1 P-адические числа

Вводный пример: Рассмотрим:

$$x^2 \equiv 2 \ (mod \ 7^n), \ n \in \mathbb{Z}_{\geq 1} \tag{1}$$

Пусть сначала:

$$] \ n = 1 : \ x^2 \equiv 2 \ (mod \ 7) \Rightarrow \ x = \pm \ 3 \ (7) \tag{2}$$

Пусть теперь:

$$] \ n = 2 : \ x^2 \equiv 2 \ (mod \ 49) \tag{3}$$

Ищем решение вида:

$$x_1 = x_0 + 7t; x_0 = 3 \Rightarrow \ (3 + 7t)^2 = 2 \ (7^2) \tag{4}$$

$$9 + 6 \cdot 7t + 7^2t^2 = 2 \ (7^2) \ \Rightarrow \tag{5}$$

$$7 + 6 \cdot 7t + 7^2t^2 = 0 \ (7^2) \ \Rightarrow \tag{6}$$

$$1 + 6t + 7t^2 = 0 \ (7) \ \Rightarrow \tag{7}$$

$$6t \equiv -1 \ (7) \ \Rightarrow \tag{8}$$

$$t_1 = 1 \ \Rightarrow \tag{9}$$

$$x_1 = x_0 + 7t = 3 + 7 = 10 \ (7^2) \tag{10}$$

Продолжим:

$$] \ n = 3 : \ x^2 \equiv 2 \ (mod \ 7^3) \tag{11}$$

Ищем:

$$x_2 = x_1 + 7^2t_2 \ (7^3) \tag{12}$$

И т.д.
Обратим внимание, что:

$$x_n \equiv x_{n-1} \ (7^n) \tag{13}$$

И что:

$$x_n^2 \equiv 2 \ (7^{n+1}) \tag{14}$$

Определение 1. *$\forall p-$простого, $\forall n \in \mathbb{Z}_{>0} \ \exists \ a : p^a | n, \ p^{a+1}$ не делит n, тогда $a = \nu_p(n)$, где $\nu_p(\cdot)$ - функция показатель.*

Определение 2. *Если $p-$простое, то последовательность $(x_n) = \{x_0, x_1, x_2, ...\}, \ x_n \in \mathbb{Z} \ \forall n$ и $x_n \equiv x_{n-1} \ (p^n), n \geq 1$ называется согласованной. Более того, две согласованных последовательности $(x_n), (x_n^{'})$ называются эквивалентыми, если $x_n \equiv x_n^{'} \ (p^{n+1}) \ \forall n$.*

Определение 3. *Множество классов эквивалентности назовем целыми $p-$адическими числами. Множество целых $p-$адических чисел будем обозначать $\mathbb{Z}_p$.*

В примере выше: $(x_0, x_1, ...) = \alpha, \ \alpha^2 = 2$. По сути: α это $7-$адический корень из 2.

Определение 4. *Последовательность (x_n) называется канонической, если $\forall n : 0 \leq x_n < p^{n+1}$ и $\overline{x_n} \equiv x_n \ (p^{n+1})$ и тогда $\overline{(x_n)} \sim (x_n)$.*

Лемма 1. *Различные канонические последовательности определяют различные $p-$адические целые числа.*

Доказательство. Пусть $(x_n) \sim \alpha$, - каноническая последовательность. Тогда $x_{n+1} = x_n + a_{n+1}p^{n+1}$

$$0 \leq x_{n+1} < p^{n+2} \tag{15}$$
$$0 \leq x_n < p^{n+1} \tag{16}$$
$$\Rightarrow 0 \leq a_{n+1} < p \tag{17}$$
$$x_n = a_0 + a_1 p + a_2 p^2 + ... + a_n p^n. \tag{18}$$

□

Лемма 2. *$\mathbb{Z}_p$ имеет мощьность континуум.*

Доказательство. Доказательство аналогично доказательству аналогичного утверждения для вещественных чисел в математическом анализе. □

Введем операции кольца (определим их как покоординатное сложение/умножение):

$$\alpha \sim (x_n), \beta \sim (y_n) \tag{19}$$
$$\alpha + \beta \sim (x_n + y_n) \tag{20}$$
$$\alpha \cdot \beta \sim (x_n \cdot y_n) \tag{21}$$

Лемма 3. *Предлагается доказать, что $\alpha + \beta$ и $\alpha \cdot \beta$ корректно введены.*

Лемма 4. *$\mathbb{Z}_p-$коммутативное кольцо с единицей без делителей нуля.*

Определение 5. *Пусть $\alpha, \beta \in \mathbb{Z}_p$. Будем обозначать $\alpha|\beta$, если $\exists \gamma \in \mathbb{Z}_p : \beta = \alpha\gamma$.*

Лемма 5. *$\alpha = (x_n) \in \mathbb{Z}_p-$обратимый $\iff x_0 \not\equiv 0 \ (p)$*

Доказательство.
Необходимость:
$\alpha-$ единичный (обратимиый) $\Rightarrow \exists \beta \in (y_n) : \alpha\beta = 1 \iff \forall n \ x_n y_n \equiv 1 \ (p^{n+1}); x_0 y_0 \equiv 1 \ (p) \Rightarrow x_0 \not\equiv 0 \ \forall n$.
Достаточночть:
$x_0 \not\equiv 0 \ (p)$; так как $x_n \equiv x_{n-1} \equiv ... \equiv x_0 \ (p) \ \Rightarrow x_n \not\equiv 0 \ (p) \ \Rightarrow x_n$ обратим по p. □

Теорема 1. *$\forall \alpha \in \mathbb{Z}_p/\{0\} : \alpha = p^m\epsilon$, причем такое разложение единственно, где ϵ является $p-$адическим обратимым числом, то есть $\epsilon \in \mathbb{Z}_p^*-$ множество обратимых элементов.*

Доказательство.
$] \ \alpha \not\equiv e \iff x_0 \not\equiv 0 \ (p) \ \alpha \not\equiv 0 \Rightarrow \exists m : x_m \not\equiv 0 \ (p^{m+1}) \ x_{m+s} \equiv x_{m-1} \equiv 0 \ (p^m) \ \forall s \Rightarrow y_s \equiv \frac{x_{m+s}}{p_m}-$целые числа $\in \mathbb{Z}$. Согласованность очевидна.
$y_0 = \equiv \frac{x_m}{p_m} \not\equiv 0 \ (p) \ (y_s) \sim \epsilon \ p^m y_s = x_{m+s} \equiv x_s \ (p^{s+1}) \ \alpha = p^m\epsilon$
Докажем единственность:
$\alpha = p^k\mu \ \mu \sim (\mathbb{Z}_s) \Rightarrow p^m\epsilon = p^k\mu \Rightarrow p^m y_s = p^k z_s \ (p^{s+1}) \ y_0, z_0 \not\equiv 0 \ (p) \Rightarrow s = m \Rightarrow p^m y_m \equiv p^k z_m \ (p^{m+1})$ Так как это выполняется для всех m, то $k = m$. $p^m y_{s+m} \equiv p^m z_{s+m} \ (p^{s+1}) \Rightarrow y_{s+1} \equiv z_{s+1} \Rightarrow \epsilon = \mu$ □

$\forall \alpha \in \mathbb{Z}_p \Rightarrow \alpha = p^m \epsilon \Rightarrow \nu_p(\alpha) = m \Rightarrow \nu_p(\alpha\beta) = \nu_p(\alpha) + \nu_p(\beta)$ Делаем вывод: подтягиваются все свойства показательной функции.

Теорема 2. $\alpha \equiv \beta\ (\gamma) \Longleftrightarrow \gamma|(\alpha - \beta) в\ \mathbb{Z}_p \Longleftrightarrow p^n|(\alpha - \beta)$. *Считаем, что* $\gamma = p^n \epsilon$

Поезность ввода $p-$адических чисел:
$i.\ \forall\ \alpha \in \mathbb{Z}_p :\ \exists\ a \in \mathbb{Z} :\ \alpha \equiv a\ (p^n)$. Тогда $a \equiv b\ (p^n) \Longleftrightarrow a \equiv b\ (p^n)$. В первом случае сравнение происходит в кольце целых $p-$адических чисел $\mathbb{Z}_p$, а во втором - в поле характеристики p^n : $\mathbb{F}_{p^n}$. То есть можно убрать "хвост"и получить обычное сравнение в кольце вычетов.