Мультипликативный порядок и периоды степенных последовательностей по модулю n

Дремова Александра Владимировна
Студент (бакалавр)
Санкт-Петербургский государственный университет,
Санкт-Петербург, Россия
E-mail: alexandra5.dream@yandex.ru

Научный руководитель *— Кумачёва Сурия Шакировна*

Рассмотрим последовательность вычетов $x_k \equiv a^k \pmod{n}$, где $k \geq 0$, $a, n \in \mathbb{Z}$, $n \geq 2$ и $\gcd(a, n) = 1$. Члены последовательности принадлежат группе единиц $U(n) = (\mathbb{Z}/n\mathbb{Z})^\times$, которая является конечной абелевой группой порядка $\varphi(n)$, где φ — функция Эйлера [1]. Мультипликативным порядком элемента a по модулю n называется минимальное натуральное число t, для которого $a^t \equiv 1 \pmod{n}$. Обозначение: $\mathrm{ord}_n(a)$.

Теорема 1 (Лагранж)**.** *Пусть G — конечная группа порядка $|G|$ и H — её подгруппа. Тогда порядок $|H|$ делит $|G|$.*

Следствие. Порядок любого элемента $a \in G$ делит $|G|$. В частности, для группы $U(n)$ имеем $\mathrm{ord}_n(a) \mid \varphi(n)$ для всех $a \in U(n)$ [2].

Следовательно, длина периода последовательности $a^k \bmod n$ является делителем $\varphi(n)$. Целью работы является описание условий максимальности периода.

При каноническом разложении $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ по китайской теореме об остатках группа $U(n)$ изоморфна прямому произведению $U(n) \cong \prod_{i=1}^{r} U(p_i^{\alpha_i})$ [1], откуда вытекает формула

$$\mathrm{ord}_n(a) = \mathrm{lcm}\big(\mathrm{ord}_{p_1^{\alpha_1}}(a), \ldots, \mathrm{ord}_{p_r^{\alpha_r}}(a)\big).$$

Анализ сводится к изучению структуры групп $U(p^\alpha)$ для простых степеней.

Теорема 2 (о структуре $U(p^\alpha)$)**.** *Для нечётного простого p и любого $\alpha \geq 1$ группа $U(p^\alpha)$ циклична порядка $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$. Для степеней двойки: группа $U(4)$ циклична порядка 2, но при $\alpha \geq 3$ группа $U(2^\alpha)$ изоморфна $C_2 \times C_{2^{\alpha-2}}$ и максимальный порядок элемента равен $2^{\alpha-2}$.*

Основной результат работы представлен в следующей теореме:

Теорема 3. *Группа $U(n)$ циклична тогда и только тогда, когда $n \in \{1, 2, 4, p^\alpha, 2p^\alpha\}$, где p — нечётное простое, $\alpha \geq 1$ [3, 4]. В этом случае существуют примитивные корни — элементы порядка $\varphi(n)$, и период последовательности $a^k \bmod n$ может достигать максимального значения $\varphi(n)$.*

Для произвольного модуля n максимально возможный период определяется функцией Кармайкла $\lambda(n)$ — экспонентой группы $U(n)$:

$$\lambda(n) = \operatorname{lcm}\bigl(\lambda(p_1^{\alpha_1}), \ldots, \lambda(p_r^{\alpha_r})\bigr),$$

где $\lambda(p^\alpha) = \varphi(p^\alpha)$ для нечётного простого p, $\lambda(2) = 1$, $\lambda(4) = 2$, $\lambda(2^\alpha) = 2^{\alpha-2}$ при $\alpha \geq 3$ [5]. По теореме Лагранжа $\lambda(n)$ делит $\varphi(n)$ [2]. В конечной абелевой группе всегда существует элемент, порядок которого равен экспоненте группы [2].

Критерий примитивного корня: пусть $U(n)$ циклична. Элемент $a \in U(n)$ является примитивным корнем тогда и только тогда, когда $a^{\varphi(n)/q} \not\equiv 1 \pmod{n}$ для каждого простого делителя q числа $\varphi(n)$ [3].

Средний мультипликативный порядок элементов в $U(n)$ асимптотически пропорционален $\lambda(n)$.

Литература

1. Виноградов И. М. Основы теории чисел. 9-е изд. М.: Наука, 1981.
2. Постников А. Г. Введение в алгебру. М.: Наука, 1973.
3. Брагин В., Клячко А., Скопенков А. Когда любая группа из n элементов циклическая? // Квант. 2011. № 6. С. 6–9.
4. Ireland K., Rosen M. A Classical Introduction to Modern Number Theory. 2nd ed. New York: Springer, 1990.
5. Bach E., Shallit J. O. Algorithmic Number Theory. Vol. 1: Efficient Algorithms. Cambridge, MA: MIT Press, 1996.