

Chceme ukázat, že se ideál generovaný $g(x)$ rozkládá na prvoideály. (10)

$$g(x^a) = g(\omega^{-da})$$

$$g(x) \mathbb{Z}[\zeta_{mp}] = \prod_{a \in R} \mathcal{P}^{\sigma_a^{-1} \nu_{\mathcal{P}}(g(x^a))}$$

kde R je systém reprezentativů faktorgrupy $\mathbb{Z}_m^x / \langle [p]_m \rangle$

probit se do $\mathbb{Q}(\zeta_{q-1}, \zeta_p) / \mathbb{Q}(\zeta_p)$ měřítko, je

$$\nu_{\mathcal{P}}(g(x^a)) = \nu_{\mathcal{P}}(g(x^a)) = G(ad)$$

Podle lemmatu 9 je $G(ad) = (p-1) \sum_{i=0}^{f-1} \left\langle \frac{p^i ad}{q-1} \right\rangle = (p-1) \sum_{i=0}^{f-1} \left\langle \frac{p^i a}{m} \right\rangle$

$$g(x) \mathbb{Z}[\zeta_{mp}] = \mathcal{P}^{\sum_{a \in R} G(ad) \sigma_a^{-1}}$$

$$\sum_{a \in R} G(ad) \sigma_a^{-1} = (p-1) \sum_{a \in R} \sigma_a^{-1} \sum_{i=0}^{f-1} \left\langle \frac{p^i a}{m} \right\rangle$$

Odtud

$$g(x) \mathbb{Z}[\zeta_{mp}] = \mathcal{P}^{(p-1) \sum_{a \in R} \sum_{i=0}^{f-1} \left\langle \frac{p^i a}{m} \right\rangle \sigma_{ap^i}^{-1}} = \mathcal{P}^{(p-1) \sum_{\substack{t=1, \dots, m \\ (t, m)=1}} \left\langle \frac{t}{m} \right\rangle \sigma_t^{-1}}$$

Prolo

$$g(x)^m \mathbb{Z}[\zeta_m] = \mathfrak{p}^{m\theta_m}$$

neboť $\mathfrak{p}^{(p-1)} = \mathfrak{p} \mathbb{Z}[\zeta_{mp}]$