

Об одном условии представимости показательно-степенной функции в унарах

Армен А. Согоян

Институт проблем информатики и автоматизации НАН РА и ЕрГУ

Аннотация

В работе предлагается необходимое и достаточное условие представимости показательно-степенной функции в индукционных моделях — унарах.

Рассматривается представление арифметических функций в унарах; основные определения, связанные с подобными представлениями, даны в [1].

Возможность представления показательно-степенной функции в унарах используется как для формулировки, так и для решения многих задач, некоторые из которых приведены в [1] и [2]. Под показательно-степенной функцией мы понимаем функцию x^y от двух аргументов.

Задача о нахождении необходимого и достаточного условия представимости этой функции была поставлена А. Машпурином. Такое условие предложено в работе [2].

Нами получено другое необходимое и достаточное условие (содержащее аналог функции Эйлера), в некоторых случаях более удобное для проверки.

Напомним, что каждому унару в соответствие ставится пара натуральных чисел (n, k) — характеристика унара, где n — длина "хвостовой" части унара, k — длина "кольцевой" части. Характеристика унара однозначно определяет его.

Пусть $k = p_1^{\alpha_1} \dots p_s^{\alpha_s}$ (p_i — простые числа). Обозначим через $A(k)$ и $h(k)$ следующие функции:

$$A(k) = \begin{cases} 1, & \text{при } k = 1, 2 \\ 2, & \text{при } k = 4 \\ 2^n, & \text{при } k = 2^{n+2}, n \geq 1 \\ p^{\alpha-1}(p-1), & \text{при } k = p^\alpha, p \neq 2 \\ [A(u), A(v)], & \text{при } k = u \cdot v, (u, v) = 1, \end{cases} \quad (1)$$

(где через $[a, b]$ обозначено наименьшее общее кратное чисел a и b),

$$h(k) = \max\{\alpha_1, \dots, \alpha_s\}. \quad (2)$$

Функция $A(k)$, как легко убедиться, обладает целым рядом свойств функции Эйлера $\varphi(k)$. В [3] доказывается, что

$$\forall x \ x^{h(k)+A(k)} \equiv x^{h(k)} \pmod{k}.$$

В [2] доказано, что для того, чтобы показательно-степенная функция была представима в унаре характеристики (n, k) , необходимо и достаточно, чтобы выполнялись следующие два условия:

$$\forall p \ (p|k \implies (p-1)|k) \quad (p - \text{простое число}) \quad (3)$$

и

$$n \geq h(k). \quad (4)$$

На основе этих условий устанавливается следующее условие представимости:

Теорема. Для того, чтобы показательно-степенная функция была представима в унаре характеристики (n, k) , необходимо и достаточно, чтоб выполнялись следующие два условия:

$$A(k)|k \quad (5)$$

и

$$n \geq h(k). \quad (6)$$

Доказательство. Покажем, что условия (5) и (6) эквивалентны условиям (3) и (4). Для этого достаточно показать, что $(5) \sim (3)$.

1. $(5) \Rightarrow (3)$. Пусть имеет место (5) — $A(k)|k$. Если $p|k$, тогда существует α такое, что $k = p^\alpha \cdot m$, $(p, m) = 1$, и, согласно (1),

$$A(k) = A(p^\alpha \cdot m) = [A(p^\alpha), A(m)] = [(p-1)p^{\alpha-1}, A(m)],$$

откуда получаем $(p-1)|A(k)$, а так как $A(k)|k$, то $(p-1)|k$, то есть имеет место также и (3).

2. $(3) \Rightarrow (5)$. Доказательство проведем индукцией по s — количеству простых делителей k .

Для $s = 0$ получаем $k = A(k) = 1$, и $A(k)|k$ — утверждение верно.

Пусть для чисел s с простыми делителями утверждение верно. Покажем, что оно верно для $k = p_1^{\alpha_1} \dots p_s^{\alpha_s} p_{s+1}^{\alpha_{s+1}}$.

Допустим для k выполнено условие (3) — $p|k \Rightarrow (p-1)|k$. Учитывая (1), получаем

$$\begin{aligned} A(k) &= A(p_1^{\alpha_1} \dots p_s^{\alpha_s} p_{s+1}^{\alpha_{s+1}}) = [A(p_1^{\alpha_1} \dots p_s^{\alpha_s}), A(p_{s+1}^{\alpha_{s+1}})] = \\ &= [A(p_1^{\alpha_1} \dots p_s^{\alpha_s}), (p_{s+1}-1) \cdot p_{s+1}^{\alpha_{s+1}-1}] = \\ &= [A(p_1^{\alpha_1} \dots p_s^{\alpha_s}), (p_{s+1}-1), p_{s+1}^{\alpha_{s+1}-1}] \end{aligned}$$

(последнее равенство получаем, учитывая, что $(p_{s+1}-1, p_{s+1}^{\alpha_{s+1}-1}) = 1$).

Наша задача — доказать, что

$$A(k) = [A(p_1^{\alpha_1} \dots p_s^{\alpha_s}), (p_{s+1}-1), p_{s+1}^{\alpha_{s+1}-1}] | k.$$

а) Очевидно, что $p_{s+1}^{\alpha_{s+1}-1} | k$.

б) Так как $p_1^{\alpha_1} \dots p_s^{\alpha_s}$ удовлетворяет условию (3) $(p|p_1^{\alpha_1} \dots p_s^{\alpha_s} \Rightarrow p|k \Rightarrow (p-1)|k)$, а так как $p-1 < p_{s+1}$, то $(p-1, p_{s+1}) = 1 \Rightarrow (p-1)|p_1^{\alpha_1} \dots p_s^{\alpha_s}$, то согласно индукционному предположению $A(p_1^{\alpha_1} \dots p_s^{\alpha_s})|p_1^{\alpha_1} \dots p_s^{\alpha_s}|k$, то есть $A(p_1^{\alpha_1} \dots p_s^{\alpha_s})|k$.

в) $(p_{s+1}-1)|k$, так как k удовлетворяет (3).

Из а), б) и в) следует, что $A(k)|k$.

Литература

- [1] А. С. Машурян, "Ряды Полла и представимость функций в конечных моделях некоторых арифметических теорий", Известия НАН РА, Математика, т. XXX, No. 1, 1995.
- [2] S. Burris, S. Lee, "Small Models of the High School Identities", International Journal of Algebra and Computation, Vol. 2, No. 2 (1992), 139-178.
- [3] D. Singmaster, "A maximal generalization of Fermat's theorem", Math. Mag., 1966, 39, No 2, 103-107.