2021年8月10日 11:59

p-adic 方程与 Hensel 引理

$\mathbb{Q} \subset \mathbb{Q}_p$

$\mathbb{Q} \subset \mathbb{R} = \mathbb{Q}_\infty$

有限域上解方程

=

大致 结论：

在 $\mathbb{Z}_p$ 中解多项式方程 $\Longleftrightarrow$ 在 $\mathbb{Z}/p\mathbb{Z}$, $\mathbb{Z}/p^2$, $\mathbb{Z}/p^3$, $\cdots$ 中解同余方程

p-adic 分析 $\longleftrightarrow$ 初等数论

$\Uparrow$ $\Downarrow$

$\mathbb{Z}$ 中解方程 有解 $\Longrightarrow$ $\forall n$ $\mathbb{Z}/n\mathbb{Z}$ 也有解

---

lem $\cdots \to D_n \xrightarrow{\phi_n} D_{n-1} \to \cdots \to D_1$ 射影系统 $D = \varprojlim_n D_n \subset \prod D_n$

若 $D_n \neq \phi$ 且有限，则 $D \neq \phi$

Pf. 若 ϕ_n 全满射. 取 $x = (x_n) \in D$

$\exists x_1 \in D_1$ ϕ_2 满 $\exists x_2 \in D_2$ $\phi_2(x_2) = x_1$

$\cdots$ $\exists x_3 \in D_3$ $\cdots\cdots$

$\vdots$

一般情况. $\mathrm{Im}\left(D_{n+p} \to D_{n+p-1} \to \cdots \to D_n\right) = D_{n,p} \neq \phi$ 有限

固定 n. $D_{n,p} \supset D_{n,p+1} \supset \cdots$ 以 n 为主

即 $p \gg 0$ $\phi \neq D_{n,p} = D_{n,p+1} = D_{n,p+2} = \cdots$ 不依赖于 p.

E_n //

$$\begin{array}{ccc} \phi_n : D_n & \longrightarrow & D_{n-1} \\ \cup & & \cup \\ E_n & \longrightarrow\!\!\!\!\rightarrow & E_{n-1} \end{array}$$

$\phi \neq \varprojlim_n E_n \subset \varprojlim_n D_n$ #

记号 $f \in \mathbb{Z}_p[X_1, \cdots, X_m]$ $n \geq 1$

$f_n = f$ 在 $\mathbb{Z}_p/p^n[X_1, \cdots, X_m]$ 的像

$f_n = f$ 在 $\mathbb{Z}_p/p^n[X_1,\dots,X_n]$ 的像
$\Vert$
$\mathbb{Z}/p^n[X_1,\dots,X_n]$

Prop $f^{(i)} \in \mathbb{Z}_p[X_1,\dots,X_m]$ 以下等价

(1) $f^{(i)}$ 在 $\mathbb{Z}_p$ 中有公共解

(2) $\forall n\ge 1$ $f_n^{(i)}$ 在 $\mathbb{Z}/p^n$ 中有公共解

Pf: $D=\{f^{(i)}$ 在 $\mathbb{Z}_p$ 中公共解$\}$

$D_n=\{f_n^{(i)}$ 在 $\mathbb{Z}/p^n$ —— $\}$ 有限 且 $D=\varprojlim_n D_n$

(2)⇒(1) 由 lem.

(1)⇒(2) ✓ #

Rk 这并不表明 ($f_n^{(i)}$ 在 $\mathbb{Z}/p^n$ 中分别有解, 拼合是否一起就是 f 的解.)

上面是说 D 非空 并非构造性证明.

Def $x=(x_1,\dots,x_m)\in(\mathbb{Z}_p)^m$ 是本原的, 若某个 x_i 可逆 ($x_i\in\mathbb{Z}_p^\times$)

同理可定义 $(\mathbb{Z}/p^n)^m$ 中的本原元素/向量

Prop $f^{(i)}\in\mathbb{Z}_p[X_1,\dots,X_m]$ 齐次多项式, 以下等价.

(1) $f^{(i)}$ 在 $(\mathbb{Q}_p)^m$ 中有非平凡公共解

(2) $f^{(i)}$ 在 $(\mathbb{Z}_p)^m$ 中有非平凡本原公共解

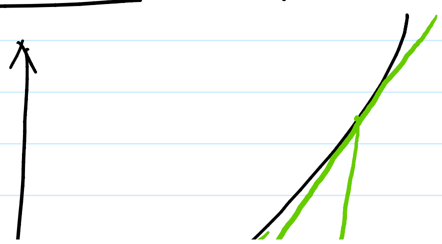
(3) $\forall n\ge 0$ $f_n^{(i)}$ 在 $(\mathbb{Z}/p^n)^m$ 中有非平凡本原公共解.

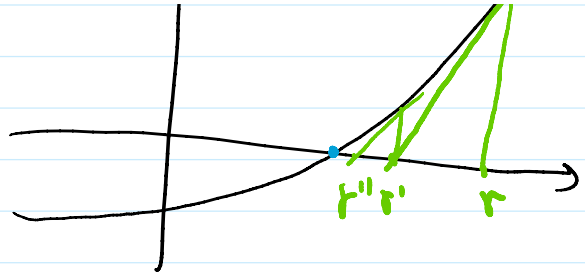
Pf (1)⇒(2) $h=\inf(v_p(x_1),\dots,v_p(x_m))$

令 $(y_1,\dots,y_m)=p^{-h}\cdot(x_1,\dots,x_m)$ 是本原的

(2)⟺(3) 几乎同上述方法. #

Newton 切线方法 $\mathbb{R}$. 求 $f(x)=0$ r, r', r''





Lem $f \in \mathbb{Z}_p[X]$ $x \in \mathbb{Z}_p$ $n, k \in \mathbb{Z}$ 使得

① $0 \le 2k < n$ $f(x) \equiv 0 \ (p^n)$ $\left(\Leftrightarrow |f(x)|_p \le \frac{1}{p^n}\right.$ x 近似解$)$

② $v_p(f'(x)) = k$ $(\Rightarrow f'(x) \not\equiv 0 \ (p)$ $f \bmod p$ 在 x 处光滑$)$

则 $\exists y \in \mathbb{Z}_p$ 使

$$\begin{cases} \checkmark\ f(y) \equiv 0 \ (p^{n+1}) \\ \checkmark\ v_p(f'(y)) = k \\ \checkmark\ y \equiv x \ (p^{n-k}) \end{cases} \qquad \left(|f(y)|_p \le \frac{1}{p^{n+1}} \quad y \text{ 更近似}\right)$$

证: 令 $y = x + p^{n-k} z$, 再求 $z \in \mathbb{Z}_p$

Taylor 公式 $f(y) = f(x) + p^{n-k} z f'(x) + p^{2n-2k} \cdot a$ 其中 $a = z^2 f''(\theta) \in \mathbb{Z}_p$

条件有 $f(x) = p^n b$ 且 $f'(x) = p^k \cdot c$, $b \in \mathbb{Z}_p$ $c \in \mathbb{Z}_p^\times$

于是取 $z \in \mathbb{Z}_p$ 使 $b + zc \equiv 0 \ (p)$ $(\text{即取 } z = -bc^{-1} \in \mathbb{Z}_p)$

则有 $f(y) = f(x) + p^{n-k} z f'(x) + p^{2n-2k} a$

$$= p^n b + p^{n-k} z p^k c + p^{2n-2k} a$$

$$= p^n (b + zc) + p^{2n-2k} a \equiv 0 \quad (p^{n+1})$$

$\uparrow$ $0 \le 2k < n \Rightarrow 2n - 2k > n$

f' 的 Taylor 公式: $f'(y) = f'(x) + p^{n-k} z f''(\theta) \equiv p^k c \ (p^{n-k})$

$n - k > k \Rightarrow v_p(f'(y)) = k$ 证毕

Th (Hensel) $f \in \mathbb{Z}_p[X_1, \cdots, X_m]$ $x = (x_i) \in (\mathbb{Z}_p)^m$ $n, k \in \mathbb{Z}$ $j \in \mathbb{Z}$ $0 \le j \le m$

设 $n > 2k < n$ 且 $f(x) \equiv 0 \ (p^n)$

$j\in\mathbb{Z}$ $0\le j\le m$

设 $0<2k<n$ 且 $f(x)\equiv 0\ (p^n)$

$$v_p\left(\frac{\partial f}{\partial x_j}(x)\right)=k$$

则 存在 f 在 $(\mathbb{Z}_p)^m$ 中的零点 y 使 $y\equiv x\ (p^{n-k})$

Pf 先处理 $m=1$. 一元多项

对 $x^{(0)}=x$ 和 n 用 lem 得 $x^{(1)}\in\mathbb{Z}_p$ 使 $x^{(1)}\equiv x^{(0)}\ (p^{n-k})$ 且

$$\begin{cases} f(x^{(1)})\equiv 0 & (p^{n+1}) \\ v_p(f'(x^{(1)}))=k \end{cases}$$

再对 $x^{(1)}$ 和 $n+1$ 用 lem. 得 $x^{(2)}$:

...... $x^{(3)}$ ...... 满足:

$$\begin{cases} x^{(q+1)}\equiv x^{(q)} & (p^{n+q-k}) \\ f(x^{(q)})\equiv 0 & (p^{n+q}) \end{cases}$$

$\Rightarrow$ 即 $x^{(q)}$ Cauchy 列 $x^{(q+1)}-x^{(q)}\longrightarrow 0$ ($当 q\to+\infty$)

取 $y=\lim_{q\to+\infty}x^{(q)}\in\mathbb{Z}_p$

$y\equiv x\ (p^{n-k})$

$|f(x^{(q)})|_p\le\frac{1}{p^{n+q}}$ 取 $q\to+\infty$

$f(y)=0$.

一般 m 多元 只看作 X_j 的多项

其它 X_i $(i\neq j)$ 在 f 中代入 $X_i=x_i$ 得 $\tilde{f}\in\mathbb{Z}_p[X_j]$ 成为一元多项

只需改变 x_j 的值，逐步逼近，取极限 $\longrightarrow$ 精确零点. #

Cor $f\in\mathbb{Z}_p[x]$ $\tilde{f}\in\mathbb{F}_p[x]$ 为 f mod p.

则 $\tilde{f}$ 的单根 均可以提升为 f 在 $\mathbb{Z}_p$ 中的一个解

Pf 取 $n=1$, $k=0$ 时情况 #

例. $f\in\mathbb{Z}[x]\subset\mathbb{Z}_p[x]$ 可分多项式 (f 与 f' 互素)

对几乎所有 p f mod $p\in\mathbb{F}_p[x]$ 仍是可分多项式.

于是由 Cor, mod p 解可提升为 $\mathbb{Z}_p$ 解.

于是由 Cor，mod p 解可提升为 $\mathbb{Z}_p$ 解.

Cor $p\neq 2$ $f(X)=\sum a_{ij}X_iX_j$ 二次型 $a_{ij}=a_{ji}\in\mathbb{Z}_p$

非退化（即 $\det(a_{ij})$ 可逆） $a\in\mathbb{Z}_p$

则 $f(x)\equiv a\ (p)$ 的<u>未原解</u>可提升为 $\mathbb{Z}_p$ 解.

Pf 仍取 $n=1$，$k=0$. 条件是要说明 x 不会使所有 $\frac{\partial f}{\partial x_i}(x)\bmod p$ 为 0

而 $\frac{\partial f}{\partial x_i}=2\sum_j a_{ij}x_j$

$\det(a_{ij})\in\mathbb{Z}_p^\times \Rightarrow \det(a_{ij})\not\equiv 0\ (p)$

x 未原解：有一分量 mod p 可逆

即 $\exists i$ $\frac{\partial f}{\partial x_i}(x)\not\equiv 0\ (p)$ （用到 $p\neq 2$） #

Cor $p=2$ $f=\sum a_{ij}X_iX_j$ $a_{ij}=a_{ji}\in\mathbb{Z}_2$ $a\in\mathbb{Z}_2$

x 为 $f(x)\equiv a\ (8)$ 的<u>未原解</u>.

充 x 不使所有 $\frac{\partial f}{\partial x_i}(x)\bmod 4$ 为 0 （$\Leftarrow \det(a_{ij})\in\mathbb{Z}_2^\times$）

则 x 可提升为 $\mathbb{Z}_2$ 解

Pf 仍取 $n=3$. $k=1$. #

例 $f(x)=x^2+1=0$ $\mathbb{R}$ 中无解

问，$\mathbb{Q}_5$ 中？ $2^2+1\equiv 0\ (5)$

$f'=2x$ $f'(2)=4\not\equiv 0\ (5)$ 即 $f\bmod 5$ 在 2 处光滑.

从而 $x=2$ 可提升为 $\mathbb{Z}_5$ 解

$x_1=2$， $x_2=2+5t$

$0=x_2^2+1=(2+5t)^2+1$ (25)

$=5+20t$ (25)

$\Rightarrow 0\equiv 1+4t\ (5)$

$\Rightarrow t=1$ 是解.

$x_3=2+1\cdot 5+t\cdot 5^2$ $0\equiv x_3^2+1$ $(5^3=125)$

$\Rightarrow t=1$ 是解.

$x_3 = 2 + 1\cdot 5 + t\cdot 5^2$ $\quad 0 \equiv x_3^2+1 \quad (5^3=125)$

$= 7 + 25t$ $\quad \equiv (7+25t)^2+1 \quad (125)$

$\rightsquigarrow$ $t=2$ 是解

$x_3 = 2 + 1\cdot 5 + 2\cdot 5^2$

$x = 2 + 1\cdot 5 + 2\cdot 5^2 + \cdots \in \mathbb{Z}_5$

例 $f(x) = x^2+5$, $\mathbb{Q}_5$ 中求解

$f'(x) = 2x$

$0^2+5 \equiv 0 \ (5)$

$f'(0) = 2\cdot 0 = 0$ $\quad v_5(f'(0)) = +\infty$

$\rightsquigarrow$ 0不一定可提升为 $\mathbb{Z}_5$ 解.

事实上, ~~若有解~~ $x^2 = -5 \in \mathbb{Q}_5$

$v_5(x^2) = v_5(5) = 1$

$\| $

$2v_5(x)$ $\quad v_5(x) \in \mathbb{Z}$ 矛盾.

例 $f(x) = x^2 + \frac{1}{100} = 0$ $\quad \mathbb{Q}_5$ 中求解

$x^2 = -\frac{1}{100} \iff (5x)^2 = -\frac{1}{4} \in \mathbb{Z}_5^\times$

$v_5(4) = 0$

$y^2 = -\frac{1}{4} \in \mathbb{Z}_5[y]$

mod 5 $\quad y^2 \equiv -4^{-1} \ (5)$

$\equiv -(-1)^{-1} \ (5)$

$\equiv 1 \ (5)$

$y_1 = 1$ $\quad y_2 = 1+t\cdot 5$

$y_2^2 \equiv (1+5t)^2 \equiv -4^{-1} \ (25)$

$\equiv -19 \equiv 6 \ (25)$

$\Rightarrow t = 3$

$y_2 = 1+3\cdot 5$ $\quad \cdots \quad x_3 \quad \cdots$

$y = 1 + 3\cdot 5 + ?\cdot 5^2 + ?\cdot 5^3 + \cdots$

$x = \frac{1}{t}\cdot y = \frac{1}{t} + 3 + ?\cdot 5 + ?\cdot 5^2 + \cdots$

$$x = \frac{1}{5} \cdot y = \frac{1}{5} + 3 + ? \cdot 5 + ? \cdot 5^2 + \cdots$$

总结 $p \geq 3$ $x^2 = a \neq 0$ 在 $\mathbb{Q}_p$ 中有解 $\Leftrightarrow$ $t = v_p(a)$ 是偶数

$a = p^t \cdot a_0$, $a_0 \in \mathbb{Z}_p^\times$

$\left(\frac{\bar{a}_0}{p}\right) = 1$ $\bar{a}_0 \in \mathbb{Z}_p / p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$

另外 $p = 2$ 时

$x^2 = a \neq 0$ $\mathbb{Q}_2$ 中有解 $\Leftrightarrow$ $t = v_2(a)$ 偶数, 且

$\bar{a}_0 \equiv 1 \ (8)$

$\mathbb{Q}_p$ 上的二次型

在 $\mathbb{R}$ 上 (n元) 二次型 是否有非零解 可以用它的符号 (p, g) 来判断

(Sylvester 惯性定理)

当 $p = n$, $g = 0$ 时 正定, 无非零解.

在 $\mathbb{Q}_p$, char $\mathbb{Q}_p = 0$. 二次型仍合同于对角型

$Q = a_1 x_1^2 + \cdots + a_n x_n^2$ $a_i \neq 0$. $\in \mathbb{Q}_p$ 即 $rk Q = n$. 非退化二次型

通过把 a_i 换成 $a_i p^{2t}$ $(t \in \mathbb{Z})$ 总可设 $a_i \in \mathbb{Z}_p$ $v_p(a_i) = \begin{cases} 0 \\ 1 \end{cases}$

$Q(x) = a_1 x_1^2 + \cdots + a_s x_s^2 + p(a_{s+1} x_{s+1}^2 + \cdots + a_n x_n^2)$

$a_i \in \mathbb{Z}_p^\times$

lem $p > 2$, $f = a_1 x_1^2 + a_2 x_2^2 + a_3 x_3^2 = 0$ $(a_i \in \mathbb{Z}_p^\times)$ 在 $\mathbb{Q}_p$ 中总有非零解.

Pf $p > 2$. 只要 f mod p 有非平凡解 + Hensel lem 提升为 $\mathbb{Z}_p$.

由于如以下 Prop. #

Prop $(p > 2)$, $a_i \in \mathbb{F}_p^\times$ $a_1 x_1^2 + a_2 x_2^2 + a_3 x_3^2 = 0$ 总有非零解.

Pf 抽屉原理 $\Rightarrow$ 总有两个元相加是二次剩余 (与另外二次剩余

Pf 抽屉原理 ⇒ 总有两个系数同时是二次剩余或同时非二次剩余.

只需考虑前者. 可设 $\left(\frac{a_1}{p}\right)=1$, $\left(\frac{a_2}{p}\right)=1$.

变量替换后 $x_1^2+x_2^2=-a_3x_3^2$, 只需证以下引理 #

Lem ($p>2$) $\mathbb{F}_p$ 中元素均是平方和

$[\mathbb{F}_p^{\times}:\mathbb{F}_p^{\times 2}]=2 \Rightarrow |\mathbb{F}_p^{\times 2}|=\frac{p-1}{2}$, 0 是一平方数

$\mathbb{F}_p$ 中平方数是 $\frac{p-1}{2}+1=\frac{p+1}{2}$

$\mathbb{F}_p$ 中非平方 $p-\frac{p+1}{2}=\frac{p-1}{2}$

$\forall c\in\mathbb{F}_p$ 考虑 $|\{c-x^2 \mid x\in\mathbb{F}_p\}|=\frac{p+1}{2}$

它必含一个平方数 #

Cor $n\geq 5$, n元二次型在 $\mathbb{Q}_p$ 上总有非零解

Pf $p=2$ 也对, 但只证 $p>2$.

$Q(x)=a_1x_1^2+\cdots+a_sx_s^2+p(a_{s+1}x_{s+1}^2+\cdots+a_nx_n^2)$

$n\geq 5$ s 与 $n-s$ 总有一个 ≥ 3 $a_i\in\mathbb{Z}_p^{\times}$

由之前 lem 可知 $Q(x)=0$ 有非零解 #

Th (Hasse-Minkowski) $\mathbb{Q}$ 上二次型 Q

Q 在 $\mathbb{Q}$ 上有非零解 ⟺ $\forall p\leq\infty$ Q 在 $\mathbb{Q}_p$ 上有非零解 ($\mathbb{Q}_\infty=\mathbb{R}$)

pf: J.-P. Serre 《A Course in Arithmetic》

$\mathbb{Q}$ ⇝ K 数域

Cor $n\geq 5$ 元 $\mathbb{Q}$ 上二次型 在 $\mathbb{Q}$ 上有非零解 ⟺ 在 $\mathbb{R}$ 上非正定

三次型反例: Selmer $3x^3+4y^3+5z^3=0$ $C\subset\mathbb{P}^2$

三次型反例：Selmer $3x^3+4y^3+5z^3=0$ $C\subset\mathbb{P}^2$

在 $\mathbb{Q}$ 上只有零解，在 $\mathbb{Q}_p$, $\mathbb{R}$ 上均有非零解。

$g(C)$ $C(\mathbb{Q}_p)\neq\phi$ $C(\mathbb{R})\neq\phi$ 但 $C(\mathbb{Q})=\phi$.

$E=\mathrm{Jac}(C)$ $[C]\in\mathrm{Ker}\left(H^1(\mathbb{Q},E)\to\prod_{p\leq\infty}H^1(\mathbb{Q}_p,E)\right)$

$\| $

$Ш(E/\mathbb{Q})<+\infty$ (Conj)

Galois 上同调

Th $F(x_1,\dots,x_n)=0$ 三次型，$\mathbb{Q}$ 系数.

(1) (Lewis) $n\geq10$ F 在 $\mathbb{Q}_p$ 上有非零解

(2) (Heath-Brown) 若 F 光滑，$n\geq10$ 则 F 在 $\mathbb{Q}$ 中有非零解.

(3) (Hooley) $n=9$，F 光滑，且在 $\mathbb{Q}_p$ 中均有非零解，
则在 $\mathbb{Q}$ 中也有非零解.

Conj 去掉"光滑"也成立