

Pro libovolné $a \in \mathbb{N}$, $(a, m) = 1$ označme $\sigma_a \in \text{Gal}(\mathbb{Q}(\zeta_m) / \mathbb{Q}(\zeta_p))$ automorfismu daný předpisem $\sigma_a(\zeta_m) = \zeta_m^a$ (tedy $\sigma_a(\zeta_p) = \zeta_p$).

Pak

$$N_{\mathbb{P}^{\sigma_a^{-1}}} (g(x)) = N_{\mathbb{P}} (g(x)^{\sigma_a}) = N_{\mathbb{P}} (g(x^a)),$$

neboli

$$g(x)^{\sigma_a} = \left(- \sum_{b \in \mathbb{F}_q^*} \chi(b) \psi(b) \right)^{\sigma_a} = - \sum_{b \in \mathbb{F}_q^*} (\chi(b))^a \cdot \psi(b) = g(x^a).$$

Pro libovolné $a \in \mathbb{N}_0$ definujeme

$$G(a) = N_{\mathbb{P}} (g(x^a))$$

Odtud $G(0) = 0$ podle LS (c), $G(a+b) \leq G(a) \cdot G(b)$ pro každé $a, b \in \mathbb{N}_0$ podle LS (f), $G(pa) = G(a)$ pro každé $a \in \mathbb{N}_0$ podle LS (e).

Dále platí

$$\left(\prod_{a=1}^{q-2} g(x^a) \right)^2 = \prod_{a=1}^{q-2} g(x^a) \cdot \prod_{a=1}^{q-2} g(x^{q-1-a}) \stackrel{m|q-1}{=} \prod_{a=1}^{q-2} (g(x^a) \cdot g(x^{-a})) = \prod_{a=1}^{q-2} (g(x^a) \cdot g(\bar{x}^a))$$

$$\overline{g(x^a)} = - \sum_{b \in \mathbb{F}_q^*} \bar{\chi}^a(b) \cdot \bar{\psi}(b) = - \sum_{b \in \mathbb{F}_q^*} \bar{\chi}^a(b) \cdot \psi(-b) = - \bar{\chi}^a(-1) \cdot \sum_{b \in \mathbb{F}_q^*} \bar{\chi}^a(-b) \psi(-b) =$$

$$= \bar{\chi}^a(-1) \cdot g(x^a)$$

Odtud využijeme LS (b)

$$g(x^a) \cdot g(\bar{x}^a) = \begin{cases} x^a(-1) & \text{je-li } \chi^a \text{ trivialní} \\ x^a(-1) \cdot q & \text{je-li } \chi^a \text{ netrivialní} \end{cases}$$

Přidáme-li předpoklad $m = q - 1$ (to je tedy pouze speciální případ):

$$\left(\prod_{a=1}^{q-2} g(x^a) \right)^2 = \prod_{a=1}^{q-2} ((x(-1))^a \cdot q) = \pm q^{q-2}$$

Odtud

$$\sum_{a=1}^{q-2} G(a) = \frac{1}{2} N_{\mathbb{P}} (q^{q-2}) = \frac{1}{2} (q-2) \cdot N_{\mathbb{P}} (q) = (q-2) \cdot f \cdot (p-1)$$