MODULARNE FORME: TREĆA ZADAĆA

(1) Neka je p prost broj, $q = p^k$, $k > 1$. Dokažite da je norma sa $\mathbb{F}_q$ u $\mathbb{F}_p$ surjektivno preslikavanje.

(2) Neka je p neparan prost broj, $q = p^k$, $N \in \mathbb{N}$ neparan, $N > 1$ i χ multiplikativan karakter polja $\mathbb{F}_q$ reda $2N$ (postoji jer je $q \equiv 1 \pmod{2N}$). Neka je $E^N : y^2 = x(x+1)(x+t^N)$ eliptička ploha. Dokažite

$$\#E^N(\mathbb{F}_q) = q^2 + \sum_{i=1}^{N-1} \chi^{2i}(-1) J(\chi^{2i}, \chi^N),$$

gdje $\#E^N(\mathbb{F}_q)$ označava broj rješenja $(x, y, t) \in \mathbb{F}_q^3$ gornje jednadžbe (samo afina rješenja), dok je $J(\chi_1, \chi_2) = \sum_{x \in \mathbb{F}_q} \chi_1(x)\chi_2(1-x)$ Jacobijeva suma.