Mas afinal, quem são os inteiros p-ádicos?

Thiago & Thiago

Novembro de 2021

Disclaimers

¯_(ツ)_/¯

- ~~Solov~~ Thiago!
- Há 2^+ anos atrás...
- $\mathbb{Z}/n\mathbb{Z} = \{\text{inteiros mod } n\} = \{0, 1, \ldots, n-1\}$
- Pergunte!

Raízes em $\mathbb{Z}$

- Encontre um inteiro n tal que os primeiros 3 dígitos de n são os mesmos que os primeiros 3 dígitos de n^2

$$5^2 = 25$$
$$25^2 = 625$$
$$625^2 = 390625$$

- $625^2 \equiv 625 \pmod{10^3}$

$$\begin{aligned} 5^2 &\equiv 5 \pmod{10} \\ 25^2 &\equiv 25 \pmod{10^2} \\ 625^2 &\equiv 625 \pmod{10^3} \\ &\vdots \\ \ldots 6962890625^2 &\equiv \ldots 6962890625 \pmod{10^n} \end{aligned}$$

- $5^{2^k} \longrightarrow \ldots 6962890625$

Raízes em $\mathbb{Z}$

$$\begin{aligned} 5^2 &\equiv 5 \pmod{10} \\ 25^2 &\equiv 25 \pmod{10^2} \\ &\vdots \end{aligned}$$

- Começamos com uma raiz $n_1 = 5$ de $x^2 - x$ em $\mathbb{Z}/10\mathbb{Z}$
- Dada a raiz n_k em $\mathbb{Z}/10^k\mathbb{Z}$, $n_{k+1} = n_k^2$ é raiz em $\mathbb{Z}/10^{k+1}\mathbb{Z}$
- $n_k \equiv n_l \pmod{10^k}$ para $k \leqslant l$
- Queremos encontrar raízes inteiras de f com coeficientes inteiros
- Para $f = x^2 - x$ é fácil, mas e para $f = x^5 + 3x^3 - 4x^2 + 5x - 27$?

Lema (Hensel)

Se n_k é uma raiz simples de f em $\mathbb{Z}/p^k\mathbb{Z}$ então

$$n_{k+1} = n_k - \frac{f(n_k)}{f'(n_k)}$$

é raiz simples em $\mathbb{Z}/p^{k+1}\mathbb{Z}$ com $n_{k+1} \equiv n_k \pmod{p^k}$.

Raízes em $\mathbb{Z}$

- Encontrar uma raiz (simples) em $\mathbb{Z}/p\mathbb{Z}$ é suficiente para encontrar uma raiz em $\mathbb{Z}/p^k\mathbb{Z}$!
- $n_k = 5^{2^k}$ são raízes de $x^2 - x$ em $\mathbb{Z}/2^k\mathbb{Z}$ e $\mathbb{Z}/5^k\mathbb{Z}$
- Colagem de raízes
- Se $(n_k)_k$ é eventualmente constante então temos uma raiz inteira!

$$p^k \mid f(n), \forall k \implies f(n) = 0$$

- Mas vimos que

$$5^{2^k} \longrightarrow \ldots 6962890625$$

- $\ldots 6962890625$ não é uma raiz? Sim! Mas não é uma raiz inteira...
- $\ldots 6962890625$ tem uma quantidade infinita de dígitos não nulos!
- $\ldots 6962890625$ é um inteiro 10-ádico!

Os Inteiros n-ádicos

- Um inteiro 10-adico é um número cujos dígitos continuam infinitamente para a esquerda
  - $\ldots 6962890625 = 5 \cdot 10^0 + 2 \cdot 10^1 + 6 \cdot 10^2 + 0 \cdot 10^3 + \cdots$
  - $\ldots 0000000013 = 3 \cdot 10^0 + 1 \cdot 10^1 + 0 \cdot 10^2 + 0 \cdot 10^3 + \cdots$
- Podemos fazer o mesmo para n qualquer!
  - $\ldots 01100 = 0 \cdot 2^0 + 0 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3 + \cdots$ em base 2
  - $\ldots 0000c = 13 \cdot 16^0 + 0 \cdot 16^1 + 0 \cdot 16^2 + \cdots$ em base 16
  - $\ldots 11111 = 1 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^3 + \cdots$
- Os inteiros n-ádicos $\mathbb{Z}_n$ são os números da forma

$$\ldots a_2\, a_1\, a_0 = a_0\, n^0 + a_1\, n^1 + a_2\, n^2 + \cdots$$

  com $0 \leqslant a_i < n$
- $\mathbb{Z} \subseteq \mathbb{Z}_n$!
- Vamos focar em $\mathbb{Z}_p$ para p primo

Aritmética em $\mathbb{Z}_p$

- Podemos fazer contas com n-ádicos
- Como? Igual você fazia na quinta série!

$$\begin{array}{r} \ldots 696289062 + \\ \ldots 000000013 \\ \hline \ldots 696289075 \end{array}$$

$$\begin{array}{r} \ldots 696289062 \cdot \\ \ldots 000000013 \\ \hline \ldots 696289062 \\ \ldots 000000003 \cdot \\ \ldots 962890620 + \\ \ldots 000000001 \cdot \\ \hline \ldots 051757806 \end{array}$$

- E o menos? Queremos b tal que $a + b = 0$

$$\begin{array}{r} \ldots 111111111 + \\ \ldots 000000001 \\ \hline \ldots 000000000 \end{array}$$

$$\begin{array}{r} \ldots 696289062 + \\ \ldots 303710937 \\ \hline \ldots 999999999 \end{array}$$

- Inteiros 2-ádicos diretamente no seu computador
- Mas já passamos da quinta série...

Aritmética em $\mathbb{Z}_p$

- Como fazer a conta na prática? Podemos truncar!

$$\left(\sum_{i=0}^{n} a_i p^i\right) + \left(\sum_{i=0}^{n} b_i p^i\right) \longrightarrow \left(\sum_{i=0}^{\infty} a_i p^i\right) + \left(\sum_{i=0}^{\infty} b_i p^i\right)$$

$$\left(\sum_{i=0}^{n} a_i p^i\right) \cdot \left(\sum_{i=0}^{n} b_i p^i\right) \longrightarrow \left(\sum_{i=0}^{\infty} a_i p^i\right) \cdot \left(\sum_{i=0}^{\infty} b_i p^i\right)$$

$$\begin{aligned}
(p-1)(1+p+p^2+\cdots) &= \lim_{n\longrightarrow\infty} (p-1)(1+p+\cdots+p^{n+1}) \\
&= \lim_{n\longrightarrow\infty} p^{n+1} - 1 \\
&= \lim_{n\longrightarrow\infty} \ldots 010 \ldots 0 - 1 \\
&= \lim_{n\longrightarrow\infty} -1 \\
&= -1
\end{aligned}$$

- $\frac{1}{1-p} = 1 + p + p^2 + \cdots$ em $\mathbb{Z}_p$!

Aritmética em $\mathbb{Z}_p$

- Também podemos avaliar polinômios nos p-ádicos
- Vimos que $f(\ldots 6962890625) = 0$ para $f = x^2 - x$

Lema (Hensel)

Se n_1 é uma raiz simples de f em $\mathbb{Z}/p\mathbb{Z}$ então podemos garantir que existe uma raiz p-ádica.

- A raiz p-adica n será o limite de n_k tendendo a infinito
- Podemos encontrar raízes p-ádicas e conferir se elas são inteiras

A Geometria de $\mathbb{Z}_p$

- $v_p(\ldots a_2\, a_1\, a_0) = \min\{i : a_i \neq 0\}$
- $|a|_p = \frac{1}{p^{v_p(a)}}$
- $d(a,b) = |a-b|_p$
- $5^{2^k} \longrightarrow \ldots 6962890625$ em $\mathbb{Z}_{10}$!
- É aqui que mora a graça...
  $\mathbb{C} \ncong \overline{\mathbb{Q}_p}$

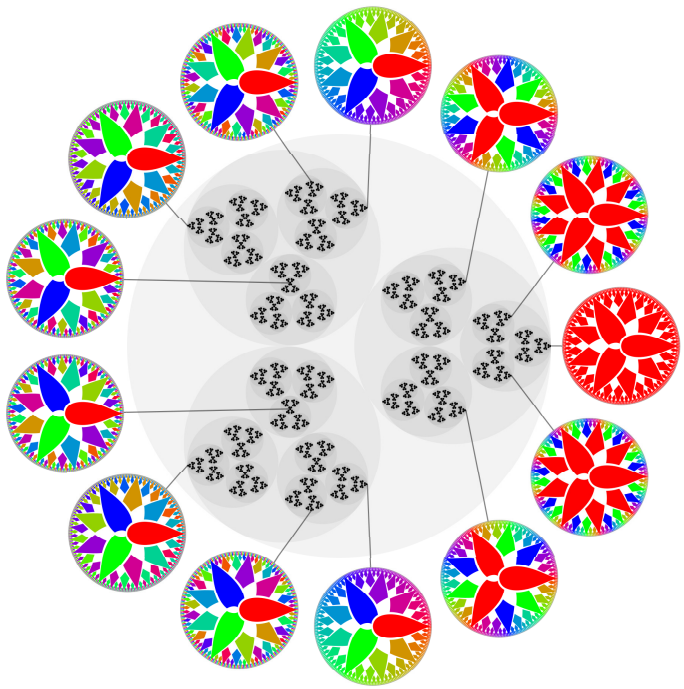
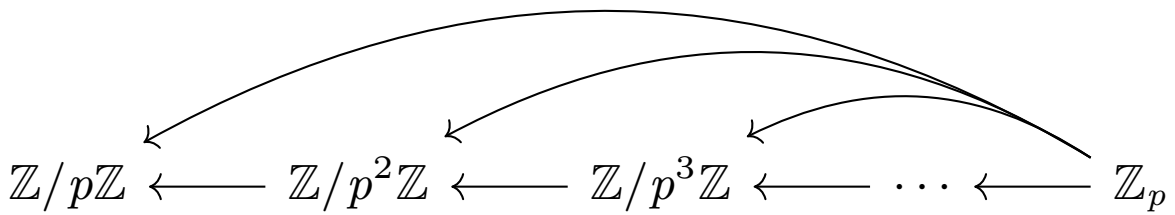


Figure: A geometria de $\mathbb{Z}_3$

Grupos Profinitos

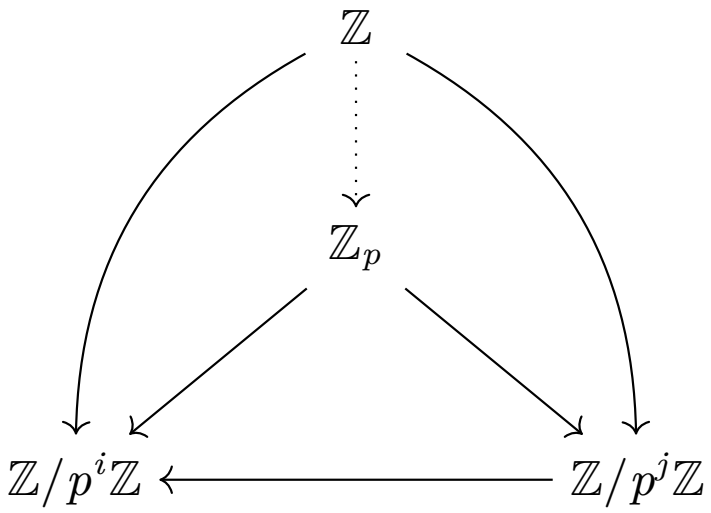
- O contexto geral...

$$\pi_i^j : \mathbb{Z}/p^j\mathbb{Z} \longrightarrow \mathbb{Z}/p^i\mathbb{Z} \qquad \pi_k : \mathbb{Z}_p \longrightarrow \mathbb{Z}/p^k\mathbb{Z}$$
$$\overline{a} \longmapsto \overline{a} \qquad \ldots a_2\, a_1\, a_0 \longmapsto a_{k-1} \ldots a_1\, a_0$$



- $\mathbb{Z}_p$ é o *menor* grupo que projeta em todos os $\mathbb{Z}/p^k\mathbb{Z}$
- $\mathbb{Z}_p$ pode ser *aproximado* por partes finitas e discretas

Grupos Profinitos



- Posso trocar $\mathbb{Z}$ por X qualquer!
- Posso trocar $\mathbb{Z}/p^i\mathbb{Z}$ por G_i qualquer!
- Grupos profinitos!

$$G = \varprojlim_i G_i$$

$$\mathbb{Z}_p = \varprojlim_k \mathbb{Z}/p^k\mathbb{Z}$$

$$\hat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z}$$

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = \varprojlim_{K/\mathbb{Q}} \mathrm{Gal}(K/\mathbb{Q})$$