

Piccolo teorema di Fermat

Leonardo Bizzoni

October 25, 2023

Sia p un numero primo.

Ogni intero $a \in \mathbb{Z}$ soddisfa la congruenza:

$$a^p \equiv a \pmod{p}$$

Esempio: $3^2 \equiv 3 \pmod{2} \rightarrow 2 \mid 3^2 - 3 \rightarrow 2 \mid 6$

Ogni intero $a \in \mathbb{Z} : p \nmid a$ soddisfa la congruenza:

$$a^{p-1} \equiv 1 \pmod{p}$$

Esempio: $3 \equiv 1 \pmod{2} \rightarrow 2 \mid 3 - 1 \rightarrow 2 \mid 2$