ESERCIZI ALGEBRA

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 (per comodità calcoli)

$(a = 168,\ b = 1911)$

$63 = b - 11 \cdot a$

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

$= 63 - 168 + 2 \cdot 63$

$21 = -168 + 3 \cdot 63$

$63 = 1911 - 11 \cdot 168$

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

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

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

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 $2^3 = 8 \equiv 1 \mod 7$

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

• per 3^{11}, so che $3 \equiv 2 \mod 7$ (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 pò di semplificazioni ottengo quindi $2x \equiv 5 \mod 7$

② una condizione necessaria perché ci sia soluzione, è che l'MCD tra il coeff. della x e il modulo divida il resto (qui MCD(2,7) | 5)

$MCD(2,7) = 1$ $\quad 1 \mid 5$? sì - c'è soluzione

③ si cerca di trovare una soluzione, usando proprietà (come il PTF), o inversi

con PTF ($n^{p-1} \equiv_p 1$) → so che $2^6 \equiv_7 1$

moltiplico per 2^5

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

ora, semplifico con le congruenze

$x \equiv 2^4 \cdot 2 \cdot 5 \iff x \equiv 2 \cdot 2 \cdot 5$ ($16 = 14 + 2$)

$\iff x \equiv_7 20 \iff x \equiv 6$

usando "a mano"

cerco l'inverso di $2 - 8 \equiv_7 1$ e $2^3 = 8$,

quindi $2^2 \cdot 2x \equiv_7 5 \cdot 2^2$

$\iff x \equiv_7 20 \iff x \equiv_7 6$

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

TEOREMA DEL RESTO CINESE

$$\begin{cases} 1025x \equiv \overset{c_1}{5312065} & \overset{r_1}{\text{mod. } 8} \\ 36x \equiv \overset{c_2}{322} & \overset{r_2}{\text{mod } 5} \\ 4x \equiv \overset{c_3}{7} & \overset{r_3}{\text{mod. } 3} \end{cases}$$

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

② Si semplificano le congruenze

$1025 \text{ mod. } 8 \quad . \quad 1025 = 1024 + 1 = 2^{10} + 1 = \underbrace{(2^3)^2 \cdot 2}_{\equiv 0 \text{ mod } 8 \text{ perché } 2^3 = 8} + 1 \equiv 1 \text{ mod } 8$

- $5312065 \text{ mod. } 8$ ($8 \mid 40$ quindi $8 \mid 40 \cdot 10\mathbb{Z}$ → notiamo che $5312065 = 4000000 + 1312065$)

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

- $36 \equiv_5 1$, $322 \quad 5 \mid 320 \equiv_5 2$
- $4 \equiv_3 1$, $7 \equiv_3 1$

il sistema diventa quindi $\begin{cases} X \equiv 1 & \text{mod. } 8 \\ X \equiv 2 & \text{mod. } 5 \\ X \equiv 1 & \text{mod. } 3 \end{cases}$

③ Si calcolano R, R_i

prodotto di tutti gli r

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