Асланян Л.Х.¹, Асланян Г.С.²**Применение алгоритма решения приписывающих диофантовых задач в области банковского дела и криптографии**¹Абовянский государственный колледж²Армянский государственный экономический университет¹(Армения, Абовян)²(Армения, Ереван)

doi: 10.18411/lj-08-2019-59

idsp: ljjournal-08-2019-59

Аннотация

Работа посвящена алгоритму решения приписывающих задач и его применению в области банковского дела, экономике и криптологии. Автор Л. Х. Асланян разработал и построил теоретическую основу приписывающих диофантовых задач и дал алгоритм их решения, которые имеют прикладной характер в разных отраслях народного хозяйства. Авторы предполагают, что алгоритм решения применим в области экономики, банковском деле, криптологии, гос.инспекции, при распределении номерных знаков автомашин, внутренних дел, для выдачи гражданам паспортов, в загсах для выдачи свидетельств о рождении, а также для выдачи документов при регистрации бракосочетания и т.д.

Ключевые слова: элементы теории сравнения, объединения множеств, полные вычеты, теорема Гаусса, теорема П. Эйлера, последовательности.

Abstract

Work is devoted to an algorithm of the solution of the attributing tasks and its application in the field of banking, economy and cryptology. The author L. Kh. Aslanyan developed and built the theoretical basis of the attributing diophantine tasks and gave an algorithm for their solutions, which have an applied character in different branches of the national economy. The authors suggest that the algorithm of a solution is applicable in the field of economy, banking, cryptology, state. inspections, at distribution of license numbers of cars, internal affairs, for issuing passports to citizens, in registry offices for issuing birth certificates, as well as for issuing documents during marriage registration & etc.

Keywords: elements of the theory of comparison, union of sets, full deductions, Gauss's theorem, P. Euler's theorem, sequences.

Приписывающие задачи встречаются в школьном курсе математики, на олимпиадах, в разных сборниках задач и в теории чисел. В этих задачах всегда известны некоторые параметры, которые позволяют решать поставленную задачу. КПН, доцент Л. Х. Асланян построил новые теоретические основы для общих и частных приписывающих диофантовых задач. Результаты исследования опубликованы в разных научно-методических журналах Армении и в тезисах международных научных конференций. В рецензии, заведующий кафедрой “Высшей алгебры и геометрии” гос.университета, доктор ФМН, профессор Ю. М. Мовсисян отметил: “Первый раз в истории математики оформлены классы частных и общих приписывающих диофантовых задач”. Старший научный сотрудник отдела теории чисел Института математики НАН Беларуси, КФН Э. И. Ковалевская в своем отзыве на работу Л. Х. Асланяна “Обобщение функции $\varphi(m)$ Л. Эйлера и ее применение при построении теоретической основы общих и частных приписывающих диофантовых задач” отметила, что она будет полезна для учеников старших классов, а также научных работников в области криптографии. В 2006 году опубликована книга автора под названием “Алгоритмы решения приписывающих диофантовых задач” (Асланян Л. Х. Ереван, Зангак 87, 2006г). В ходе исследования были определены общие и

частные приписывающие диофантовые задачи. Автор выдвинул следующие проблемы: 1). Обосновать и определить содержание и теоретическую основу правосторонних, левосторонних и двусторонних приписывающих диофантовых задач. 2). Исследовать всевозможные варианты и дать алгоритмическое решение поставленных задач, которые на наш взгляд найдут свое применение в курсе “Теории чисел”, в разных отраслях народного хозяйства и техники.

К первой части относятся те приписывающие задачи, которые входят в область так называемых **кратных задач**, где функциональная связь неизвестных характеризуется следующими неопределенными уравнениями:

$$\begin{aligned} \text{а) } \overline{xy} &= k \cdot x, \\ \text{б) } \overline{yx} &= k \cdot x, \text{ г) } \overline{yxz} = k \cdot x, k \in N. \end{aligned}$$

Ко второй части относятся те приписывающие задачи, где условия и требования связаны следующими неопределенными уравнениями:

$$\begin{aligned} \text{в) } \overline{xy} &= \frac{u}{v} \cdot x, \\ \text{г) } \overline{yx} &= \frac{u}{v} \cdot x, \\ \text{д) } \overline{yxz} &= \frac{u}{v} \cdot x, \end{aligned}$$

где $u \in N, v \in N$ и $v \neq 1, (u, v) = 1$ (взаимно простые числа).

В ходе исследования задачи было доказано “Обобщение функции $\varphi(m)$ Л. Эйлера” на любом натуральном отрезке $[a, b]$, которое позволяет решить сложные диофантовые уравнения типа в), г), д).

Теперь коротко о правосторонних приписывающих задачах и ее применении в банковском деле и криптографии.

Предположим, что A_n и A_p конечные подмножества натуральных чисел, т.е.

$$A_n = \{x \in N / 10^{n-1} \leq x \leq 10^n - 1\} \text{ и } A_p = \{y \in N / 10^{p-1} \leq y \leq 10^p - 1\},$$

где x – (n)-значное, а y – (p)-значное числа.

Постановка задачи. Допустим, произвольному элементу (x) из множества A_n с правой стороны приписывается элемент (y) из множества A_p . Полученный элемент $\overline{xy}$

из множества A_{n+p} в $\left(\frac{u}{v}\right)$ раз больше элемента (x). Требуется найти все четверки натуральных чисел вида (x, y, u, v) , удовлетворяющие условию задачи и дать алгоритм решения, где $(u, v) = 1$.

Решение. По условию поставленной задачи, можем написать: $\overline{xy} = \frac{u}{v} \cdot x$, где $v \neq 1$

Если $v=1$, то получим уравнение вида $\overline{xy} = k \cdot x$, так называемая задача (k) кратности.

Имеем: $10^p \cdot x + y = \frac{u}{v} \cdot x$. Чтобы $(x, y, u, v) \in N$, необходимо и достаточно, чтобы $x = v \cdot t$, где $1 \leq t < x$. Если $t=x$, тогда $v=1$, в результате получим $\overline{xy} = ut$, которая была названа задачей (u) кратности. Вместо (x) подставим $x=vt$, получим $10^p \cdot vt + y = u \cdot t$. При изменении параметра (t) получим совокупность системы уравнений, в общем количестве $(i=x-1)$, которые представлены в следующем виде: 1) $\{10^p \cdot v + y = u, t=1\}$, 2) $\{10^p \cdot 2v + y = 2u, t=2,$

$x=2v\}$, ..., i) $\{10^p \cdot vt + y = u, t, x=vt\}$. Исходя из того, что $y \in A_p$ можем записать: $\{y=u \cdot t - 10^p \cdot vt\}$ и одновременно существует: $10^{p-1} \leq ut - 10^p vt \leq 10^p - 1$, $x=vt$. После преобразования получаем: $(10^{p-1}/t + 10^p v \leq u \leq (10^p - 1)/t + 10^p v$. Для удобства, целые части границы изменения числовой функции (u) обозначим через (a) и (b), $a \leq u \leq b$, где $[(10^{p-1}/t + 10^p v)=a, [(10^p - 1)/t + 10^p v]=b$. Наша цель состоит в том, чтобы из последовательности натуральных чисел (a, a+1, a+2, ..., b-2, b-1, b) выбрать те и только те числа, которые должны быть взаимно простыми с фиксированным числом (v). Чтобы работа была доступной читателям, рассмотрим частные задачи. Предположим, что $v=3$,

где $(u, 3) = 1$, $x \in A_1 = \{1, 2, \dots, 9\}$, $y \in A_2 = \{10, 11, \dots, 99\}$, тогда имеем: $\overline{xy} = \frac{u}{3} \cdot x$. Чтобы уравнение имело натуральные решения, необходимо и достаточно, чтобы $x=3t$. После преобразования, получим диофантовые уравнения вида: $10^2 \cdot x + y = ut$ или $y = ut - 10^2 \cdot 3t$. Найдем область изменения параметра (t). Считая, что $x \in A_1, y \in A_2$, то $1 \leq x \leq 9, 10 \leq y \leq 99$, или $(1 \leq 3t \leq 9), (10 \leq ut - 10^2 \cdot 3t \leq 99)$, где $1 \leq t \leq 3$. Последовательно подставим значения (t). Получим три системы уравнений

1. $\{10 \leq u - 300 \leq 99, t = 1, x = 3t = 3, y = ut - 300t = u - 300\}$
2. $\{10 \leq y = 2u - 600 \leq 99, t = 2, x = 6\}$
3. $\{10 \leq y = 3u - 900 \leq 99, t = 3, x = 9\}$

Найдем пределы изменения параметра (u):

1. $\{310 \leq u \leq 399, t = 1, x = 3\}$,
2. $\{305 \leq u \leq 349, t = 2, x = 6\}$,
3. $\{304 \leq u \leq 332, t = 3, x = 9\}$.

Исходя из того, что $(u, v) = (u, 3) = 1$, то необходимо все числа каждого отрезка разделить на три, чтобы найти те числа, которые взаимно просты с (3). Тогда получим множество чисел с остатками: $r=0, r=1, r=2$. Из остатков один и два взаимно простыми с числом $v=3$. После объединения чисел с равными остатками, получаем множества с полными вычетами, которые имеют вид $\{3q\}$, $\{3q+1\}$, $\{3q+2\}$. Элементы множеств $\{3q+1\}$ и $\{3q+2\}$ взаимно просты с модулем (3), т.е. $(3q+1, 3)=1, (3q+2, 3)=1$. Такие множества в теории чисел имеют особое название: **приведенные вычеты по модулю три**. Для исследования берем первый интервал, т.е. $[310, 399]$. Из данного отрезка найдем те числа, которые имеют представления: $(3q+1)$ и $(3q+2)$. Найдем элементы данных множеств. $\{3q+1\} = \{310, 313, 316, 319, \dots, 397\}$, их количество вычисляется по известной формуле $a_n = a_1 + (n-1)d$. И имеем: $n = (a_n - a_1)/d + 1 = (397 - 310)/3 + 1 = 30$. $\{3q+2\} = \{311, 314, \dots, 398\}$, $n = (398 - 311)/3 + 1 = 30$.

В отрезке $[310, 399]$ существует 60 чисел, которые взаимно просты с числом три. Т.е. $\{u\} = \{3q+1\} \cup \{3q+2\} = \{310, 313, 316, 319, \dots, 397\} \cup \{311, 314, 317, 320, \dots, 398\}$. Найдем значения (y). Если $t=1$, то $\{y\} = \{u-300\} = \{10, 13, 16, 19, \dots, 97\} \cup \{11, 14, 17, 20, \dots, 98\}$. $x=3, v=3$. Таким образом, если $v=3, t=1, x=3$, то существуют 60 чисел: $\{xy\} = \{310, 313, 316, \dots, 397\} \cup \{311, 314, 317, \dots, 398\}$. Таким же методом найдутся решения данной задачи для остальных интервалов, когда $(t=2, x=6, v=3)$ и $(t=3, x=9, v=3)$. Возникает вопрос. Алгоритм и ее решения данной задачи носит чисто математический характер, и какое применение он может иметь в банковском деле и криптографии? Чтобы ответить на этот вопрос, сформулируем следующую задачу. Пусть центральный банк имеет нескольких отделений. И для клиентов предоставляются банковский счет и (PIN) код, так, что: (1) Никто из клиентов не должен знать о

банковских счетах и (PIN) кодах других. Как это можно решить, чтобы кроме клиента и банка никто не знал о тайности счета и (PIN) кода. Сформулируем следующую задачу. Пусть (PIN) код состоит из (m) цифр, т.е. m-значное число, а банковский счет состоит из (n+p) цифр. Сколькими вариантами можно сделать так, чтобы они отличались друг от друга, т.е. были разными. Через буквы (s) обозначим номер банковского счета, то есть она является представителем банковского счета любого клиента. Для примера, пусть банковский счет состоит из пяти цифр, т.е. оно является пяти значным числом, где первые две цифры принадлежат множеству двузначных чисел, т.е. $\{x\}=\{10,11,12,\dots,98,99\}$, а три последние числа принадлежат множеству трехзначных чисел, то есть $\{y\}=\{100,101,102,\dots,999\}$. Тогда банковский счет (s) является представителем пятизначных чисел, то есть $\{s\}=\{10100,10101,10102,\dots,99999\}$. Тогда $s=\overline{xy}=10^p \cdot x + y$. Предположим, что для любого клиента существует счет со следующим

уловием: $S = \frac{u}{24} \cdot x$, или $s = \overline{xy} = \frac{u}{24} \cdot x$.

Сформулированная задача приводится к так называемым приписывающим

задачам, т.е. $\overline{xy} = \frac{u}{v} \cdot x$, где $x \in A_n, y \in A_p$ и $(u, 24)=1$. В нашем примере $n=2, p=3, v=24$. По

условию задачи имеем: $s = \overline{xy} = \frac{u}{24} \cdot x$. Чтобы задача имела натуральные решения, необходимо и достаточно, чтобы $x=24t, t < x \in N$. Как уже предполагали, (x) – двузначное число, а (y) – трехзначное число, тогда существуют неравенства: $10 \leq x \leq 99$ и $100 \leq y \leq 999$. Найдем интервал изменения параметра (t), вместо (x) подставим $x=24t$, получим: $10 \leq 24t \leq 99$, или $1 \leq t \leq 4$. Таким же методом найдем интервал изменения параметра (u) из следующих неравенств: $100 \leq ut - 10^3 24t \leq 999$, где $\{t\}=\{1,2,3,4\}$. С изменением параметра (t) последовательно рассмотрим каждый вариант.

1. Если $t = 1$, то $\{100 \leq u - 10^3 24 \leq 999, t = 1, x = 24\}$ или $\{24100 \leq u \leq 24999, t = 1, x = 24\}$

2. Если $t = 2$, то $\{100 \leq 2u - 10^3 48 \leq 999, t = 2, x = 48\}$ или $\{24050 \leq u \leq 24499, t = 2, x = 48\}$

3. Если $t = 3$, то $\{100 \leq 3u - 10^3 72 \leq 999, t = 3, x = 72\}$ или $\{24034 \leq u \leq 24333, t = 3, x = 72\}$

4. Если $t = 4$, то $\{100 \leq 4u - 10^3 96 \leq 999, t = 4, x = 96\}$ или $\{24025 \leq u \leq 24249, t = 4, x = 96\}$

Найдем те числа, которые взаимно просты с числом $v=24$.

Такие числа представляются в следующем виде: $\{24r+1\}, \{24r+5\}, \{24r+7\}, \{24r+11\}, \{24r+13\}, \{24r+17\}, \{24r+19\}, \{24r+23\}$. Или коротко $\{24r+\alpha, 24\}=1$ (взаимно простые по модулю 24, где $\alpha \in \{1,5,7,9,11,13,17,19,23\}$ и их количество по определению

функции $\varphi(m)$ Л. Эйлера равно: $\varphi(m) = \varphi(24) = 24(1 - \frac{1}{2})(1 - \frac{1}{3}) = 8$. Нахождение этих чисел, естественно трудная работа. Но по разработке функции $\varphi(m)$ Л. Эйлера (автор Л. Асланян) очень облегчается исследование и нахождение этих чисел, потому что

$$\varphi^*(m) = \varphi^*(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_i^{\alpha_i}) = \varphi^*(p_1 \cdot p_2 \dots p_i).$$

Тогда можем констатировать, что

$$\varphi^*(m) = \varphi^*(24) = \varphi^*(2^3 \cdot 3) = \varphi^*(2 \cdot 3) = \varphi^*(6) = ([\frac{b}{6}] - [\frac{a-1}{6}])\varphi(6) + k_2 - k_1$$

где (а) начало и (b) конец данного отрезка. Функции $\varphi^*(m)$ являются обобщением функции $\varphi(m)$ Л. Эйлера и показывают количество взаимно простых чисел по модулю (m) в любом натуральном отрезке [a,b]. Число (k_2) показывает количество приведенных вычетов, не превосходящее остаток, которое получается при делении числа (b) на (m=6), а (k_1) , соответственно, количество приведенных вычетов, которое не превосходит остаток при делении числа (a-1) на (m) (см. книгу Л. Х. Асланяна "Алгоритмы решения приписывающих диофантовых задач", Ереван-2006, Зангак-97, ст. 39-42). Таким образом, вместо восьми приведенных вычетов мы рассматриваем два вычета: $r=1$ и $r=5$. Тогда необходимо найти те числа, которые представляются в виде $\{6q+1\}$ и $\{6q+5\}$. Элементы этих множеств взаимно простые по модулю 24. Теперь перейдем к решению данной задачи. Если $t=1$, то $x=24$ и $24100 \leq u \leq 24999$, в неравенстве вместо (u) подставим соответственно $(6q+1)$ и $(6q+5)$, объединение этих множеств дает $\{u\} = \{6q+1\} \cup \{6q+5\}$, где $24100 \leq 6q+1 \leq 24999, 24100 \leq 6q+5 \leq 24999$
 $\{6q+1\} = \{24103, 24109, 24115, 24121, \dots, 24997\}$,
 $\{6q+5\} = \{24101, 24107, 24113, 24119, \dots, 24995\}$.
 $\{u\} = \{6q+1\} \cup \{6q+5\} = \{24103, 24109, 24115, 24121, \dots, 24997\} \cup \{24101, 24107, 24113, 24119, \dots, 24995\}$.

Найдем количество чисел в этих множествах: $n = (24997-24103):6+1=150$, $n = (24995-24101):6+1=150$. На отрезке $[24100, 24999]$ есть 300 чисел, которые взаимно простые по модулю (6) или по модулю (24). Чтобы работа была доступной и читатель знал о мощности обобщающей функции, найдем на данном отрезке те числа, которые взаимно просты с числом (24). Как уже сказано, все остатки $\{1, 5, 7, 11, 13, 17, 19, 23\}$ взаимно просты с числом 24. Классическим методом необходимо найти все элементы из следующих приведенных вычетов: $\{24q+1\}$, $\{24q+5\}$, $\{24q+7\}$, $\{24q+11\}$, $\{24q+13\}$, $\{24q+17\}$, $\{24q+19\}$ и $\{24q+23\}$. Имеем:

1. $\{24q+1\} = \{24121, 24145, \dots, 24985\}$, $n = (24985-24121):24+1=37$.
2. $\{24q+5\} = \{24101, 24125, \dots, 24989\}$, $n = (24989-24101):24+1=38$
3. $\{24q+7\} = \{24103, 24127, \dots, 24991\}$, $n = (24991-24103):24+1=38$
4. $\{24q+11\} = \{24107, 24131, \dots, 24995\}$, $n = (24995-24107):24+1=38$
5. $\{24q+13\} = \{24109, 24133, \dots, 24997\}$, $n = (24997-24109):24+1=38$
6. $\{24q+17\} = \{24113, 24137, \dots, 24977\}$, $n = (24977-24113):24+1=37$
7. $\{24q+19\} = \{24115, 24139, \dots, 24979\}$, $n = (24979-24115):24+1=37$
8. $\{24q+23\} = \{24119, 24143, \dots, 24983\}$, $n = (24983-24119):24+1=37$.

Всего $4 \cdot 37 + 4 \cdot 38 = 300$ чисел, которые взаимно просты с числом (24) или с (6). Как видно, здесь работы очень много. Если применить обобщение функции $\varphi(m)$ Л. Эйлера и ее свойства, то работа в (4) раза сокращается. То есть вместо восьми приведенных вычетов, мы берем два: $\{6q+\}$ и $\{6q+5\}$. На отрезке $[24100, 24999]$ применяем обобщающую функцию для функции $\varphi(m)$ Л. Эйлера (разработанная автором, см. книгу Л. Х. Асланяна "Алгоритмы решения приписывающих диофантовых задач", Ереван-2006, Зангак-97, стр. 39-42)).

$$\varphi^*(m) = \varphi^*(24) = \varphi^*(2^3 \cdot 3) = \varphi^*(2 \cdot 3) = \varphi^*(6) = \left(\left[\frac{b}{6}\right] - \left[\frac{a-1}{6}\right]\right) \varphi(6) + k_2 - k_1$$

$$= ([24999:6] - [24099:6]) \cdot \varphi(6) + k_2 - k_1 = (4166 - 4016) \cdot 2 + 3 - 3 = 150 \cdot 2 = 300.$$

Значит самый короткий путь является применение свойства функции $\varphi^*(m)$ на любом натуральном отрезке [a,b]. Если $t=1$, то $x=24$, $s = \frac{u}{xy} = \frac{u}{24} \cdot x$. Или $\{u\} = \{6q+1\} \cup \{6q+5\} = \{24103, 24109, 24115, 24121, \dots, 24997\} \cup \{24101, 24107, 24113, 24119, \dots, 24995\}$.

В каждом числе первые два места занимают двузначные числа из множества A_2 , а на втором месте – трехзначные числа из множества A_3 . Таким же метом найдутся остальные пятизначные числа, которые могут служить банковским счетом для клиентов. Если множество приведенных вычетов не хватает, то можно использовать те числа, которые кратны числам (6) и с числом (6) имеет общий делитель отличный от единицы, т.е. $(u,6)=d \neq 1$. Количество таких чисел определяется по следующей формуле

(разработанное автором): $\overline{\varphi(m)}^* = (\lfloor \frac{b}{m} \rfloor - \lfloor \frac{a-1}{m} \rfloor)(m - \varphi(m)) + t_2 - t_1$, или вместо (m) поставим

$\overline{\varphi(6)}^* = (\lfloor \frac{24999}{6} \rfloor - \lfloor \frac{24100-1}{6} \rfloor)(6 - \varphi(6)) + t_2 - t_1 = (4166-4016)(6-2) + 3-3=600$.
 $m=6$, получим

Чтобы читатель был уверен, что действительно их число равно (600), необходимо найти все элементы из следующих множеств: $\{6q\}$, $\{6q+2\}$, $\{6q+3\}$, $\{6q+4\}$. Из условия $(24100 \leq 6q \leq 24999)$ найдем те числа, которые кратны 6-и, т.е. $\{6q\} = \{24102, 24108, 24114, \dots, 24996\}$, $n=(24996-24102):6+1=150$. По той же аналогии найдем элементы множеств $\{6q+2\}$, $\{6q+3\}$, $\{6q+4\}$. Имеем:

$\{6q+2\} = \{24104, 24110, \dots, 24998\}$, $n=(24998-24104):6+1=150$. $\{6q+3\} = \{24105, 24111, \dots, 24999\}$, $n=(24999-24105):6+1=150$. $\{6q+4\} = \{24106, \dots, 24994\}$, $n=(24994-24100):6+1=150$. Получили, что действительно их число равно 600. Если $t=1$, $x=24, v=24$, то из множества пятизначных чисел можно составить $300+600=900$ банковских счетов, которые отличаются друг от друга и цифры не повторяются. Первые две цифры всегда являются (24), если $t=1$, а второе место занимают трехзначные числа. Продолжаем работу. Если $t=2$, то $x=24t=48$. Найдем те значения параметра (u), которые будут взаимно простыми с числом (24) или (6). Из условия (2) имеем: Если $t=2$, то $\{100 \leq 2u \cdot 10^3 \cdot 48 \leq 999 \mid x=48, t=2\}$, получим: $\{24050 \leq u \leq 24499, t=2, x=48\}$, где $\{6q+1\} = \{24055, 24061, \dots, 24499\}$, $n=(24499-24055):6+1=75$. $\{6q+5\} = \{24053, 24059, \dots, 24498\}$, $n=(24498-24053):6+1=75$. Значит их объединение есть $\{u\} = \{24055, 24061, \dots, 24499\} \cup \{24053, 24059, \dots, 24497\}$. Найдем множество чисел (y): $y=2u-48000$. Например, если $u=6q+1=24055$, то $y=2 \cdot 24055 - 48000 = 48110 - 48000 = 110$. Если $u=6q+5=24053$, то $y=2 \cdot 24053 - 48000 = 106$. Тогда $\{y\} = \{2u-48000\} = \{110, 122, \dots, 998\} \cup \{106, 118, 130, \dots, 994\}$. Составим банковский счет для клиентов: $\{s\} = \{xy\} = \{48110, 48122, 48134, \dots, 48998\} \cup \{48106, 48118, 48130, \dots, 48994\}$, всего $75+75=150$. Если

мы хотим увеличить количество клиентов, тогда необходимо найти все кратные (6) числа и те числа, которое с (6) имеют общий делитель ($d \neq 1$). Из интервала $\{24050 \leq u \leq 24499, t=2, x=48\}$ следует: $24050 \leq 6q \leq 24499$. Найдем элементы $\{6q\} = \{24054, 24060, 24066, \dots, 24498\}$, всего: $n=(24498-24054):6+1=75$. Найдем значения (y) по формуле $y=2u-48000=2 \cdot 24072 - 48000 = 108$. Составим банковский счет для клиентов: $\{s\} = \{xy\} = \{48108, 48114, 48120, \dots, 48996\} \cdot \{6q+2\} = \{24050, 24056, \dots, 24494\}$, $n=(24494-24050):6+1=75$. $\{6q+3\} = \{24051, 24057, \dots, 24495\}$, $n=(24495-24051):6+1=75$. $\{6q+4\} = \{24052, 24058, \dots, 24496\}$, $n=(24496-24052):6+1=75$. $\{6q+4\} = \{24052, 24058, \dots, 24496\}$, $n=(24496-24052):6+1=75$. Найдем $\{y\}$, $y=\{2 \cdot 6q - 48000\} \cup \{2(6q+2) - 48000\} \cup \{2(6q+3) - 48000\} \cup \{2(6q+4) - 48000\} = \{108, 114, \dots, 996\} \cup \{100, 106, \dots, 998\} \cup \{102, 106, \dots, 990\} \cup \{104, 108, \dots, 992\}$. Составим банковский счет, то есть $\{s=xy\} = \{48108, 48114, \dots, 48996\} \cup \{48100, 48106, \dots, 48998\} \cup \{48102, 48106, \dots, 48990\} \cup \{48104, 48108, \dots, 48992\}$, всего 300. Если $t=3$, то $\{100 \leq 3u \cdot 10^3 \cdot 72 \leq 999, x=72, t=3\}$, или $\{24034 \leq u \leq 24333, t=3, x=72\}$. Найдем элементы множеств $\{6q+1\}$, $\{6q+5\}$ и $\{6q\}$ из данного интервала. Имеем: $\{6q+1\} = \{24037, 24043, 24049, \dots, 24331\}$, $n=(24331-24037):6+1=50$. $\{6q+5\} = \{24035, 24041, 24047, 24053, \dots, 24329\}$, $n=(24329-24035):6+1=50$. $\{6q\} =$

$\{24036, 24042, \dots, 24048, 24054, \dots, 24330\}, n = (24330 - 24036) : 6 + 1 = 50$. $\{6q+2\} = \{24038, 24044, \dots, 24332\}, n = (24332 - 24038) : 6 + 1 = 50$
 $\{6q+3\} = \{24039, 24045, \dots, 24333\}, n = (24333 - 24039) : 6 + 1 = 50$.
 $\{6q+4\} = \{24034, 24040, \dots, 24328\}, n = (24328 - 24034) : 6 + 1 = 50$.

Всего $150 + 200 = 350$. $\{y\} = \{3(6q+1) - 72000\} \cup \{3(6q+5) - 72000\} \cup \{3(6q) - 72000\} \cup$
 $\{3(6q+2) - 72000\} \cup \{3(6q+3) - 72000\} \cup \{3(6q+4) - 72000\} =$
 $\{111, 129, \dots, 993\} \cup \{105, 123, \dots, 987\} \cup \{108, 126, \dots, 990\} \cup \{114, 132, \dots, 996\} \cup \{117, 135, \dots, 999\} \cup$
 $\{102, 120, \dots, 984\}$. Составим банковский счет. $\{s = \overline{xy}\} = \{72111, 72129, \dots, 72993\} \cup$
 $\{72105, 72123, \dots, 72987\} \cup \{72108, 72126, \dots, 72990\} \cup \{72114, 72132, \dots, 72996\} \cup$
 $\{72117, 72135, \dots, 72999\} \cup \{72102, 72120, \dots, 72984\}$. Рассмотрим последний вариант.

4. Если $t=4$, то $\{100 \leq 4u - 10^3 \cdot 96 \leq 999, t=4, x=96\}$ или $\{24025 \leq u \leq 24249, t=4, x=96\}$. Вместо (u) последовательно подставим $(6q+1)$, $(6q+5)$, $(6q)$, $(6q+2)$, $(6q+3)$ и $(6q+4)$ в неравенство и найдем все числа, которые взаимно просты с числом (24), или с 6, на данном отрезке. Получим: $\{6q+1\} = \{24025, 24031, \dots, 24247\}, n = (24247 - 24025) : 6 + 1 = 38$. $\{6q+5\} = \{24029, 24035, \dots, 24245\}, n = (24245 - 24029) : 6 + 1 = 37$. $\{6q\} = \{224030, 24036, 24042, 24048, \dots, 42246\}, n = (42246 - 24036) : 6 + 1 = 36$. Всего $38 + 37 + 36 = 111$. $\{6q+2\} = \{24026, 24032, \dots, 24248\}, n = (24248 - 24026) : 6 + 1 = 38$. $\{6q+3\} = \{24027, 24033, \dots, 24249\}, n = (24249 - 24027) : 6 + 1 = 38$. $\{6q+4\} = \{24028, 24034, \dots, 24244\}, n = (24244 - 24028) : 6 + 1 = 37$. Всего $38 + 37 + 36 + 38 + 38 + 37 = 224$. Найдем множество $\{y\}$ по формуле: $y = 4 \cdot u - 96000 = 4 \cdot 24025 - 96000 = 96100 - 96000 = 100$. $\{x = 24t\} = \{24, 48, 72, 96\}$, $\{u\} = \{6q+1\} \cup \{6q+5\} \cup \{6q\} \cup \{6q+2\} \cup \{6q+3\} \cup \{6q+4\}$.

Банковский счет будет составлен следующего образом: сначала найдем соответствующие числа из множества $\{y\}$ по формуле $y = ut - 10^3 \cdot 24t$, где $\{t\} = \{1, 2, 3, 4\}$, потом справа от значения элемента (x) приписываем соответствующее значение (y) и

получаем счет $s = \overline{xy} = \frac{u}{v} \cdot x$. Например, если $u = 6q+1, t=4, x=96$ то множество чисел (y)-а вычисляется в аналитической форме, т.е. $\{y = 4 \cdot u - 96000\} = \{100, 124, \dots, 988\}, 6$. Если $u = 6q+5$, то $\{y = 4 \cdot u - 96000\} = \{116, 140, 164, \dots, 980\}$. Если $u = 6q$, то $\{y\} = \{4 \cdot u - 96000\} = \{144, 168, \dots, 984\}$ и т.д. После этого составляем банковский счет, который состоит из пятизначных чисел. Согласно постановке задачи,

если $u = 6q+1, x=24$, то $\{s = \overline{xy} = \frac{u}{24} \cdot x\} \subset \{24103, 24109, \dots, 24997\}$.

Если $u = 6q+5, x=24$, то $\{s = \overline{xy} = \frac{u}{24} \cdot x\} \subset \{24101, 24107, \dots, 24995\}$.

Если $u = 6q, x=24$, то $\{s = \overline{xy} = \frac{u}{24} \cdot x\}$ или $\subset \{24102, 24108, \dots, 24996\}$ и так далее.

Мы рассмотрели такие примеры, которые доступны читателям, в основном такими исследователями, которые занимаются банковскими счетами и вопросами криптографии. Мы считаем, что можно составить банковский счет из восьмизначных или двенадцатизначных чисел, а PIN код из четырехзначных чисел, чтобы оно было

полностью защищено. То есть $s = \overline{xy} = \frac{u}{24} \cdot x$, где $x \in A_5, y \in A_7$. Это относится к двенадцатизначным банковским счетам, а для восьмизначных банковских счетов:

$x \in A_3, y \in A_5$, где $s = \overline{xy} = \frac{u}{24} \cdot x$. Для PIN кода взять числа, которые состоят из четырех цифр, то есть составить всевозможные комбинации из десяти цифр по четыре, или

$A_{10}^4 = 10 \cdot 9 \cdot 8 \cdot 7 = 5040$, без повторения цифр (0,1,2,...,8,9). Если PIN кода не хватает для крупных стран (как например Китай, Индия, и т.д), тогда можно применять формулы комбинаторики с повторением, то есть кортежи длиной k , составленные из элементов m -множества, называют размещениями с повторениями из элементов по k , а их число обозначают $\overline{A_m^k} = m^k$, где в нашем примере $m=10$, $k=4$ и $A_0 = \{0,1,2,...,8,9\}$. Если хватает количество PIN кодов, тогда можно применять формулы размещения без повторений, то есть размещение из двести элементов по четыре: $A_{10}^4 = 10 \cdot 9 \cdot 8 \cdot 7 = 5040$. Если количество не хватает, необходимо взять более многозначные множества чисел.

Например $A_5 = \{x \in N(10^4 \leq x \leq 10^5 - 1)\} = \{x \in N(10000 \leq x \leq 99999)\}$. Их количество равно: $99999 - 10000 + 1 = 90000$, а для $A_7 = \{y \in N(1000000 \leq y \leq 9999999)\}$ $n=9000000$. На наш взгляд, если мы хотим строгую тайность, предлагаем, для клиента составить банковский счет в аналитической форме, т.е. $s = \overline{xy} = \frac{u}{24} \cdot x$, где $y = ut - 10^7 \cdot 24t$, $u = 6q + 1$ или $u = 6q + 5$, $417 \leq t \leq 4166$. Если $t = 450$, то $x = 24 \cdot 450 = 10800$, $y = 450(6q + 1 - 24 \cdot 10^7)$

, $q = 40.000.371$. Тогда $y = 450 \cdot 2227 = 1.002.150$, $s = \overline{xy} = \frac{u}{24} \cdot x = 108001002150$ (двенадцатизначное число), их количество равно 19993, которые имеют $(6q + 1)$ вид. По таким методики состояются для вычетов $(6q + 5), (6q), (6q + 2), (6q + 3)$ и $(6q + 4)$. Таким же образом можно констатировать: если один из параметров сохранить тайно, то ни какой хакер не сможет узнать банковский счет клиента. На наш взгляд поставленная задача имеет огромное применение и она защищена от хакеров. Одновременно мы предлагаем второй подход: Чтобы в мире была единая банковская счет, необходимо: Любого гражданина мира выделить банковский счет так, как оно изложено выше указанном алгоритме, а PIN код ставляются имя государства данного лица.

1. Л. Х. Асланяна "Алгоритмы решения приписывающих диофантовых задач", Ереван-2006, Зангак-97, стр. 39-42. Источник №2
2. И. М. Виноградов, Основы теории чисел. Издательство «Наука» Москва 1965.
3. Хрестоматия по истории математики, под редакцией А. П. Юшкевича. Москва «Просвещение», 1976.

Вихорева А.С., Деменкова В.В., Смирнова Л.И.
О направлениях повышения финансовых результатов продаж
сельскохозяйственной продукции

ФГБОУ ВО «Кубанский государственный аграрный университет имени И. Т. Трубилина
(Россия, Краснодар)

doi: 10.18411/lj-08-2019-60
idsp: ljjournal-08-2019-60

Аннотация

В статье рассматриваются направления повышения результативности деятельности путем расширения временных границ продаж сельскохозяйственной продукции за счет сорта, более полного использования возможностей рынка путем изменения ценовой политики.

Ключевые слова: финансовый результат, продажи, сельскохозяйственная продукция, цена, анализ разрывов.