# Zad 15

niedziela, 20 listopada 2022 23:11

15. Udowodnij indukcyjnie małe twierdzenie Fermata mówiące, że dla dowolnej liczby pierwszej $p$ i naturalnej $a$

$$a^p \equiv a \bmod p.$$

Wsk.: rozwiń $(a+1)^p$ posługując się wzorem dwumiennym i określ kiedy $\binom{p}{i}$ dzieli się przez $p$.

$n=1$

$1^p = 1 \equiv_p 1$

załóżmy, że $a^p \equiv_p a$ dla $a \geq 1$. $\rightarrow a^p + 1 \equiv_p a+1$

$$(a+1)^p = \sum_{k=0}^{p} \binom{p}{k} a^k = a^0 + a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k$$

$$\binom{p}{k} = \frac{p^{\underline{k}}}{k!} = \frac{p(p-1)\cdots(p-k+1)}{k!}$$

$1 \leq k \leq p-1$, zatem żaden z czynników $k!$ nie jest równy $p$, ponadto $p$ jest liczbą pierwszą, zatem żaden czynnik $k!$ jej nie dzieli (oprócz 1). Wiemy także, że $\binom{p}{k} \in \mathbb{Z}$, zatem $\binom{p}{k}$ musi być jakąś wielokrotnością $p$, czyli $p \mid \binom{p}{k}$ dla $k = 1, 2, \ldots, p-1$. Mamy więc

$$a^0 + a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k \equiv_p a^0 + a^p = a^p + 1 \equiv a+1$$

z zał. ind.

czyli $(a+1)^p \equiv_p a+1$ $\square$