

Martyna Soszyńska i Patrycja Matys
7 listopada 2012

Zadanie 2.2

Niech $|G| < \infty$. Udowodnić, że liczba elementów rzędu n jest wielokrotnością $\varphi(n)$, gdzie φ jest funkcją Eulera.

Dowód:

Przypomnijmy:

$$\varphi(n) = |\{k \leq n : \text{NWD}(k, n) = 1\}|,$$

Stwierdzenie 2.7 Jeżeli $o(g)=n$, to $o(g^k) = \frac{n}{\text{NWD}(n,k)}$ (ze skryptu do wykładu).

Rozważmy dwa przypadki:

1. W grupie G nie istnieje element rzędu n . Wtedy liczba elementów rzędu n wynosi $0=0 * \varphi(n)$

2. W grupie G istnieje co najmniej jeden element rzędu n :

◇ $n=1$ (z definicji grupy: w grupie G istnieje jeden element rzędu 1)
dla tego elementu mamy: $1=\varphi(1)=1 * \varphi(1)=1 * \varphi(n)$

◇ $n \neq 1$ Rozpatrzmy maksymalny zbiór elementów grupy $G: \{g_1, g_2, \dots, g_k\}$, gdzie $k \in \mathbb{N}$, dla którego są spełnione warunki:

★ $\forall_i o(g) = n$, gdzie $i \in \{1, 2, \dots, k\}$

★★ $\forall_i \forall_{j \neq i} g_i \notin \langle g_j \rangle$, gdzie $i, j \in \{1, 2, \dots, k\}$

(**Uwaga:** Zauważmy, że z ★★ dla $i \neq j$ mamy: $\langle g_i \rangle \cap \langle g_j \rangle = \{1\}$ nie mają wspólnego elementu g , takiego, że $o(g) = n$.

Dowód:

Jeżeli $g \in \langle g_i \rangle$, to $\langle g \rangle \subseteq \langle g_i \rangle$,

ale $|\langle g \rangle| = |\langle g_i \rangle| < \infty \Rightarrow \langle g \rangle = \langle g_i \rangle$,

analogicznie, jeśli $g \in \langle g_j \rangle$, to $\langle g \rangle \subseteq \langle g_j \rangle$,

ale $|\langle g \rangle| = |\langle g_j \rangle| < \infty \Rightarrow \langle g \rangle = \langle g_j \rangle$.

Zatem z przechodniości mamy: $\langle g_i \rangle = \langle g_j \rangle$, co jest sprzeczne z ★★. □)

Weźmy dowolne $i \in \{1, 2, \dots, k\}$, wtedy $\langle g_i \rangle = \{1, g_i, g_i^2, \dots, g_i^{n-1}\}$,

ze **Stwierdzenia 2.7** wiemy, że $o(g_i^r) = \frac{n}{\text{NWD}(n,r)} \leq n$,

dla $r \in \{0, 1, \dots, n-1\}$, zatem dla każdego r takiego, że $\text{NWD}(n,r)=1$ mamy:
 $o(g_i^r) = o(g_i) = n$, czyli w $\langle g_i \rangle$ istnieje $\varphi(n)$ elementów rzędu n .

Przeprowadzając analogiczne rozumowanie dla pozostałych $i \in \{1, 2, \dots, k\}$ otrzymujemy, że w grupie G znajduje się $k * \varphi(n)$ elementów rzędu n . □