Algoritmo d'Euclide

Progetto Lauree Scientifiche

prof.Sandro Pistori

L.S.S: "G. Galilei"

30 Gennaio 2007

Algoritmo Euclideo

Prendiamo a, b interi con $a, b > 0$ e supponiamo $0 < a < b$.
Dividiamo b per a, avremo che:

$$b = q_1 \cdot a + r_1, \qquad \text{con} \quad 0 \leq r_1 \leq a.$$

Algoritmo Euclideo

Prendiamo a, b interi con $a, b > 0$ e supponiamo $0 < a < b$.
Dividiamo b per a, avremo che:

$$b = q_1 \cdot a + r_1, \qquad \text{con} \quad 0 \leq r_1 \leq a.$$

Osserviamo che

Algoritmo Euclideo

Prendiamo a, b interi con $a, b > 0$ e supponiamo $0 < a < b$.
Dividiamo b per a, avremo che:

$$b = q_1 \cdot a + r_1, \qquad \text{con} \quad 0 \leq r_1 \leq a.$$

Osserviamo che

1. se $r_1 = 0$, allora $b = q_1 \cdot a$ e abbiamo giá che $\text{MCD}(a, b) = a$

Algoritmo Euclideo

Prendiamo a, b interi con $a, b > 0$ e supponiamo $0 < a < b$.
Dividiamo b per a, avremo che:

$$b = q_1 \cdot a + r_1, \qquad \text{con} \quad 0 \leq r_1 \leq a.$$

Osserviamo che

1. se $r_1 = 0$, allora $b = q_1 \cdot a$ e abbiamo giá che $\text{MCD}(a, b) = a$
2. altrimenti, preso un intero positivo d:
   - d divide sia a che b, allora dividerá anche r_1 in quanto combinazione lineare di a e b; infatti $r_1 = b - q \cdot a$

Algoritmo Euclideo

Prendiamo a, b interi con $a, b > 0$ e supponiamo $0 < a < b$.
Dividiamo b per a, avremo che:

$$b = q_1 \cdot a + r_1, \qquad \text{con} \quad 0 \leq r_1 \leq a.$$

Osserviamo che

1. se $r_1 = 0$, allora $b = q_1 \cdot a$ e abbiamo giá che $\text{MCD}(a, b) = a$
2. altrimenti, preso un intero positivo d:
   - d divide sia a che b, allora dividerá anche r_1 in quanto combinazione lineare di a e b; infatti $r_1 = b - q \cdot a$
   - viceversa, se d divide sia a che r_1, dividerá anche b per la stessa proprietà sopra.

Algoritmo Euclideo

Prendiamo a, b interi con $a, b > 0$ e supponiamo $0 < a < b$.
Dividiamo b per a, avremo che:

$$b = q_1 \cdot a + r_1, \qquad \text{con} \quad 0 \leq r_1 \leq a.$$

Osserviamo che

1. se $r_1 = 0$, allora $b = q_1 \cdot a$ e abbiamo giá che $\text{MCD}(a, b) = a$
2. altrimenti, preso un intero positivo d:
   - d divide sia a che b, allora dividerá anche r_1 in quanto combinazione lineare di a e b; infatti $r_1 = b - q \cdot a$
   - viceversa, se d divide sia a che r_1, dividerá anche b per la stessa proprietà sopra.

Quindi possiamo concludere che $\text{MCD}(a, b) = \text{MCD}(a, r_1)$, con il vantaggio che $r_1 < a < b$.

Algoritmo Euclideo

Ora ripetiamo lo stesso procedimento sostituendo al posto di a e b i nuovi valori a e r_1 con $r_1 < a$:

$$a = q_2 \cdot r_1 + r_2, \qquad \text{con} \quad 0 \leq r_2 < r_1$$

Algoritmo Euclideo

Ora ripetiamo lo stesso procedimento sostituendo al posto di a e b i nuovi valori a e r_1 con $r_1 < a$:

$$a = q_2 \cdot r_1 + r_2, \qquad \text{con} \quad 0 \leq r_2 < r_1$$

dove

Algoritmo Euclideo

Ora ripetiamo lo stesso procedimento sostituendo al posto di a e b i nuovi valori a e r_1 con $r_1 < a$:

$$a = q_2 \cdot r_1 + r_2, \qquad \text{con} \quad 0 \leq r_2 < r_1$$

dove

- se $r_2 = 0$, si ha che r_1 divide a, quindi $\text{MCD}(a, b) = \text{MCD}(a, r_1) = r_1$;

Algoritmo Euclideo

Ora ripetiamo lo stesso procedimento sostituendo al posto di a e b i nuovi valori a e r_1 con $r_1 < a$:

$$a = q_2 \cdot r_1 + r_2, \qquad \text{con} \quad 0 \leq r_2 < r_1$$

dove

- se $r_2 = 0$, si ha che r_1 divide a, quindi $\text{MCD}(a, b) = \text{MCD}(a, r_1) = r_1$;
- altrimenti, si ripetono le stesse conclusioni giungendo a definire che $\text{MCD}(a, b) = \text{MCD}(a, r_1) = \text{MCD}(r_1, r_2)$.

Algoritmo Euclideo

Ora ripetiamo lo stesso procedimento sostituendo al posto di a e b i nuovi valori a e r_1 con $r_1 < a$:

$$a = q_2 \cdot r_1 + r_2, \qquad \text{con} \quad 0 \leq r_2 < r_1$$

dove

- se $r_2 = 0$, si ha che r_1 divide a, quindi $\text{MCD}(a, b) = \text{MCD}(a, r_1) = r_1$;
- altrimenti, si ripetono le stesse conclusioni giungendo a definire che $\text{MCD}(a, b) = \text{MCD}(a, r_1) = \text{MCD}(r_1, r_2)$.

Continuiamo a costruire queste successioni di resto sino ad arrivare all'i-esima iterazione dove

$$r_i - 1 = q_i + 1 \cdot r_i + r_{i+1}, \qquad \text{con} \quad 0 \leq r_{i+1} < r_i$$

Algoritmo Euclideo

Ora ripetiamo lo stesso procedimento sostituendo al posto di a e b i nuovi valori a e r_1 con $r_1 < a$:

$$a = q_2 \cdot r_1 + r_2, \qquad \text{con} \quad 0 \leq r_2 < r_1$$

dove

- se $r_2 = 0$, si ha che r_1 divide a, quindi $\text{MCD}(a, b) = \text{MCD}(a, r_1) = r_1$;
- altrimenti, si ripetono le stesse conclusioni giungendo a definire che $\text{MCD}(a, b) = \text{MCD}(a, r_1) = \text{MCD}(r_1, r_2)$.

Continuiamo a costruire queste successioni di resto sino ad arrivare all'i-esima iterazione dove

$$r_i - 1 = q_i + 1 \cdot r_i + r_{i+1}, \qquad \text{con} \quad 0 \leq r_{i+1} < r_i$$

e avremo che

Algoritmo Euclideo

Ora ripetiamo lo stesso procedimento sostituendo al posto di a e b i nuovi valori a e r_1 con $r_1 < a$:

$$a = q_2 \cdot r_1 + r_2, \qquad \text{con} \quad 0 \leq r_2 < r_1$$

dove

- se $r_2 = 0$, si ha che r_1 divide a, quindi $\text{MCD}(a, b) = \text{MCD}(a, r_1) = r_1$;
- altrimenti, si ripetono le stesse conclusioni giungendo a definire che $\text{MCD}(a, b) = \text{MCD}(a, r_1) = \text{MCD}(r_1, r_2)$.

Continuiamo a costruire queste successioni di resto sino ad arrivare all'i-esima iterazione dove

$$r_i - 1 = q_i + 1 \cdot r_i + r_{i+1}, \qquad \text{con} \quad 0 \leq r_{i+1} < r_i$$

e avremo che

- se $r_i = 0$, allora $\text{MCD}(a, b) = r_{i-1}$;

Algoritmo Euclideo

Ora ripetiamo lo stesso procedimento sostituendo al posto di a e b i nuovi valori a e r_1 con $r_1 < a$:

$$a = q_2 \cdot r_1 + r_2, \qquad \text{con} \quad 0 \leq r_2 < r_1$$

dove

- se $r_2 = 0$, si ha che r_1 divide a, quindi $\text{MCD}(a, b) = \text{MCD}(a, r_1) = r_1$;
- altrimenti, si ripetono le stesse conclusioni giungendo a definire che $\text{MCD}(a, b) = \text{MCD}(a, r_1) = \text{MCD}(r_1, r_2)$.

Continuiamo a costruire queste successioni di resto sino ad arrivare all'i-esima iterazione dove

$$r_i - 1 = q_i + 1 \cdot r_i + r_{i+1}, \qquad \text{con} \quad 0 \leq r_{i+1} < r_i$$

e avremo che

- se $r_i = 0$, allora $\text{MCD}(a, b) = r_{i-1}$;
- altrimenti, continuiamo il procedimento

Algoritmo Euclideo

Poiché gli r_i sono interi non negativi e la successione di resti é decrescente, ad un certo punto ci dovremo fermare, cioé esisterá un r_n diverso da zero tale che $r_{n+1} = 0$, allora il nostro MCD(a, b) sará uguale all'ultimo resto diverso da zero della catena di divisioni.

Algoritmo Euclideo

Poiché gli r_i sono interi non negativi e la successione di resti é decrescente, ad un certo punto ci dovremo fermare, cioé esisterá un r_n diverso da zero tale che $r_{n+1} = 0$, allora il nostro MCD(a, b) sará uguale all'ultimo resto diverso da zero della catena di divisioni. Questo procedimento é vantaggioso perché non dobbiamo scomporre in fattori primi e si utilizzano divisioni sempre piú facili.

Algoritmo Euclideo

Poiché gli r_i sono interi non negativi e la successione di resti é decrescente, ad un certo punto ci dovremo fermare, cioé esisterá un r_n diverso da zero tale che $r_{n+1} = 0$, allora il nostro MCD(a, b) sará uguale all'ultimo resto diverso da zero della catena di divisioni. Questo procedimento é vantaggioso perché non dobbiamo scomporre in fattori primi e si utilizzano divisioni sempre piú facili.
Esempio: Calcolare $(1547, 560)$ utilizzando l'Algoritmo Euclideo.

$$1547 \quad = \quad 2 \cdot 560 + 427$$

Algoritmo Euclideo

Poiché gli r_i sono interi non negativi e la successione di resti é decrescente, ad un certo punto ci dovremo fermare, cioé esisterá un r_n diverso da zero tale che $r_{n+1} = 0$, allora il nostro MCD(a, b) sará uguale all'ultimo resto diverso da zero della catena di divisioni. Questo procedimento é vantaggioso perché non dobbiamo scomporre in fattori primi e si utilizzano divisioni sempre piú facili.
Esempio: Calcolare $(1547, 560)$ utilizzando l'Algoritmo Euclideo.

$$\begin{aligned} 1547 &= 2 \cdot 560 + 427 \\ 560 &= 1 \cdot 427 + 133 \end{aligned}$$

Algoritmo Euclideo

Poiché gli r_i sono interi non negativi e la successione di resti é decrescente, ad un certo punto ci dovremo fermare, cioé esisterá un r_n diverso da zero tale che $r_{n+1} = 0$, allora il nostro MCD(a, b) sará uguale all'ultimo resto diverso da zero della catena di divisioni. Questo procedimento é vantaggioso perché non dobbiamo scomporre in fattori primi e si utilizzano divisioni sempre piú facili.
Esempio: Calcolare $(1547, 560)$ utilizzando l'Algoritmo Euclideo.

$$\begin{aligned} 1547 &= 2 \cdot 560 + 427 \\ 560 &= 1 \cdot 427 + 133 \\ 427 &= 3 \cdot 133 + 28 \end{aligned}$$

Algoritmo Euclideo

Poiché gli r_i sono interi non negativi e la successione di resti é decrescente, ad un certo punto ci dovremo fermare, cioé esisterá un r_n diverso da zero tale che $r_{n+1} = 0$, allora il nostro MCD(a, b) sará uguale all'ultimo resto diverso da zero della catena di divisioni. Questo procedimento é vantaggioso perché non dobbiamo scomporre in fattori primi e si utilizzano divisioni sempre piú facili.
Esempio: Calcolare $(1547, 560)$ utilizzando l'Algoritmo Euclideo.

$$\begin{aligned} 1547 &= 2 \cdot 560 + 427 \\ 560 &= 1 \cdot 427 + 133 \\ 427 &= 3 \cdot 133 + 28 \\ 133 &= 4 \cdot 28 + 21 \end{aligned}$$

Algoritmo Euclideo

Poiché gli r_i sono interi non negativi e la successione di resti é decrescente, ad un certo punto ci dovremo fermare, cioé esisterá un r_n diverso da zero tale che $r_{n+1} = 0$, allora il nostro MCD(a, b) sará uguale all'ultimo resto diverso da zero della catena di divisioni. Questo procedimento é vantaggioso perché non dobbiamo scomporre in fattori primi e si utilizzano divisioni sempre piú facili.
Esempio: Calcolare $(1547, 560)$ utilizzando l'Algoritmo Euclideo.

$$\begin{aligned} 1547 &= 2 \cdot 560 + 427 \\ 560 &= 1 \cdot 427 + 133 \\ 427 &= 3 \cdot 133 + 28 \\ 133 &= 4 \cdot 28 + 21 \\ 28 &= 1 \cdot 21 + 7 \end{aligned}$$

Algoritmo Euclideo

Poiché gli r_i sono interi non negativi e la successione di resti é decrescente, ad un certo punto ci dovremo fermare, cioé esisterá un r_n diverso da zero tale che $r_{n+1} = 0$, allora il nostro MCD(a, b) sará uguale all'ultimo resto diverso da zero della catena di divisioni. Questo procedimento é vantaggioso perché non dobbiamo scomporre in fattori primi e si utilizzano divisioni sempre piú facili.
Esempio: Calcolare $(1547, 560)$ utilizzando l'Algoritmo Euclideo.

$$\begin{aligned} 1547 &= 2 \cdot 560 + 427 \\ 560 &= 1 \cdot 427 + 133 \\ 427 &= 3 \cdot 133 + 28 \\ 133 &= 4 \cdot 28 + 21 \\ 28 &= 1 \cdot 21 + 7 \\ 21 &= 3 \cdot 7 + 0. \end{aligned}$$

Algoritmo Euclideo

Poiché gli r_i sono interi non negativi e la successione di resti é decrescente, ad un certo punto ci dovremo fermare, cioé esisterá un r_n diverso da zero tale che $r_{n+1} = 0$, allora il nostro MCD(a, b) sará uguale all'ultimo resto diverso da zero della catena di divisioni. Questo procedimento é vantaggioso perché non dobbiamo scomporre in fattori primi e si utilizzano divisioni sempre piú facili.
Esempio: Calcolare $(1547, 560)$ utilizzando l'Algoritmo Euclideo.

$$\begin{aligned} 1547 &= 2 \cdot 560 + 427 \\ 560 &= 1 \cdot 427 + 133 \\ 427 &= 3 \cdot 133 + 28 \\ 133 &= 4 \cdot 28 + 21 \\ 28 &= 1 \cdot 21 + 7 \\ 21 &= 3 \cdot 7 + 0. \end{aligned}$$

e quindi MCD$(1547, 560) = 7$.

Algoritmo Euclideo

Teorema di Euclide esteso (Formula di Bezout)
Sia $d = (a, b)$, $a > b$. Allora esistono $u, v \in \mathbb{Z}$ tali che

$$d = u \cdot a + v \cdot b$$

Algoritmo Euclideo

Teorema di Euclide esteso (Formula di Bezout)
Sia $d = (a, b)$, $a > b$. Allora esistono $u, v \in \mathbb{Z}$ tali che

$$d = u \cdot a + v \cdot b$$

Proviamo ora a ricostruire u, v procedendo a ritroso nell'algoritmo euclideo: presi $\text{MCD}(a, b) = r_{i-1}$ e $u \cdot a + v \cdot b = r_{i-1}$, possiamo scrivere

Algoritmo Euclideo

Teorema di Euclide esteso (Formula di Bezout)
Sia $d = (a, b)$, $a > b$. Allora esistono $u, v \in \mathbb{Z}$ tali che

$$d = u \cdot a + v \cdot b$$

Proviamo ora a ricostruire u, v procedendo a ritroso nell'algoritmo euclideo: presi $\text{MCD}(a, b) = r_{i-1}$ e $u \cdot a + v \cdot b = r_{i-1}$, possiamo scrivere

$$r_{i-1} = r_{i-3} - q_{i-1} \cdot r_{i-2}$$

Algoritmo Euclideo

Teorema di Euclide esteso (Formula di Bezout)
Sia $d = (a, b)$, $a > b$. Allora esistono $u, v \in \mathbb{Z}$ tali che

$$d = u \cdot a + v \cdot b$$

Proviamo ora a ricostruire u, v procedendo a ritroso nell'algoritmo euclideo: presi $\text{MCD}(a, b) = r_{i-1}$ e $u \cdot a + v \cdot b = r_{i-1}$, possiamo scrivere

$$r_{i-1} = r_{i-3} - q_{i-1} \cdot r_{i-2}$$

e andiamo sostituire il valore di r_{i-2} che si ricava dall'uguaglianza

$$r_{i-4} = q_{i-2} \cdot r_{i-3} + r_{i-2}$$

Algoritmo Euclideo

Teorema di Euclide esteso (Formula di Bezout)
Sia $d = (a, b)$, $a > b$. Allora esistono $u, v \in \mathbb{Z}$ tali che

$$d = u \cdot a + v \cdot b$$

Proviamo ora a ricostruire u, v procedendo a ritroso nell'algoritmo euclideo: presi $\text{MCD}(a, b) = r_{i-1}$ e $u \cdot a + v \cdot b = r_{i-1}$, possiamo scrivere

$$r_{i-1} = r_{i-3} - q_{i-1} \cdot r_{i-2}$$

e andiamo sostituire il valore di r_{i-2} che si ricava dall'uguaglianza

$$r_{i-4} = q_{i-2} \cdot r_{i-3} + r_{i-2} \Rightarrow r_{i-2} = q_{i-2} \cdot r_{i-3} + r_{i-4}$$

Algoritmo Euclideo

Teorema di Euclide esteso (Formula di Bezout)
Sia $d = (a, b)$, $a > b$. Allora esistono $u, v \in \mathbb{Z}$ tali che

$$d = u \cdot a + v \cdot b$$

Proviamo ora a ricostruire u, v procedendo a ritroso nell'algoritmo euclideo: presi $\text{MCD}(a, b) = r_{i-1}$ e $u \cdot a + v \cdot b = r_{i-1}$, possiamo scrivere

$$r_{i-1} = r_{i-3} - q_{i-1} \cdot r_{i-2}$$

e andiamo sostituire il valore di r_{i-2} che si ricava dall'uguaglianza

$$\begin{aligned} r_{i-4} &= q_{i-2} \cdot r_{i-3} + r_{i-2} \Rightarrow r_{i-2} = q_{i-2} \cdot r_{i-3} + r_{i-4} \\ r_{i-1} &= r_{i-3} - q_{i-1} \cdot (r_{i-4} - q_{i-2} \cdot r_{i-3}) \end{aligned}$$

Algoritmo Euclideo

Teorema di Euclide esteso (Formula di Bezout)
Sia $d = (a, b)$, $a > b$. Allora esistono $u, v \in \mathbb{Z}$ tali che

$$d = u \cdot a + v \cdot b$$

Proviamo ora a ricostruire u, v procedendo a ritroso nell'algoritmo euclideo: presi $\text{MCD}(a, b) = r_{i-1}$ e $u \cdot a + v \cdot b = r_{i-1}$, possiamo scrivere

$$r_{i-1} = r_{i-3} - q_{i-1} \cdot r_{i-2}$$

e andiamo sostituire il valore di r_{i-2} che si ricava dall'uguaglianza

$$\begin{aligned} r_{i-4} &= q_{i-2} \cdot r_{i-3} + r_{i-2} \Rightarrow r_{i-2} = q_{i-2} \cdot r_{i-3} + r_{i-4} \\ r_{i-1} &= r_{i-3} - q_{i-1} \cdot (r_{i-4} - q_{i-2} \cdot r_{i-3}) = (1 + q_{i-1} \cdot q_{i-2}) \cdot r_{i-3} - q_{i-1} \cdot r_{i-} \end{aligned}$$

Algoritmo Euclideo

Teorema di Euclide esteso (Formula di Bezout)
Sia $d = (a, b)$, $a > b$. Allora esistono $u, v \in \mathbb{Z}$ tali che

$$d = u \cdot a + v \cdot b$$

Proviamo ora a ricostruire u, v procedendo a ritroso nell'algoritmo euclideo: presi $\text{MCD}(a, b) = r_{i-1}$ e $u \cdot a + v \cdot b = r_{i-1}$, possiamo scrivere

$$r_{i-1} = r_{i-3} - q_{i-1} \cdot r_{i-2}$$

e andiamo sostituire il valore di r_{i-2} che si ricava dall'uguaglianza

$$\begin{aligned} r_{i-4} &= q_{i-2} \cdot r_{i-3} + r_{i-2} \Rightarrow r_{i-2} = q_{i-2} \cdot r_{i-3} + r_{i-4} \\ r_{i-1} &= r_{i-3} - q_{i-1} \cdot (r_{i-4} - q_{i-2} \cdot r_{i-3}) = (1 + q_{i-1} \cdot q_{i-2}) \cdot r_{i-3} - q_{i-1} \cdot r_{i-} \end{aligned}$$

Ora sostituiamo in questa equazione il valore di r_{i-3} che si ottiene da $r_{i-5} = q_{i-3} \cdot r_{i-4} + r_{i-3}$ e avremo r_{i-1} come espressione in r_{i-3} e r_{i-4}.

Algoritmo Euclideo

Teorema di Euclide esteso (Formula di Bezout)
Sia $d = (a, b)$, $a > b$. Allora esistono $u, v \in \mathbb{Z}$ tali che

$$d = u \cdot a + v \cdot b$$

Proviamo ora a ricostruire u, v procedendo a ritroso nell'algoritmo euclideo: presi $\text{MCD}(a, b) = r_{i-1}$ e $u \cdot a + v \cdot b = r_{i-1}$, possiamo scrivere

$$r_{i-1} = r_{i-3} - q_{i-1} \cdot r_{i-2}$$

e andiamo sostituire il valore di r_{i-2} che si ricava dall'uguaglianza

$$\begin{aligned} r_{i-4} &= q_{i-2} \cdot r_{i-3} + r_{i-2} \Rightarrow r_{i-2} = q_{i-2} \cdot r_{i-3} + r_{i-4} \\ r_{i-1} &= r_{i-3} - q_{i-1} \cdot (r_{i-4} - q_{i-2} \cdot r_{i-3}) = (1 + q_{i-1} \cdot q_{i-2}) \cdot r_{i-3} - q_{i-1} \cdot r_{i-} \end{aligned}$$

Ora sostituiamo in questa equazione il valore di r_{i-3} che si ottiene da $r_{i-5} = q_{i-3} \cdot r_{i-4} + r_{i-3}$ e avremo r_{i-1} come espressione in r_{i-3} e r_{i-4}.Quindi andremo a sostituire r_{i-3} e continueremo questo procedimento fino ad ottenere r_{i-1} come combinazione lineare dei soli a e b.

Algoritmo Euclideo

Con i dati dell'esempio precedente:

Algoritmo Euclideo

Con i dati dell'esempio precedente:

$$7 \quad = \quad 28 - 1 \cdot 21 = 28 - 1 \cdot (133 - 4 \cdot 28)$$

Algoritmo Euclideo

Con i dati dell'esempio precedente:

$$\begin{aligned} 7 &= 28 - 1 \cdot 21 = 28 - 1 \cdot (133 - 4 \cdot 28) \\ &= 5 \cdot 28 - 1 \cdot 133 = 5(427 - 3 \cdot 133) - 1 \cdot 133 \end{aligned}$$

Algoritmo Euclideo

Con i dati dell'esempio precedente:

$$\begin{aligned} 7 &= 28 - 1 \cdot 21 = 28 - 1 \cdot (133 - 4 \cdot 28) \\ &= 5 \cdot 28 - 1 \cdot 133 = 5(427 - 3 \cdot 133) - 1 \cdot 133 \\ &= 5 \cdot 427 - 16 \cdot 133 = 5 \cdot 427 - 16(560 - 1 \cdot 427) \end{aligned}$$

Algoritmo Euclideo

Con i dati dell'esempio precedente:

$$\begin{aligned} 7 &= 28 - 1 \cdot 21 = 28 - 1 \cdot (133 - 4 \cdot 28) \\ &= 5 \cdot 28 - 1 \cdot 133 = 5(427 - 3 \cdot 133) - 1 \cdot 133 \\ &= 5 \cdot 427 - 16 \cdot 133 = 5 \cdot 427 - 16(560 - 1 \cdot 427) \\ &= 21 \cdot 427 - 16 \cdot 560 = 21 \cdot (1547 - 2 \cdot 560) - 16 \cdot 560 \end{aligned}$$

Algoritmo Euclideo

Con i dati dell'esempio precedente:

$$
\begin{aligned}
7 &= 28 - 1 \cdot 21 = 28 - 1 \cdot (133 - 4 \cdot 28) \\
&= 5 \cdot 28 - 1 \cdot 133 = 5(427 - 3 \cdot 133) - 1 \cdot 133 \\
&= 5 \cdot 427 - 16 \cdot 133 = 5 \cdot 427 - 16(560 - 1 \cdot 427) \\
&= 21 \cdot 427 - 16 \cdot 560 = 21 \cdot (1547 - 2 \cdot 560) - 16 \cdot 560 \\
&= 21 \cdot 1547 - 58 \cdot 560
\end{aligned}
$$

Algoritmo Euclideo

Con i dati dell'esempio precedente:

$$\begin{aligned} 7 &= 28 - 1 \cdot 21 = 28 - 1 \cdot (133 - 4 \cdot 28) \\ &= 5 \cdot 28 - 1 \cdot 133 = 5(427 - 3 \cdot 133) - 1 \cdot 133 \\ &= 5 \cdot 427 - 16 \cdot 133 = 5 \cdot 427 - 16(560 - 1 \cdot 427) \\ &= 21 \cdot 427 - 16 \cdot 560 = 21 \cdot (1547 - 2 \cdot 560) - 16 \cdot 560 \\ &= 21 \cdot 1547 - 58 \cdot 560 \end{aligned}$$

da cui segue

Algoritmo Euclideo

Con i dati dell'esempio precedente:

$$\begin{aligned} 7 &= 28 - 1 \cdot 21 = 28 - 1 \cdot (133 - 4 \cdot 28) \\ &= 5 \cdot 28 - 1 \cdot 133 = 5(427 - 3 \cdot 133) - 1 \cdot 133 \\ &= 5 \cdot 427 - 16 \cdot 133 = 5 \cdot 427 - 16(560 - 1 \cdot 427) \\ &= 21 \cdot 427 - 16 \cdot 560 = 21 \cdot (1547 - 2 \cdot 560) - 16 \cdot 560 \\ &= 21 \cdot 1547 - 58 \cdot 560 \end{aligned}$$

da cui segue $u = 21$ e $v = -58$.

Algoritmo Euclideo

Gli elementi a di $\mathbb{Z}_n$ che hanno inverso moltiplicativo sono tutti e soli quelli per cui $(a, n) = 1$.

Algoritmo Euclideo

Gli elementi a di $\mathbb{Z}_n$ che hanno inverso moltiplicativo sono tutti e soli quelli per cui $(a, n) = 1$.

$$a \cdot x = 1 (\mathrm{mod} n) \quad \text{se e solo se} \quad (a, n) = 1$$

Algoritmo Euclideo

Gli elementi a di $\mathbb{Z}_n$ che hanno inverso moltiplicativo sono tutti e soli quelli per cui $(a, n) = 1$.

$$a \cdot x = 1 (\mathrm{mod} n) \quad \text{se e solo se} \quad (a, n) = 1$$

Dim:
Sia $d = (a, n)$. Se $d > 1$ non puó esistere un b tale che $a \cdot b = 1 (\mathrm{mod} n)$ perché si avrebbe che d divide $(ab - 1)$ e quindi, siccome d divide a, d divide 1 che é contraddittorio con l'assunzione $d > 1$.

Algoritmo Euclideo

Gli elementi a di $\mathbb{Z}_n$ che hanno inverso moltiplicativo sono tutti e soli quelli per cui $(a, n) = 1$.

$$a \cdot x = 1 (\mathrm{mod} n) \quad \text{se e solo se} \quad (a, n) = 1$$

Dim:
Sia $d = (a, n)$. Se $d > 1$ non puó esistere un b tale che $a \cdot b = 1 (\mathrm{mod} n)$ perché si avrebbe che d divide $(ab - 1)$ e quindi, siccome d divide a, d divide 1 che é contraddittorio con l'assunzione $d > 1$.
Allora $d = 1$.

Algoritmo Euclideo

Gli elementi a di $\mathbb{Z}_n$ che hanno inverso moltiplicativo sono tutti e soli quelli per cui $(a, n) = 1$.

$$a \cdot x = 1 (\mathrm{mod} n) \quad \text{se e solo se} \quad (a, n) = 1$$

Dim:
Sia $d = (a, n)$. Se $d > 1$ non puó esistere un b tale che $a \cdot b = 1 (\mathrm{mod} n)$ perché si avrebbe che d divide $(ab - 1)$ e quindi, siccome d divide a, d divide 1 che é contraddittorio con l'assunzione $d > 1$.
Allora $d = 1$.
Suppongo, senza ledere, che $a < n$. Utilizzando l'Algoritmo Euclideo, sappiamo che esistono u, v tali che $u \cdot a + v \cdot n = 1$ e quindi l'inverso di a é esattamente u dal momento che $u \cdot a = 1 - v \cdot n$