Ref : Théorie de Galois ; Gozard ; p. 85.

Théorème :

$p \in \mathcal{P}$; $n \in \mathbb{N}^*$. soit $q = p^n$.

- Il existe un unique corps à q elts à $\mathbb{F}_p$-iso près.
  C'est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$.

Déf : Un corps est dit premier s'il ne contient aucun ss-corps strict.

Démo : K un corps ; le ss-corps de K engendré par 1_K est un ss-corps premier ; c'est l'intersection de tous les ss-corps de K.

- Unicité :

Soit K un corps à q elts. C'est un corps fini à q elts donc $car(K) | q$ car K fini
or $car(K) \in \mathcal{P}$ car K corps.
donc $car(K) = p$. et le ss-corps premier de K est $\mathbb{F}_p$. (c'est le ss-corps engendré par 1_K).

$(K^* ; \times)$ est un gpe à $q-1$ elts donc par thm de Lagrange ;
$\forall x \in K^*$; $x^{q-1} = 1$ d'où $\forall x \in K$; $x^q = x$.

Soit $X^q - X \in \mathbb{F}_p[X]$; de deg q qui admet donc au plus q racine dans K et comme tous les elts de K sont racine de $X^q - X$ alors K est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$.

Théorème : K un corps ; $P \in K[X]$ polynôme de deg ≥ 1.
Si Σ et Σ' deux corps de décomposition de P sur K alors il existe un K-isomorphisme entre eux.

Donc K est bien unique à $\mathbb{F}_p$-iso près.

- Existence :

Soit $K = D_{\mathbb{F}_p}(X^q - X)$ corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$.
Soit L l'ensemble des racines de $X^q - X$ dans K.

Soit $g : \begin{cases} K \to K \\ t \mapsto t^q \end{cases}$. c'est F^n où $F : \begin{cases} K \to K \\ t \mapsto t^p \end{cases}$. automorphisme de Frobenius car K de char p et K fini. (prop. $\overline{\text{VII}}$. 14).

donc g automorphisme de K.

$h = \{x \in K ; g(x) = x\} = \mathrm{Fix}(g)$ qui est un ss-corps de K.

Donc $\mathbb{F}_p \subset h$ car $\mathbb{F}_p$ est le $\underbrace{\text{ss-corps premier}}_{= \text{intersection de tous les ss-corps de } K}$ de K.

Le polynôme dérivé de $X^q - X$ est $qX^{q-1} - 1 = -1$ car $p | q$ et car$(K) = p$.

ainsi $(qX^{q-1} - 1) \wedge (X^q - X) = 1$.

Donc toutes les racines de $X^q - X$ sont simples.

Donc $\# h = q$; h est donc un corps à q elts.

(Et $h = K = D_{\mathbb{F}_p}(X^q - X)$).

Corollaire: Le produit des elts de $\mathbb{F}_q^*$ est -1.

Preuve: $\mathbb{F}_q = \{0 ; a_1 ; \cdots ; a_{q-1}\}$. $X^{q-1} - 1 = \prod_{i=1}^{q-1} (X - a_i)$ donc $-1 = a_1 \cdots a_{q-1}$.

Corollaire: (Théorème de Wilson).

$p \in \mathbb{N}$; $p \geq 2$; p premier $\Longleftrightarrow (p-1)! + 1 = 0 [p]$.

Preuve:

$\Rightarrow$] p premier alors le produit des elts de $\mathbb{F}_p^*$ est -1

donc $(p-1)! = -1 \bmod [p]$.

$\Leftarrow$] Soit $C \in (\mathbb{Z}/p\mathbb{Z})^*$; on a un représentant de la classe de C.

tq $1 \leq a \leq p-1$.

Comme $(p-1)! = -1 [p]$ alors $C \times (-\prod_{\substack{i=1 \\ i \neq a}}^{p-1} i) = 1 [p]$.

donc C inversible.

Donc $\mathbb{Z}/p\mathbb{Z}$ est un corps donc p est premier.