2014 Теоретические основы прикладной дискретной математики №1(23)

DOI 10.17223/20710410/23/3

УДК 519.6

ЭКВИВАЛЕНТНЫЕ ПО ФРОБЕНИУСУ ПРИМИТИВНЫЕ МНОЖЕСТВА ЧИСЕЛ

В. М. Фомичев

Финансовый университет при Правительстве Российской Федерации, г. Москва, Россия

E-mail: fomichev@nm.ru

Множества натуральных взаимно простых чисел $\{a_1, \ldots, a_k\}$ и $\{b_1, \ldots, b_l\}$ полагаются эквивалентными, если им соответствует одно и то же число Фробениуса, то есть $g(a_1, \ldots, a_k) = g(b_1, \ldots, b_l)$. Получены результаты, позволяющие для широкого класса множеств аргументов сократить вычисления при решении проблемы Фробениуса как в оригинальной постановке (определение числа Фробениуса $g(a_1, \ldots, a_k)$), так и в расширенной постановке (определение множества всех чисел, не содержащихся в аддитивной полугруппе, порожденной множеством $\{a_1, \ldots, a_k\}$).

Ключевые слова: *число Фробениуса, примитивное множество, порожденная множеством чисел аддитивная полугруппа.*

Введение

Основные обозначения:
$\mathbb{N}_0 = N \cup \{0\}$, где $\mathbb{N}$ — множество всех натуральных чисел;
$(a_1, \ldots, a_k)$ — наибольший общий делитель натуральных чисел $a_1, \ldots, a_k$;
$\langle A \rangle$ — аддитивная полугруппа, порожденная множеством $A \subset \mathbb{N}$;
если $A = \{a_1, \ldots, a_k\}$, $n \in \mathbb{N}_0$, то $nA = \{na_1, \ldots, na_k\}$, $n + A = \{n + a_1, \ldots, n + a_k\}$;
$A^{(i)} = \{a_1, \ldots, a_i\}$, $C(A^{(i)}) = d_i\mathbb{N}_0 \backslash \langle A^{(i)} \rangle$, $d_i = (a_1, \ldots, a_i)$, $i = 2, \ldots, k$;
$z_i = \max C(A^{(i)})$, $\overline{\langle A^{(i)} \rangle} = \{a \in \langle A^{(i)} \rangle : a < z_i\}$, $i = 2, \ldots, k$.

Диофантова проблема Фробениуса (ПФ) (другое название — Money Changing Problem) состоит в определении наибольшего натурального числа $t \notin \langle A \rangle$, то есть числа, не представимого линейной комбинацией (с неотрицательными целыми коэффициентами) взаимно простых чисел $a_1, \ldots, a_k$.

Множество $A = \{a_1, \ldots, a_k\}$ натуральных чисел, $k > 1$, называется примитивным, если $(a_1, \ldots, a_k) = 1$. Следовательно, функция Фробениуса $g(a_1, \ldots, a_k)$ определена на всех примитивных множествах $\{a_1, \ldots, a_k\}$ равенством

$$g(a_1, \ldots, a_k) = \max\{t \in \mathbb{N} : t \notin \langle A \rangle\}.$$

Определим $C(A) = C(A^{(k)})$ — множество всех натуральных чисел, не представимых линейными комбинациями чисел $a_1, \ldots, a_k$, $k > 1$. Тогда число Фробениуса $g(A) = \max C(A)$. Задача определения множества $C(A)$ называется расширенной проблемой Фробениуса (РПФ).

Описание множества $C(A)$ и формула числа Фробениуса даны Сильвестром [1] для $k = 2$ ещё в 1884 г.: $|C(A)| = (g(a_1, a_2) + 1)/2$, где

$$g(a_1, a_2) = a_1a_2 - a_1 - a_2. \tag{1}$$

При $k > 2$ активно изучался порядок множества $C(A)$ и некоторые его свойства [2, гл. 5]. В [3] анонсирован алгоритм РПФ на основе рекуррентного соотношения между множествами $C(A^{(k)})$, $k > 1$, и дана оценка его сложности.

Несмотря на то, что ПФ исследовалась намного активнее, формулы получены только для множеств частного вида при $k = 3, 4$. Объективные трудности в получении общей формулы обоснованы в [2], где показано, что уже при $k = 3$ нельзя разбить область определения на конечное число подобластей так, чтобы в каждой подобласти число Фробениуса $g(a_1, a_2, a_3)$ выражалось как значение полинома от аргументов.

Более продуктивным оказался алгоритмический подход к определению $g(a_1, \ldots, a_k)$. Построен ряд алгоритмов как при $k = 3$ [4], так и при произвольном k. В [5, 6] разработан алгоритм вычисления функции Фробениуса при любом k с помощью экспоненцирования квадратной неотрицательной матрицы M порядка a_k и определения её показателя примитивности (экспонента) с использованием соотношения

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

Вычислительная сложность алгоритма в битовых операциях равна $\mathrm{O}(a_k^3)$, требуемая память — $\mathrm{O}(a_k^2 \log a_k)$ битов. В [7] предложено улучшение этого алгоритма со сложностью $\mathrm{O}(a_k^2)$, однако обоснование корректности алгоритма не представлено.

В [8] на основе теоретико-графового подхода построен алгоритм определения $g(a_1, \ldots, a_k)$ со сложностью $\mathrm{O}(a_1(k + \log a_1))$ арифметических операций. В [9] оценка сложности этого алгоритма снижена до величины порядка $\mathrm{O}(ka_1)$ операций.

Данная работа посвящена сокращению вычислительной сложности РПФ и ПФ с использованием эквивалентности множеств аргументов функции Фробениуса. На основе исследования отношений эквивалентности РПФ и ПФ для исходного множества аргументов A редуцируются на его собственное подмножество порядка h, где $2 \leqslant h \leqslant \min(k, a_1)$. Это позволяет снизить оценку вычислительной сложности до величины $\mathrm{O}(l(A) + ha_1)$ арифметических операций, где $l(A) \leqslant k$ и числа $l(A)$ и h в ряде случаев значительно меньше k.

1. Эквивалентность множества и подмножества

Примитивное множество чисел $A = \{a_1, \ldots, a_k\}$ рассмотрим как возрастающую последовательность длины k, где $1 < a_1 < \ldots < a_k$.

Множества A и A' называются эквивалентными (обозначается $A \cong A'$), если $\langle A \rangle = \langle A' \rangle$. Наименьшие числа эквивалентных множеств равны.

Примитивные множества A и A' называются g-эквивалентными (обозначается $A \overset{g}{\cong} A'$), если $g(A) = g(A')$. Из определения следуют свойства:

1) если $D \cong D'$, то $D \overset{g}{\cong} D'$;

2) $D \cong D' \Leftrightarrow C(D) = C(D')$;

3) $A^{(i)} \cong A^{(i-1)} \Leftrightarrow a_i \in \langle A^{(i-1)} \rangle$, необходимое условие этого $d_i = d_{i-1}$, $i = 2, \ldots, k$.

Пусть $a \in \mathbb{N}$, $B \subseteq \mathbb{N}$. Положим, что a делит B (записывается $a \mid B$), если a делит без остатка некоторое число из B. В противном случае a не делит B (записывается $a \nmid B$).

Теорема 1. Примитивные множества $A^{(i)}$ и $A^{(i-1)}$ являются g-эквивалентными, если и только если $a_i \nmid (g(a_1, \ldots, a_{i-1}) - \overline{\langle A^{(i-1)} \rangle})$.

Доказательство. Свойство $a_i \nmid (g(a_1, \ldots, a_{i-1}) - \overline{\langle A^{(i-1)} \rangle})$ равносильно тому, что

$$g(a_1, \ldots, a_{i-1}) \neq b + ra_i$$

при любом $b \in \langle A^{(i-1)} \rangle$ и любом натуральном r, то есть $g(a_1, \ldots, a_{i-1}) \in C(A^{(i)})$. Вместе с тем, если $a > g(a_1, \ldots, a_{i-1})$, то по определению $a \in \langle A^{(i-1)} \rangle$ и, значит, $a \in \langle A^{(i)} \rangle$.

Следовательно, $g(a_1,\ldots,a_{i-1})$ — наибольшее натуральное число из множества $C(A^{(i)})$. Отсюда $g(a_1,\ldots,a_{i-1}) = g(a_1,\ldots,a_i)$. ■

Следствие 1. Пусть $(a_1,a_2)=1$, тогда $\{a_1,a_2\} \overset{g}{\cong} \{a_1,a_2,a_3\}$, если и только если $a_3 \not| C(A^{(2)})$, где $C(A^{(2)}) = a_1a_2 - a_1 - a_2 - \overline{\langle A^{(2)}\rangle}$.

2. Эквивалентность, связанная с линейными соотношениями

Числа a_i и a_j множества A называются a_1-эквивалентными, если $a_i \bmod a_1 = a_j \bmod a_1$. Примитивное множество $A = \{a_1,\ldots,a_k\}$ разбивается на h классов a_1-эквивалентности, где $2 \leqslant h \leqslant \min\{k, a_1\}$. Трансверсаль множества A по отношению a_1-эквивалентности, состоящую из наименьших чисел классов, назовём a_1-трансверсалью множества A и обозначим A/a_1. Обозначим $W(A/a_1)$ последовательность порядковых номеров (начиная со второго) чисел a_1-трансверсали.

Множество A называется приведённым, если $a_i \notin \langle A^{(i-1)}\rangle$, $i=2,\ldots,k$. Неприведённое примитивное множество A содержит приведённые примитивные подмножества. Приведённое подмножество B_A множества A, называемое A-базисом, строится последовательно: $a_1 \in B_A$; $a_2 \in B_A$, если и только если a_2 не кратно a_1; пусть из $\{a_1,\ldots,a_{i-1}\}$ в подмножество B_A включены числа $b_1,\ldots,b_j$, тогда $a_i \in B_A$, если и только если $d_{i-1} > d_i$ или $d_{i-1} = d_i$ и $a_i \in C(b_1,\ldots,b_j)$, $i=3,\ldots,k$. Обозначим $W(B_A)$ последовательность порядковых номеров (кроме 1) чисел A-базиса, то есть таких $i \in \{2,\ldots,k\}$, что $d_{i-1} > d_i$ или $d_{i-1} = d_i$ и $a_i \in C(a_1,\ldots,a_{i-1})$.

Пример 1. Неприведённое множество $A = \{5,14,19,28,43,49\}$ разбивается на три класса 5-эквивалентности: $C_0 = \{5\}$, $C_3 = \{28,43\}$, $C_4 = \{14,19,49\}$. Здесь $A/5 = \{5,14,28\}$ есть 5-трансверсаль множества A; A-базис есть множество $B_A = \{5,14\}$; $W(B_A) = \{2\}$.

Неприведённое множество $A = \{7,14,23,48,56,62\}$ разбивается на три класса 7-эквивалентности: $C_0 = \{7,14,56\}$, $C_2 = \{23\}$, $C_6 = \{48,62\}$. Здесь $A/7 = B_A = \{7,23,48\}$ есть 7-трансверсаль множества A и A-базис, $W(B_A) = \{3,4\}$.

Индексом примитивности множества A называется наименьшее натуральное число $p(A)$, такое, что $d_{p(A)} = 1$. Пусть $p(A) = p$, тогда $p \leqslant k$, $d_p = d_{p+1} = \ldots = d_k = 1$. Последовательность порядковых номеров $i \in \{2,\ldots,p\}$, таких, что $d_{i-1} > d_i$, обозначим $L(A)$.

Пример 2. Для множества $A = \{5,14,19,28,43,49\}$: $p(A) = 2$, $L(A) = \{2\}$.
Для множества $A' = \{6,18,27,28,42,63,79\}$: $p(A') = 4$, $L(A') = \{3,4\}$.

Теорема 2. Для любого множества A выполнено:
а) $B_A \subseteq A/a_1 \subseteq A$, $B_A \cong A/a_1 \cong A$;
б) $L(A) \subseteq W(B_A) \subseteq W(A/a_1)$;
в) $|B_A| \leqslant |A/a_1| \leqslant \min\{k, a_1\}$, и последняя оценка достижима.

Доказательство.
а) По построению $A/a_1 \subseteq A$ и $B_A \subseteq A$, покажем, что $B_A \subseteq A/a_1$, или, что равносильно, $A\backslash A/a_1 \subseteq A\backslash B_A$. Пусть $a_j \notin A/a_1$, тогда найдётся число $a_i \in A/a_1$, такое, что $a_i < a_j$ и $a_i \bmod a_1 = a_j \bmod a_1$. Тогда $a_j = a_i + ra_1$ при некотором $r \in \mathbb{N}$, следовательно, $a_j \notin B_A$.

Из доказанных включений следует, что $\langle B_A\rangle \subseteq \langle A/a_1\rangle \subseteq \langle A\rangle$. Вместе с тем каждое из чисел множества $A\backslash B_A$ есть линейная комбинация чисел B_A, значит, $\langle A\rangle = \langle A/a_1\rangle = \langle B_A\rangle$.

б) Включение $W(B_A) \subseteq W(A/a_1)$ следует из условия $B_A \subseteq A/a_1$. Если $i \in L(A)$, то $d_{i-1} > d_i$, значит, $i \in W(B_A)$. Следовательно, $L(A) \subseteq W(B_A)$.

в) По построению $|A/a_1| \leqslant k$. Вместе с тем $|A/a_1|$ не превышает числа наименьших неотрицательных вычетов по модулю a_1. Достижимость оценки очевидна. ■

Следствие 2. Всякое примитивное множество $A = \{a_1, \ldots, a_k\}$ содержит эквивалентное подмножество порядка не больше $\min\{k, a_1\}$.

3. Эквивалентность быстро возрастающих последовательностей

Далее положим, что примитивное множество $A = A/a_1$, то есть $k \leqslant a_1$ и числа $a_1, \ldots, a_k$ несравнимы по модулю a_1, где $a_1 \geqslant 3$.

Пусть $L(A) = \{n_2, \ldots, n_r\}$, $1 < r < k$, то есть $d_{n_j-1} > d_{n_j}$, $j = 2, \ldots, r$. Тогда последовательность разбивается на r отрезков $A_1, \ldots, A_r$, где $A_j = (a_{n_j}, \ldots, a_{n_{j+1}-1})$, $j = 1, \ldots, r$, $n_1 = 1$, $n_r = p$, $n_{r+1} = k + 1$.

Обозначим: $J_1 = A_1 \backslash \{a_1\}$; $J(A)$ — множество чисел a_i из A, таких, что $d_{i-1} = d_i$ и a_i не делит множество $C(A^{(i-1)})$ (то есть $J(A) \subseteq \{n_2 + 1, \ldots, k\} \backslash \{n_2, \ldots, n_r\}$); $W(J)$ — возрастающая последовательность номеров чисел множества $J(A)$.

Отметим некоторые известные свойства:

1) если $B \subset A$ и $A \backslash B \subset \langle B \rangle$, то $A \cong B$;
2) множество $A^{(i)}/d_i = \{a_1/d_i, \ldots, a_i/d_i\}$ примитивное, $\langle A^{(i)} \rangle = d_i \langle A^{(i)}/d_i \rangle$, $i = 2, \ldots, k$;
3) $g(a_1, \ldots, a_k) \leqslant (a_1 - 1)(a_k - 1) - 1$ [4, теорема 3.1.1].

Теорема 3. $A \cong A \backslash J(A)$; если $n_2 > 2$, то $A \cong A \backslash (J_1 \cup J(A))$.

Доказательство. Если $d_{i-1} = d_i$ и a_i не делит множество $C(A^{(i-1)})$, то $C(A^{(i)}) = C(A^{(i-1)})$, $i = n_2 + 1, \ldots, k$. Отсюда если $a_i \in J(A)$, то $C(A^{(j)}) = C(B^{(j-1)})$ при любом $j \in \{i, \ldots, k\}$, где $B = A \backslash \{a_i\}$. В частности, при $j = k$ получаем $C(A) = C(A \backslash \{a_i\})$, следовательно, $A \cong A \backslash \{a_i\}$.

Пусть $W(J) = \{i_1, \ldots, i_t\}$. В силу произвольности рассмотренного множества A и числа $a_i \in J(A)$ рассуждения верны для множества A и числа a_{i_1}; для множества $A \backslash \{a_{i_1}\}$ и числа a_{i_2}; ..., для множества $A \backslash \{a_{i_1}, \ldots, a_{i_{t-1}}\}$ и числа a_{i_t}. Значит,

$$A \cong A \backslash \{a_{i_1}\} \cong \ldots \cong A \backslash \{a_{i_1}, \ldots, a_{i_{t-1}}\} \cong A \backslash J(A).$$

Если $n_2 > 2$, то числа $a_2, \ldots, a_{n_2-1}$ кратны a_1. Следовательно, $J_1 \subset \langle a_1 \rangle$ и $J_1 \subset \subset \langle (A \backslash J(A)) \backslash J_1 \rangle$. Тогда по утверждению a теоремы 2

$$A \backslash J(A) \cong (A \backslash J(A)) \backslash J_1 = A \backslash (J_1 \cup J(A)),$$

значит, $A \cong A \backslash (J_1 \cup J(A))$. ■

Далее без ущерба для общности считаем, что n_2=2.

Обозначим: $\gamma_j = d_{n_j}((a_1/d_{n_j} - 1)(a_{n_j}/d_{n_j} - 1) - 1)$, $l_1 = 1$, l_j — наибольший номер, такой, что $n_j \leqslant l_j < n_{j+1}$ и $a_{l_j} \leqslant \gamma_j$ (при $a_1 \geqslant 3$ корректность этих условий вытекает из утверждений *б* и *в* теоремы 2); $S_1 = (a_1)$, $S_j = (a_{n_j}, \ldots, a_{l_j})$, то есть отрезок S_j составлен из первых (наименьших) $l_j - n_j + 1$ чисел отрезка A_j, $j = 2, \ldots, r$; $S(A)$ есть конкатенация отрезков $S_1, S_2, \ldots, S_r$; $l(A)$ — длина последовательности $S(A)$.

Следствие 3. $A \cong S(A)$, $l(A) \leqslant \min\{k, a_1 a_p - a_1 - 2a_p + p\}$, где $p = p(A)$.

Доказательство. При $j = 2, \ldots, r$ выполнена цепь вложений $C(A^{(n_j)}) \supseteq \ldots \supseteq \supseteq C(A^{(n_{j+1}-1)})$. Тогда в соответствии с утверждениями *б* и *в* теоремы 2 каждое число

множеств $C(A^{(n_j)}), \ldots, C(A^{(n_{j+1}-1)})$ не превышает γ_j. Если $l_j < n_{j+1} - 1$, то по определению числа l_j каждое из чисел $a_{l_j+1}, \ldots, a_{n_{j+1}-1}$ больше γ_j и, следовательно, не делит ни одно из чисел множеств $C(A^{(n_j)}), \ldots, C(A^{(n_{j+1}-1)})$. Тогда по теореме 1 $A \cong S(A)$.

По построению $l(A) \leqslant k$, так как $S(A) \subseteq A$. Заметим, что наибольшее число из $S(A)$ не превышает γ_p, где $\gamma_p = a_1a_p - a_1 - a_p$, поэтому $l(A) \leqslant a_1a_p - a_1 - a_p$. Вместе с тем $\{\{1, \ldots, a_p\} \backslash \{a_1, \ldots, a_p\}\} \cap A = \varnothing$; тогда, учитывая, что $\gamma_p > a_p$ при $a_1 \geqslant 3$, получаем $l(A) \leqslant \gamma_p - a_p + p = a_1a_p - a_1 - 2a_p + p$. ■

Алгоритмы построения множеств A/a_1 и $A \backslash S(A)$ являются полиномиальными. Алгоритм построения множества $A \backslash J(A)$ экспоненциальный, по сложности он равносилен решению расширенной проблемы Фробениуса [4].

Наибольшее сокращение вычислительной сложности РПФ и ПФ достигается в тех случаях, когда $\{a_1, \ldots, a_k\} \cong \{a_1, a_2\}$.

Пример 3. Пусть $A = \{5, 13, 18, 20, 57\}$. Вычисляем $A/5$: $5 = 20 = 0 \pmod 5$, $13 = 18 = 3 \pmod 3$, $57 = 2 \pmod 5$. Тогда $A/5 = \{5, 13, 57\}$. Следовательно, $A \cong \cong \{5, 13, 57\}$.

Вычисляем $J(A/5)$: $L(A/5) = \{13\}$, $r = 2$, $A_1 = \{5\}$, $A_2 = \{13, 52\}$, $\gamma_2 = 47 < 57$. Тогда $J(A/5) = \{57\}$, $(A/5) \backslash J(A/5) = \{5, 13\}$. Окончательно имеем $A \cong \{5, 13\}$.

4. Эквивалентность примитивных пар чисел

Обозначим: $[A]$ — класс g-эквивалентности, содержащий примитивное множество A; $[A]_m$ — класс всех примитивных множеств порядка m, g-эквивалентных A, $m = 2, 3, \ldots$

Теорема 4. Пусть $(a, b) = 1$. Тогда

$$[\{a, b\}]_2 = \{(a + \delta, b + \varepsilon) : a - b + 1 < \varepsilon < 0,\ \delta = (1 - a)\varepsilon/(b + \varepsilon - 1) \in \mathbb{N},$$
$$1 - a < \delta < 0,\ \varepsilon = (1 - b)\delta/(a + \delta - 1) \in \mathbb{N}\}.$$

Доказательство. Пусть $(a, b) \overset{g}{\cong} (a + \delta, b + \varepsilon)$, то есть $g(a, b) = g(a + \delta, b + \varepsilon)$, где $g(a, b) = ab - a - b$ в соответствии с (1). Тогда

$$b\delta + a\varepsilon + \delta\varepsilon - \delta - \varepsilon = 0. \tag{2}$$

Так как функция $g(a, b)$ монотонно возрастает при $a, b > 1$, то при заданных a, b уравнение (2) относительно δ, ε выполнено лишь при условии $\delta\varepsilon < 0$. Следовательно, множество $[\{a, b\}]_2$ состоит из примитивных пар вида $(a + \delta, b + \varepsilon)$, где $a + \delta < b + \varepsilon$ и $\delta\varepsilon < 0$. Пусть $\delta > 0$, $\varepsilon < 0$, тогда по условию задачи $a - b + 1 < \varepsilon < 0$ и из (1) следует

$$\delta = (1 - a)\varepsilon/(b + \varepsilon - 1). \tag{3}$$

Тогда $[\{a, b\}]_2$ включает все примитивные пары $(a + \delta, b + \varepsilon)$, где при $\varepsilon > a - b + 1$ число δ, определяемое формулой (3), является натуральным.

Пусть $\delta < 0$, $\varepsilon > 0$, тогда по условию задачи $1 - a < \delta < 0$ и из (2) следует

$$\varepsilon = (1 - b)\delta/(a + \delta - 1). \tag{4}$$

Тогда $[\{a, b\}]_2$ включает все примитивные пары $(a + \delta, b + \varepsilon)$, где при $1 - a < \delta < 0$ является натуральным число ε, определяемое формулой (4). ■

Следствие 4. Если $a > 2$, то $(2, g(a, b) + 2) \in [\{a, b\}]_2$;
если $a > 3$, то $(3, (g(a, b) + 3)/2) \in [\{a, b\}]_2$.

Доказательство. Если $a > 2$, то при $\delta = 2 - a$ в соответствии с (4) получаем $\varepsilon = (1-b)(2-a) \in \mathbb{N}$. Следовательно, $\{a, b\} \overset{g}{\cong} \{2, g(a,b)+2\}$.

Если $a > 3$, то при $\delta = 3 - a$ в соответствии с (4) получаем $\varepsilon = (1-b)(3-a)/2$. Хотя бы одно из чисел примитивной пары (a, b) нечётное. Следовательно, $\varepsilon \in \mathbb{N}$ и $\{a, b\} \overset{g}{\cong} \{3, (g(a,b)+3)/2\}$. ■

Пример 4. Построим множество $[\{13, 22\}]_2$, где $g(13, 22) = 251$. При $\delta > 0$ имеем $-8 < \varepsilon < 0$, соответствующие значения δ приведены в табл. 1.

Таблица 1

Значения δ

ε	-7	-6	-5	-4	-3	-2	-1
δ	6	72/15	60/16	48/17	2	24/19	12/20

Из табл. 1 следует, что $(\delta, \varepsilon) \in \{(2, -3), (6, -7)\}$. Паре $(13, 22)$ g-эквивалентна примитивная приведённая упорядоченная пара $(15, 19)$. Пара $(19, 15)$ не упорядочена, поэтому она исключена из класса $[\{13, 22\}]_2$.

При $\varepsilon > 0$ имеем $-12 < \delta < 0$; соответствующие значения ε приведены в табл. 2.

Таблица 2

Значения ε

δ	-11	-10	-9	-8	-7	-6	-5	-4	-3	-2	-1
ε	231	105	63	42	147/5	21	15	84/8	7	42/10	21/11

Тогда $(\delta, \varepsilon) \in \{(-3, 7), (-5, 15), (-6, 21), (-8, 42), (-9, 63), (-10, 105), (-11, 231)\}$, и пара $(13, 22)$ g-эквивалентна семи примитивным приведённым упорядоченным парам: $(10, 29)$, $(8, 37)$, $(7, 43)$, $(5, 64)$, $(4, 85)$, $(3, 127)$ и $(2, 253)$. Итак, класс g-эквивалентности $[\{13, 22\}]_2$ содержит (вместе с самой парой $(13, 22)$) девять примитивных приведённых упорядоченных пар.

Заключение

Отношения эквивалентности примитивных множеств позволяют сократить сложность решения РПФ и ПФ путём редукции заданного примитивного множества к его собственному подмножеству, выполняемой с помощью полиномиального алгоритма.

Редукция множества A к множествам A/a_1 и $A \backslash S(A)$ позволяет понизить известные оценки сложности вычисления функции Фробениуса. В частности, сложность алгоритма экспоненцирования квадратной неотрицательной матрицы [5, 6] понижается до величины порядка $\mathrm{O}(a^3)$, где a — наибольшее число редуцированного множества $(A/a_1) \backslash S(A/a_1)$. Оценка Боккера — Липтак [9] понижается до величины порядка $\mathrm{O}(l(A) + ha_1)$, где h — порядок множества $(A/a_1) \backslash S(A/a_1)$, то есть в ряде случаев при больших значениях k оценка понижается до величины порядка $\mathrm{O}(a_1)$.

ЛИТЕРАТУРА

1. *Sylvester J. J.* Problem 7382 // Mathematical Questions from the Educational Times. 1884. V. 37. P. 26.
2. *Curtis F.* On formulas for the Frobenius number of a numerical semigroup // Math. Scand. 1990. No. 67. P. 190–192.
3. *Фомичев В. М.* Эквивалентность примитивных множеств // Прикладная дискретная математика. Приложение. 2013. № 6. С. 20–24.

4. *Alfonsin J. R.* The Diophantine Frobenius Problem. Oxford University Press, 2005.
5. *Heap B. R. and Lynn M. S.* A graph-theoretic algorithm for the solution of a linear Diophantine problem of Frobenius // Numerische Math. 1964. No. 6. P. 346–354.
6. *Heap B. R. and Lynn M. S.* On a linear Diophantine problem of Frobenius: an improved algorithm // Numerische Math. 1965. No 7. P. 226–231.
7. *Bogart C.* Calculating Frobenius numbers with Boolean Toeplitz matrix multiplication // For Dr. Cull, CS 523, March 17, 2009. Oregon State University.
8. *Nijenhuis M.* A minimal-path algorithm for the "money changing problem" // Am. Math. Monthly. 1979. V. 86. P. 832–835.
9. *Bocker S. and Liptak Z.* The "money changing problem" revisited: computing the Frobenius number in time $O(ka_1)$. Technical Report No. 2004-2, Univ. of Bielefeld, Technical Faculty, 2004.