

УСЛОВИЯ NP-ПОЛНОТЫ ПРОВЕРКИ СОВМЕСТИСТИ НЕСКОЛЬКИХ ВИДОВ СИСТЕМ ЛИНЕЙНЫХ ДИОФАНТОВЫХ СРАВНЕНИЙ И УРАВНЕНИЙ

Н. К. Косовский, Т. М. Косовская, Н. Н. Косовский

Санкт-Петербургский государственный университет,
Российская Федерация, 199034, Санкт-Петербург, Университетская наб., 7-9

В статье предлагаются три серии теоретико-числовых задач с явно выделенными параметрами, касающиеся систем сравнений по модулю m и систем диофантовых уравнений с решениями из заданного отрезка. Доказываются ограничения на параметры, при выполнении которых любая задача каждой серии NP-полна.

Доказывается, что при любых m_1 и m_2 ($m_1 < m_2$ и m_1 не является делителем m_2) задача проверки совместности системы линейных сравнений по модулям m_1 и m_2 одновременно, каждое из которых содержит ровно 3 переменные, NP-полна.

Также доказывается, что при всяком $m > 2$ задача проверки совместности на подмножестве, содержащем по крайней мере 2 элемента, множества $\{0, \dots, m-1\}$ системы линейных сравнений по модулю m , каждое из которых содержит ровно 3 переменные, NP-полна. При этом если $P \neq NP$, в формулировке теоремы термин «3-дизсравнение» не может быть заменен на термин «2-дизсравнение».

Для систем линейных диофантовых уравнений, каждое из которых содержит ровно 3 переменные, доказана NP-полнота задачи проверки их совместности на заданном отрезке целых чисел. Если $P \neq NP$, в формулировке теоремы термин «3-уравнение» не может быть заменен на термин «2-уравнение». Эта задача допускает также и простую геометрическую интерпретацию об NP-полноте задачи проверки наличия внутри многомерного куба целочисленной точки пересечения заданных гиперплоскостей, отсекающих на произвольных трех осях равные отрезки и параллельных всем остальным осям.

Среди задач сформулированной серии имеются задачи полезные для практики. Поскольку множество значений переменной компьютерного типа *integer* может рассматриваться как целочисленные значения отрезка, доказывается неполиномиальность любого алгоритма решения таких систем в множестве чисел типа *integer*, если $P \neq NP$. Библиогр. 6 назв.

Ключевые слова: система линейных диофантовых уравнений, система линейных диофантовых сравнений, принадлежность целочисленной точки из ограниченной области пересечению гиперплоскостей, NP-полнота.

Введение. Настоящая статья является продолжением статьи [1], опубликованной в предыдущем номере журнала, в которой рассматривались задачи проверки совместности систем специального вида линейных 3-дизсравнений и 2-дизсравнений по модулю m (термин дизсравнение означает несравнимость $\neq$ левой и правой частей выражения). Были доказаны условия их NP-полноты.

В настоящей статье предлагаются серии теоретико-числовых задач с явно выделенными параметрами и доказываются условия на параметры, при выполнении которых каждая задача серии NP-полна. Сравнения используются в современных исследованиях по теории чисел, например в [2].

Задачи рассматриваемых серий имеют практическое значение в случае использования в компьютерной программе переменных типа *integer*. В частности, совместность системы линейных уравнений на отрезке целых неотрицательных чисел позволяет утверждать ее совместность на множестве всех натуральных чисел [3, 4].

1. Системы линейных сравнений (СЛС). Пусть m_1 и m_2 — различные натуральные числа, большие 1, $L(x_1, \dots, x_n)$ — линейная комбинация с ненулевыми ко-

эффициентами переменных $x_1, \dots, x_n$ плюс константа. Сформулируем следующую серию задач.

3-СЛС по двум модулям m_1 и m_2

УСЛОВИЕ. Дана СЛС по модулям m_1 и m_2 , в которой для каждого сравнения вида $L_j(x_{i_1^1}, x_{i_1^2}, x_{i_1^3}) \equiv 0 \pmod{m_k}$ система содержит сравнение $L_j(x_{i_1^1}, x_{i_1^2}, x_{i_1^3}) \equiv 0 \pmod{m_{(3-k)}}$ (при каждом $k = 1, 2$).

ВОПРОС. Совместна ли система в числах, сравнимых по модулю m с числами из множества $\{0, 1, \dots, m-1\}$, где $m = \max\{m_1, m_2\}$?

Иначе говоря, задачи этой серии являются задачами по проверке существования общего решения двух систем линейных сравнений, в которых каждое сравнение присутствует в каждой из систем, но в одной из них — по модулю m_1 , а в другой — по модулю m_2 .

Лемма 1. *Каковы бы ни были различные натуральные числа m_1 и m_2 , большие 1, сужение задачи 3-СЛС по двум модулям m_1 и m_2 на случай, когда все коэффициенты при переменных принадлежат множеству $\{-1, 1\}$, при проверке совместности системы в числах, сравнимых с элементами множества $\{0, 1\}$, является NP-полным.*

ДОКАЗАТЕЛЬСТВО. То, что задача принадлежит классу **NP**, очевидно, так как длина записи «претендента» на решение не превосходит полинома от длины записи системы, так же как и число шагов, требуемое на проверку того, действительно ли «претендент» является решением. К задаче, сформулированной в лемме, полиномиально сводится задача **3-вып при одном истинном литерале** из [5].

Действительно, истинность ровно одного литерала в дизъюнкции $x_1 \vee x_2 \vee x_3$ (где x_1, x_2, x_3 — переменные или их отрицания) может быть записана с помощью системы из двух сравнений $x_1 + x_2 + x_3 \equiv 1 \pmod{m_i}$ при $i = 1, 2$. При этом вместо $\neg u_i$ подставляем $1 - u_i$. ■

Теорема 1. *Каковы бы ни были два различных натуральных числа m_1 и m_2 такие, что $m_1 < m_2$ и m_1 не является делителем m_2 , сужение задачи 3-СЛС по двум модулям m_1 и m_2 на случай, когда все коэффициенты при переменных принадлежат множеству $\{-1, 1\}$, является NP-полным.*

ДОКАЗАТЕЛЬСТВО. То, что задача принадлежит классу **NP**, очевидно, как и при доказательстве леммы 1.

Так как m_1 не является делителем m_2 , для некоторых $b \geq 1$ и $c \in [1, m_1 - 1]$ имеет место равенство $m_2 = bm_1 + c$. Для того чтобы воспользоваться леммой 1, в которой речь идет о решениях системы в числах из $\{0, 1\}$, заметим, что для любых $b \geq 1$ и $c \in [1, m_1 - 1]$ справедлива равносильность

$$\begin{aligned} x \equiv 0 \pmod{bm_1 + c} \vee x \equiv 1 \pmod{bm_1 + c} &\Leftrightarrow \\ \Leftrightarrow \exists x' (x' \in [0, m_2 - 1] \&(x + x' \equiv 1 \pmod{m_1}) \&(x + x' \equiv 1 \pmod{bm_1 + c}))) &(1) \end{aligned}$$

Докажем эту равносильность. Значение $(2, m_1 - 1)$ для пары (x, x') не является решением этой системы из-за второго сравнения. Пары вида $(2, bm_1 + c - 1)$, $(3, bm_1 + c - 2)$, $\dots$, $(bm_1 + c - 1, 2)$ не являются решениями этой системы из-за первого сравнения и того, что $c \neq 0$. Следовательно, $x \equiv 0 \pmod{bm_1 + c} \vee x \equiv 1 \pmod{bm_1 + c}$.

Если в сравнении число переменных равно двум, добавляем в сравнение фиктивные тождественно равные нулю переменные аналогично тому, как это было сделано в конце доказательства теоремы 1 из [1].

Осталось применить лемму 1. ■

Следствие 1 теоремы 1. *Каковы бы ни были два различных натуральных числа m_1 и m_2 такие, что $m_1 < m_2$ и m_1 не является делителем m_2 , задача 3-СЛС по двум модулям m_1 и m_2 является NP-полной.*

При $m_1 = 2$, $m_2 = 3$ другое следствие обеспечивает NP-полноту одной из наиболее просто формулируемых и интересных теоретико-числовых задач.

Следствие 2 теоремы 1. *Задача проверки выполнимости в числах из множества $\{0, 1, 2\}$ системы, состоящей из пар сравнений вида $L_j(x_{i_1^1}, x_{i_1^2}, x_{i_1^3}) \equiv 0 \pmod{2}$ и $L_j(x_{i_1^1}, x_{i_1^2}, x_{i_1^3}) \equiv 0 \pmod{3}$, где каждое сравнение содержит ровно 3 различные переменные с коэффициентами при них из $\{-1, 1\}$, является NP-полной.*

Может показаться, что в этом следствии система сравнений по модулям 2 и 3 может быть заменена на систему сравнений по модулю 6 (умножением каждого сравнения на 3 и 2 соответственно), проверка совместности которой принадлежит классу P. Однако это не так. Но такая замена возможна, если решение новой системы ищется среди чисел, сравнимых по модулю 6 как с числами из множества $\{0, 1, 2\}$, так и с числами из множества $\{0, 1, 2, 3\}$.

Можно получить более общий результат. Сформулируем серию задач.

3-СЛС по модулю m в неполном наборе остатков

УСЛОВИЕ. Пусть задана система, состоящая из линейных сравнений вида $L_j(x_{i_1^1}, x_{i_1^2}, x_{i_1^3}) \equiv 0 \pmod{m}$, в которой каждое сравнение содержит ровно 3 различные переменные.

Задано собственное подмножество M множества $\{0, 1, \dots, m-1\}$, содержащее более одного элемента.

ВОПРОС. Совместна ли система в числах, сравнимых по модулю m с числами из множества M ?

Следующая теорема обобщает лемму 1 из [1].

Теорема 2. *Каково бы ни было целое число $m \geq 3$, сужение задачи 3-СЛС по модулю m в неполном наборе остатков на случай, когда все коэффициенты при переменных принадлежат множеству $\{-1, 1\}$, является NP-полным.*

ДОКАЗАТЕЛЬСТВО. То, что задача принадлежит классу NP, очевидно, как и при доказательстве леммы 1.

Задача **3-вып при одном истинном литерале** полиномиально сводится к задаче, сформулированной в теореме 2.

Пусть m_0 — наименьшее число из $\{0, 1, \dots, m-1\} \setminus M$, m_1, m_2 — различные наименьшие элементы множества M . Выполнимость одного истинного литерала в дизъюнкте $x_1 \vee x_2 \vee x_3$ с литералами x_1, x_2, x_3 заменяется проверкой существования решения сравнения $x_1 + x_2 + x_3 \equiv 2m_1 + m_2 \pmod{m}$. При этом в литералах переменная u_i заменяется на x_i , а отрицание переменной $\neg u_i$ заменяется на $m_1 + m_2 - x_i$. Здесь значения m_1 и m_2 играют роль констант *ложь* и *истина* соответственно.

Отметим, что $3m_1 \not\equiv 2m_1 + m_2 \not\equiv m_1 + 2m_2 \not\equiv 3m_2 \not\equiv 2m_1 + m_2 \pmod{m}$. Это обеспечивает корректность предложенной замены.

Кроме этого, для каждой переменной x_i добавляется система сравнений вида $x_i - d + m_0 \equiv x_{j_d} \pmod{m}$, где $d \in M$ и $d \neq m_1$, $d \neq m_2$ и $d \neq m_0$. Такая система обеспечивает условие, при котором x_i может принимать только одно из двух значений m_1 или m_2 . ■

Следствие 1 теоремы 2. *Каково бы ни было целое число $m \geq 3$, задача 3-СЛС по модулю m в неполном наборе остатков является NP-полной.*

Следствие 2 теоремы 2. *Каковы бы ни были различные числа m_1, m_2 , задача проверки совместности в этих числах системы сравнений с коэффициентами при переменных из $\{-1, 1\}$ по модулю 3 является NP-полной.*

Это очевидное следствие позволяет иметь простые примеры теоретико-числовых NP-полных задач.

2. Системы линейных уравнений (СЛУ). Пусть целые числа m и m' таковы, что $m < m'$. Сформулируем серию задач, каждая из которых является частным случаем задачи целочисленного линейного программирования [6], поскольку всякое уравнение вида $f(x) = 0$ равносильно системе из двух неравенств $f(x) \geq 0$ и $f(x) \leq 0$.

3-СЛУ на отрезке целых чисел $[m, m']$

УСЛОВИЕ. Пусть задана система, состоящая из линейных уравнений вида $L_j(x_{i1}, x_{i2}, x_{i3}) = 0$, в которой каждое уравнение содержит ровно 3 различные переменные.

ВОПРОС. Совместна ли система в целых числах из отрезка $[m, m']$?

Теорема 3. *Каковы бы ни были целые числа m и m' ($m < m'$) сужение задачи 3-СЛУ на отрезке целых чисел $[m, m']$ на случай, когда все коэффициенты при переменных принадлежат множеству $\{-1, 1\}$, является NP-полной задачей.*

ДОКАЗАТЕЛЬСТВО. То, что задача принадлежит классу NP, очевидно, как и при доказательстве леммы 1.

Покажем, что задача **3-вып при одном истинном литерале** полиномиально сводится к рассматриваемой задаче.

Прежде всего заметим, что $\exists y(x + t = y) \iff m \leq x + t \leq m'$. Уравнение

$$x + m' - m - 1 = z \quad (2)$$

имеет решение в числах из отрезка $[m, m']$ тогда и только тогда, когда $x \in \{m, m+1\}$.

Уравнения такого вида добавим к системе для каждой переменной. Поскольку в каждом уравнении этой системы только две переменные, добавим тождественно равную m переменную w в качестве слагаемого в левые части систем вида (2) и константу m в правые части тех же уравнений, а также уравнение $w + u + v = 3m$.

Истинность ровно одного литерала в дизъюнкции $x_1 \vee x_2 \vee x_3$ (где x_1, x_2, x_3 — переменные или их отрицания) равносильна наличию целочисленного решения уравнения $x_1 + x_2 + x_3 = 3m + 1$. При этом вместо $\neg u_i$ подставляем $2m + 1 - u_i$. ■

Следствие теоремы 3. *Каковы бы ни были целые числа m и m' ($m < m'$), задача 3-СЛУ на отрезке целых чисел $[m, m']$ является NP-полной.*

Теорема 3 допускает геометрическую интерпретацию. Точнее, она может быть сформулирована в виде утверждения.

Утверждение. *Пусть заданы различные целые числа m и m' , многомерный куб, каждая координата вершин которого принадлежит множеству $\{m, m'\}$, и гиперплоскости, высекающие на произвольных трех осях равные отрезки и параллельные всем остальным осям. Тогда задача проверки наличия внутри многомерного куба целочисленной точки пересечения всех гиперплоскостей NP-полна.*

Литература

1. Косовский Н. К., Косовская Т. М., Косовский Н. Н. Условия NP-полноты проверки совместности нескольких видов систем линейных диофантовых дизъюнкций // Вестн. С.-Петербург. ун-та. Сер. 1. 2016. Т. 3(61), вып. 1. С. 25–31.
2. Zhe Feng Xu. On the difference between an integer and its m -th power mod n // Sci. China Math. 2013. Vol. 56, N 8. P. 1597–1606.
3. Hernando A., de Ledesma L., Laita L. M. Showing the non-existence of solutions in systems of linear Diophantine equations // Mathematics and Computers in Simulation. 2009. Vol. 79, Issue 11. P. 3211–3220.
4. Feng Jiejian, Liu Liming, Wan Yat-wah. Irreducibility of joint inventory positions in an assemble-to-order system under (r, nQ) policies // Naval Research Logistics (NRL). 2012. Vol. 59, Issue 1. P. 18–25.
5. Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. М.: Мир, 1982.
6. Схрейвер А. Теория линейного и целочисленного программирования. Т. 2. М.: Мир, 1991.

Статья поступила в редакцию 5 июня 2015 г.

Сведения об авторах

Косовский Николай Кириллович — доктор физико-математических наук, профессор;
kosov@nk1022.spb.edu

Косовская Татьяна Матвеевна — доктор физико-математических наук, профессор;
kosovtm@gmail.com

Косовский Николай Николаевич — кандидат физико-математических наук, доцент;
kosovnn@pdmi.ras.ru

NP-COMPLETENESS CONDITIONS FOR SOME TYPES OF SYSTEMS OF LINEAR DIOPHANTINE COMPARISONS AND EQUATIONS CONSISTENCY CHECKING

Nikolay K. Kosovskii, Tatiana M. Kosovskaya, Nikolay N. Kosovskii

St. Petersburg State University, Universitetskaya nab., 7-9, St. Petersburg, 199034, Russian Federation;
kosov@nk1022.spb.edu, kosovtm@gmail.com, kosovnn@pdmi.ras.ru

Three series of number-theoretic problems concerning systems of modulo m comparisons and systems of Diophantine linear equations with explicitly pointed out parameters are proposed in this part of the paper. Conditions upon the parameters implying that every problem of a series is an NP-complete one are proved.

It is proved that for every m_1 and m_2 ($m_1 < m_2$ and m_1 is not a divisor of m_2) the consistency problem for a system of simultaneously modulo m_1 and m_2 comparisons every of which contains exactly 3 variables is NP-complete.

It is also proved that for every $m > 2$ the consistency on the subset containing at least two elements of the set $\{0, \dots, m-1\}$ problem for a system of modulo m comparisons every of which contains exactly 3 variables is NP-complete. If $P \neq NP$ then the statement of the proved theorem can not be changed by means of replacing the term «3-comparison» with the term «2-comparison».

For a system of Diophantine linear equations every of which contains exactly 3 variables it is proved the NP-completeness of the problem of its consistency on the interval of integers. If $P \neq NP$ then the statement of the proved theorem can not be changed by means of replacing the term «3-equation» with the term «2-equation». This problem also admits a simple geometrical interpretation concerning NP-completeness of the checking whether there exists inside a many-dimensional cube an integer-valued point of intersection of hyperplanes which cut off equal segments of three axes and are parallel to the other ones.

Among the problems of the series there are practically useful problems. If $P \neq NP$ then, as the set of all values for a variable of a computer type *integer* may be considered as the set of integer values from a segment then theorem proves that there does not exist a polynomial algorithm solving such a system in the set of all numbers of the type *integer*. Refs 6.

Keywords: system of linear Diophantine equations, system of linear Diophantine comparisons, belonging of a integer-valued point from a bounded domain to the intersection of hyperplanes, NP-completeness.

References

1. Kosovskii N. K., Kosovskaya T. M., Kosovskii N. N., "NP-completeness conditions for some types of systems of linear Diophantine dis-comparisons consistency checking", *Vestnik St. Petersburg. Univ.: Math.* **49**, Issue 1, 18–22 (2016).
2. Zhe Feng Xu, "On the difference between an integer and its m -th power mod n ", *Sci. China Math.* **56**(8), 1597–1606 (2013).
3. Hernando A., de Ledesma L., Laita L. M., "Showing the non-existence of solutions in systems of linear Diophantine equations", *Mathematics and Computers in Simulation* **79**, Issue 11, 3211–3220 (2009).
4. Feng Jiejian, Liu Liming, Wan Yat-wah, "Irreducibility of joint inventory positions in an assemble-to-order system under (r, nQ) policies", *Naval Research Logistics (NRL)* **59**, Issue 1, 18–25 (2012).
5. Garey M. R., Johnson D. S., *Computers and Intractability: A Guide to the Theory of NP-Completeness* (Freeman, New York, 1979).
6. Schrijver A., *Theory of Linear and Integer Programming. A Wiley-Interscience Publication* (John Wiley & Sons, New York, 1986).