Applicazioni dell'Algoritmo di Euclide

Applicazione dell'Algoritmo di Euclide al calcolo del Massimo Comune Divisore tra due interi

Mostriamo un esempio di come "l'algoritmo di Euclide" permetta di calcolare il M.C.D. tra due numeri naturali a e b e di esprimerlo come combinazione lineare di a e b a coefficienti interi.

1) Siano

$$a = 1705, \qquad b = 625$$

Calcolare $(a, b) := M.C.D.(a, b)$ ed esprimerlo come combinazione lineare di a e b.

<u>*Soluzione*</u>. Applichiamo l'algoritmo di Euclide e per ogni divisione effettuata esplicitiamo i resti delle divisioni come combinazioni lineari

$1705 : 625 = 2$ $\longrightarrow$ $1705 = (2)625 + 455$ $\longrightarrow$ $455 = 1705 - (2)625$
455

$625 : 455 = 1$ $\qquad 625 = (1)455 + 170$ $\qquad 170 = 625 - (1)455$
170

$455 : 170 = 2$ $\qquad 455 = (2)170 + 115$ $\qquad 115 = 455 - (2)170$
115

$170 : 115 = 1$ $\qquad 170 = (1)115 + 55$ $\qquad 55 = 170 - (1)115$
55

$115 : 55 = 2$ $\qquad 115 = (2)55 + \boxed{5}$ $\qquad \boxed{5} = 115 - (2)55$
$\boxed{5}$

– – – – – – – – $\qquad$ – – – – – – – – – – – $\qquad$ – – – – – – – – –

$55 : 5 = 11$ $\qquad 55 = (11)5$
0

Il M.C.D.(a,b) è l'ultimo resto NON NULLO che si ottiene, in questo caso vale dunque 5.

Utilizzando la colonna con le combinazioni dei resti, risalendo di una combinazione alla volta e sostituendo i valori trovati si ottiene

$$
\begin{aligned}
\boxed{5} &= 115 + (-2)55 \\
&= 115 + (-2)\{170 + (-1)115\} && = (3)115 + (-2)170 \\
&= (3)\{455 + (-2)170\} + (-2)170 && = (-8)170 + (3)455 \\
&= (-8)\{625 + (-1)455\} + (3)455 && = (11)455 + (-8)625 \\
&= (11)\{1705 + (-2)625\} + (-8)625 && = (-30)625 + (11)1705
\end{aligned}
$$

La scrittura di 5 come combinazione lineare a coefficienti interi di 625 e 1705 è pertanto

$$\boxed{5 = (-30)625 + (11)1705}$$

Applicazione dell'Algoritmo di Euclide per risolvere un sistema di congruenze con il Teorema cinese del resto

2) Stabilire se il seguente sistema di congruenze ammette soluzioni e in caso affermativo determinarle tutte

$$\begin{cases} x \equiv -7 \mod 21 \\ x \equiv 41 \mod 81 \end{cases}$$

Soluzione.
1° passo. Dal Teorema cinese del resto sappiamo che il sistema ammette soluzioni se e solo se

$$41 - (-7) \text{ è multiplo di } (21, 81)$$

Ora

$$
\begin{aligned}
&41-(-7)=48\\
&21=3\cdot 7\\
&81=3^4
\end{aligned}
$$

Dunque

$$(21,81)=3$$

Poiché 3 divide $48 = 3\cdot 16$ sappiamo, dal Teorema cinese del resto, che il sistema ammette soluzione.

2° passo. Applichiamo l'Algoritmo di Euclide per determinare 3 come combinazione lineare di 21 e 81 a coefficienti interi.

$$
\begin{array}{lclcl}
81:21=3 & \longrightarrow & 81=(3)21+18 & \longrightarrow & 18=81-(3)21\\
18 & & & & \\
& & & & \\
21:18=1 & & 21=(1)18+\boxed{3} & & \boxed{3}=21-(1)18\\
\boxed{3} & & & & \\
& & & & \\
-\,-\,-\,-\,-\,-\,- & & -\,-\,-\,-\,-\,-\,-\,- & & -\,-\,-\,-\,-\,-\,-\,-\\
18:3=6 & & 18=(6)3 & & \\
0 & & & &
\end{array}
$$

Si ottiene allora

$$
\begin{aligned}
\boxed{3} &= 21+(-1)18\\
&= 21+(-1)\big\{81+(-3)21\big\} = (4)21+(-1)81
\end{aligned}
$$

La scrittura di 3 come combinazione lineare a coefficienti interi di 21 e 81 è pertanto

$$\boxed{3=(4)21+(-1)81}$$

3° passo. La combinazione che ci interessa è però quella relativa a 48

$$\begin{aligned}
\boxed{41-(-7)} &= 48 = 16\cdot 3\\
&= 16\cdot\big\{(4)21+(-1)81\big\}\\
&= \big\{(16\cdot 4)21+(16\cdot(-1))81\big\}\\
&= \boxed{\big\{(64)21+(-16)81\big\}}
\end{aligned}$$

Mettendo insieme il 41 con l'81 e il -7 con il 21 otteniamo una soluzione particolare del sistema

$$\begin{aligned}
x_0 &= 41-(-16)81\\
&= +(-7)+(64)21\\
&= 1337
\end{aligned}$$

Per determinare tutte le soluzioni del sistema, calcoliamo il Minimo Comune Multiplo tra 21 e 81

$$[21,81]=\frac{21\cdot 81}{(21,81)}=\frac{21\cdot 81}{3}=567$$

L'insieme delle soluzioni del sistema considerato è pertanto

$$\begin{aligned}
\text{Sol} &= \{1337+m\cdot 567 \mid m\in\mathbb{Z}\}\\
&= \big[1337\big]_{567}\\
&= \big[203\big]_{567}
\end{aligned}$$

Applicazione dell'Algoritmo di Euclide per risolvere una potenza modulo un intero n

3) Risolvere, se possibile, la seguente congruenza

$$x^{33}\equiv 2 \mod 55 \tag{1}$$

<u>*Soluzione*</u>.

1° passo. Poiché

$$(2,55)=1$$

sappiamo che 2 è invertibile $\mod 55$

$$2 \in \left(\mathbb{Z}/55\mathbb{Z}\right)^*$$

Pertanto, **SE** esiste una soluzione x dell'equazione (1), allora x deve essere invertibile modulo 55.

2° passo. Il numero di elementi di $\left(\mathbb{Z}/55\mathbb{Z}\right)^*$ è dato dalla funzione di Eulero ϕ applicata in 55

$$\begin{aligned}\phi(55) &= \phi(5)\cdot\phi(11)\\ &= (5-1)\cdot(11-1)\\ &= 4\cdot 10\\ &= 40\end{aligned}$$

Poiché

$$(33, 40) = 1$$

sappiamo che l'esponente 33 è invertibile modulo $40 = \phi(55)$

$$33 \in \left(\mathbb{Z}/40\mathbb{Z}\right)^*$$

Segue allora che l'applicazione

$$\begin{array}{ccc}\left(\mathbb{Z}/55\mathbb{Z}\right)^* & \rightarrow & \left(\mathbb{Z}/55\mathbb{Z}\right)^*\\ x & \mapsto & x^{33}\end{array}$$

è invertibile. L'applicazione inversa si ottiene determinando d, l'inverso di 33 modulo $\phi(55) = 40$

$$\begin{array}{ccc}\left(\mathbb{Z}/55\mathbb{Z}\right)^* & \leftarrow & \left(\mathbb{Z}/55\mathbb{Z}\right)^*\\ x^d & \leftarrow & x\end{array}$$

Applichiamo quindi il Teorema di Eulero-Fermat che ci fornisce una soluzione dell'equazione (1)

$$x = 2^d$$

3° passo. Troviamo d applicando l'algoritmo di Euclide. Per far questo esplicitiamo $1 = (33, 40)$ come combinazione lineare di 33 e 40 e consideriamo il coefficiente di 33.

$$
\begin{array}{lll}
40 : 33 = 1 \quad \longrightarrow & 40 = (1)33 + 7 \quad \longrightarrow & 7 = 40 - (1)33 \\
7 & & \\
 & & \\
33 : 7 = 4 & 33 = (4)7 + 5 & 5 = 33 - (4)7 \\
5 & & \\
 & & \\
7 : 5 = 1 & 7 = (1)5 + 2 & 2 = 7 - (1)5 \\
2 & & \\
 & & \\
5 : 2 = 2 & 5 = (2)2 + \boxed{1} & \boxed{1} = 5 - (2)2 \\
\boxed{1} & & \\
 & & \\
- - - - - - - - & - - - - - - - - -- & - - - - - - - -- \\
2 : 1 = 2 & 2 = (2)1 & \\
0 & &
\end{array}
$$

Utilizzando la colonna con le combinazioni dei resti, risalendo di una combinazione alla volta e sostituendo i valori trovati si ottiene

$$
\begin{aligned}
\boxed{1} &= 5 + (-2)2 \\
&= 5 + (-2)\big\{7 + (-1)5\big\} && = (3)5 + (-2)7 \\
&= (3)\big\{33 + (-4)7\big\} + (-2)7 && = (3)33 + (-14)7 \\
&= (3)33 + (-14)\big\{40 + (-1)33\big\} && = (17)33 + (-14)40
\end{aligned}
$$

La scrittura di 1 come combinazione lineare a coefficienti interi di 33 e 40 è pertanto

$$\boxed{1 = (17)33 + (-14)40}$$

L'inverso di 33 modulo 40 è allora

$$d = 17$$

4° passo.

Per il Teorema di Eulero-Fermat le soluzioni sono pertanto

$$x \equiv 2^{17} \mod 55$$

Determiniamo il minimo rappresentante positivo di 2^{17} modulo 55.

$$\begin{aligned} 2^{17} &= 2^6 \cdot 2^6 \cdot 2^5 &&= 64 \cdot 64 \cdot 32 \equiv \\ &\equiv 9 \cdot 9 \cdot 32 &&= 81 \cdot 32 \equiv \\ &\equiv 26 \cdot 32 &&= 2 \cdot 13 \cdot 32 = \\ &= 13 \cdot 64 &&\equiv 13 \cdot 9 = \\ &= 117 &&\equiv 7 && \mod 55 \end{aligned}$$

Dunque

$$\text{Sol} = \left[2^{17}\right]_{55} = [7]_{55}$$