ZMĚNA OZNAČENÍ

Lemma 1 $\to$ Lemma 8

Lemma 2 $\to$ Lemma 9, navíc přidáno $F(0)=0$ do (iv).

Důkaz Lemmatu 9:

Pro libovolné $\alpha \in \{0,1,\dots,p^n-2\}$ máme zápis v p-adické poziční soustavě:

$$\alpha = a_0 + a_1 p + \dots + a_{n-1} p^{n-1}, \qquad (*)$$

kde $a_0,\dots,a_{n-1} \in I := \{0,1,\dots,p-1\}$.

Z (i), (ii) a (iv) plyne

$$F(\alpha) \overset{(i),(ii)}{\le} F(a_0) + F(a_1) + \dots + F(a_{n-1}) \overset{(i),(iv)}{\le} a_0 + a_1 + \dots + a_{n-1} =: S(\alpha).$$

Ukážeme, že pro všechna $\alpha \in \{0,1,\dots,p^n-2\}$ platí $F(\alpha) = S(\alpha)$.

Je-li $p^n-2 < 2$, plyne z (iv), dále tedy předpokládáme $p^n \ge 2$.

$$\sum_{\alpha=0}^{p^n-1} S(\alpha) = \sum_{(a_0,\dots,a_{n-1})\in I^n} \sum_{j=0}^{n-1} a_j = \frac{1}{2} \sum_{(a_0,\dots,a_{n-1})\in I^n} \left(\sum_{j=0}^{n-1} a_j + \sum_{j=0}^{n-1} (p-1-a_j) \right) = \frac{1}{2} \sum_{(a_0,\dots,a_{n-1})\in I^n} \sum_{j=0}^{n-1} (p-1) =$$

$$= \frac{1}{2} p^n \cdot n \cdot (p-1)$$

Odtud vzhledem k $S(0)=0$ plyne

$$\sum_{\alpha=1}^{p^n-2} S(\alpha) = \frac{1}{2} p^n \cdot n(p-1) - S(p^n-1) = \frac{1}{2} p^n n(p-1) - n(p-1) = \frac{1}{2} n(p-1)(p^n-2).$$

Vzhledem k (iii) žádná z nerovností $F(\alpha) \le S(\alpha)$, kde $\alpha = 1,2,\dots,p^n-2$, není ostrá, ale platí rovnost. Zbývá ukázat, že

$$S(\alpha) = (p-1) \sum_{i=0}^{n-1} \left\langle \frac{p^i \alpha}{p^n-1} \right\rangle$$

pro každé $\alpha = 1,2,\dots,p^n-2$. Rozepišme α ve tvaru (*) výše:

$$\alpha = a_0 + a_1 p + \dots + a_{n-2} p^{n-2} + a_{n-1} p^{n-1}$$

$$p\alpha \equiv a_0 p + a_1 p^2 + \dots + a_{n-2} p^{n-1} + a_{n-1} \pmod{p^n-1},$$

obecně $p^i\alpha \equiv a_0 p^i + a_1 p^{i+1} + \dots + a_{n-i-1} p^{n-1} + a_{n-i} + \dots + a_{n-1} p^{i-1} \pmod{p^n-1}$

pro každé $i = 0,\dots,n-1$, tedy vzhledem k tomu, že pravá strana je nezáporná a menší než p^n-1 (případ $a_0 = a_1 = \dots = a_{n-1} = p-1$ nenastane, protože $\alpha < p^n-1$), jde o zbytek po dělení $p^i\alpha$ číslem p^n-1, tj.

$$(p^n-1) \cdot \left\langle \frac{p^i\alpha}{p^n-1} \right\rangle = a_0 p^i + a_1 p^{i+1} + \dots + a_{n-i-1} p^{n-1} + a_{n-i} + \dots + a_{n-1} p^{i-1}.$$

Sečtením

$$\sum_{i=0}^{n-1} \left\langle \frac{p^i\alpha}{p^n-1} \right\rangle = \frac{1}{p^n-1} \cdot S(\alpha) \cdot \frac{p^n-1}{p-1} = \frac{S(\alpha)}{p-1}.$$

$\blacksquare$