Maurycy Borkowski

20.10.2020

L2Z2

Założenie: $p \nmid n$

Dowód. Weźmy liczbę pierwszą $p > n$
Weźmy dowolny element grupy: $n \in \mathbb{Z}_p^* = (\{1, 2, \ldots, p-1\}, *)$

Oznaczmy rząd tego elementu: $k = ord(n)$
z definicji rzędu:

$$n^k = e_{\mathbb{Z}_p^*} = 1$$

Z Tw. Lagrange'a: w grupie skończonej rząd dowolnej jej podgrupy jest dzielnikiem rzędu grupy, mamy więc:

$$k \mid p-1$$

więc dla pewnej $m \in \mathbb{Z}$:

$$p - 1 = km$$

dalej:

$$n^{p-1} \equiv n^{km} \equiv (n^k)^m \equiv (1)^m \equiv 1$$

$$n^{p-1} \equiv 1$$

$$n^{p-1} - 1 \equiv 0$$

$$p \mid n^{p-1} - 1$$

□

a

Wzór: $\frac{n^3+5n+6}{6}$

* wiemy, że N prostych może podzielić płaszczyznę na maksymalnie $\frac{n^2+n+2}{2}$ obszarów.

Dowód.

Podstawa

Jedną płaszczyzną możemy podzielić przestrzeń na maksymalnie:

$$\frac{1+5+6}{2} = 2$$

Krok

Załóżmy, że przestrzeń możemy podzielić n płaszczyznami na $\frac{n^3+5n+6}{6}$ części. Jednym przecięciem płaszczyzną możemy maksymalnie dodać tyle kawałków przestrzeni ile możemy podzielić jedną płaszczyznę prostymi:

$$\frac{n^3+5n+6}{6} + \frac{n^2+n+2}{2} = \frac{n^3+3n^2+8n+12}{6} = \frac{(n+1)^3+5(n+1)+6}{6}$$

□