



## MCD ALGORITMO EUCLIDEO

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

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

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

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

- ② prendo il divisore di prima  
e lo divido per il resto

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

$$63 = 1 \cdot 42 + 21$$

- ③ ripeto ② fino a ottenere  
resto 0

$$42 = 2 \cdot 21 + 0$$

- 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  
 $42 = a - 2 \cdot 63$   
 $42 = a - 2(b - 11 \cdot a)$   
 $42 = -2b + 23a$

- ③ sostituisco quella che ho  
già calcolato

$$\begin{aligned} 21 &= 63 - 1 \cdot 42 \\ 21 &= (b - 11 \cdot a) - 1 \cdot (-2b + 23a) \\ 21 &= b - 11 \cdot a + 2b - 23a \\ 21 &= 3b - 34a \end{aligned}$$

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)

$$21 = 63 - 1 \cdot 42$$

- ② prendo il resto della riga sopra  
e lo sostituisco

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

$$\begin{aligned} 21 &= 63 - 1(168 - 2 \cdot 63) \\ &= 63 - 168 + 2 \cdot 63 \end{aligned}$$

- ③ faccio i calcoli e ripeto

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

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

$$\begin{aligned} 21 &= -168 + 3(1911 - 11 \cdot 168) \\ &= -168 + 3 \cdot 1911 - 33 \cdot 168 \end{aligned}$$

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

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  $2^3 = 8 \equiv 1 \pmod{7}$

$$2^{10} = 2^9 \cdot 2 = (2^3)^3 \cdot 2 \equiv 1^3 \cdot 2 \equiv 2 \pmod{7}$$

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

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

• dopo un po' di semplificazioni ottengo quindi  $2x \equiv 5 \pmod{7}$

- ② una condizione necessaria perché ci sia soluzione, è che  
l'MCD tra il coeff. della  $x$  e il modulo divida il resto (qui  $\text{MCD}(2, 7) \mid 5$ )  
 $\text{MCD}(2, 7) = 1 \mid 5$ ? Sì - c'è soluzione

- ③ si cerca di trovare una soluzione, usando proprietà (come il PTF), o inversi  
con PTF ( $n^{p-1} \equiv 1$ )  $\rightarrow$  so che  $2^6 \equiv 1$

moltiplico per  $2^5$

$$2 \cdot 2^5 x \equiv 5 \cdot 2^5 \Leftrightarrow x \equiv 2^5 \cdot 5$$

ora, semplifico con le congruenze

$$x \equiv 2^4 \cdot 2 \cdot 5 \Leftrightarrow x \equiv 2 \cdot 2 \cdot 5$$

$$\Leftrightarrow x \equiv 20 \Leftrightarrow x \equiv 6$$

autunno "à mano"

cerco l'inverso di  $2 - 8 \equiv 1$  e  $2^3 = 8$ ,

$$\begin{aligned} \text{quindi } 2^2 \cdot 2x &\equiv 5 \cdot 2^2 \\ \Leftrightarrow x &\equiv 20 \Leftrightarrow x \equiv 6 \end{aligned}$$

- ④ generalizzare le soluzioni  $\mathbb{E} = \text{modulo } 7 + \text{resto}$   $\mathbb{E} = 7\mathbb{Z} + 6$

# TEOREMA DEL RESTO CINESE

$$\begin{cases} 1025x \equiv 5312065 \pmod{8} & r_1 \\ 36x \equiv 322 \pmod{5} & r_2 \\ 4x \equiv 7 \pmod{3} & r_3 \end{cases}$$

① perché ci siano soluzioni,  $r_1, r_2, r_3$  devono essere primi tra loro ✓

② Si semplificano le congruenze

$$1025 \pmod{8} \quad 1025 = 1024 + 1 = 2^{10} + 1 = (2^3)^2 \cdot 2 + 1 \equiv 1 \pmod{8}$$

$\equiv 1 \pmod{8}$   
perché  $2^3 \equiv 8$

•  $5312065 \pmod{8}$  ( $8 \mid 40$  quindi  $8 \mid 40 \cdot 102$  → notiamo che  $5312065 = 4000000 + 1312065$ )

$$5312065 \equiv_8 1312065 \quad 8 \mid 12000000 \equiv_8 112065 \quad 8 \mid 120000 \equiv_8 -7935 \quad 8 \mid 8000 \equiv_8 65 \equiv_8 1$$

•  $36 \equiv_5 1$  ,  $322 \equiv_5 2$  ,  $4 \equiv_3 1$  ,  $7 \equiv_3 1$

il sistema diventa quindi

$$\begin{cases} x \equiv 1 \pmod{8} \\ x \equiv 2 \pmod{5} \\ x \equiv 1 \pmod{3} \end{cases}$$

③ Si calcolano  $R, R_i$

prodotto di tutti gli  $r$

$$R = r_1 \cdot r_2 \cdot \dots \cdot r_i = r_1 \cdot r_2 \cdot r_3 = 8 \cdot 5 \cdot 3 = 120$$