



MCD ALGORITMO EUCLIDEO

$$\text{MCD}(168, 1911)$$

- ① divido il numero maggiore per quello minore
nella forma:

$$1911 = x \cdot 168 + r \quad \text{--- } 1911 - x \cdot 168$$

$$1911 = 11 \cdot 168 + 63 \quad \text{② prendo il divisore di prima e lo divido per il resto}$$

$$168 = 2 \cdot 63 + 42 \quad (168/63)$$

$$63 = 1 \cdot 42 + 21 \quad \text{③ ripeto ② fino a ottenere resto 0}$$

$$42 = 2 \cdot 21 + 0 \quad \text{questo}$$

$$\text{④ ho trovato il MCD! è } 21$$

BÉZOUT METODO TUTOR

- ① parto da sopra (algo eucl) e scrivo in funzione del resto
• scrivo a, b invece dei numeri di cui ho calcolato MCD
($a = 168, b = 1911$) per comodità calcoli

$$63 = b - 11 \cdot a$$

- ② proseguo scrivendolo per il prossimo resto $42 = a - 2 \cdot 63$ ③ sostituisco quella che ho già calcolato
 $42 = a - 2(b - 11 \cdot a)$
 $42 = -2b + 23a$

$$\begin{aligned} 21 &= 63 - 1 \cdot 42 \\ 21 &= (b - 11 \cdot a) - 1 \cdot (-2b + 23a) \\ 21 &= b - 11 \cdot a + 2b - 23a \\ 21 &= 3b - 34a \end{aligned} \quad \text{--- } \text{sostituisco anche le cose calcolate più su}$$

$$\text{trovati: } 21 = 3 \cdot 1911 - 34 \cdot 168$$

IDENTITÀ DI BÉZOUT metodo Pellorin

L'identità di Bézout mostra che il MCD tra a e b può essere rappresentato come
 $d = a \cdot x + b \cdot y$.
Dobbiamo trovare x e y .

- ① parto dalla penultima formula dell'algoritmo di Euclide (ma in funzione del resto)

$$21 = 63 - 1 \cdot 42 \quad \text{② prendo il resto della riga sopra e lo sostituisco}$$

$$42 = 168 - 2 \cdot 63$$

$$21 = 63 - 1(168 - 2 \cdot 63) \quad \text{③ faccio i calcoli e ripeto}$$

$$= 63 - 168 + 2 \cdot 63$$

$$21 = -168 + 3 \cdot 63$$

$$63 = 1911 - 11 \cdot 168$$

$$21 = -168 + 3(1911 - 11 \cdot 168)$$

$$= -168 + 3 \cdot 1911 - 33 \cdot 168$$

$$21 = \underbrace{-34 \cdot 168}_x + \underbrace{3 \cdot 1911}_y$$

abbiamo trovato x e y ! bravi tutti

EQ. CONGRUENZIALI

$$2^{10}x \equiv 3^{11} \pmod{7}$$

- ① il mio obiettivo è scriverla nella forma $X \equiv \text{qualcosa}$
quindi INIZIO A SEMPLIFICARE

• lavoro su $2^{10} \pmod{7}$. Mi ricordo che $2^3 = 8 \equiv 1 \pmod{7}$

$$2^{10} \equiv 2^9 \cdot 2 \equiv \underbrace{(2^3)^3}_{\text{congr 1 e } 1^3 = 1} \cdot 2 \equiv 2 \pmod{7}$$

• per 3^{11} , so che $3 \equiv 2 \pmod{7}$ ho visto sopra $\equiv 1$

$$3^{11} \equiv (3^2)^5 \cdot 3 \equiv 2^5 \cdot 3 \equiv 2^3 \cdot 2^2 \cdot 3 \equiv 4 \cdot 3 \equiv 12 \equiv 5$$

• dopo un po' di semplificazioni ottengo quindi $2x \equiv 5$

