Chevalley-Warning & Erdös-Ginzburg-Ziv

Théorème : Soient p premier, $r \in \mathbb{N}^*$, $q = p^r$.
Soient $f_1, \dots, f_s \in \mathbb{F}_q[X_1, \dots, X_n]$, $\sum_{i=1}^{s} \deg f_i < n$, $V = \{x \in \mathbb{F}_q^n, \forall i \in \{1,\dots,s\}, f_i(x) = 0\}$.
$\#V \equiv 0 \ [p]$.

Posons $P = \prod_{i=1}^{s} (1 - f_i^{q-1})$. Soit $x \in \mathbb{F}_q^n$.
- Si $x \in V$, alors $\forall i$, $f_i(x) = 0$ donc $P(x) = 1$.
- Si $x \notin V$, alors $\exists i_0$, $f_{i_0}(x) \neq 0$ donc $f_{i_0}(x)^{q-1} = 1$ dans $\mathbb{F}_q$ donc $P(x) = 0$.

Considérons $S : f \mapsto \sum_{x \in \mathbb{F}_q^n} f(x)$. On a : $S(P) = \sum_{x \in \mathbb{F}_q^n} P(x) = \sum_{x \in V} 1 \ [q]$
$\equiv \#V \ [p]$ car $q = p^r$

Lemme : Si $u = 0$ ou $(q-1) \nmid u$, alors $s(X^u) = \sum_{x \in \mathbb{F}_q} x^u = 0$ avec la convention $0^0 = 1$.

- Si $u = 0$, alors $s(X^u) = \sum_{x \in \mathbb{F}_q} 1 = q = 0$.
- Sinon, par division euclidienne, $u = (q-1)k + r$ avec $0 < r < q-1$.
$\mathbb{F}_q^\times$ est cyclique : soit y un générateur.
$s(X^u) = \sum_{x \in \mathbb{F}_{q_k}} x^u = \sum_{x \in \mathbb{F}_q^\times} x^u = \sum_{x \in \mathbb{F}_q^\times} (yx)^u = y^u s(X^u)$ donc $(1 - y^u) s(X^u) = 0$.
Or $y^u = (y^{q-1})^k y^r = y^r \neq 1$ car $0 < r < q-1$, donc par intégrité de $\mathbb{F}_q$, $s(X^u) = 0$.

$\deg P = \sum_{i=1}^{s} (q-1) \deg f_i < n(q-1)$ par hypothèse.
Donc on peut écrire $P = \sum_{|u| < n(q-1)} \alpha_u X^u$ où $\alpha_u \in \mathbb{F}_q$, $X^u = X_1^{u_1} \cdots X_n^{u_n}$
et $|u| = \sum_{j=1}^{n} u_j$.

Si $|u| < n(q-1)$, $S(X^u) = \sum_{x \in \mathbb{F}_q^n} x_1^{u_1} \cdots x_n^{u_n}$
$= \left(\sum_{x_1 \in \mathbb{F}_q} x_1^{u_1}\right) \cdots \left(\sum_{x_n \in \mathbb{F}_q} x_n^{u_n}\right) = \prod_{i=1}^{n} s(X^{u_i})$.

Puisque $\sum_{j=1}^{n} u_j < n(q-1)$, $\exists j_0 \in \{1, \dots, n\}$, $u_{j_0} < q-1$ donc par lemme, $s(X^{u_{j_0}}) = 0$.

Donc $S(P) = 0$, $\#V \equiv 0 \ [p]$.

Théorème : Soit p premier. Soit $(a_1, \dots, a_{2p-1}) \in \mathbb{Z}^{2p-1}$.
On peut en trouver p dont la somme est divisible par p.

Soient $P_1 = \sum_{k=1}^{2p-1} X_k^{p-1}$, $P_2 = \sum_{k=1}^{2p-1} \bar{a}_k X_k^{p-1} \in \mathbb{F}_p[X_1, \dots, X_{2p-1}]$
$\deg P_1 + \deg P_2 < 2p-1$ et $(0, \dots, 0)$ est une racine commune à P_1 et P_2.
Par le théorème précédent, il y en a au moins une autre, notée $(x_1, \dots, x_{2p-1})$.
$P_1(x) = 0 = \sum_{i=1}^{2p-1} x_i^{p-1}$. Or $x_i^{p-1} = \begin{cases} 0 \text{ si } x_i = 0 \\ 1 \text{ sinon} \end{cases}$
Donc comme les x_i sont non tous nuls, il y en a p non nuls, notés
$x_{\eta_1}, \dots, x_{\eta_p}$. De là, $P_2(x) = 0$ assure $\sum_{i=1}^{p} \overline{a_{\eta_i}} = 0$.