① Китайская теорема об остатках

Рассмотрим следующую систему сравнений:

$$x \equiv a_i \pmod{m_i}, \quad i = \overline{1,n} \qquad (1)$$

Лемма. Пусть $x_0 \in \mathbb{Z}$ – решение системы (1). Тогда множество целых чисел, удовлетворяющих (1), совпадает с классом вычетов

$$x \equiv x_0 \pmod{M},$$

$$M = \text{НОК}\,[m_1, \ldots, m_n]$$

Док-во. Достаточность:

пусть $x \equiv x_0 \pmod{M}$, тогда $x = x_0 + kM$, где $M$ кратно любому $m_i$, поэтому

$$x \equiv x_0 \equiv a_i \pmod{m_i},$$

то есть является решением системы (1)

Необходимость:

пусть $x$ – решение (1), тогда

$$x \equiv a_i \equiv x_0 \pmod{m_i},$$

поэтому $(x-x_0)$ кратно любому $m_i$, т.е. $(x-x_0)$ – общее кратное $m_1, \ldots, m_n$, поэтому $(x-x_0)$ делится на $M$, поэтому $x \equiv x_0 \pmod{M}$.

---

Дополнительные главы фундаментальной математики

Пашко Я.А. 2021 Билет №5

Scanned by TapScanner

Китайская теорема об остатках. Пусть $m_i$ попарно взаимно простые. Тогда система (1) имеет решение и оно определяется следующим образом. Пусть

$$M = \prod_i m_i, \quad M_i = \frac{M}{m_i}, \quad i = \overline{1,n}.$$

Найдём $b_i$, удовлетворяющие сравнения

$$M_i b_i \equiv a_i \pmod{m_i}, \quad i = \overline{1,n} \qquad (2)$$

Тогда множество целых чисел, удовлетворяющих (1), совпадает с классом вычетов

$$x \equiv (M_1 b_1 + \dots + M_n b_n) \pmod{M}$$

Док-во. Т.к. модули $m_i$ попарно взаимно простые, то $M = \text{нок}\{m_1, \dots, m_n\}$. Поэтому достаточно доказать, что $x_0 = M_1 b_1 + \dots + M_n b_n$ удовлетворяет (1).

Т.к. модули $m_i$ попарно взаимно простые, то $\text{нод}(M_i, m_i) = 1$ $\Rightarrow$ существуют $b_i$, удовлетворяющие (2). Для любого $i$

$m_i \mid M_j \ (j \neq i)$, поэтому

$$x_0 \equiv M_i b_i \equiv a_i \pmod{m_i},$$

т.е. $x = x_0$ — решение (1)

---

Дополнительные главы фундаментальной математики

Пачко Ф.А. 202/1 Билет №5

Scanned by TapScanner

(2) Алгоритм нахождения жордановых форм над полем комплексных чисел и над полем разложения характеристического многочлена в случае полей Галуа

Идея: для любой матрицы над полем P существует некоторый (жорданов) базис, в котором эта матрица имеет наиболее простой вид, а именно:

$$J = P^{-1} A P,$$ где A – матрица,

P – матрица перехода к новому базису,

J – жорданова форма,

J имеет вид $\begin{bmatrix} J_1 & & 0 \\ & J_2 & \\ 0 & & \ddots \; J_k \end{bmatrix}$, где $J_i$ – жордановы блоки

$J_i = \begin{bmatrix} \lambda_i & p_1 & & 0 \\ & \ddots & p_2 & \\ 0 & & \ddots & \lambda_i \end{bmatrix}$, где $p_j$ – нули или единицы.

Алгоритм поиска жордановой формы:

1) Найти все собственные числа $\lambda_i$ с их кратностями $a_i$

2) Для каждого собственного числа $\lambda_i$ найти $r_i$ количество собственных векторов для него

3) Для каждого собственного числа $\lambda_i$ заполнить жорданову клетку $J_i$: на главной диагонали стоит значение $\lambda_i$, на второй диагонали стоит $(a_i - r_i)$ единиц, все остальные элементы нулевые

4) Объединить жордановы блоки $J_i$

---

Дополнительные главы фундаментальной математики

Пасько В. А. 2021 Билет №5

Scanned by TapScanner

3) $\begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 5 \pmod 7 \\ x \equiv 7 \pmod 9 \end{cases}$

Согласно китайской теореме об остатках, решение представляется в виде

$$x = \left(\sum_i M_i b_i\right) \pmod M, \text{ где}$$

$M = 5 \cdot 7 \cdot 9 = 315$, $M_1 = \frac{M}{5} = 63$, $M_2 = 45$, $M_3 = 35$,

а $b_i$ – решения сравнений

$$63 b_1 \equiv 3 \pmod 5$$
$$45 b_2 \equiv 5 \pmod 7$$
$$35 b_3 \equiv 7 \pmod 9$$

Т.к. НОД$(63, 5) =$ НОД$(45, 7) =$ НОД$(35, 9) = 1$, то каждое из уравнений имеет только 1 решение. Найдём эти решения через обратные элементы:

$\frac{63}{5} = [12; \frac{5}{3}] = [12; 1, \frac{3}{2}] = [12; 1, 1, 2]$

| $q_i$ | | 12 | 1 | 1 | 2 |
|---|---|---|---|---|---|
| $Q_i$ | 0 | 1 | 1 | $\boxed{2}$ | 5 |

$n = 3$

$b_1 = 3 \cdot 2 \cdot (-1)^{n-1} = +6$

$\frac{45}{7} = [6; \frac{7}{3}] = [6; 2, 3]$

| $q_i$ | 0 | 6 | 2 | 3 |
|---|---|---|---|---|
| $Q_i$ | 0 | 1 | $\boxed{2}$ | 7 |

$n = 2$

$b_2 = 5 \cdot 2 \cdot (-1)^{2-1} = -10$

$\frac{35}{9} = [3; \frac{9}{8}] = [3; 1, 8]$

| $q_i$ | | 3 | 1 | 8 |
|---|---|---|---|---|
| $Q_i$ | 0 | 1 | $\boxed{1}$ | 9 |

$n = 2$

$b_3 = 7 \cdot 1 \cdot (-1)^{2-1} = -1$

$x \equiv (6 \cdot 63 - 10 \cdot 45 - 1 \cdot 35) \pmod{315} = -317 \pmod{315} =$
$= 313 \pmod{315}$

Пасько Д.А. 2021/1 Билет №5

Scanned by TapScanner