

**Linguaggio e Metodi della Matematica**

Proprietà su numeri primi, numeri composti e mcd

- Lemma “Primo o Composto”:  $\forall n. (n > 1 \rightarrow n \text{ primo} \vee n \text{ composto})$
- Lemma “Divisibilità #1”:  $\forall a, b, c. (a|b \wedge a|c \rightarrow a|b+c)$
- Lemma “Divisibilità #2”:  $\forall a, b, c. (a|b \rightarrow a|b \cdot c)$
- Lemma “Divisibilità #3”:  $\forall a, b, c. (a|b \wedge b|c \rightarrow a|c)$
- Teorema “Test di Divisibilità”:  $\forall n. (n \text{ composto} \rightarrow \exists d. 1 < d \leq \sqrt{n} \wedge d|n)$
- Corollario “Test di Divisibilità”:  
 $\forall n. (n \text{ composto} \rightarrow \exists p. 1 < p \leq \sqrt{n} \wedge p|n \wedge p \text{ primo})$
- Lemma “Sequenze di Composti”:  $\forall n. \exists x. \forall i. (1 \leq i \leq n \rightarrow x+i \text{ composto})$
- Lemma “Primi non maggiorabili”:  $\forall n. \exists p. (p \text{ primo} \wedge p > n)$
- Lemma “Quadrati Dispari”:  $\forall n. (n \text{ dispari} \rightarrow n^2 \text{ dispari})$
- Lemma “Quadrati Pari”:  $\forall n. (n^2 \text{ pari} \rightarrow n \text{ pari})$
- Proprietà “Divisori di Primi #1”:  $\forall p. (p \text{ primo} \rightarrow \text{Div}(p) = \{1, p\})$
- Proprietà “Divisori di Primi #2”:  
 $\forall p, n. (p \text{ primo} \rightarrow \text{mcd}(p, n) = 1 \vee \text{mcd}(p, n) = p)$
- Proprietà “Divisori di Primi #3”:  
 $\forall p, q. (p \text{ primo} \wedge q \text{ primo} \wedge p|q \rightarrow p = q)$
- Proprietà “Divisori Primi”:  
 $\forall p, a. (a > 1 \wedge p \text{ primo} \rightarrow (p|a \leftrightarrow \text{mcd}(p, a) = p \leftrightarrow \text{mcd}(p, a) \neq 1))$
- Proposizione “Co-primalità dei Fattori”:  
 $\forall a, b. (a > 0 \wedge b > 0 \rightarrow \text{mcd}(\frac{a}{\text{mcd}(a, b)}, \frac{b}{\text{mcd}(a, b)}) = 1)$
- Teorema “Algoritmo di Divisione”:  
 $\forall a, d. (d > 0 \rightarrow \exists! q. \exists! r. a = d \cdot q + r \wedge 0 \leq r < d)$
- Teorema “Algoritmo di Euclide”:  
 $\forall a, b, q, r. (a = b \cdot q + r \rightarrow \text{mcd}(a, b) = \text{mcd}(b, r))$
- Teorema “di Bezout”:  
 $\forall a, b. (a, b > 0 \rightarrow \text{mcd}(a, b) = \min\{a \cdot x + b \cdot y \mid x, y \in \mathbb{Z} \wedge a \cdot x + b \cdot y > 0\})$
- Corollario “di Bezout #1”:  $\forall a, b. (a, b > 0 \rightarrow \exists s, t. \text{mcd}(a, b) = a \cdot s + b \cdot t)$
- Corollario “di Bezout #2”:  $\forall a, b, d. (a, b > 0 \wedge d|a \wedge d|b \rightarrow d|\text{mcd}(a, b))$
- Proposizione “Conseguenza di Bezout #1”:  
 $\forall a, b, c. (a|c \wedge b|c \wedge \text{mcd}(a, b) = 1 \rightarrow a \cdot b|c)$
- Proposizione “Conseguenza di Bezout #2”:  
 $\forall a, b, c. (a|b \cdot c \wedge \text{mcd}(a, b) = 1 \rightarrow a|c)$