Universidad de Concepción
Facultad de Ciencias Físicas y Matemáticas
Departamento de Matemática

Listado 03: Lema de Hensel
Teoría de Números (527288)

El objetivo de este listado es construir una demostración del siguiente resultado:
Teorema (lema de Hensel, versión aritmética modular).
Sea $f(x)$ un polinomio con coeficientes enteros. Sean p es 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 $v \equiv u \pmod{p^e}$.
Más aún, esta solución v se puede construir explícitamente (en la demostración se detallará cómo).

El plan de esta demostración es proceder recursivamente: a partir de una solución de $f(x) \equiv 0$ módulo p^e construir una solución de $f(x) \equiv 0$ módulo p^{e+1} que esté por encima de la anterior.

1. Mostrar: existe un entero l tal que $f(u) = lp^e$.
2. Mostrar: $f'(u)$ es invertible módulo p^{e+1}.
3. Mostrar: para cualquier exponente i y cualquier entero n,
$$(x + np^e)^i - x^i \equiv ix^{i-1} \cdot np^e \pmod{p^{e+1}}$$
4. Mostrar: para cualquier entero n,
$$f(u + np^e) - f(u) \equiv f'(u) \cdot np^e \pmod{p^{e+1}}$$
(Sugerencia: escribir $f(x) = c_n x^n + c_{n-1}x^{n-1} + \ldots + c_1 x + c_0$ y usar el item anterior.)
5. Usando el primer item y el anterior, mostrar: existe un único valor de $n \in \{0, \ldots, p-1\}$ tal que $f(u + np^e) \equiv 0 \pmod{p^{e+1}}$.
6. Concluir: hay una única solución v de $f(x) \equiv 0 \pmod{p^{e+1}}$ por encima de u.
7. Más aún: concluir que esta solución es
$$v = u - f(u) \cdot (f'(u))^{-1} \pmod{p^{e+1}}$$
8. Utilizando recursivamente el resultado recién demostrado, resolver $x^3 - 3 \equiv 0 \pmod{5^n}$ para $n = 1, 2, 3, 4$.