Лекция 6. Китайская теорема об остатках. Алгебраические структуры. Таблица Кэли

#вшпи #дискретная_математика #теория #теория_чисел

Автор конспекта: Гридчин Михаил

Китайская теорема об остатках

Теорема (Китайская теорема об остатках). Пусть $a_1, a_2, \dots, a_n$ - попарно взаимно простые числа, $r_1, r_2, \dots, r_n : 0 \le r_i < a_i$. Тогда

$$\exists N : \forall i \in \{1, 2, 3, \dots, n\} \implies N \equiv r_i \pmod{a_i}$$

Если N_1 и N_2 - решения системы сравнений, то $N_1 \equiv N_2 \pmod{a_1 \cdot a_2 \cdot \dots \cdot a_n}$.

☐ Докажем по индукции по n.
База. $n = 1$. Очевидно, $\exists N_1 : N_1 \equiv r_1 \pmod{a_1}$ и
$\exists N_2 : N_2 \equiv r_1 \pmod{a_1} \implies N_1 \equiv N_2 \pmod{a_1}$.
Шаг. Пусть утверждение верно для $n \le k$. Рассмотрим $n = k + 1$. По предположению системы существует решение системы x:

$$\begin{cases} x \equiv r_1 \pmod{a_1} \\ x \equiv r_2 \pmod{a_2} \\ \dots \\ x \equiv r_k \pmod{a_k} \end{cases} \quad \exists N \text{ - решение системы}$$

Положим $d := a_1 \cdot a_2 \cdot \dots \cdot a_k$. По условию теоремы $(d, a_{k+1}) = 1$. Выпишем следующие числа:

$$N \quad N + d \quad N + 2d \quad \dots \quad N + (a_{k+1} - 1)d$$

Все эти числа дают разные остатки при делении на a. Действительно, положим, что это не так и существуют два числа $N + di$ и $N + dj$, которые дают одинаковый остаток при делении на a. Но тогда $(N + di) - (N + dj) \equiv 0 \pmod{a_{k+1}} \implies d(i - j) \equiv 0 \pmod{a_{k+1}}$. Но $(d, a_{k+1}) = 1 \implies i - j \equiv 0 \pmod{a_{k+1}} \implies i \equiv j \pmod{a_{k+1}} \implies i = j$. Так как $i, j < a_{k+1}$. Значит среди всех этих чисел представлены все остатки от деления на a_{k+1}, в том числе и r_{k+1}
Пусть оно имеет вид $N + jd \equiv r_{k+1} \pmod{a_{k+1}}$. Теперь, если мы рассмотрим все остатки этого числа $N + jd$ на все остальные числа $a_1, a_2, \dots, a_k$, то поскольку $d \mid a_i$, то $N + jd \equiv r_i \pmod{a_i}, \forall i \le k$. То есть $N + jd$ всё ещё подходит. Мы доказали первую часть теоремы, так как смогли предъявить такое подходящее число $N' := N + jd$. Докажем

теперь вторую часть теоремы. Рассмотрим два различных решения N_1, N_2, тогда из формулировки теоремы следует, что

$$\begin{cases} N_1 \equiv r_i \pmod{a_i} \\ N_2 \equiv r_i \pmod{a_1} \end{cases} \implies N_1 - N_2 \equiv 0 \pmod{a_i}$$

Получаем требуемое:

$$\begin{aligned} N_1 - N_2 \mid d \\ N_1 - N_2 \mid a_{k+1} \end{aligned} \implies N_1 - N_2 \mid d \cdot a_{k+1} \quad ((d, a_{k+1}) = 1)$$

■

Алгебраические структуры

Пусть дано множество M и операция $\times$, определённая на нём. Будем работать только с такими операциями, которые не выводят за пределы множества, то есть $\forall a, b : a \in M, b \in M \implies a \times b \in M$.

Def. Пусть задано множество M и операция $\circ$, заданная на нём. Если выполнена ассоциативность, т.е.

$$a \circ (b \circ c) = (a \circ b) \circ c$$

То эту структуру назовём *полугруппой*.
Пример: слова из алфавита $\{0, 1\}$ и операция конкатенации, определённая на этом множестве.

Def. Полугруппу, у которой существует единственный нейтральный элемент, то есть

$$\exists! e : a \circ e = e \circ a = a$$

Назовём *моноидом*.
Пример: слова из алфавита $\{0, 1\} \cup \{\epsilon\}$ (пустое слово) и операцией конкатенации слов, определённой на этом множестве.
Свойство: можно записать уравнение вида $a \circ x = b$, но не всегда можно решить.

Def. Моноид, для каждого элемента которого существует единственный обратный элемент, то есть

$$\forall x \exists! y : x \circ y = y \circ x = e$$

Назовём *группой*.

Про группы будем говорить всю следующую часть семестра.

Пример решения уравнения:

$$x \circ a = b$$
$$x \circ a \circ a^{-1} = b \circ a^{-1}$$
$$x \circ e = b \circ a^{-1}$$
$$\boxed{x = b \circ a^{-1}}$$

Пример: повороты пространства вокруг центра координат

Пример: пусть $m \in \mathbb{Z}$. $M := \{0, 1, \dots, m-1\}$ с операцией $+_m$ (сложение по модулю m) образует группу. Стандартное обозначение $(\mathbb{Z}_m, +)$.

Пример: пусть $p \in \mathbb{N}$, p - простое. Тогда $M := \{1, 2, \dots, p-1\}$ с операцией $\times_p$ (умножение по модулю p) образует группу. Стандартное обозначение $(\mathbb{Z}_p \backslash \{0\}, \times)$. Действительно, по малой теореме Ферма $a^{p-1} \equiv 1 \pmod p \iff a^{p-2} \equiv a^{-1} \pmod p$. Следовательно, для каждого элемента множества есть существует обратный элемент. (нейтральный элемент - 1)

Пример: рассмотрим M - множество перестановок (биекций) длины n. Обозначение перестановки:

$$\pi := \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ i_1 & i_2 & i_3 & \dots & i_n \end{pmatrix}, \quad \pi(j) = i_j$$

Определим операцию "композиция перестановок" на M ($\circ$) следующим образом:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ i_1 & i_2 & i_3 & \dots & i_n \end{pmatrix}, \quad \pi' = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ j_1 & j_2 & j_3 & \dots & j_n \end{pmatrix}$$
$$\pi \circ \pi' = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \pi(\pi'(1)) & \pi(\pi'(2)) & \pi(\pi'(3)) & \dots & \pi(\pi'(n)) \end{pmatrix}$$

Нейтральный элемент

$$e =: id := \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & 2 & 3 & \dots & n \end{pmatrix}$$

Обратный элемент

$$y = x^{-1} \iff y(x(i)) = i$$

Заметим, что поскольку функция $x(i)$ биективна, то она обратима, то есть $\forall x \exists! y = x^{-1} \implies$ это группа.

Свойство: можно решить уравнение вида $a \circ x = b$.

Def. *Кольцо* $(M, +, \times)$ - это

1. коммутативная группа по сложению (то есть $+$ также коммутативен).
2. ассоциативна по $\times$
3. дистрибутивна $a \times (a + c) = a \times b + a \times c$.

   Пример: $(\mathbb{Z}_m, +, \times)$ - кольцо.

Пример: $(\mathbb{Z}_2, \oplus, \wedge)$. Коммутативно по $\oplus$, нейтральный элемент - 0, обратный элемент - само число. Ассоциативна по $\wedge$. Также $(a \oplus b) \wedge c = a \wedge c \oplus b \wedge c \implies$ кольцо.
Свойство: можно записать уравнение вида $a \times x + b = c$, но не всегда можно решить. Чтобы уравнение можно было решить, нужно определение поля.

Def. *Поле* $(M, +, \times)$ - это

1. коммутативная группа по $+$
2. $M \backslash \{0\}$ - коммутативная группа по $\times$
3. $a \times (b + c) = a \times b + a \times c$
   Пример: множества $\mathbb{Q}, \mathbb{R}, \mathbb{C}, (\mathbb{Z}_p, +, \times)$ - поля.

Конечные группы

Def. *Порядок группы* - количество элементов в ней.
Def. *Мультипликативная запись*:

$$
\begin{gathered}
(a \circ b) \circ c = a \circ (b \circ c) \\
\exists ! e := 1 \\
a \circ 1 = 1 \circ a = a \\
\forall x \exists ! x^{-1} \\
x \circ x^{-1} = x^{-1} x = 1
\end{gathered}
$$

Def. *Аддитивная запись*:

$$
\begin{gathered}
(a + b) + c = a + (b + c) \\
\exists ! e := 0 \\
a + 0 = 0 + a = a \\
\forall x \exists ! (-x) \\
x + (-x) = (-x) + x = 0
\end{gathered}
$$

Пример. Группы порядка k: $(\mathbb{Z}_k, +)$.

Def. *Таблица Кэли* - таблица для записи результатов применения операции ко всем парам элементов

Пример: таблица Кэли для группы порядка 2. В ней обязательно должен быть нейтральный элемент e и оставшийся элемент $a \neq e$. Заметим, что вариант может быть всего один, поскольку $ae = a, ea = a, ee = e$, остаётся только aa, значит, a - обратный элемент для $a \implies aa = e$

$$
\begin{array}{c|cc}
\circ & e & a \\
\hline
e & e & a \\
a & a & e
\end{array}
$$

Значит, любые группы порядка 2 изоморфны (см. далее).

Пусть теперь $n = 3$. По аналогии заполним:

$$\begin{array}{c|ccc} \circ & e & a & b \\ \hline e & e & a & b \\ a & a & b & e \\ b & b & e & a \end{array}$$