Llista 2 d'Aritmètica. Nombres p-adics.

El lema de Hensel

Lema (Hensel): Donat $f \in \mathbb{Z}[x]$ un polinomi en una variable a coeficients enters. Sigui p un nombre primer i suposem que existeixen $k, n, x \in \mathbb{Z}$ amb $0 \leq 2k < n$ complint les condicions següents:
1. $f(x) \equiv 0 \pmod{p^n}$,
2. $f'(x) \equiv 0 \left(\bmod p^k\right)$,
3. $f'(x) \not\equiv 0 \left(\bmod p^{k+1}\right)$.

Llavors existeix $y \in \mathbb{Z}$ complint les condicions següents:
1. $y \equiv x \left(\bmod p^{n-k}\right)$,
2. $f(y) \equiv 0 \left(\bmod p^{n+1}\right)$,
3. $f'(y) \equiv 0 \left(\bmod p^k\right)$,
4. $f'(y) \not\equiv 0 \left(\bmod p^{k+1}\right)$.

En particular existex $\tilde{y} \in \mathbb{Z}_p$ tal que $f(\tilde{y}) = 0$.

1. Existeix $x \in \mathbb{Z}_p$ tal que $x^2 = 2$ a $\mathbb{Z}_3, \mathbb{Z}_5$ o $\mathbb{Z}_7$? Calcula'n els 4 primers digits en cas afirmatiu.
2. Calcula els primers 4 digits padics de les arrels del polinomi $5x^3 + x^2 - 1$ a $\mathbb{Q}_5$.

Exponencial i logaritme

3. Demostra que l'exponencial padica

$$\exp(x) \stackrel{\text{def}}{=} \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

convergeix en $x \in \mathbb{Q}_p$ si i només si

$$\begin{cases} x \in p\mathbb{Z}_p & \text{si } p \text{ senar,} \\ x \in 4\mathbb{Z}_2 & \text{si } p = 2. \end{cases}$$

4. Demostra que el logarítme p-adic

$$\log(t) \stackrel{\text{def}}{=} \sum_{n=1}^{\infty} (-1)^{n-1} \frac{(t-1)^n}{n}$$

convergeix si i només si $t - 1 \in p\mathbb{Z}_p$.

La definició del logarítme es pot extende a $\mathbb{Q}_p$ definint $\log(p) = 0$ (o qualsevol altre valor).

5. Demostreu que en el radi de convergència, exp i log satisfàn les propietats usuals:
   a) $\exp(x_1 + x_2) = \exp(x_1)\exp(x_2)$.
   b) $\log(t_1 t_2) = \log(t_1) + \log(t_2)$.
   c) $\exp(\log(1 + x)) = 1 + x$ i $\log(\exp(x)) = x$.
6. Sigui p un primer senar i $m \geq 1$ o bé $p = 2$ i $m \geq 2$, demostreu l'isormorfisme de grups:

$$\begin{aligned} (p^m\mathbb{Z}_p, +) &\xrightarrow{\cong} (1 + p^m\mathbb{Z}_p, \cdot\,) \\ x &\longmapsto \exp(x) \\ \log(t) &\longleftarrow\!\shortmid t. \end{aligned}$$

Factorització a $\mathbb{Q}_p[x]$ i poligons de Newton

7. Sigui $f(x) = \sum_{i=0}^{N} a_i x^i \in \mathbb{Q}_p[x]$ amb $a_0 a_N \neq 0$. L cos de descomposició, sobre $\mathbb{Q}_p$ de f.

$$X = \left\{ \left(i, v_{p(a_i)} \right) \in \mathbb{R}^2 \mid i = 1, ..., N \right\}.$$

   $N(f) =$ Polígon de Newton.

   Si la línea del segment del polígon de Newton de f té $(r, v(a_r)), ..., (s, v(a_s))$ de pendent m_j (dins del polígon.) Aleshores f té $s - r$ arrels $\alpha_1, ..., \alpha_{s-r}$ de valoració $\omega(\alpha_i) = m$ on $\omega(x) \stackrel{\text{def}}{=} \frac{1}{[L:\mathbb{Q}_p]} v_{p\left(N_{L/K}(\alpha)\right)}$. I en questa situació

$$f(x) = a_N \prod_{j=1}^{t} f_j(x)$$

   és la factorització de f a $\mathbb{Q}_p[x]$, on

$$f_j = \prod_{w(\alpha_i) = m_j} (x - \alpha_i).$$

   (a $L[x]$)

8. Si $f \in \mathbb{Z}_p[x]$ de grau N. Si $N(f)$ només té una pendent i no passa per cap punt amb coordenades enteres, aleshores f és irreductible a $\mathbb{Q}_p$.
9. *Criteri d'Eiseinstein.* Sigui $f \in \mathbb{Z}_p[x]$ un polinomi de grau N, que satisfà:

$$v_p(a_N) = 0, \quad v_p(a_0) = 1 \quad i \quad v_p(a_i) \geq 1.$$

   Demostreu que f és irreductible a $\mathbb{Q}_p[x]$.

L'exercici següent us pot ser útil pels problemes 35, 36, 39 per entregar.

10. Sigui p un primer senar. Estudia els grups següents:
    a) $\left(1 + p\mathbb{Z}_p, \cdot\right)$
    b) $\left(1 + p\mathbb{Z}_p, \cdot\right) / \left(1 + p\mathbb{Z}_p, \cdot\right)^2$