On presentations of finite unars by means of residue classes

For an arbitrary integer m we obtain the construction of an unar (an algebra with one unary operation) defined by a multiplication on the residue of a fixed integer a. We prove that each finite unar is embedded into the such unar for some integers a and m. We also show that each finite unar admits infinitely many presentations in the given form.

Известно, что не каждая конечная коммутативная полугруппа изоморфна некоторой подполугруппе полугруппы классов вычетов по модулю [1]. В нашей работе показано, что для конечных унаров ответ на аналогичный вопрос будет положителен.

Умножение на фиксированное натуральное число a с последующим приведением по модулю задает на множестве классов вычетов по модулю данного натурального числа m отображение в себя. Тем самым, на множестве классов вычетов по модулю m задается структура унара.

Например, умножение на 2 задает на множестве классов вычетов по модулю 12 унар, изображенный на рисунке 1:

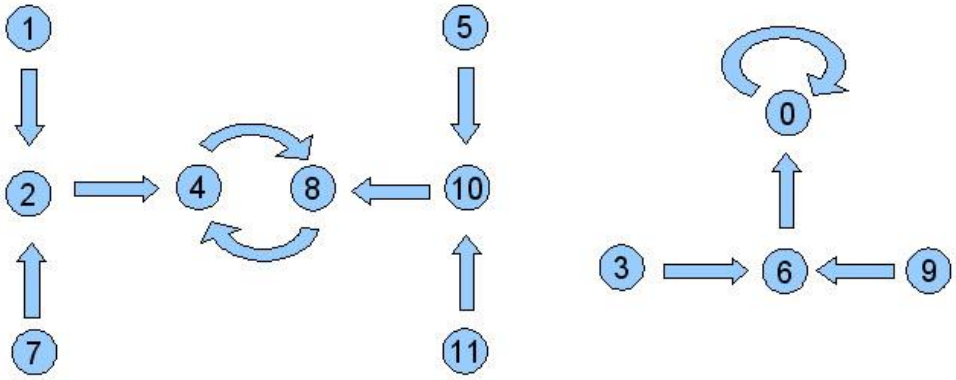

Рис. 1

Цель работы - показать, что для любого конечного унара U можно подобрать такие числа a (множитель) и m (модуль), что унар, порожденный некоторыми классами вычетов по модулю m умножением на a, будет изоморфен унару U.

Введем термины и обозначения, которых будем придерживаться в дальнейшем.

Пусть U – конечное множество и φ – унарная операция, заданная на U. Для $x \in U$ обозначим через $x\varphi$ результат применения φ к x, а через $x\varphi^n$ – результат n-кратного применения операции φ.

Элемент x назовем циклическим, если $\exists\, t \in N\ x\varphi^t = x$. Наименьшее такое t назовем длиной цикла. Наименьшее целое неотрицательное h такое, что $x\varphi^h$ является циклическим, назовем глубиной элемента x. Степенью элемента x назовем мощность множества $\{y \in U \mid y\varphi = x\}$.

Введем на множестве U отношение $x \sim y \Leftrightarrow \exists\, t,s \in N\ x\varphi^t = y\varphi^s$. Введенное отношение будет отношением эквивалентности. Классы эквивалентности этого отношения назовем компонентами связности унара U.

Нами изучено строение унара U(m,a), порожденного на множестве классов вычетов по модулю m умножением на фиксированное число (фиксированный класс) a.

Пусть d = GCD(a, m), $a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k} a_0$, $m = p_1^{\mu_1} p_2^{\mu_2} \ldots p_k^{\mu_k} m_0$, где $GCD(a_0, m_0) = 1$.

Лемма 1.

Степень элемента b равна d, если d делит b, и 0 – в противном случае.

Лемма 2.

Элемент $b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k} b_0$ является циклическим тогда и только тогда, когда $\beta_i \geq \mu_i\ \forall i \in \{1,\ldots, k\}$.

Лемма 3.

Глубина элемента $b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k} b_0$ равна наименьшему натуральному числу h, такому что $\beta_i + h\alpha_i \geq \mu_i\ \forall i \in \{1,\ldots, k\}$.

Лемма 4.

Пусть где $m(b) = m_0/GCD(m_0, b)$. Длина цикла циклического элемента b равна $ord_{m(b)}(a)$ (т.е. порядку числа a по модулю m(b)), если $m(b) > 1$ и 1, в случае $m(b) = 1$.

Лемма 5.

Число компонент связности унара U(m,a) равно

$$1+\sum_{d|m_0,d>1}\frac{\varphi(d)}{ord_d(a)}.$$

Основной результат:

Для любого конечного унара U найдутся такие числа a (множитель), m (модуль) и $b_1, b_2,\ldots, b_r$, что унар, порожденный элементами $b_1, b_2,\ldots, b_r$ умножением на a по модулю m, будет изоморфен унару U.

При доказательстве этого утверждения мы опирались на приведенные выше леммы, а также на китайскую теорему об остатках и теорему Дирихле о простых числах в арифметической прогрессии.

Доказательство является конструктивным и позволяет находить нужные a, m и набор b_i для любого наперед заданного конечного унара.

Более того, из доказательства следует, что для любого конечного унара существует бесконечно много представлений классами вычетов по модулю.

Пусть, например, нам надо представить унар, изображенный на рисунке 2.

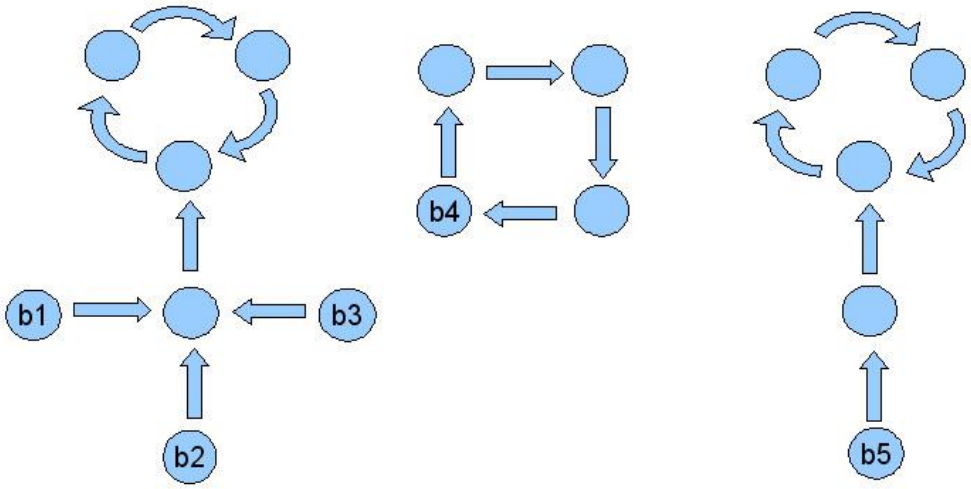

Рис. 2

Получить данный унар можно, положив m = 585, a = 3, $b_1 = 5$, $b_2 = 200$, $b_3 = 395$, $b_4 = 117$, $b_5 = 10$. Другой способ – взять m = 2448, a = 4, $b_1 = 17$, $b_2 = 629$, $b_3 = 1241$, $b_4 = 144$, $b_5 = 34$. Еще одно представление получим, положив m = 18515, a = 23, $b_1 = 5$, $b_2 = 810$, $b_3 = 1615$, $b_4 = 3703$, $b_5 = 15$. И т. д.

Вопрос о нахождении наименьшего модуля, подходящего для представления данного унара, является в общем случае достаточно сложным (см. [2])

Литература:

1. Parker E. T., On Multiplicative Semigroups of Residue Classes. – Proceedings of the American Mathematical Society Vol. 5, No. 4 (Aug., 1954), pp. 612-616
2. Архив конкурса «Математический марафон», задача ММ60. – режим доступа: http://www-old.fizmat.vspu.ru/konkurs/ans60.htm . – [3.01.2012]