MCD ALGORITMO EUCLIDEO

MCD(168, 1911)

① divido il numero maggiore per quello minore nella forma: $1911 = x \cdot 168 + r$ (1911 − x·168)

$1911 = 11 \cdot 168 + 63$ ② prendo il divisore di prima e lo divido per il resto (168/63)

$168 = 2 \cdot 63 + 42$

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

$42 = 2 \cdot 21 + 0$ (questo)

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 quello che ho già calcolato

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

$42 = -2b + 23a$

$21 = 63 - 1 \cdot 42$ (sostituisco anche le cose calcolate più su)

$21 = (b - 11 \cdot a) - 1 \cdot (-2b + 23a)$

$21 = b - 11 \cdot a + 2b - 23a$

$21 = 3b - 34a$

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

IDENTITÀ DI BÉZOUT metodo Pellerin

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

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

$42 = 168 - 2 \cdot 63$

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

$= 63 - 168 + 2 \cdot 63$

$21 = -168 + 3 \cdot 63$

$63 = 1911 - 11 \cdot 168$

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

$= -168 + 3 \cdot 1911 - 22 \cdot 168$

$21 = \underbrace{-34 \cdot 168}_{x} + \underbrace{3 \cdot 1911}_{y}$

abbiamo trovato x e y! bravi tutti

EQ. CONGRUENZIALI

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

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

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

$2^{10} = 2^9 \cdot 2 = \underbrace{(2^3)^3}_{1} \cdot 2$