Китайская теорема об остатках

Прямое произведение колец

$A_1, A_2, \ldots, A_n$

$$A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid \forall i \; a_i \in A_i\}$$

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$$

прямое произведение абелевых групп это абелева группа с нулём

$$0 = (0, \ldots, 0)$$

если A_i - кольца, то можно задать умножение:

$$(a_1 \ldots a_n)(b_1 \ldots b_n) = (a_1 b_1, a_2 b_2, \ldots, a_n b_n)$$

получится кольцо. Если у каждого A_i есть 1, то

$(1, \ldots, 1)$ - это единица

в прямом произведении.

Замечание: Семейство может быть не обязательно конечно

Можно рассмотреть любое множество полей A_x, $x \in X$.

$$\prod_{x\in X} A_x \text{ — это семейства}$$

$$(a_x)_{x\in X}, \quad a_x \in A_x \ \forall x \in X.$$

Функции $\mathbb{R} \longrightarrow \mathbb{R}$ — это

$$\prod_{x\in\mathbb{R}} \mathbb{R}_x \qquad f:\mathbb{R}\to\mathbb{R}$$

$$\Big\downarrow$$

$$(a_x)=(f(x))_{x\in\mathbb{R}}$$

операции на прямом произведении — поточечное сложение и умножение функций.

В частности, в $\prod A_i$ всегда есть делители нуля

$$\begin{array}{r}(1,1,0,0)\\ \times\ (0,0,1,1)\end{array} = (0,0,0,0)$$

Теорема (КТО): Если числа $n_1, \dots, n_m \in \mathbb{Z}$ попарно взаимно-просты, и $n = n_1 \cdot \ldots \cdot n_m$ — их произведение, то имеется изоморфизм колец:

$$\mathbb{Z}/(n) \xrightarrow{\psi} \frac{\mathbb{Z}}{(n_1)} \times \frac{\mathbb{Z}}{(n_2)} \times \dots \times \frac{\mathbb{Z}}{(n_m)}$$

$$[k]_n \longmapsto ([k]_{n_1}, [k]_{n_2}, \dots, [k]_{n_m})$$

Док-во: ψ корректно определён

$$[k_1]_n = [k_2]_n \Rightarrow [k_1]_{n_i} = [k_2]_{n_i} \quad \forall i$$

$$\psi([k_1] + [k_2]) = \psi([k_1]) + \psi([k_2])$$

$$\psi([k_1][k_2]) = \psi([k_1])\psi([k_2])$$

$$[k_1]_n + [k_2]_n = [k_1 + k_2]_n \longmapsto$$

$$\begin{array}{ccc} \to ([k_1+k_2]_{n_1}, & \dots, & [k_1+k_2]_{n_m}) \\ \| & & \| \\ ([k_1]_{n_1} + [k_2]_{n_1}, & \dots, & [k_1]_{n_m} + [k_2]_{n_m}) \\ & & \| \end{array}$$

$$\underset{\varphi([k_1]_n)}{\underset{\parallel}{([k_1]_{n_1}, \dots, [k_1]_{n_m})}} + \underset{\varphi([k_2]_n)}{\underset{\parallel}{([k_2]_{n_1}, \dots, [k_2]_{n_m})}}$$

φ инъективен, поскольку $\ker \varphi = 0$

$$[k] \hookrightarrow (0, \dots, 0).$$

k делится на $n_1, n_2, \dots, n_k$

т.к. они попарно взаимно просты, k делится и на их произведение

($a|c$, $b|c$ и $\text{НОД}(a,b)=1 \Rightarrow ab|c$)

т.е. $[k]_n = 0$.

Сюръективность следует из того, что в $\mathbb{Z}/(n)$ и в $\frac{\mathbb{Z}}{(n_1)} \times \frac{\mathbb{Z}}{(n_2)} \times \dots \times \frac{\mathbb{Z}}{(n_m)}$ одинаковое число элементов

$$n = n_1 \times n_2 \times \dots \times n_m$$

теорема доказана

На житейском языке: ∀ набора остатков $r_1, \dots, r_m$ по модулю $n_1, \dots, n_m$ соответственно можно подобрать такое число $k \in \mathbb{Z}$, что $k \equiv r_i \bmod n_i$ сразу для всех i, причём ∀ двух таких чисел k_1, k_2 разность $(k_1 - k_2) \vdots n$.

Как явно найти k?

Сначала надо найти такие числа $l_1, \dots, l_m$, которые дают наборы

остатков $(1, 0, \dots, 0)$ для l_1
$(0, 1, \dots, 0$ для l_2
$\vdots$
$(0, \dots, 0, 1)$ для l_m

Если мы нашли такие l_i, что

$$l_i \equiv \begin{matrix} 1 \pmod{n_i} \\ 0 \pmod{n_j} \ \forall j \neq i \end{matrix}$$

Для любого набора остатков
$r_1, \dots, r_m$ можем взять
$$k = r_1 \cdot l_1 + r_2 l_2 + \dots + r_m l_m$$

[Как искать l_i?

положим $q_i = \prod\limits_{j \neq i} n_j = \frac{n}{n_i}$

произведение всех n_j кроме n_i

НОД$(n_i, q_i) = 1 \Rightarrow \exists\, x_i, y_i$:

$$\boxed{x_i n_i + y_i q_i = 1}$$

$l_i = y_i q_i$ — делится на $q_i = \prod\limits_{j \neq 1} n_j$

$l_i \equiv 1 \pmod{n_i}$

Кольца многочленов
и кольца вычетов, которые
из них получаются

K - любое кольцо

многочлен

$K[x] = \{a_0 + a_1 x + a_2 x^2 + \dots + a_m x^m\}$

где x - формальный символ

$a_i \in K$.

формальный степенной ряд

$K[[x]] = \{a_0 + a_1 x + a_2 x^2 + \dots$ вообще говоря, бесконечная$\}$

$a_i \in K$

$(a_0, a_1, a_2, \dots)$

что-то типа бесконечной десятичной

$A = a_0 + a_1 x + a_2 x^2 + \dots$ $\quad B = b_0 + b_1 x + b_2 x^2 + \dots$

$S = A + B =$

$= s_0 + s_1 x + s_2 x^2 + \dots$

$P = AB =$

$= p_0 + p_1 x + p_2 x^2 + \dots$

$s_i = a_i + b_i$

$p_0 = a_0 b_0$

$p_1 = a_0 b_1 + a_1 b_0$

$\dots$

$$p_k = a_0 b_k + a_1 b_{k-1} + \ldots + a_k b_0$$

Будем называть алгебраической операцией над формальными рядами такую операцию $f_1, \ldots, f_n \longmapsto f$, что для вычисления каждого к-та у f надо совершить конечное число арифметических действий.

Пример: Обращение. Пусть K - комм. кольцо с 1. Тогда ряд

$A = a_0 + a_1 x + a_2 x^2 + \ldots$ обратим $\Leftrightarrow$ в $K[[x]]$

a_0 обратим в K.

$$(a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \ldots) \cdot (b_0 + b_1 x + b_2 x^2 + \ldots) = 1$$

при x^0 $\quad a_0 b_0 = 1$

при x^1 $\quad a_0 b_1 + a_1 b_0 = 0$

. . . . .

при x^k $\underline{a_0b_k + a_1b_{k-1} + \ldots + a_kb_0 = 0}$

если ряд B существует $\Rightarrow$ a_0 обратим.

наоборот: если a_0 обратим в K

получаем: $b_0 = a_0^{-1}$

$$b_k = -a_0^{-1}(\underbrace{a_1b_{k-1} + \ldots + a_kb_0}_{\text{уже есть}})$$

Подставлять в ряд число $\alpha \in K$ нельзя.

Единственное исключение:

$f(0) = a_0$ $\quad$ $f = a_0 + a_1x + a_2x^2 + \ldots$

Самый левый ненулевой a_i наз. младшим коэфф-том.

$$(a_ix^i + \ldots)(b_jx^j + \ldots)$$

$a_i, b_j \neq 0$

если $a_ib_j \neq 0$ в K $\Rightarrow$ a_ib_j — это младший к-т в произведении.

Если в K нет делителей нуля, то и в $K[[x]]$ тоже нет делителей нуля.

$K[x] \subset K[[x]]$

если $f = a_0 + a_1 x + \dots + a_n x^n$ многочлен и $a_n \neq 0$

то n называется степенью

$$\deg f := n$$

a_n – старший коэф-т.

если в K нет делителей нуля, то

$$(a_0 + \dots + a_n x^n)(b_0 + \dots + b_m x^m) =$$

$$= \dots \underbrace{a_n b_m}_{\text{старший к-т}} x^{n+m}$$

т. е. $\boxed{\deg fg = \deg f + \deg g}$

обратимы в $K[x]$ только обратимые константы (= многочлены степени нуль)

Если f, g - два многочлена и старший коэфф-т у g обратим в K

то $\exists$ многочлены $q, r \in K[x]$:

$$(1) \quad f = \underset{\text{неполное частное}}{q} \cdot g + \underset{\text{остаток от деления } f \text{ на } g}{r}$$

(2) либо $r = 0$

либо $\deg r < \deg g$

Если в K нет делителей нуля, то такие q и r единственны для данных f и g.

$$\overbrace{a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0}^{f} \; \underline{\big|\, \overset{g}{b_m x^m + \ldots}}$$

если $m > n$, то $q = 0$, $r = f$ годится

$$f = 0 \cdot g + f$$

если $m \leq n$ $\quad f$

$$\begin{array}{l|l} \; a_n x^n + \dots & b_m x^m + \dots \\ \cline{2-2} -\; a_n x^n + \dots & a_n b_m^{-1} x^{n-m} + \\ \cline{1-1} \end{array}$$

многочлен
степени $< n$

Делим пока степень разности не станет меньше m.

$$q_1 g + r_1 = q_2 g + r_2$$

$$(q_1 - q_2) \cdot g = \underbrace{r_1 - r_2}$$

$$\deg \geq \deg g \;\Big|\; \deg < \deg g$$

$$q_1 - q_2 = 0 \qquad r_1 - r_2 = 0$$