alpha} \leq a_{\mu+1}(2^{-1} + 2^{-2} + \dots + 2^{-\mu}) < a_{\mu+1}.$$

Отсюда $\phi(b_2^{-\alpha}, b_3^{-\alpha}, \dots, b_p^{-\alpha}) < (p - \mu - 1)a_p + a_{\mu+1} \leq (p - \mu)a_p$. Лемма 3 доказана.

Предположим, что множество $A = \{a_1, \dots, a_l\}$ получено из исходного множества A'' порядка k после двухэтапной редукции, $p_A = p$.

Алгоритм РПФ. Корректность алгоритма следует из теоремы 1 и свойств редуцированного множества. Алгоритм основан на последовательном «просмотре» чисел a_1, a_2, \dots, a_l в порядке возрастания и на построении упорядоченных множеств $C(A^{(i)})$, $i = 2, \dots, l$, $l > 1$.

ШАГ 1. Определение упорядоченного множества $C(A^{(2)})$.

Определить и упорядочить множество

$$C(A^{(2)}) = \{a_1 a_2 / d_2 - t a_1 - j a_2 > 0 \mid t, j \in \mathbb{N}\}.$$

ШАГ $i - 1$. Определение $C(A^{(i)})$, $i = 3, \dots, l$.

1. Проверить свойство $a_i \in C(A^{(i-1)})$, $i = 3, \dots, l$.
2. Если $d_i = d_{i-1}$ и $a_i \notin C(A^{(i-1)})$, то $C(A^{(i)}) = C(A^{(i-1)})$.

При $i \leq l$ перейти на шаг i , п. 1.

3. Если $d_i = d_{i-1}$ и $a_i \in C(A^{(i-1)})$ или $d_i < d_{i-1}$,
то определить множество $C(A^{(i-1)}) \setminus S^{(i-1)}(a_i)$:
в $C(A^{(i-1)})$ найти подмножество Ξ_{i-1} чисел, кратных $\delta_i a_i$;
если $\Xi_{i-1} = \emptyset$, то $S^{(i-1)}(a_i) = \emptyset$;
если $\Xi_{i-1} \neq \emptyset$, то $\eta \in S^{(i-1)}(a_i) \Leftrightarrow \eta = j\delta_i a_i + \xi$,
где $\xi \in \langle A^{(i-1)} \rangle$, $j\delta_i a_i \in \Xi_{i-1}$, $j \in \mathbb{N}$, $i = 3, \dots, l$.
Если $d_i = d_{i-1}$ и $a_i \in C(A^{(i-1)})$,
то $C(A^{(i)}) = C(A^{(i-1)}) \setminus S^{(i-1)}(a_i)$, $i = 3, \dots, l$.
4. Если $d_i < d_{i-1}$, то для всех $i \in M(A)$ определить множество

$$C(A^{(i)}) = \bigcup_{r=0}^{\delta_i-1} V_r^{(i)} \cup \{(C(A^{(i-1)}) \setminus S^{(i-1)}(a_i)) + ra_i\}$$

следующим образом:

- определить упорядоченное множество $V_r^{(i)}$,
вычислив $q_i(r)$ и суммы $q_i(r) + td_{i-1}$ для $t = 0, \dots, m_r^i$,
где $q_i(r) + m_r^i d_{i-1} = ra_i$;
для $r = 0, \dots, \delta_i - 1$ определить упорядоченные множества
 $\{(C(A^{(i-1)}) \setminus S^{(i-1)}(a_i)) + ra_i\}$;
упорядочить $C(A^{(i)})$ слиянием множеств $V_r^{(i)}$
и $\{(C(A^{(i-1)}) \setminus S^{(i-1)}(a_i)) + ra_i\}$, $r = 0, \dots, \delta_i - 1$,
определённых на предыдущих этапах.

Замечание 2. Алгоритм решает РПФ и по ходу решения определяет A -базис. Число шагов, на которых алгоритм РПФ выполняет пп. 3 и 4, равно λ_A и μ_A соответственно.

Замечание 3. Для вычисления $g(a_1, \dots, a_l)$ после $(l-1)$ -го шага алгоритма следует определить $z_{l-1} = \max C(A^{(l-1)}) \setminus S^{(l-1)}(a_l)$. Тогда $g(a_1, \dots, a_l) = z_{l-1} + (d_{l-1} - 1)a_l$.

Пример 3 (определение $g(A)$). 1. $A = \{6, 10, 15\}$ — примитивное приведённое множество. Вычислим $d_2 = \delta_3 = 2$, $z_2 = 14$. Так как $30 > z_2$, то $S^{(2)}(15) = \emptyset$ и $g(A) = z_2 + (\delta_3 - 1)15 = 29$.

2. $A = \{18, 21, 29\}$ — примитивное приведённое множество. Вычислим $d_2 = \delta_3 = 3$, $z_2 = 87$,

$$C(A^{(2)}) = \{3, 6, 9, 12, 15, 24, 27, 30, 33, 45, 48, 51, 66, 69, 87\}.$$

В множестве $C(A^{(2)})$ имеется единственное число, кратное 87. Поэтому $S^{(2)}(29) = \{87\}$ и $\max(C(A^{(2)}) \setminus S^{(2)}(29)) = 69$. Следовательно, получаем $g(A) = 69 + (\delta_3 - 1)29 = 127$.

3. $A = \{12, 20, 24, 28, 55\}$ — примитивное неприведённое множество. Определим A -базис $B = \{12, 20, 28, 55\}$. Далее для выписанного B вычислим $d_2 = d_3 = 4$, $\delta_3 = 1$, $\delta_4 = 4$, $z_2 = 28$, тогда

$$C(B^{(2)}) = \{4, 8, 16, 28\}, \quad S^{(2)}(28) = \{28\},$$

так что $C(B^{(2)}) \setminus S^{(2)}(28) = \{4, 8, 16\}$.

Биекция q_3 вырождена. Значит, в этом случае имеют место равенства $C(B^{(3)}) = C(B^{(2)}) \setminus S^{(2)}(28) = \{4, 8, 16\}$, $S^{(3)}(55) = \emptyset$ и $z_3 = 16$. Отсюда $g(A) = g(B) = z_4 = 16 + 3 \cdot 55 = 181$.

4. $A = \{22, 26, 27, 29\}$ — приведённое множество, где $d_2 = \delta_3 = 2$, $d_3 = \delta_4 = 1$, $z_2 = 238$. Дальнейшие вычисления представлены в табл. 1. В итоге получим $g(A) = z_4 = 94$.

Таблица 1

$C(A^{(2)})$	чётные: 2, ..., 20, 24, 28, ..., 42, 46, 50, 54, ..., 64, 68, 72, 76, 80, ..., 86, 90, 94, 98, 102, 106, 108, 112, 116, 120, 124, 128, 134, 138, 142, 146, 150, 160, 164, 168, 172, 186, 190, 194, 212, 216, 238
$S^{(2)}(27, 54)$	чётные: 54, 76, 80, 98, 102, 106, 120, 124, 128, 142, 146, 150, 164, 168, 172, 186, 190, 194, 212, 216, 238
$S^{(2)}(27, 108)$	чётные: 108, 134, 160, 186, 212, 238
$S^{(2)}(27, 216)$	чётные: 216, 238
$C(A^{(2)}) \setminus S^{(2)}(27)$	чётные: 2, ..., 20, 24, 28, ..., 42, 46, 50, 56, ..., 64, 68, 72, 82, 84, 86, 90, 94, 112, 116, 138
$C(A^{(3)}), q_3 = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$	чётные: 2, ..., 20, 24, 28, ..., 42, 46, 50, 56, ..., 64, 68, 72, 82, 84, 86, 90, 94, 112, 116, 138 нечётные: 1, ..., 25, 29, ..., 47, 51, 55, ..., 69, 73, 77, 83, ..., 91, 95, 99, 109, 111, 113, 117, 121, 139, 143, 165
$S^{(3)}(29, 29)$	чётные: 56, 82 нечётные: 29, 51, 55, 73, 77, 83, 95, 99, 109, 117, 121, 139, 143, 165
$S^{(3)}(29, 58)$	чётные: 58, 84, 112, 138 нечётные: 85, 111, 139, 165
$S^{(3)}(29, 87)$	чётные: \emptyset нечётные: 87, 109, 113, 139, 165
$S^{(3)}(29, 116)$	чётные: 116, 138 нечётные: 143, 165
$C(A^{(3)}) \setminus S^{(3)}(29)$	чётные: 2, ..., 20, 24, 28, ..., 42, 46, 50, 60, 62, 64, 68, 72, 86, 90, 94 нечётные: 1, ..., 25, 31, ..., 47, 57, ..., 69, 73, 77, 83, 89, 91

Оценим вычислительную сложность алгоритмов в битовых операциях, используя двоичные представления чисел. Битовую сложность сложения, вычитания и сравнения n -разрядных чисел оценим величиной порядка $O(\log n)$, умножение (деление) n -разрядного числа на m -разрядное число оценим величиной порядка $O(\log n \log m)$. Битовую сложность алгоритмов РПФ и ПФ для множества A обозначим соответственно через $T_{\text{РПФ}}(A)$ и $T_{\text{ПФ}}(A)$.

Теорема 2. Для примитивного множества $A'' = \{a_1, \dots, a_k\}$ при $k \geq 3$ справедливы следующие утверждения.

1. Сложность этапа 1 редукции множества A'' в примитивное эквивалентное множество $A' = \{a_1, \dots, a_s\}$ не больше $O\left(\log a_1 \sum_{i=2}^k \log a_i\right)$, где $s = s_{A''} \leq a_1$.

2. Сложность этапа 2 редукции множества A' в примитивное эквивалентное множество $A = \{a_1, \dots, a_l\}$ не больше $O(\pi \log^2 a_\pi)$, где $2 \leq l \leq s$, $\pi = p_{A'}$, $\max A \leq a_1 a_\pi - a_1 - a_\pi$.

3. Сложность $T_{\text{РПФ}}(A)$ не больше $O((\lambda_A - \mu_A) a_1^2 a_p \log^2 a_p)$, где $p = p_A$. Требуемая память имеет порядок $O(a_1 a_p \log a_p)$ битов.

ДОКАЗАТЕЛЬСТВО. 1. Сложность вычисления $a_i \bmod a_1$ имеет порядок $O(\log a_1 \log a_i)$, $i = 2, \dots, k$.

2. Удаление «больших» чисел на втором этапе редукции требует вычисления d_2, \dots, d_π , вычисления границ, определяемых правыми частями неравенств (6), и сравнения с каждой границей всех чисел a_j соответствующего класса за исключением наименьшего числа класса. Сложность вычисления $d_i = \gcd(d_{i-1}, a_i)$ не больше $O(\log^2 a_i)$, $i = 2, \dots, \pi$. Величина границ менее $a_1 a_\pi$, тогда сложность вычисления μ границ, где $\mu = \mu'_A$, и сравнения их с не более чем s числами равна

$$O(\pi \log^2 a_\pi + \mu(\log a_1 \log a_\pi + \log s \log a_\pi)) \leq O(\pi \log^2 a_\pi).$$

Следовательно, сложность этапа 2 редукции не больше $O(\pi \log^2 a_\pi)$.

3. Оценим сложность РПФ(A), где $l \leq s$ и $a_l < a_1 a_p$. Согласно утверждению 1(7) и следствию 3 $\max C(A^{(i)}) < a_1 a_i / d_i \leq a_1 a_p$, тогда $|C(A^{(i)})| < a_1 a_i / d_i^2 \leq a_1 a_p$, так как числа из $C(A^{(i)})$ кратны d_i , и разрядность чисел из $C(A^{(i)})$ не превышает $O(\log a_p)$, $i = 2, \dots, l$.

При a_2 , не кратном a_1 , вычисление множества $C(A^{(2)})$ в соответствии с утверждениями 1(2) и 1(3) требует порядка $|C(A^{(2)})| < a_1 a_2 / d_2^2$ сложений и вычитаний чисел, меньших $a_1 a_2 / d_2$, тогда сложность вычисления $C(A^{(2)})$ не больше $O((a_1 a_2 / d_2^2) \log a_2)$. Сложность упорядочения множества $C(A^{(2)})$ методом вставок не больше $O((a_1 a_2 / d_2^2) \log^2 a_2)$.

Следовательно, битовая сложность первого шага алгоритма не больше $O((a_1 a_2 / d_2^2) \log^2 a_2)$.

Проверка свойства $a_i \in C(A^{(i-1)})$ требует не более $O(\log a_p)$ сравнений, т. е. не более $O(l \log^2 a_p) \leq O(a_1 \log^2 a_p)$ битовых операций для всех $i = 3, \dots, l$.

Поскольку все числа из Ξ_{i-1} кратны $\delta_i a_i$, для $i = 3, \dots, l$ имеем

$$|\Xi_{i-1}| \leq z_{i-1} / \delta_i a_i < a_1 a_{i-1} / d_{i-1} \delta_i a_i < a_1 / d_{i-1}.$$

Сложность вычисления и поиска в $C(A^{(i-1)})$ всех чисел $\lambda_j = j \delta_i a_i$, где $j \in \mathbb{N}$, не превосходит $O(|\Xi_{i-1}| \log^2 a_p)$. Тогда сложность вычисления множеств Ξ_2, \dots, Ξ_{l-1} не больше

$$O(a_1 \log^2 a_p (d_2^{-1} + \dots + d_{l-1}^{-1})) \leq O(l a_1 \log^2 a_p) \leq O(a_1^2 \log^2 a_p).$$

Сложность построения множества $S^{(i-1)}(a_i)$ и определения множества $C(A^{(i-1)}) \setminus S^{(i-1)}(a_i)$ в худшем случае (при $S^{(i-1)}(a_i) \neq \emptyset$) не больше $|\Xi_{i-1}| |C(A^{(i-1)})| \log^2 |C(A^{(i-1)})|$. Тогда с учётом леммы 3 сложность построения множеств $C(A^{(i-1)}) \setminus S^{(i-1)}(a_i)$ для $i \in M(A)$ не больше $O(a_1^2 a_p \log^2 a_p)$. Сложность построения множеств $C(A^{(i-1)}) \setminus S^{(i-1)}(a_i)$ для $i \in L(A) \setminus M(A)$ не больше $O((\lambda_A - \mu_A) a_1^2 a_p \log^2 a_p)$. На остальных шагах построение этих множеств не выполняется. Следовательно, сложность построения множеств $C(A^{(i-1)}) \setminus S^{(i-1)}(a_i)$ для $i = 3, \dots, l$ не больше $O((\lambda_A - \mu_A) a_1^2 a_p \log^2 a_p)$.

При всех $i = 3, \dots, p$ определение чисел ra_i для $r = 1, \dots, \delta_i - 1$ с помощью суммирования a_i требует не более чем $O(pd_2 \log a_p)$ операций, определение $V_r^{(i)}$ с помощью вычитаний $ra_i - td_{i-1}$, $t = 1, \dots, m_r^i$, требует не более $O(pd_2 a_p \log a_p)$ операций, наконец, вычисление множества

$$\{(C(A^{(i-1)}) \setminus S^{(i-1)}(a_i)) + ra_i\}, \quad r = 1, \dots, \delta_i - 1,$$

т. е. чисел из $C(A^{(i)})$, требует не более $O(pa_1 a_p \log a_p)$ операций.

Сложность упорядочения множеств $C(A^{(i)})$ путём слияния множеств

$$V_r^{(i)} \cup \{(C(A^{(i-1)}) \setminus S^{(i-1)}(a_i)) + ra_i\}, \quad r = 1, \dots, \delta_i - 1,$$

для всех $i = 3, \dots, p$ не больше $O(pa_1 a_p \log a_p)$. Так как $p \leq a_1$, порядок величины $\text{ТРПФ}(A)$ определяется сложностью вычисления множеств $C(A^{(i-1)}) \setminus S^{(i-1)}(a_i)$ для $i = 3, \dots, l$, т. е. величиной порядка $O((\lambda_A - \mu_A) a_1^2 a_p \log^2 a_p)$.

Поскольку после p -го шага порядок множества $C(A^{(i)})$ не возрастает, объём требуемой памяти оценивается количеством $|C(A^{(p)})| \leq a_1 a_p$

ячеек, где в ячейках записаны числа, меньшие $a_1 a_p$. Отсюда объём памяти в битах оценивается величиной порядка $O(a_1 a_p \log a_p)$. Теорема 2 доказана.

Следствие 5. *Сложность ПФ(A'') в арифметических операциях имеет порядок $O(k + \pi \log a_\pi + l a_1)$, где l — порядок множества, полученного из A'' после двухэтапной редукции, причём $2 \leq l \leq a_1$.*

ДОКАЗАТЕЛЬСТВО. Применим двухэтапную редукцию множества A'' в множество A и алгоритм Боккера — Липтак [6] для решения ПФ(A).

Первый этап редукции состоит из k операций деления с остатком, сложность второго этапа определяется сложностью поиска π наибольших общих делителей, каждый из которых находится в результате цепи не более $\log a_\pi$ делений с остатком. Алгоритм Боккера — Липтак для множества A имеет оценку сложности $O(l a_1)$. Следствие 5 доказано.

Комментарий к полученным оценкам

Важной числовой характеристикой, определяющей вычислительную сложность решения РПФ, является индекс примитивности исходного примитивного множества $\{a_1, \dots, a_k\}$, где $k > 2$, равный наименьшему $p \in N$, при котором $\gcd(a_1, \dots, a_p) = 1$ и $\gcd(a_1, \dots, a_{p-1}) > 1$, $2 \leq p \leq k$.

Предложенная двухэтапная редукция сводит решение РПФ для исходного множества чисел $\{a_1, \dots, a_k\}$ к решению РПФ для подмножества $\{a_1, \dots, a_l\}$, где число l определяется исходным множеством и неравенствами $2 \leq p \leq l \leq k$. Таким образом, в случае $\log a_p \log a_k \leq a_1$ вычислительная сложность двухэтапной редукции не больше $O(k \log a_p \log a_k)$, т. е. не больше сложности лучшей из известных оценок для ПФ [6].

Вычислительная сложность решения РПФ по порядку величины не больше $O(c a_1^2 a_p (\log a_p)^2)$, где c — константа, определяемая множеством чисел $\{a_1, \dots, a_k\}$, $2 \leq c < k$. Данная оценка не больше сложности известных алгоритмов решения ПФ, реализуемых без использования редукции, только в тех случаях, когда константа c мала, а число k велико, а именно, если $c a_1 a_p (\log a_p)^2 \leq k$.

Вычислительная сложность решения ПФ с помощью предложенной редукции и алгоритма Боккера — Липтак из [6] по порядку величины не больше $O(k + p \log a_p + l a_1)$, где l — мощность входного множества после двухэтапной редукции, $2 \leq l \leq a_1$. Эта оценка лучше, чем аналогичная оценка для алгоритма Боккера — Липтак, применяемого для нередуцированного множества, если $l < k$ и $\log a_p < a_1$.

Выводы

1. Описана двухэтапная редукция примитивного входного множества задачи в эквивалентное примитивное множество, позволяющая улучшить оценки сложности РПФ и ПФ в некоторых из тех случаев, когда редукция приводит к существенному сокращению порядка входного множества.

2. Определён закон нестационарной рекурсии, связывающий множества $C(A^{(i-1)})$ и $C(A^{(i)})$, $i = 3, 4, \dots$. Рекурсия с использованием теоретико-множественных операций позволяет построить новые алгоритмы (отличные от известных теоретико-графовых алгоритмов) определения множества $C(a_1, \dots, a_k)$ всех натуральных чисел, не содержащихся в аддитивной полугруппе $\langle a_1, \dots, a_k \rangle$, в частности, числа Фробениуса $g(a_1, \dots, a_k)$. Полученные оценки сложности решения РПФ и ПФ на основе данной рекурсии не улучшают существенно оценок сложности лучших известных алгоритмов.

ЛИТЕРАТУРА

1. Арнольд В. И. Экспериментальное наблюдение математических фактов. М.: МЦНМО, 2006. 119 с.
2. Устинов А. В. Решение задачи Арнольда о слабой асимптотике для чисел Фробениуса с тремя аргументами // Мат. сб. 2009. № 4. С. 131–160.
3. Устинов А. В. Геометрическое доказательство формулы Рёдсета для чисел Фробениуса // Тр. МИАН. 2012. № 276. С. 280–287.
4. Фомичёв В. М. Эквивалентные по Фробениусу примитивные множества чисел // Прикл. дискрет. математика. 2014. № 1. С. 20–26.
5. Фомичёв В. М. Оценка экспонента некоторых графов с помощью чисел Фробениуса для трех аргументов // Прикл. дискрет. математика. 2014. № 2. С. 88–96.
6. Böcker S., Lipták Zs. The Money Changing Problem revisited: Computing the Frobenius number in time $O(ka_1)$ // Computing and Combinatorics. Proc. 4th Annu. Int. Conf. (Kunming, China, Aug. 16–19, 2005). Heidelberg: Springer, 2005. P. 965–974. (Lect. Notes Comput. Sci.; Vol. 3595).
7. Bogart C. Calculating Frobenius numbers with Boolean Toeplitz matrix multiplication. <http://quetzal.bogarthome.net/frobenius.pdf>
8. Brauer A. On a problem of partitions // Am. J. Math. 1942. Vol. 64. P. 299–312.
9. Brauer A., Shockley J. E. On a problem of Frobenius // J. Reine Angew. Math. 1962. Vol. 211. P. 215–220.
10. Curtis F. On formulas for the Frobenius number of a numerical semigroup // Math. Scand. 1990. Vol. 67. P. 190–192.

11. **Heap B. R., Lynn M. S.** A graph-theoretic algorithm for the solution of a linear Diophantine problem of Frobenius // Numer. Math. 1964. Vol. 6. P. 346–354.
12. **Heap B. R., Lynn M. S.** On a linear Diophantine problem of Frobenius: an improved algorithm // Numer. Math. 1965. Vol. 7. P. 226–231.
13. **Johnson D. B.** Efficient algorithms for shortest paths in space networks // JACM. 1977. Vol. 24. P. 1–13.
14. **Nijenhuis M.** A minimal-path algorithm for the “Money changing problem” // Am. Math. Mon. 1979. Vol. 86. P. 832–835.
15. **Ramírez Alfonsín J. L.** The Diophantine Frobenius problem. Oxford: Clarendon Press, 2005. 243 p. (Oxf. Lect. Ser. Math. Appl.; Vol. 30).
16. **Sylvester J. J.** Problem 7382 // Mathematical Questions with Their Solutions: From the “Educational Times,” London: Francis Hodgson, 1884. Vol. 41. P. 21.

Фомичёв Владимир Михайлович

Статья поступила

8 апреля 2016 г.

Исправленный вариант —

31 октября 2016 г.

UDC 519.6

DOI: 10.17377/daio.2017.24.537

COMPUTATIONAL COMPLEXITY OF THE ORIGINAL
AND EXTENDED DIOPHANTINE FROBENIUS PROBLEM

V. M. Fomichev^{1,2}

¹Financial University under the Government of the Russian Federation,
49 Leningradsky Ave., 125993 Moscow, Russia,

²National Research Nuclear University MEPhI,
31 Kashirskoe Highway, 115409 Moscow, Russia,

E-mail: fomichev@nm.ru

Abstract. We deduce the law of nonstationary recursion which makes it possible, for given a primitive set $A = \{a_1, \dots, a_k\}$, $k > 2$, to construct an algorithm for finding the set of the numbers outside the additive semigroup generated by A . In particular, we obtain a new algorithm for determining the Frobenius numbers $g(a_1, \dots, a_k)$. The computational complexity of these algorithms is estimated in terms of bit operations. We propose a two-stage reduction of the original primitive set to an equivalent primitive set that enables us to improve complexity estimates in the cases when the two-stage reduction leads to a substantial reduction of the order of the initial set. Bibliogr. 16.

Keywords: Frobenius number, primitive set, additive semigroup, computational complexity.

REFERENCES

1. V. I. Arnold, *Experimental observation of mathematical facts*, MTsNMO, Moscow, 2006.
2. A. V. Ustinov, The solution of Arnold's problem on the weak asymptotics of Frobenius numbers with three arguments, *Mat. Sb.*, **200**, No. 4, 131–160, 2009. Translated in *Sb. Math.*, **200**, No. 4, 597–627, 2009.
3. A. V. Ustinov, Geometric proof of Rødseth's formula for Frobenius numbers, *Tr. Mat. Inst. Steklova*, **276**, 280–287, 2012. Translated in *Proc. Steklov Inst. Math.*, **276**, No. 1, 275–282, 2012.
4. V. M. Fomichev, Primitive sets of numbers being equivalent by Frobenius, *Prikladn. Diskretn. Mat.*, No. 1, 20–26, 2014.
5. V. M. Fomichev, Estimates for exponent of some graphs by means of Frobenius's numbers of three arguments, *Prikladn. Diskretn. Mat.*, No. 2, 88–96, 2014.

6. **S. Böcker** and **Zs. Lipták**, The Money Changing Problem revisited: Computing the Frobenius number in time $O(ka_1)$, in *Computing and Combinatorics* (Proc. 4th Annu. Int. Conf., Kunming, China, Aug. 16–19, 2005), pp. 965–974, Springer, Heidelberg, 2005 (Lect. Notes Comput. Sci., Vol. 3595).
7. **C. Bogart**, Calculating Frobenius numbers with Boolean Toeplitz matrix multiplication, 2009. Available at <http://quetzal.bogarthome.net/frobenius.pdf> (accessed Mar. 10, 2017).
8. **A. Brauer**, On a problem of partitions, *Am. J. Math.*, **64**, 299–312, 1942.
9. **A. Brauer** and **J. E. Shockley**, On a problem of Frobenius, *J. Reine Angew. Math.*, **211**, 215–220, 1962.
10. **F. Curtis**, On formulas for the Frobenius number of a numerical semigroup, *Math. Scand.*, **67**, 190–192, 1990.
11. **B. R. Heap** and **M. S. Lynn**, A graph-theoretic algorithm for the solution of a linear Diophantine problem of Frobenius, *Numer. Math.*, **6**, 346–354, 1964.
12. **B. R. Heap** and **M. S. Lynn**, On a linear Diophantine problem of Frobenius: An improved algorithm, *Numer. Math.*, **7**, 226–231, 1965.
13. **D. B. Johnson**, Efficient algorithms for shortest paths in space networks, *J. ACM*, **24**, 1–13, 1977.
14. **M. Nijenhuis**, A minimal-path algorithm for the “Money changing problem,” *Am. Math. Mon.*, **86**, 832–835, 1979.
15. **J. L. Ramírez Alfonsín**, *The Diophantine Frobenius Problem*, Clarendon Press, Oxford, 2005 (Oxf. Lect. Ser. Math. Appl., Vol. 30).
16. **J. J. Sylvester**, Problem 7382, in *Mathematical Questions with Their Solutions: From the “Educational Times,”* Vol. 41, p. 21, Francis Hodgson, London, 1884. Available at <http://archive.org/stream/mathematicalque-05unkngoog#page/n150/mode/2up>. Accessed Mar. 10, 2017.

Vladimir M. Fomichev

Received

8 April 2016

Revised

31 October 2016