Факти за полиноми над крайни полета

A. $\forall f(x) \in \mathbb{F}_2[x]$, $f(0) = 1$ съществува естествено число m, за което

$f(m)$ дели $x^m - 1$

Най-малкото такова m наричаме ред на f: $\operatorname{ord} f$.

B. Ако f е неразложим от степен n, то

$\operatorname{ord} f \mid 2^n - 1$

Ако $\operatorname{ord} f = 2^n - 1$, то f се нарича примитивен полином.

С. Брой на примитивните полиноми от степен n е $\varphi(2^n-1)/n$.

Пример.

$n=3 \quad \frac{\varphi(2^3-1)}{3} = \frac{\varphi(7)}{3} = 2$

Примитивни полиноми от степен 3:

x^3+x+1

x^3+x^2+1

$n=4 \quad \frac{\varphi(2^4-1)}{4} = \frac{\varphi(15)}{4} = 2$

Примитивни полиноми от степен 4:

x^4+x+1

x^4+x^3+1

Неприводим, но не примитивен:

$x^4+x^3+x^2+x+1$.