Listado 03: Solución al Lema de Hensel

Teoría de Números (527288)

Universidad de Concepción, Departamento de Matemática

Teorema (Lema de Hensel, versión aritmética modular)

Sea $f(x)$ un polinomio con coeficientes enteros. Sean p un número primo y $e \geq 1$ un número natural. Si $u \in \mathbb{Z}$ cumple:

$$\begin{cases} f(u) \equiv 0 \pmod{p^e} \\ f'(u) \not\equiv 0 \pmod{p} \end{cases}$$

entonces para todo exponente $k > e$ existe una única solución v de $f(v) \equiv 0 \pmod{p^k}$ "por encima" de u, es decir, tal que $v \equiv u \pmod{p^e}$.

1 Orientaciones para la Demostración

1.1 Mostrar: existe un entero l tal que $f(u) = lp^e$

Orientación: Usar la definición de congruencia.

1.2 Mostrar: $f'(u)$ es invertible módulo p^{e+1}

Orientación: Un número a es invertible módulo m si y solo si $\operatorname{mcd}(a, m) = 1$. Se tiene como hipótesis que $f'(u) \not\equiv 0 \pmod{p}$.

1.3 Mostrar: $(x + np^e)^i - x^i \equiv ix^{i-1} \cdot np^e \pmod{p^{e+1}}$

Orientación: Usar el Teorema del Binomio y $2e \geq e + 1$.

1.4 Mostrar: $f(u + np^e) - f(u) \equiv f'(u) \cdot np^e \pmod{p^{e+1}}$

Orientación: Escribir $f(x) = \sum_{i=0}^{m} c_i x^i$ y usar el Item 3.

1.5 Mostrar: existe un único valor de $n \in \{0, \ldots, p-1\}$ tal que $f(u + np^e) \equiv 0 \pmod{p^{e+1}}$

Orientación: Sustituir los Items 1 y 4 en la condición de congruencia. La unicidad del valor buscado se conecta con la unicidad de los inversos multiplicativos.

1.6 Concluir: hay una única solución v de $f(x) \equiv 0 \pmod{p^{e+1}}$ por encima de u

Orientación: Definir $v = u + n_0 p^e$ con n_0 el valor único hallado.

1.7 Más aún: concluir que esta solución es $v \equiv u - f(u) \cdot (f'(u))^{-1} \pmod{p^{e+1}}$

Orientación: Usar la relación $v = u + np^e$ y la congruencia lineal resuelta.

2 Desarrollo de la Demostración por Pasos

2.1 Mostrar: existe un entero l tal que $f(u) = lp^e$

Solución: La hipótesis $f(u) \equiv 0 \pmod{p^e}$ significa, por definición de congruencia, que p^e divide a $f(u)$. Por la definición de divisibilidad, si $p^e \mid f(u)$, **existe un entero l tal que** $f(u) = lp^e$.

2.2 Mostrar: $f'(u)$ es invertible módulo p^{e+1}

Solución: Para que $f'(u)$ sea invertible módulo p^{e+1}, se requiere $\text{mcd}(f'(u), p^{e+1}) = 1$. La hipótesis $f'(u) \not\equiv 0 \pmod{p}$ implica que $p \nmid f'(u)$, por lo que $\text{mcd}(f'(u), p) = 1$. Dado que p es primo, los divisores de p^{e+1} son potencias de p. Si $\text{mcd}(f'(u), p^{e+1}) = d > 1$, entonces d debería ser divisible por p, lo que implicaría que $p \mid f'(u)$, una contradicción. Por lo tanto, $\text{mcd}(f'(u), p^{e+1}) = 1$, y $f'(u)$ **es invertible módulo** p^{e+1}.

2.3 Mostrar: $(x + np^e)^i - x^i \equiv ix^{i-1} \cdot np^e \pmod{p^{e+1}}$

Solución: Por el Teorema del Binomio:

$$(x + np^e)^i = x^i + \binom{i}{1} x^{i-1}(np^e) + \binom{i}{2} x^{i-2}(np^e)^2 + \cdots + (np^e)^i$$

$$(x + np^e)^i - x^i = ix^{i-1}(np^e) + \sum_{k=2}^{i} \binom{i}{k} x^{i-k} n^k p^{ek}$$

Como $e \geq 1$, para todo $k \geq 2$, se cumple $ek \geq 2e \geq e + 1$. Por lo tanto, $p^{e+1} \mid p^{ek}$. La suma es congruente a cero módulo p^{e+1}:

$$(x + np^e)^i - x^i \equiv ix^{i-1} \cdot np^e \pmod{p^{e+1}}$$

2.4 Mostrar: $f(u + np^e) - f(u) \equiv f'(u) \cdot np^e \pmod{p^{e+1}}$

Solución:

$$f(u + np^e) - f(u) = \sum_{i=0}^{m} c_i (u + np^e)^i - \sum_{i=0}^{m} c_i u^i = \sum_{i=1}^{m} c_i \left[(u + np^e)^i - u^i\right]$$

Aplicando el resultado del Item 3 a cada término ($i \geq 1$):

$$f(u + np^e) - f(u) \equiv \sum_{i=1}^{m} c_i \left[iu^{i-1} \cdot np^e\right] \pmod{p^{e+1}}$$

Factorizando np^e, que no depende de i:

$$f(u + np^e) - f(u) \equiv \left[\sum_{i=1}^{m} ic_i u^{i-1}\right] \cdot np^e \pmod{p^{e+1}}$$

Dado que $f'(x) = \sum_{i=1}^{m} ic_i x^{i-1}$, la suma es $f'(u)$.

$$\mathbf{f(u + np^e) - f(u) \equiv f'(u) \cdot np^e \pmod{p^{e+1}}}$$

2.5 Mostrar: existe un único valor de $n \in \{0, \dots, p-1\}$ tal que $f(u + np^e) \equiv 0 \pmod{p^{e+1}}$

Solución: La condición a resolver es $f(u+np^e) \equiv 0 \pmod{p^{e+1}}$. Del Item 4, sustituimos $f(u+np^e)$:

$$f(u) + f'(u) \cdot np^e \equiv 0 \pmod{p^{e+1}}$$

Del Item 1, $f(u) = lp^e$. Sustituyendo:

$$lp^e + f'(u)np^e \equiv 0 \pmod{p^{e+1}}$$

Por definición de congruencia, p^{e+1} divide a $p^e(l + f'(u)n)$, lo que implica, dividiendo por p^e:

$$l + f'(u)n \equiv 0 \pmod{p} \quad \text{o} \quad f'(u)n \equiv -l \pmod{p}$$

Dado que $f'(u) \not\equiv 0 \pmod{p}$ (por hipótesis), $f'(u)$ es invertible módulo p. Por lo tanto, esta congruencia lineal tiene una **solución única para** n **en** $\{0, 1, \dots, p-1\}$:

$$n \equiv -l \cdot (f'(u))^{-1} \pmod{p}$$

2.6 Concluir: hay una única solución v de $f(x) \equiv 0 \pmod{p^{e+1}}$ por encima de u

Solución: Sea n_0 el valor único hallado en el Item 5. Definimos la solución elevada:

$$v = u + n_0 p^e$$

- **Solución:** Por el Item 5, $f(v) = f(u + n_0 p^e) \equiv 0 \pmod{p^{e+1}}$.
- **Por encima:** Como $v - u = n_0 p^e$, se tiene que $p^e \mid (v - u)$, es decir, $v \equiv u \pmod{p^e}$.

Dado que n_0 es único en su rango, **v es la única solución** $\pmod{p^{e+1}}$ que está por encima de u.

2.7 Más aún: concluir que esta solución es $v \equiv u - f(u) \cdot (f'(u))^{-1} \pmod{p^{e+1}}$

Solución: De la congruencia resuelta en el Item 5, multiplicando por p^e:

$$lp^e + f'(u)np^e \equiv 0 \pmod{p^{e+1}}$$

Sustituyendo $lp^e = f(u)$:

$$f(u) + f'(u)np^e \equiv 0 \pmod{p^{e+1}}$$

Despejando np^e:

$$f'(u)np^e \equiv -f(u) \pmod{p^{e+1}}$$

Como $f'(u)$ es invertible módulo p^{e+1} (Item 2):

$$np^e \equiv -f(u) \cdot (f'(u))^{-1} \pmod{p^{e+1}}$$

Sustituyendo $v = u + np^e$:

$$\mathbf{v \equiv u - f(u) \cdot (f'(u))^{-1} \pmod{p^{e+1}}}$$

Esta es la fórmula de **levantamiento de Hensel** (análoga al método de Newton-Raphson).