1.16 补充材料

邱才颙

2023 年 1 月 18 日

群里的 PPT 包含了 p 进数的温习

1 多项式方程（组）

设 R 是环，我们用 $R[X_1,\ldots,X_m]$ 代表以 $X_1,\ldots,X_m$ 为变量的全体 R 系数的多项式全体所构成的集合。解方程组 $f_1,\ldots,f_k$ 的意思就是，求 $a_1,\ldots,a_m$ 使得 $f_i(a_1,\ldots,a_m)=0$ 对 $i=1,\ldots,k$ 都成立

若 $\varphi: R_1 \to R_2$ 为环同态，并且 $f \in R_1[X_1,\ldots,X_m]$，则通过将 φ 作用在 f 的每一个系数上，我们可以得到 $\varphi f \in R_2[X_1,\ldots,X_m]$

定理 1.1 (系数变换定理)
设 $\varphi: R_1 \to R_2$ 为环同态

若 $f=0$ 有解则 $\varphi f=0$ 有解，若 $\varphi f=0$ 无解则 $f=0$ 无解

证明. 若 $f(a_1,\ldots,a_m)=0$，则

$$\varphi f(\varphi a_1,\ldots,\varphi a_n)=\varphi(f(a_1,\ldots,a_m))=\varphi(0)=0$$

□

可以总结为: 出发的地方有解则到达的地方有解，到达的地方无解则出发的地方也无解

例 1.2
设 $N>n$，考虑某个（整系数）方程，则此方程若模 p^N 有解，那么模 p^n 也有解，若此方程模 p^n 无解，则模 p^N 也无解。这是由于熟知的环同态

$$\mathbf{Z}/p^N\mathbf{Z} \to \mathbf{Z}/p^n\mathbf{Z}$$

定理的推论/应用 1.3
若（整系数，或更一般地，$\mathbf{Z}_p$ 系数）方程在 $\mathbf{Z}_p$ 中有解，则在所有 $\mathbf{Z}/p^n\mathbf{Z}$ 中都有解，这是使用了环同态 $\mathbf{Z}_p \to \mathbf{Z}/p^n\mathbf{Z}$

定理 1.4
若（整系数，或更一般地，$\mathbf{Z}_p$ 系数）方程在所有 $\mathbf{Z}/p^n\mathbf{Z}$ 中都有解，则在 $\mathbf{Z}_p$ 中有解。这个结论的证明等价于 p 进整数的构造方式

这个定理解释了 p 进数的某种方便之处，毕竟下面的命题不成立：
若整系数方程在所有 $\mathbf{Z}/p^n\mathbf{Z}$ 中都有解，则在 $\mathbf{Z}$ 中有解（假命题）

定理 1.5 (齐次方程)
若 $f \in \mathbf{Z}[X_1, \ldots, X_m]$ 为齐次多项式，则下面两件事情等价

- f 在 $\mathbf{Q}$ 中有除原点之外的解
- f 在 $\mathbf{Z}$ 中有解 $(a_1, \ldots, a_n)$，并且 $a_1, \ldots, a_n$ 是互素的

这个简单的事实可以直接推广到 p 进版本：

定理 1.6 (齐次方程)
若 $f \in \mathbf{Z}_p[X_1, \ldots, X_m]$ 为齐次多项式，则下面两件事情等价

- f 在 $\mathbf{Q}_p$ 中有除原点之外的解
- f 在 $\mathbf{Z}_p$ 中有解 $(a_1, \ldots, a_n)$，并且 $v_p(a_i)$ 的最小值是 0

2 Hensel 引理的叙述

对于 p 进数 $x \in \mathbf{Q}_p$，我们定义其"大小"为 $|x|_p = p^{-v_p(x)}$，两个 p 进数 $x, y \in \mathbf{Q}_p$ 之间的距离定义为 $|x-y|_p$。使用这个新的距离，微积分中的多数概念可以移植到 p 进数上

定理 2.1 (Hensel 引理)
若 $f(X) \in \mathbf{Z}_p[X]$ 是多项式，α_1 是猜测的根，只要满足

$$\frac{|f(\alpha_1)|_p}{|f'(\alpha_1)|_p} < |f'(\alpha_1)|_p$$

那么在集合 $\{x \in \mathbf{Z}_p : |x-\alpha_1|_p \leq \frac{|f(\alpha_1)|_p}{|f'(\alpha_1)|_p}\}$ 中 $f(X)$ 有唯一的根 α，并且我们还知道 $|\alpha - \alpha_1|_p = \frac{|f(\alpha_1)|_p}{|f'(\alpha_1)|_p}, |f'(\alpha)|_p = |f'(\alpha_1)|_p$

3 Hensel 引理的直接应用

设 $p \neq 2$ 为素数，m 为与 p 互素的整数，那么：

- 若 $\left(\frac{m}{p}\right) = -1$，则方程 $X^2 \equiv m (\bmod\ p^n)$ 总是无解

  证明. 这就是系数变换定理，在 $\mathbf{Z}/p\mathbf{Z}$ 上无解当然在 $\mathbf{Z}/p^n\mathbf{Z}$ 上无解 □

- 若 $\left(\frac{m}{p}\right) = 1$，则方程 $X^2 \equiv m (\bmod\ p^n)$ 总是有解

  证明. 由于 $\left(\frac{m}{p}\right) = 1$，存在整数 α_1 使得 $\alpha_1^2 - m$ 是 p 的倍数。

  换言之，$|\alpha_1^2 - m|_p \leq p^{-1}$，又因为 m 与 p 互素，故 α_1 也必定和 p 互素，从而 $|2\alpha_1|_p = 1$

  现在考虑多项式 $f(X) = X^2 - m$，那么 $f(X)$ 显然满足 Hensel 引理的条件

  $$\frac{|f(\alpha_1)|_p}{|f'(\alpha_1)|_p} = \frac{|\alpha_1^2 - m|_p}{|2\alpha_1|_p} \leq \frac{1}{p} < 1 = |2\alpha_1|_p = |f'(\alpha_1)|_p$$

  使用 Hensel 引理，根据定理 1.4，方程 $X^2 \equiv m (\bmod\ p^n)$ 总是有解 □

4 作业

上面的证明中，哪里使用到了 $p \neq 2$？说明理由

5 技术性引理

引理 5.1

若 $f(X) \in R[X]$ 是多项式，$a, b \in R$，那么存在 $d \in R$ 使得

$$f(a+b) = f(a) + bd$$

证明. 这就是二项式定理 □

引理 5.2

若 $f(X) \in R[X]$ 是多项式，$a, b \in R$，那么存在 $c \in R$ 使得

$$f(a+b) = f(a) + bf'(a) + b^2 c$$

证明. 这就是二项式定理 □

6 强三角不等式

首先注意到一个简单的事实：如果 p^a 除尽 x，p^b 除尽 y，并且 $a \neq b$，那么我们有 $p^{\min\{a,b\}}$ 除尽 $x \pm y$

例 6.1
16 是 2^4 的倍数，而 12 是 2^2 的倍数，因此 $16 + 12 = 28$ 只能是 2^2 的倍数

把上面的发现严格地说明，就是：

定理 6.2 (强三角不等式)
若 $x, y \in \mathbf{Q}_p$，并且 $v_p(x) < v_p(y)$，那么

$$v_p(x \pm y) = v_p(x)$$

或者等价地，若 $|x|_p > |y|_p$，那么

$$|x \pm y|_p = |x|_p$$

强三角不等式是 p 进数的一个巨大优点！这个结论可以重新叙述为：两个（大小不一样的）数相加的大小，恰好等于大的那个大小

强三角不等式有一系列推论：

1. 序列 α_n 收敛到某个极限，当且仅当序列的间隔 $a_{n+1} - a_n$ 的大小趋近于零

2. 如果 $|\alpha_3 - \alpha_2|_p < |\alpha_2 - \alpha_1|_p$，那么 $|\alpha_3 - \alpha_1|_p = |\alpha_2 - \alpha_1|_p$。形象地说：圆内任何一点都是这个圆的圆心

7 选学：Hensel 引理的证明（长度警告！）

假设 $f(X) \in \mathbf{Z}_p[X]$ 是一个多项式，α_1 是猜测的根，满足

$$\frac{|f(\alpha_1)|_p}{|f'(\alpha_1)|_p} < |f'(\alpha_1)|_p$$

特别地，这个条件说明 $|f'(\alpha_1)|_p \neq 0$，因此 $f'(\alpha_1) \neq 0$，从而可以做下面 β_1 的表达式的分母。从 Newton 切线迭代法受到启发，我们定义

$$\beta_1 = -\frac{f(\alpha_1)}{f'(\alpha_1)}$$

并大胆猜测 $\alpha_2 = \alpha_1 + \beta_1$ 会是一个更好的近似根，我们来验证这一点。不过在这之前，注意到，按照我们对 α_1 的假设，我们有

$$|\beta_1|_p = \left|-\frac{f(\alpha_1)}{f'(\alpha_1)}\right|_p < |f'(\alpha_1)|_p$$

等价地，这就是在说 $v_p(\beta_1) > v_p(f'(\alpha_1))$，由于 $f'(\alpha_1)$ 是 p-adic 整数，因此赋值更大的 β_1 也是 p-adic 整数而不只是 p-adic 数

（你可以类比一下：赋值越大，说明这个数的分解式里面 p 的幂越高，因此就更加是整数而不是有理数）

使用第二条技术性引理，我们知道存在 $\gamma_1 \in \mathbf{Z}_p$，使得

$$f(\alpha_2) = f(\alpha_1 + \beta_1) = f(\alpha_1) + \beta_1 f'(\alpha_1) + \beta_1^2 \gamma_1$$

回忆一下 β_1 的表达式，我们发现 $f(\alpha_1) + \beta_1 f'(\alpha_1) = 0$，因此

$$f(\alpha_2) = \beta_1^2 \gamma_1$$

注意到，一个 p-adic 整数的赋值总是非负的（参见 PPT），等价地，这就是在说 $|\gamma_1|_p = p^{-v_p(\gamma_1)} \leq 1$，因此（$p$-adic 整数越相乘越小）

$$|f(\alpha_2)|_p = |\beta_2^2 \gamma_1|_p \leq |\beta_2|_p^2 = \frac{|f(\alpha_1)|_p^2}{|f'(\alpha_1)|_p^2}$$

结合最初的条件

$$\frac{|f(\alpha_1)|_p}{|f'(\alpha_1)|_p} < |f'(\alpha_1)|_p$$

我们就得到

$$|f(\alpha_2)|_p < |f(\alpha_1)|_p$$

这说明：α_2 确实是一个比 α_1 更优的方程 $f(X) = 0$ 的近似解，接下来我们自然希望去做归纳，把上面的步骤不断重复。不过为了能够做归纳，我们需要确认 α_2 也满足和 α_1 一样的条件，也就是我们要验证

$$\frac{|f(\alpha_2)|_p}{|f'(\alpha_2)|_p} < |f'(\alpha_2)|_p$$

我们对多项式 $f'(X)$ 使用第一条技术性引理，得到：存在 $\delta_1 \in \mathbf{Z}_p$ 使得

$$f'(\alpha_2) = f'(\alpha_1 + \beta_1) = f'(\alpha_1) + \beta_1 \delta_1$$

类似前面做过的事情，由于 $\delta_1 \in \mathbf{Z}_p$，我们知道（$p$-adic 整数越相乘越小）

$$|\beta_1\delta_1|_p \le |\beta_1|_p$$

但是此前我们就推出了 $|\beta_1|_p < |f'(\alpha_1)|_p$，现在来看

$$f'(\alpha_2) = f'(\alpha_1) + \beta_1\delta_1$$

这个式子将 $f'(\alpha_2)$ 表达成两个东西的和，而其中“大小”更大的是 $f'(\alpha_1)$，利用强三角不等式，我们就知道 $f'(\alpha_2)$ 的大小，是其中大的那个数的大小

也就是说：

$$|f'(\alpha_2)|_p = \max\{|f'(\alpha_1)|_p, |\beta_1\delta_1|_p\} = |f'(\alpha_1)|_p$$

总结：我们得到的新的近似解 α_2 满足：

$$|f(\alpha_2)|_p < |f(\alpha_1)|_p, \quad |f'(\alpha_2)|_p = |f'(\alpha_1)|_p$$

简单的计算表明

$$\frac{|f(\alpha_2)|_p}{|f'(\alpha_2)|_p} < |f'(\alpha_2)|_p$$

仍然成立，因此我们可以继续下去 Newton 切线迭代法这个过程，得到 $\alpha_3, \alpha_4, \alpha_5, \ldots$，这将是一系列越来越优的近似解，因为

$$|f(\alpha_2)|_p < |f(\alpha_1)|_p, \quad |f(\alpha_3)|_p < |f(\alpha_2)|_p, \quad |f(\alpha_4)|_p < |f(\alpha_3)|_p \ldots$$

也就是说，$f(\alpha_n)$ 正在逐步变小（注：这个变小的速度是非常快的，有专门的研究来估计这个算法的速度，非常快）

所以，我们只要对序列 $\alpha_1, \alpha_2, \alpha_3, \ldots$ 取一个极限，就可以得到 $f(X)$ 的真正的根。

不过正如同微积分里所有涉及极限的问题：你要先证明有极限，或者说证明这个序列收敛

这时候我们再次使用强三角不等式的优点：我们只需要证明这个序列的间隔 $a_{n+1} - a_n$ 的大小趋近于零

这是很好算的，因为每一个 α_{n+1} 都是用 Newton 切线公式构造出来的，换言之

$$a_{n+1} - a_n = -\frac{f(\alpha_n)}{f'(\alpha_n)}$$

之前已经说明了

$$|f(\alpha_2)|_p < |f(\alpha_1)|_p, \quad |f'(\alpha_2)|_p = |f'(\alpha_1)|_p$$

$$|f(\alpha_3)|_p < |f(\alpha_2)|_p, \quad |f'(\alpha_3)|_p = |f'(\alpha_2)|_p$$

$$\vdots$$

所以我们确实有 $|a_{n+1} - a_n|_p$ 单调递减。因为 $|a_{n+1} - a_n|_p$ 只能取 p 的负整数幂，所以极限是 0：

$$\lim_{n\to\infty} |a_{n+1} - a_n|_p = \lim_{n\to\infty} \left| \frac{f(\alpha_n)}{f'(\alpha_n)} \right|_p = 0$$

到此为止，我们证明了 $f(X)$ 确实有一个精确解 $\alpha = \lim_{n\to\infty} \alpha_n$。

不过事情还可以说更多：我们要说明

1. 这个精确解 α 和初始猜测的解 α_1 的距离恰好是

   $$|\alpha - \alpha_1|_p = \frac{|f(\alpha_1)|_p}{|f'(\alpha_1)|_p}$$

   即：精确解距离一开始猜测的解，并不算远，我们甚至知道距离多远

2. 在以初始猜测的解 α_1 为中心，半径 $|f'(\alpha_1)|_p$ 的（不包含圆周）的圆内，α 是 $f(X) = 0$ 的唯一解

第一件事情是这样子说明的：我们将证明

$$|\alpha_n - \alpha_1|_p = \frac{|f(\alpha_1)|_p}{|f'(\alpha_1)|_p}$$

对所有 n 都成立，因此取极限之后就有我们要的结论了

$$|\alpha - \alpha_1|_p = \frac{|f(\alpha_1)|_p}{|f'(\alpha_1)|_p}$$

好，现在来证明这件事情，这是用归纳法来证明的。我们已经知道了

$$|\alpha_3 - \alpha_2|_p < |\alpha_2 - \alpha_1|_p$$

“圆内任何一点都是这个圆的圆心”说明

$$|\alpha_3 - \alpha_1|_p = |\alpha_2 - \alpha_1|_p = \frac{|f(\alpha_1)|_p}{|f'(\alpha_1)|_p}$$

重复这个过程，就有

$$|\alpha_4-\alpha_1|_p=|\alpha_2-\alpha_1|_p=\frac{|f(\alpha_1)|_p}{|f'(\alpha_1)|_p}$$

$$|\alpha_5-\alpha_1|_p=|\alpha_2-\alpha_1|_p=\frac{|f(\alpha_1)|_p}{|f'(\alpha_1)|_p}$$

$$\vdots$$

第二件事情，也就是根的局部唯一性，是使用反证法证明的

假设在以初始猜测的解 α_1 为中心，半径 $|f'(\alpha_1)|_p$ 的（不包含圆周）的圆内，$f(X)=0$ 除了 α，还有解 $\tilde{\alpha}$，也就是说

$$\alpha,\tilde{\alpha}\in\{x\in\mathbf{Z}_p:|x-\alpha_1|_p<|f'(\alpha_1)|_p,f(x)=0\}$$

那么必然可以分解因式，得到

$$f(X)=(X-\alpha)(X-\tilde{\alpha})g(X)$$

两边同时求导，得到

$$f'(X)=(2X-\alpha-\tilde{\alpha})g(X)+(X-\alpha)(X-\tilde{\alpha})g'(X)$$

令 $X=\alpha$，得到

$$f'(\alpha)=(\alpha-\tilde{\alpha})g(\alpha)$$

根据“p-adic 整数越乘越小” 的原则，我们有

$$|f'(\alpha)|_p\leq|\alpha-\tilde{\alpha}|_p\quad(*)$$

但是我们事先假设了 $\alpha,\tilde{\alpha}$ 都在以初始猜测的解 α_1 为中心，半径 $|f'(\alpha_1)|_p$ 的（不包含圆周）的圆内，因此：

$$|\alpha-\alpha_1|_p<|f'(\alpha_1)|_p,\quad|\tilde{\alpha}-\alpha_1|_p<|f'(\alpha_1)|_p$$

作差，考虑 $(\alpha-\alpha_1)-(\tilde{\alpha}-\alpha_1)=(\alpha-\tilde{\alpha})$，强三角不等式说明

$$|\alpha-\tilde{\alpha}|_p\leq\max\{|\alpha-\alpha_1|_p,|\tilde{\alpha}-\alpha_1|_p\}<|f'(\alpha_1)|_p$$

结合 $(*)$ 式，有

$$|f'(\alpha)|_p\leq|\alpha-\tilde{\alpha}|_p<|f'(\alpha_1)|_p$$

这就带来了矛盾，因为前面的结果说明（常数的极限还是这个常数）

$$|f'(\alpha_1)|_p=|f'(\alpha_2)|_p=|f'(\alpha_3)|_p=\cdots=|f'(\alpha)|_p$$