1 - GF(p^k)* jest cykliczna

Thursday, 20 June 2024 18:02

Niech $N = |\mathbb{F}(q)^*| = q - 1$

Niech $A_d = \{a \in \mathbb{F}_q : a^d = 1\}$

Niech $B_d = \{a \in \mathbb{F}_q : a \text{ jest rzędu } d\}$

$B_d \subseteq A_d$, $B_d \neq \emptyset \Rightarrow d \mid N$

Zauważmy, że $\sum_{d \mid N} |B_d| = N$ (każdy element ma rzęd.)

Jeśli $B_d \neq \emptyset \Rightarrow |A_d| \geq d$, bo jeśli $a \in B_d$

to $(a^j)^d = 1$ dla $0 \leq j < d$.

Dodatkowo $|A_d| \leq d$, bo $X^d - 1 = 0$ ma co najwyżej d pierwiastków.

Zatem jeśli $B_d \neq \emptyset$ to $|A_d| = d$; $|B_d| = \varphi(d)$

$|B_d| = \varphi(d)$, bo A_d jest grupą, a B_d zbiorem jej generatorów.

Zatem $|B_d| \in \{0, \varphi(d)\}$:

$$N = \sum_{d \mid N} |B_d| \leq \sum_{d \mid N} \varphi(d) = N$$

$$\sum_{d \mid N} \varphi(d) = \sum_{l=0}^{k} \varphi(p^l) = \sum_{l=0}^{k} (p-1) \cdot p^{l-1} = (p-1) \frac{p^k - 1}{p-1} = p^k - 1 = N \quad \square$$