Введение в р-адич. анализ.

Глава I: Элементарная теория чисел.

§1. Диофантовы уравнения:

def: уравнения, в которых неизвестные величины выр. целыми числами наз. диофантовыми.

↳ Диофант жил в III веке н.э. и написал „Арифметику" → там обсужд. решение ур. в $\mathbb{Z}$ и в $\mathbb{Q}$.

Рассмотрим сначала простейшее уравнение

$$ax + by = c$$

(такие наз. линейными).

Ex) Сколько решений у уравнений:

- $19x + 12y = 1$

  ↳ беск; $x = -5 + 12t$; $y = 8 - 19t$, $t \in \mathbb{Z}$.

- $2x - 6y = 3$

  ↳ не имеет решений (левая часть чётная, правая – нечётная).

Th Уравнение $ax + by = c$ $(a, b, c \in \mathbb{Z})$ разрешимо тогда и только тогда, когда $\gcd(a,b) \mid c$.

В случае разрешимости решений беск. много,

Все они имеют вид:
$$\begin{cases} x = x_0 + \dfrac{b}{\gcd(a,b)} t \\[2ex] y = y_0 - \dfrac{a}{\gcd(a,b)} t \end{cases}, \quad t \in \mathbb{Z} \quad (*)$$

где $(x_0, y_0) \in \mathbb{Z}^2$ – фикс. решение.

Д-во: Пусть (x_0, y_0) – решение.

$\gcd(a,b) \mid a$, $\gcd(a,b) \mid b \Rightarrow \gcd(a,b) \mid a x_0 + b y_0 = c$.

С другой стороны, если $\gcd(a,b) \mid c$, то по Th о линейном предст. gcd

Th Пусть $a, b \in \mathbb{Z}$. Тогда $\exists u, v \in \mathbb{Z}$: $au + bv = \gcd(a,b)$.

(докажем для идеалов в кольце.)

$\gcd(a,b) \mid c \Leftrightarrow \exists k \in \mathbb{Z}: \quad c = k \cdot \gcd(a,b)$

Тогда $\underbrace{a(u \cdot k)}_{x_0} + \underbrace{b(v \cdot k)}_{y_0} = c$ – решение.

(Есть другое д-во по индукции).

То, что (*) – решения проверяется подстановкой.

Покажем, что других решений не бывает.

Пусть (x_0, y_0) – решение описанного вида, а (x_1, y_1) – какое-то другое.

$$\begin{cases} a x_1 + b y_1 = c \\ a x_0 + b y_0 = c \end{cases} \Rightarrow a(x_1 - x_0) = b(y_0 - y_1)$$

Предст. в виде $a = \gcd(a,b) \cdot r$, $b = \gcd(a,b) \cdot s$, где $\gcd(r,s) = 1$

$\rightsquigarrow r \gcd(a,b)(x_1 - x_0) = \gcd(a,b)\, s(y_0 - y_1)$

$\Leftrightarrow r(x_1 - x_0) = s(y_0 - y_1)$

$$\begin{cases} s \mid r(x - x_0) \\ \gcd(s, r) = 1 \end{cases} \Rightarrow s \mid (x - x_0) \Leftrightarrow \exists t \in \mathbb{Z}: x - x_0 = st$$

Мы получили, что $x_1 = x_0 + st = x_0 + \frac{b}{\gcd(a,b)} t, \ t \in \mathbb{Z}$.

$(b = s \cdot \gcd(a,b))$.

Подставим это в $a(x_0 - x_1) = b(y_1 - y_0)$ и получим нужное.

$\square$.

Ясно, что на практике мы просто делаем алгоритм Евклида и лин. предст. gcd.

Тут интересно, что алгоритм Евклида записывается в матричной форме.

Напоминание: алгоритм Евклида:

$$a = r_0 = b q_1 + r_2, \quad 0 \le r_2 < b$$

$$b = r_1 = r_2 q_2 + r_3, \quad 0 \le r_3 < r_2$$

$$\vdots$$

$$r_{n-2} = r_{n-1} q_{n-1} + r_n, \quad 0 \le r_n < r_{n-1}$$

$$r_{n-1} = r_n q_n$$

Запишем в матричной форме:

$$A_i = \begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix}; \quad i = 1, \dots, n-1.$$

Тогда $\begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix} = A_i \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix}, \quad i = 1, \dots, n-1.$

Отсюда имеем:

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} r_0 \\ r_1 \end{pmatrix} = A_1 \cdot \ldots \cdot A_{n-1} \begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix}$$

К матрице $\begin{pmatrix} \alpha & 1 \\ 1 & 0 \end{pmatrix}$ легко написать обратную:

$\rightsquigarrow \begin{pmatrix} 0 & 1 \\ 1 & -\alpha \end{pmatrix}$ (легко проверить).

Отсюда, если $B_i = A_i^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix}$.

Тогда $\begin{pmatrix} r_n \\ r_{n-1} \end{pmatrix} = \underbrace{B_{n-1} \cdot \ldots \cdot B_1}_{\substack{\parallel \\ B = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}}} \begin{pmatrix} a \\ b \end{pmatrix}$.

$\begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix} = B \begin{pmatrix} a \\ b \end{pmatrix} \Rightarrow r_n = \gamma a + \delta b.$

Так можно совершенно прикладным образом перемножать матрицы и находить лин. предст. gcd.

Итак, перейдём к общ. случаю. Расм. систему:

$$\begin{cases} a_{11} x_1 + \ldots + a_1 x_n = b_1 \\ \vdots \\ a_m x_1 + \ldots + a_{mn} x_n = b_m \end{cases}$$

↙ тут все уравнения диофантовы.

$(u\ a_{ij}, b_i \in \mathbb{Z})$.

↳ с неб св. матрицы'

$A = [a_{ij}]_{i,j=1}^{m,n}$ и $B = (A|b)$, $b = (b_1 \ldots b_m)^T$.

$\uparrow$ матрица системы $\qquad\qquad$ $\uparrow$ расш. матрица системы.

$\rightsquigarrow$ $Ax = b$ (это наша система).

Тут можно также просто описать алгоритм, проверяющий разрешимость и строящий явную формулу.

Кратко: (подробнее — в теории колец).

Элем. преобр. — прибавить к одной строке другую, умн. на целое число.

Прим. такого преобр. $\Leftrightarrow$ умн. слева на матрицу из $SL_n(\mathbb{Z})$.

Если мы так делаем со столбцами, то это $\Leftrightarrow$ умн. справа на нек. матрицу из $SL_n(\mathbb{Z})$.

В итоге получим: $UAVy = Ub$

И решения этой и исх. системы взаимно-одн. соотв. решениям исходной по формуле $x = Vy$.

Действуя, как в алг. Евклида с помощью элем. преобр. можно привести матрицу к диаг. виду:

$$D = \begin{pmatrix} d_1 & 0 & & & \\ 0 & d_2 & & 0 & \\ & & \ddots & & \\ & 0 & & d_r & \dots \\ & & & \vdots & \end{pmatrix} \Rightarrow$$

система имеет вид:

$d_i y_i = c_i$, $i \le r$,
$c_i = 0$ для ост.

$\Rightarrow$ Критерий совм-сти системы: $d_i \mid c_i \; \forall i$.

Отсюда следует, что для совместности системы $Ax=b$ над $\mathbb{Z}$, чтоб система

$$Ax \equiv b \mod p^m$$

$\forall p \in \mathbb{P}, \forall m \in \mathbb{N}$

а это — совместность над $\mathbb{Z}_p$ $\forall p \in \mathbb{P}$.