Some slides for 22nd Lecture, Algebra 2

Diego Ruano

Department of Mathematical Sciences
Aalborg University
Denmark

25-04-2013

Lemma 4.8.3

Let τ, d and n be natural numbers, where $\tau > 1$. Then $\tau^d - 1$ divides $\tau^n - 1$ if and only if d divides n.

$$X^{p^n} - X = X(X^{p^n-1} - 1) = X \prod_{d | p^n - 1} \Phi_d$$

Theorem 4.8.8

The polynomial $X^{p^n} - X \in \mathbb{F}_p[X]$ is the product

$$X^{p^n} - X = f_1 \cdots f_r$$

of the monic irreducible polynomials $f_1, \ldots, f_r$ in $\mathbb{F}_p[X]$ of degree d, where $1 \leq d \leq n$ and $d | n$.

Corollary 4.8.9

Let N_d denote the number of monic irreducible polynomials of degree d in $\mathbb{F}_p[X]$. Then

$$p^n = \sum_{d|n} d N_d$$