Extra opgaven bij het college Coderingstheorie

Opgave 1. We beschouwen lineaire codes C over $\mathbb{F}_q$ met redundantie $r = 3$ en minimumafstand $d = 4$.
(i) Bewijs: er bestaat een dergelijke code C van lengte $n \geq 4$ dan en slechts dan als er n punten bestaan in $\mathbb{P}^2(\mathbb{F}_q)$ waarvan er geen drie op één lijn liggen.
(ii) Bewijs dat de lengte n van een dergelijke code voldoet aan $n \leq q + 2$.
(iii) Kun je, voor elke $q > 2$, een lineaire code geven over $\mathbb{F}_q$ van lengte $q + 1$, redundantie 3 en minimumafstand 4? Hint: beschouw de niet-ontaarde kwadriek Q in $\mathbb{P}^2$ gegeven door de vergelijking $x_0^2 = x_1 x_2$.
(iv) Kun je, als q even is, een dergelijke code geven van lengte $q + 2$? Hint: de raaklijnen aan Q gaan allemaal door één punt.

Opgave 2. Zij n oneven en zij $\mathcal{S}$ een cyclotomische nevenklasse modulo n ten opzichte van $\mathbb{F}_2$. Laat $e \in \mathbb{F}_2[X]$ de bijbehorende elementaire idempotent. Kies een element α van multiplicatieve orde n in een uitbreidingslichaam van $\mathbb{F}_2$. Met $\mathcal{S}$ correspondeert dan een cyclische code C van lengte n. Brengt e de code C voort?