$A(n,q) :=$ ensemble polynomes irréductibles unitaires de degré n sur $\mathbb{F}_q[X]$

$I(n,q) = \# A(n,q)$

Théorème : $\forall n \geq 1 \quad I(n,q) \geq 1$ et $I(n,q) \underset{n\to+\infty}{\sim} \dfrac{q^n}{n}$

preuve : $n \geq 1$, q

- $X^{q^n} - X = \prod_{d|n} \prod_{P\in A(d,q)} P$

Soit d un diviseur de n, $P \in A(d,q)$ et $K = \mathbb{F}_q(x) \simeq \mathbb{F}_q[X]/_{\langle P\rangle}$ un corps de rupture de P où x est une racine de P.
On a $[K:\mathbb{F}_q] = \deg P = d$ et donc par unicité des corps finis K est isomorphe à $\mathbb{F}_{q^d}$. Comme $\mathbb{F}_{q^d}$ est l'ensemble des racines de $X^{q^d} - X$ on a $x^{q^d} = x$. Or comme $d|n$

$$x^{q^n} = \underbrace{\left[\left(x^{q^d}\right)^{q^d} \cdots\right]^{q^d}}_{\frac{n}{d}\text{ fois}} = \underbrace{\left(x^{q^d}\right)^{q^d} \cdots\Big)^{q^d}}_{\frac{n}{d}-1\text{ fois}} = \cdots = x^{q^d} = x$$

D'où x est racine de $X^{q^n} - X$, P étant le polynome minimal de x, on en déduit $P | X^{q^n} - X$

Soit P un facteur irréductible de $X^{q^n} - X$, d son degré
$X^{q^n} - X$ est scindé sur $\mathbb{F}_{q^n}$. Si on note x une racine de P dans $\mathbb{F}_{q^n}$, $K = \mathbb{F}_q(x)$ est un corps intermédiaire entre $\mathbb{F}_q$ et $\mathbb{F}_{q^n}$ de degré d sur $\mathbb{F}_q$. Comme $[\mathbb{F}_{q^n} : K][K:\mathbb{F}_q] = [\mathbb{F}_{q^n}, \mathbb{F}_q] = n$ on a $d | n$

Les racines de $X^{q^n} - X$ sont simples dans $\mathbb{F}_{q^n}$, donc tous les facteurs irréductibles de $X^{q^n} - X$ dans $\mathbb{F}_q[X]$ interviennent avec une multiplicité égale à 1.
On a alors $X^{q^n} - X = \prod_{d|n} \prod_{P\in A(d,q)} P$

En regardant les degré on obtient

$$\sum_{d|n} d\, I(d,q) = q^n$$

En appliquant la formule d'inversion de Möbius à $n \to n\, I(n,q)$ on obtient

$$n\, I(n,q) = \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$$

Soit $I(n,q) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$

On pose alors $I(n,q) = \frac{q^n + r_n}{n}$ où $r_n = \sum_{\substack{d|n \\ d<n}} \mu\left(\frac{n}{d}\right) q^d$

On majore alors r_n

$$|r_n| \leqslant \sum_{d=1}^{\lfloor \frac{n}{2} \rfloor} q^d = q\, \frac{q^{\lfloor \frac{n}{2} \rfloor} - 1}{q-1}$$

En particulier $|r_n| \leqslant \frac{q^{\lfloor \frac{n}{2} \rfloor + 1}}{q-1}$ et donc r_n est négligeable

devant q^n lorsque n tend vers $+\infty$

D'où l'équivalent $I(n,q) \sim \frac{q^n}{n}$

On a aussi $|r_n| \leqslant \frac{q^{\lfloor \frac{n}{2} \rfloor + 1}}{q/2} \leqslant 2 q^{\lfloor \frac{n}{2} \rfloor} < q^n$

D'où $\forall n \geqslant 1$ $I(n,q) > 0$