Дискретные структуры

осень 2013

Александр Дайняк

www.dainiak.com

Коммутативные группы

- Группа G *коммутативная* или *абелева*, если
$$\forall a, b \in G \quad a \circ b = b \circ a$$

Примеры абелевых групп:

- $(\mathbb{Z}, +)$
- $(\mathbb{Q} \setminus \{0\}, \times)$

Примеры неабелевых групп:

- группы подстановок
- группа всех аффинных преобразований плоскости

Смежные классы

Пусть $H \leq G$. Для любого $a \in G$ множество

$$a \circ H := \{a \circ b \mid b \in H\}$$

называется *левым смежным классом элемента* a *по подгруппе* H.

Аналогично, множество

$$H \circ a := \{b \circ a \mid b \in H\}$$

называется *правым смежным классом*.

(Для абелевых групп соответствующие левые и правые смежные классы совпадают.)

Теоремы Лагранжа и Силова

- Если $H \leq G,$ то $|H|$ делит $|G|$
- Если число вида p^{α} делит $|G|$, то $\exists H \leq G$: $|H| = p^{\alpha}$

Остаток от деления

Для любых $n \in \mathbb{Z}$ и $m \in \mathbb{Z} \setminus \{0\}$ существуют и однозначно определены $k, r \in \mathbb{N}_0$, такие, что

$$n = k \cdot m + r$$
$$r < m$$

Число r — *остаток от деления n на m*, или *вычет числа n по модулю m*.

Обозначение:

$$r = n \bmod m$$

Равенство по модулю

Если

$$n_1 \bmod m = n_2 \bmod m$$

то пишут

$$n_1 \equiv n_2 \pmod m$$

и говорят, что

$$n_1 \text{ и } n_2 \textit{ равны по модулю } m$$

Мы ещё будем обозначать это так:

$$n_1 \overset{m}{=} n_2$$

Равенство по модулю

Утверждение.

Пусть $n_1 \overset{m}{=} n_2$ и $n_3 \overset{m}{=} n_4$.

Тогда

$$n_1 + n_3 \overset{m}{=} n_2 + n_4$$

$$n_1 - n_3 \overset{m}{=} n_2 - n_4$$

$$n_1 n_3 \overset{m}{=} n_2 n_4$$

Равенство по модулю

Доказательство:

По условию,

$$n_1 = k_1 \cdot m + r'$$
$$n_2 = k_2 \cdot m + r'$$
$$n_3 = k_3 \cdot m + r''$$
$$n_4 = k_4 \cdot m + r''$$

Отсюда

$$n_1 + n_3 = (k_1 + k_3) \cdot m + r' + r'' \overset{m}{=} r' + r''$$
$$n_2 + n_4 = (k_2 + k_4) \cdot m + r' + r'' \overset{m}{=} r' + r''$$

Следовательно,

$$n_1 + n_3 \overset{m}{=} n_2 + n_4$$

Равенство по модулю

$$n_1 = k_1 \cdot m + r'$$
$$n_2 = k_2 \cdot m + r'$$
$$n_3 = k_3 \cdot m + r''$$
$$n_4 = k_4 \cdot m + r''$$

Отсюда

$$n_1 n_3 = (k_1 k_3 m + k_1 r'' + k_3 r') \cdot m + r' r'' \overset{m}{=} r' r''$$

Аналогично, $n_2 n_4 \overset{m}{=} r' r''$.

Следовательно,

$$n_1 n_3 \overset{m}{=} n_2 n_4$$

Равенство по модулю

Утверждение.
Если $n_1 \overset{m}{=} n_2,$ то $n_1^k \overset{m}{=} n_2^k$ для любого k.

Доказательство: индукцией по k с использованием предыдущего утверждения.

Пример вычислений по модулю

Задача.

Какому числу из $[0,10]$ равно по модулю 11 значение выражения $4^{100} \cdot 10^6 + 18^{85}$?

Решение:

$$4^{100} \cdot 10^6 + 18^{85} =$$

$$= (11+5)^{50} \cdot (11-1)^6 + (22-4)^{85} \overset{11}{=} 5^{50} \cdot (-1)^6 + (-4)^{85} =$$

$$= 25^{25} - 2^{10 \cdot 17} = (22+3)^{25} - (93 \cdot 11 + 1)^{17} \overset{11}{=} 3^{25} - 1 \overset{11}{=}$$

$$= 243^5 - 1 = (2 \cdot 121 + 1)^5 - 1 \overset{11}{=} 0$$

Аддитивная группа вычетов

Утверждение.
Множество чисел

$$\mathbb{Z}_m := \{0,1,\dots,m-1\}$$

образует группу относительно операции $\bigoplus$, где $x \bigoplus y$ — это такое число $z \in \mathbb{Z}_m$, что $z \overset{m}{=} x + y$

($\bigoplus$ — операция *сложения по модулю* m)

Пример. Если мы работаем в $\mathbb{Z}_5$, то

$$3 \bigoplus 2 = 0, \quad 4 \bigoplus 4 = 3$$

Операцию $\bigoplus$ будем обычно обозначать просто $+$

Аддитивная группа вычетов

Утверждение.
Множество чисел $\mathbb{Z}_m := \{0,1,\dots,m-1\}$ образует группу относительно операции $\bigoplus$.

Доказательство:

- Ассоциативность операции:

Пусть $a \bigoplus (b \bigoplus c) = z'$ и $(a \bigoplus b) \bigoplus c = z''$. Тогда $z' \overset{m}{=} a + d$, где $d \overset{m}{=} b + c$, и следовательно

$$z' \overset{m}{=} a + b + c$$

Аналогично, $z'' \overset{m}{=} a + b + c$. Так как $z' \overset{m}{=} z''$ и $z', z'' < m$, то $z' = z''$.

Аддитивная группа вычетов

Продолжение доказательства:

- Нейтральный элемент: 0
- Существование обратных элементов:

Для 0 обратный элемент 0.

Для $a \neq 0$ обратным будет $(m - a)$, т.к.

$$a + (m - a) = m \overset{m}{=} 0$$

Циклические группы

Определение.
Если конечная группа G изоморфна группе $\mathbb{Z}_{|G|}$, то G называется *циклической* группой.

Также циклическими называют бесконечные группы, изоморфные группе $(\mathbb{Z}, +)$.

Циклические группы

Примеры циклических групп:

- Группа поворотов плоскости относительно начала координат на угол, кратный $\frac{2\pi}{m}$
- $\mathbb{Z}_m^\times$ для любого m (определение $\mathbb{Z}_m^\times$ см. дальше)
- Группа чисел вида $\{n^a \mid a \in \mathbb{Z}\}$ относительно умножения (при фиксированном n)

Порядок элемента

Пусть $\mathbb{G}$ — группа с операцией $\circ$

Порядком элемента $a \in \mathbb{G}$ называется такое наименьшее k, для которого

$$\underbrace{a \circ a \circ \cdots \circ a}_{k \text{ раз}} = e$$

где e — нейтральный элемент в $\mathbb{G}$.

Если такого k не существует, порядок элемента считается равным ∞.

Обозначается порядок так: $\operatorname{ord} a$

Порядок элемента

Утверждение.
У каждого элемента в *конечной* группе есть конечный порядок.

Доказательство:

В последовательности $a, a \circ a, a \circ a \circ a, \ldots$ обязательно возникнет повторение: для $k > 0$

$$\underbrace{a \circ a \circ \cdots \circ a}_{s \text{ раз}} = \underbrace{a \circ a \circ \cdots \circ a}_{s+k \text{ раз}}$$

Отсюда сразу следует, что $\underbrace{a \circ a \circ \cdots \circ a}_{k \text{ раз}} = e.$

Циклические подгруппы

Для каждого $k \in \mathbb{N}$ обозначим

$$a^{\circ k} := \underbrace{a \circ a \circ \cdots \circ a}_{k \text{ раз}}$$

По определению положим

$$a^{\circ 0} := e$$

где e — нейтральный элемент группы.

Циклические подгруппы

Утверждение.
Пусть $a \in \mathbb{G}$ и $\operatorname{ord} a < \infty$. Тогда множество

$$\mathbb{H} := \{\, a^{\circ k} \mid k \in [0, \operatorname{ord} a) \,\}$$

является подгруппой группы $\mathbb{G}$, и $|\mathbb{H}| = \operatorname{ord} a$.

Доказательство:

Нейтральный элемент $e \in \mathbb{H}$.
При $s \geq 1$ для элемента $a^{\circ s} \in \mathbb{H}$ обратным будет элемент $a^{\circ(\operatorname{ord} a - s)}$.

При этом $|\mathbb{H}| = \operatorname{ord} a$, поскольку если $m < n$ и $a^{\circ m} = a^{\circ n}$,
то $|m - n| \geq \operatorname{ord} a$.

Циклические подгруппы

Утверждение.
Пусть $a \in \mathbb{G}$ и $\operatorname{ord} a = r$. Тогда множество

$$\mathbb{H} \coloneqq \{\, a^{\circ k} \mid k \in [0, r) \,\}$$

образует *циклическую* группу, изоморфную $\mathbb{Z}_r$

Доказательство:
Изоморфизм $\phi\colon \mathbb{H} \to \mathbb{Z}_r$ очевиден:

$$\forall k \in [0, r) \qquad \phi\left(a^{\circ k}\right) \coloneqq k$$

Тогда поскольку $a^{\circ m} \circ a^{\circ n} = a^{\circ\left((m+n) \bmod r\right)}$, то

$$\phi(a^{\circ m} \circ a^{\circ n}) = (m + n) \bmod r = \phi(a^{\circ m}) \bigoplus \phi(a^{\circ n})$$

то есть ϕ сохраняет групповую операцию, ч.т.д.

Циклические подгруппы

Утверждение.
Пусть $a \in \mathbb{G}$ и $\operatorname{ord} a = r$. Тогда множество

$$\mathbb{H} \coloneqq \{\, a^{\circ k} \mid k \in [0, r) \,\}$$

образует *циклическую* группу, изоморфную $\mathbb{Z}_r$

$\mathbb{H}$ называется подгруппой, *порождённой элементом* a,
обозначается: $\langle a \rangle$

Мультипликативная группа вычетов

Утверждение.

Множество чисел

$$\mathbb{Z}_m^\times = \{k \in (0, m) \mid k \text{ взаимно просто с } m\}$$

образует группу относительно операции $\odot$.

$\odot$ — операция *умножения по модулю* m.

По определению $x \odot y = z$, если $z \in \mathbb{Z}_m^\times$ и

$$z \overset{m}{=} x \cdot y$$

Примеры: в $\mathbb{Z}_9^\times$ имеем $2 \odot 5 = 1, \quad 4 \odot 4 = 7$

Операцию $\odot$ будем обычно обозначать просто $\cdot$

Мультипликативная группа вычетов

Утверждение.
Множество чисел

$$\mathbb{Z}_m^{\times} = \{k \in (0, m) \mid k \text{ взаимно просто с } m\}$$

образует группу относительно операции $\odot$.

Доказательство:

- Ассоциативность $\odot$ доказывается, как и для $\oplus$
- Нейтральный элемент: 1
- Нетривиально только существование обратных элементов…

Мультипликативная группа вычетов

Доказательство существования обратных:

Пусть $a \in \mathbb{Z}_m^\times$ и $a \neq 1$.

Так как $\mathbb{Z}_m^\times$ конечно, то в последовательности

$$a, \quad a \odot a, \quad a \odot a \odot a, \ldots$$

есть повторяющиеся элементы.

То есть $a^{k+l} \overset{m}{=} a^k$ для некоторых $k, l \in \mathbb{N}$.

Заметим, что элемент $b := a^{l-1} \bmod m$ и будет обратным к a.

Мультипликативная группа вычетов

$$b \coloneqq a^{l-1} \bmod m$$

Поскольку $a^{k+l} \overset{m}{=} a^k$, то

$$a^{k+l} - a^k \overset{m}{=} 0 \quad \Rightarrow \quad a^k(a^l - 1) \overset{m}{=} 0$$

Так как a и m взаимно просты, то отсюда следует

$$a^l - 1 \overset{m}{=} 0$$

А значит

$$a \odot b \overset{m}{=} a^l \overset{m}{=} 1$$

то есть, по определению, b обратен к a.

Мультипликативная группа вычетов

Утверждение.
Множество чисел

$$\mathbb{Z}_m^{\times} = \{k \in (0, m) \mid k \text{ взаимно просто с } m\}$$

образует группу относительно операции $\odot$.

Следствие.
Для любого простого p множество $\mathbb{Z}_p \setminus \{0\}$ образует мультипликативную группу относительно умножения по модулю p.

Функция Эйлера

Через $\varphi(m)$ обозначается *функция Эйлера*:

$$\varphi(m) := \#\{k < m \mid m \text{ и } k \text{ взаимно просты}\}$$

Примеры:

- $\varphi(2^n) = 2^{n-1}$ для любого $n \in \mathbb{N}$
- $\varphi(p) = p - 1$ для любого простого p
- $\varphi(30) = \#\{1,7,11,13,17,19,21,23,29\} = 9$

Теорема Эйлера—Ферма

Теорема.
Если $a, m \in \mathbb{N}$ — взаимно простые числа, то

$$a^{\varphi(m)} \overset{m}{=} 1$$

Доказательство:
Пусть $b := a \bmod m$. Достаточно доказать, что

$$b^{\varphi(m)} \overset{m}{=} 1$$

Заметим, что $b \in \mathbb{Z}_m^\times$, и рассмотрим группу $\langle b \rangle$.
Имеем $|\langle b \rangle| = \operatorname{ord} b$, $|\mathbb{Z}_m^\times| = \varphi(m)$.

Теорема Эйлера—Ферма

Имеем $|\langle b\rangle| = \operatorname{ord} b, \;\; |\mathbb{Z}_m^\times| = \varphi(m).$

Поскольку $\langle b\rangle$ — подгруппа $\mathbb{Z}_m^\times$, то по теореме Лагранжа получаем

$$\varphi(m) = t \cdot \operatorname{ord} b$$

для некоторого $t \in \mathbb{N}$.

Отсюда

$$b^{\varphi(m)} = b^{t\cdot \operatorname{ord} b} = \left(b^{\operatorname{ord} b}\right)^t \overset{m}{=} 1$$

Теорема Эйлера—Ферма

Теорема.
Если $a, m \in \mathbb{N}$ — взаимно простые числа, то

$$a^{\varphi(m)} \overset{m}{=} 1$$

Следствие. (Малая теорема Ферма)
Для любого простого p и для любого a

$$a^{p} \overset{p}{=} a$$

Пример вычислений по модулю, с применением теоремы Ферма

Задача.

Какому числу из $[0,10]$ равно по модулю 11 значение выражения $4^{100} \cdot 10^6 + 18^{85}$?

Решение:

$$4^{100} \cdot 10^6 + 18^{85} \overset{11}{=} (4^{10})^{10} \cdot (-1)^6 + (-4)^{80+5} \overset{11}{=}$$

$$\overset{11}{=} 1 + \left((-4)^8\right)^{10} \cdot (-4)^5 \overset{11}{=} 1 - 4^5 = 1 - 2^{10} \overset{11}{=} 0$$