Il presente <u>Fascicolo A</u> contiene i seguenti argomenti

1) Algoritmo euclideo per il calcolo del massimo comun divisore di due interi a, b.

2) Identità di Bézout.

3) Esempi illustrativi

Fascicolo A

L'algoritmo euclideo (per il calcolo del massimo comun divisore (a,b)) ①

Poniamoci il seguente problema

"È possibile calcolare il massimo comun divisore di due numeri naturali a e b <u>senza</u> conoscere la fattorizzazione prima di a e b?"

Per fortuna la risposta è affermativa: si può risolvere il problema mediante il cosiddetto "algoritmo euclideo" (o delle divisioni ripetute).

Vediamo come.

Dati due naturali a e b con $1 < b < a$, dividiamo a per b, cioè scriviamo

1) $a = bq + r$, con $0 \leq r < b$

La relazione 1) ci consente di dimostrare che l'insieme dei divisori comuni ad a e b coincide con l'insieme dei divisori comuni a b ed r, quindi anche i massimi dei due insiemi coincidono, cioè

2) $(a,b) = (b,r)$

Infatti se $d|a$ e $d|b$ si ha $a = dk$ e $b = dh$ con $h, k \in \mathbb{N}$ e dalla 1) segue

3) $a - bq = d(k - hq) = r$

che implica $d|r$. Se viceversa $d|b$ e $d|r$ si ha $b = dh$, $r = dl$ e dalla 1) segue (2)

4) $$a = d(hq + l)$$

che implica $d|a$.

Ciò prova la relazione 2).

L'uguaglianza 2) è molto importante poiché riconduce il problema iniziale ad un altro problema dello stesso tipo ma più semplice: infatti $b < a$ e $r < b$. Conviene quindi iterare il procedimento nel modo seguente.

Poniamo, per comodità di notazione, $r_0 = a$ e $r_1 = b$ e consideriamo la catena di divisioni seguenti (algoritmo euclideo)

5) $$\begin{cases} r_0 = r_1 q_1 + r_2 \\ r_1 = r_2 q_2 + r_3 \\ r_2 = r_3 q_3 + r_4 \\ \text{— — —} \\ r_J = r_{J+1} q_{J+1} + r_{J+2} \\ \text{— — —} \\ r_{n-2} = r_{n-1} q_{n-1} + r_n \\ r_{n-1} = r_n q_n + 0 \end{cases}$$

Siccome la successione dei resti è, per definizione di divisione, strettamente decrescente, cioè

$$r_0 > r_1 > r_2 > r_3 > \ldots$$

si deve necessariamente giungere ad un resto nullo dopo un numero finito di passi (ricordare che gli r_j sono interi positivi) e quindi la situazione è quella illustrata dalla formula 5). Ciò implica, per la formula 2),

$$6)\quad (a,b)=(r_0,r_1)=(r_1,r_2)=(r_2,r_3)=\cdots\cdots=(r_{n-1},r_n)=r_n$$

Le 5) e 6) dimostrano che il massimo comun divisore di due naturali a e b è l'ultimo resto non nullo dell'algoritmo delle divisioni successive, o algoritmo euclideo.

Dall'algoritmo euclideo 5) discende un altro fatto molto importante: partendo dalla generica relazione $r_j = r_{j+1} q_{j+1} + r_{j+2}$ si ottiene ovviamente

$$7)\quad r_{j+2} = 1 \cdot r_j - q_{j+1} r_{j+1}$$

cioè ogni resto è esprimibile come combinazione lineare a coefficienti interi dei due resti precedenti. Partendo da r_n si ottiene

$$8)\quad r_n = r_{n-2} - q_{n-1} r_{n-1}$$

ed il procedimento si può iterare esprimendo r_{n-1} come combinazione lineare di r_{n-2} e r_{n-3}, infatti dalla 7) con $j = n-3$ si ottiene

$$9)\quad r_{n-1} = r_{n-3} - q_{n-2} r_{n-2}$$

che sostituita nella 8) fornisce

$$10)\qquad r_n = r_{n-2} - q_{n-1}(r_{n-3} - q_{n-2} r_{n-2})$$
$$= (1 + q_{n-1} q_{n-2}) r_{n-2} - q_{n-1} r_{n-3}$$

A questo punto iteriamo nuovamente; dalla 7) con $j = n-4$ otteniamo

$$11)\qquad r_{n-2} = r_{n-4} - q_{n-3} r_{n-3}$$

che sostituita nella 10) consente di esprimere r_n come combinazione lineare (a coefficienti interi) di r_{n-3} e r_{n-4}. Quindi il procedimento termina con l'espressione di r_n come combinazione lineare di r_1 ed r_0, cioè con una formula del tipo

$$12)\qquad r_n = r_0 h + r_1 k \quad , \text{ con } h, k \in \mathbb{Z}$$

Essendo $r_0 = a$, $r_1 = b$ e $r_n = (r_0, r_1) = (a, b)$ la 12) diviene

$$13)\qquad (a,b) = ah + bk, \text{ con } h, k \in \mathbb{Z}.$$

Possiamo riassumere quanto abbiamo visto in un unico importante enunciato. Vale infatti il teorema seguente.

Teorema

Dati due interi a e b con $1 < b < a$ si consideri l'algoritmo euclideo (delle divisioni successive) dato dalle 5), dove $a = r_0$, $b = r_1$. Valgono allora i risultati seguenti:

i) l'ultimo resto non nullo dell'algoritmo euclideo è il massimo comun divisore di a e b, cioè

$$14) \qquad r_n = (a, b)$$

ii) il massimo comun divisore di a e b è esprimibile come combinazione lineare (a coefficienti interi) di a e b, cioè esistono $h, k \in \mathbb{Z}$ tali che

$$15) \qquad r_n = (a, b) = ah + bk$$ (Identità di Bézout)

Esempi illustrativi

Calcoliamo $(1751, 253)$ mediante l'algoritmo euclideo. Si ha

$$16) \quad \begin{aligned} 1751 &= 253 \cdot 6 + 233 \\ 253 &= 233 \cdot 1 + 20 \\ 233 &= 20 \cdot 11 + 13 \\ 20 &= 13 \cdot 1 + 7 \\ 13 &= 7 \cdot 1 + 6 \\ 7 &= 6 \cdot 1 + 1 \\ 6 &= 1 \cdot 6 + 0 \end{aligned}$$

L'ultimo resto non nullo dell'algoritmo è 1, quindi $(1751, 253) = 1$, cioè 1751 e 253 sono relativamente primi.

Esprimiamo ora il massimo comun divisore di 1751 e 253 (cioè il numero 1) come combinazione lineare (a coefficienti interi) di 1751 e 253. Si ha, partendo dalla 16),

17)
$$\begin{aligned}
1 &= 7-6 = 7-(13-7) = 2.7-13 = 2(20-13)-13 = \\
&= 2.20-3.13 = 2.20-3(233-20.11) = 35.20-3.233 = \\
&= 35(253-233)-3.233 = 35.253-38.233 = \\
&= 35.253-38(1751-253.6) = \\
&= (35+38.6).253-38.1751 = 263.253-38.1751
\end{aligned}$$

La 17) può essere verificata! infatti

$$263.253 = 66539$$
$$38.1751 = 66538$$

—

Vediamo ora un altro esempio. Calcoliamo $(147, 45)$. Si ha

18)
$$\begin{cases}
147 = 45.3+12 \\
45 = 12.3+9 \\
12 = 9.1+3 \\
9 = 3.3+0
\end{cases}$$

Si ha quindi $(147, 45) = 3$.

Esprimiamo ora 3 come combinazione lineare di 147 e 45.

Si ha

$$19) \quad 3 = 12-9 = 12-(45-12\cdot 3) = 4\cdot 12 - 45 = $$
$$= 4(147-45\cdot 3) - 45 = 4\cdot 147 - 13\cdot 45$$

infatti $4\cdot 147 = 588$ e $13\cdot 45 = 585$

Osservazione importante

L'algoritmo euclideo è, come vedremo, fondamentale per risolvere in tempi rapidi le congruenze lineari, cioè $ax \equiv b \pmod m$. Per intuire qual'è il legame basta osservare che, ad esempio, la 17) risolve immediatamente la congruenza

$$20) \quad 253x \equiv 1 \ (1751)$$

(la soluzione è $x = 263$),
e la 19) risolve la congruenza

$$21) \quad 45x \equiv 3 \ (147)$$

(la soluzione è $x \equiv -13 \equiv 134 \pmod{147}$).

Questi importanti aspetti della teoria verranno analizzati in un prossimo fascicolo.