УДК 51.681.3

С.Л. Крывый, А.В. Невмержицкий

О НЕСОВМЕСТНОСТИ ОДНОГО ВИДА НЕЛИНЕЙНЫХ УРАВНЕНИЙ В МНОЖЕСТВЕ НАТУРАЛЬНЫХ ЧИСЕЛ

Рассматривается проблема определения несовместности нелинейных уравнений вида $x^m + y^m = z^m$ в множестве положительных натуральных чисел при условии простоты чисел m и z. Общее решение данного уравнения, имеющего название «великой» теоремы Ферма, получено чрезвычайно сложными методами и его можно найти в [1, 2]. Приведенный в данной статье результат получен совершенно элементарным способом.

Введение

В связи с интенсивным развитием логического программирования и, в частности, констрейнтного логического программирования (CLP), проблема определения совместности системы ограничений (констрейнтов) играет важную роль. Случай систем линейных ограничений исследовался во многих работах [3−9]. Изложенное в данной статье можно рассматривать как некоторый шаг на пути обобщения линейного случая. Важность проблемы определения совместности системы констрейнтов состоит в том, что во многих реальных задачах нет необходимости вычислять все множество решений такой системы или базис ее множества решений, а достаточно только знать, что данная система ограничений совместна (т.е. имеет хотя бы одно решение).

1. Формулировка задачи

Пусть N обозначает множество натуральных чисел, $N^+ = N \setminus \{0\}$ — множество положительных натуральных чисел и N_p — множество простых натуральных чисел.

Задача определения совместности, рассматриваемая в данной статье, состоит в следующем: совместно ли уравнение вида

$$x^m + y^m = z^m, \qquad (1)$$

где x, y, z — неизвестные, принимающие свои значения в множестве N^+, а $m, z \in N_p$.

В случае $m = 1$ это будет линейное уравнение и методы его решения известны. При $m = 2$ проблема совместности сводится к проблеме нахождения пифагоровых троек и методы поиска таких троек тоже известны [10]. Не ограничивая общности, можно считать, что выполнены условия

$$\text{НОД}(x, y) = 1 \text{ и } \text{НОД}(x, y, z) = 1,$$

поскольку всегда можно сократить обе части уравнения (1) на их общий делитель. Следует также заметить, что общие случаи уравнения (1) при $m = 3$ и $m = 4$ были исследованы соответственно Л. Эйлером и П. Ферма. Поэтому в дальнейшем будет рассматриваться случай простых чисел m и z, где $m \geq 3$. Рассмотрим некоторые общие свойства чисел x, y, z, входящих в уравнение (1), которые сформулируем в виде следующей теоремы.

Теорема 1. Для произвольных натуральных чисел x и y верны такие утверждения:

(a) если $m = 2l + 1$ нечетное, то $x^m + y^m \equiv 0 \,(\mathrm{mod}\,(x + y))$;

(b) если $m = 2l$ четное, то $x^m + y^m \equiv (-1)^l 2 S_2{}^l \,(\mathrm{mod}\, S_1{}^2)$, где $S_1 = x + y$, $S_2 = xy$.

Доказательство. Справедливость пункта (a) непосредственно вытекает из следующего простого тождества:

$$x^{2l+1} + y^{2l+1} = (x + y)(x^{2l} - x^{2l-1} y + \\ + x^{2l-2} y^2 - \ldots - x y^{2l-1} + y^{2l}).$$

Доказательство пункта (b) выполняется индукцией по числу l такому, что $m = 2l$.

Базис индукции (l = 1) очевидно имеет место, т.к. $x^2 + y^2 = (x+y)^2 - 2xy$, и поэтому $x^2 + y^2 \equiv -2xy \,(\mathrm{mod}\, S_1^2)$.

Шаг индукции. Предположим, что для любого $k \le 2l$ утверждение леммы верно. Рассмотрим случай $k = 2l + 2$. Тогда можем записать

$$x^{2l+2} + y^{2l+2} = S_1(x^{2l+1} + y^{2l+1}) -$$
$$-S_2(x^{2l} + y^{2l}) = S_1 S_1 R - S_2(x^{2l} + y^{2l})$$

на основании пункта (a) теоремы, если его применить к первому слагаемому данного выражения. Но из предположения индукции, если его применить ко второму слагаемому выражения, получаем

$$x^m + y^m \equiv (-1)^l 2 S_2{}^l \,(\mathrm{mod}\, S_1^2).$$

Теорема доказана.

2. Структуризация переменных

Заметим, что поскольку $x, y, z \in N^+$, то $x < z$, $y < z$ и $x + y > z$. Поэтому можно положить $z = x + t'$ и $z = y + t$, где $t, t' > 0$. Используя малую теорему Ферма (напомним, что $m \ge 3$ — простое число), получаем справедливость следующих сравнений:

$$x^m \equiv x(\mathrm{mod}\, m),\ y^m \equiv y(\mathrm{mod}\, m) \text{ и}$$
$$z^m \equiv z(\mathrm{mod}\, m).$$

Из уравнения (1) и общих свойств сравнений получаем

$$x^m + y^m \equiv (x+y)(\mathrm{mod}\, m) \text{ и}$$
$$z^m = x^m + y^m \equiv z(\mathrm{mod}\, m),$$

и, следовательно, $x + y \equiv z(\mathrm{mod}\, m)$. Кроме того, из условия простоты числа $m \ge 3$ получаем НОД(2, m) = 1, а из того, что числа x, y, z связаны равенством (1), получаем $x + y \equiv z(\mathrm{mod}\, 2)$. Тогда из того, что два числа сравнимы по разным модулям, следует их сравнимость по модулю, являющемуся их наименьшим общим кратным, получаем справедливость сравнения $x + y \equiv z(\mathrm{mod}\, 2m)$ и, значит,

$$x + y = z + 2mT. \qquad (2)$$

Отсюда, учитывая то, что $z = x + t'$ и $z = y + t$, получаем

$$x = z + 2mT - y = y + t + 2mT - y = 2mT + t, \qquad (3)$$
$$y = z + 2mT - x = x + t' + 2mT - x = 2mT + t', \qquad (4)$$
$$z = x + y - 2mT = 2mT + t + 2mT + t' -$$
$$- 2mT - y = 2mT + t + t'. \qquad (5)$$

Используя уравнение (1), получаем

$$x^m + y^m = z^m = (x+t')^m = (y+t)^m, \qquad (6)$$

или

$$x^m + y^m = x^m + \sum_{i=1}^{m-1} C_m^{m-i} x^{m-i} (t')^i + (t')^m =$$
$$= y^m + \sum_{i=1}^{m-1} C_m^{m-i} y^{m-i} t^i + t^m.$$

Отсюда получаем

$$x^m = \sum_{i=1}^{m-1} C_m^{m-i} y^{m-i} t^i + t^m, \qquad (7)$$

$$y^m = \sum_{i=1}^{m-1} C_m^{m-i} x^{m-i} (t')^i + (t')^m. \qquad (8)$$

И, соответственно,

$$x^m = t^m (\mathrm{mod}\, mty) \Rightarrow x^m = 0 \,(\mathrm{mod}\, t), \qquad (9)$$

$$y^m = (t')^m (\mathrm{mod}\, mt'x) \Rightarrow y^m \equiv 0 \,(\mathrm{mod}\, t). \qquad (10)$$

Используя пункт (a) теоремы 1, получаем

$$z^m = (x + y - 2Tm)^m = (S_1 - 2Tm)^m \equiv 0 \,(\mathrm{mod}\, S_1),$$

а отсюда следует, что

$$(2Tm)^m \equiv 0 \,(\mathrm{mod}\, S_1) \text{ и}$$
$$(t + t') = (S_1 - 4Tm)^m \equiv 0 \,(\mathrm{mod}\, S_1),$$

а также

$$(t + t') \equiv 0 \,(\mathrm{mod}\, S_1).$$

Это означает, что все простые делители числа $S_1 = x + y$ являются делителями каждого из чисел z, $2Tm$ и $t + t'$. Следовательно число S_1 не может быть простым, так как в противном случае

из сравнения $z^m \equiv 0 \pmod{S_1}$ получаем, что $z \equiv 0 \pmod{S_1}$, но $z < S_1$. Аналогично число S_1 не может иметь два разных простых делителя. Может быть, однако, случай, когда $S_1 = z^k$ $(k > 1)$. Но это равенство не может быть справедливым, поскольку по условию имеем $z < x + y < 2z$ и, следовательно, S_1 не может быть равно z^k при $k > 1$ и $z \geq 2$. А из того, что число S_1 составное, следует, что и число z составное.

Таким образом, из всего вышесказанного следует справедливость такого утверждения.

Теорема 2. Если $m \geq 3$ — простое число, то m-я степень любого простого числа z не может быть равна сумме m-х степеней двух натуральных чисел, т.е. $x^m + y^m \neq z^m$, если $x, y \in N^+$, m, $z \in N_p$ и $m \geq 3$.

Заключение

Рассмотренные случаи ограничений типа (1) часто возникают в практических приложениях (например, в криптоанализе) и, кроме того, имеют прямое отношение к знаменитой «великой» теореме Ферма [1, 2]. Полученный результат показывает несовместность данного ограничения при условии простоты чисел m и z в области положительных натуральных чисел.

1. *Wiles A.* Modular elliptic curves and Fermat's Last Theorem // Annals of Mathemat. — 1995. — **2**, — N 141. — P. 443–551.
2. *Taylor R., Wiles A.* Ring-theoretic properties of certain Hecke algebras // Ibid. — P. 553–572.
3. *Contenjean E., Devie H.* Solving systems of linear diophantine equations // Proc. 3rd Workshop on Unification. — Lambrecht: University of Kaiserslautern, 1989. — P. 19–26.
4. *Pottier L.* Minimal solutions of linear diophantine systems: bounds and algorithms // Proc. of the Fourth Intern. conf. on Rewriting Techniques and Applications. — Como, — 1991. — P. 162–173.
5. *Domenjoud E.* Outils pour la deduction automatique dans les theories associatives-commutatives. Thesis de Doctorat d'Universite: Universite de Nancy I. France. — 1991. — 176 p.
6. *Clausen M., Fortenbacher A.* Efficient solution of linear diophantine equations // J. Symbolic Computation. — 1989. — **8**, — N 1, 2. — P. 201–216.
7. *Romeuf J. F.* A polinomial Algorithm for Solving systems of two linear Diophantine equations // TCS. — 1990. — **74**, — N 3. — P. 329–340.
8. *Filgueiras M., Tomas A.P.* A Fast Method for Finding the Basis of Non-negative Solutions to a Linear Diophantine Equation // J. Symbolic Computation. — 1995. —**19**, — N 2. — P. 507–526.
9. *Кривой С.Л.* О некоторых методах решения и критериях совместности систем линейных диофантовых уравнений в множестве натуральных чисел // Кибернетика и системный анализ. — 1999. — N 4. — P. 12–36.
10. *Живые* числа. Пять экскурсий. В. Боро, Ю. Цагир, Ю. Рельфо и др. — М.: Мир. — 1985. — 126 с.

Получено 28.08.03

Об авторах

Крывый Сергей Лукьянович
доктор физ.-мат. наук, профессор, вед. науч. сотрудник

Невмержицкий Александр Васильевич
аспирант института

Место работы авторов:
Институт кибернетики им. В.М. Глушкова НАН Украины,
просп. Академика Глушкова, 42,
Киев-187, 03680, Украина
Тел. 266 0458
E-mail: krivoi@i.com.ua