MAT. DISCRETA 4

DIOFANTEA

Un’equazione diofantea è un’equazione lineare (o più in generale polinomiale) dove cerchiamo **soluzioni intere** (tipicamente in $\mathbb{Z}$).

Qui abbiamo la forma semplice
$8x + 13y = 3$
con $x, y \in \mathbb{Z}$. Vogliamo trovare **tutte** le coppie intere (x,y) che soddisfano questa uguaglianza.

M.C.D. (massimo comune divisore)

Il Massimo Comune Divisore (MCD) è il più grande numero naturale che divide esattamente due o più numeri dati, senza lasciare resto.
Per trovarlo, si scompongono i numeri in fattori primi e si prendono solo i fattori comuni, moltiplicandoli con l'esponente più piccolo.

Perché si chiama Massimo Comune Divisore?

- **Massimo:** Indica che è il numero più grande possibile.
- **Comune:** Significa che è presente come divisore in tutti i numeri considerati.
- **Divisore:** È un numero che divide esattamente un altro numero, ottenendo un numero intero.

Esempio pratico:
Consideriamo i numeri 12 e 30.

1. **Scomposizione in fattori primi:**
   - $12 = 2^2 \times 3$
   - $30 = 2 \times 3 \times 5$
2. **Identificazione dei fattori comuni:** I fattori comuni sono 2 e 3.
3. **Scelta dell'esponente minimo:**
   - Per il 2, l'esponente più piccolo è 1 (da 30).
   - Per il 3, l'esponente più piccolo è 1.
4. **Moltiplicazione dei fattori comuni con l'esponente minimo:** $2^1 \times 3^1 = 6$.

Quindi, il MCD(12, 30) è 6, perché è il numero più grande che divide sia 12 che 30.

Tornando all'esercizio precedente $8x + 13y = 3$, poiché 8 e 13 sono primi tra loro (13 è primo e non divide 8), $mcd(8, 13) = 1$.
Conclusione: **esistono soluzioni** e, perché $mcd = 1$.

Nel nostro caso dato che 13 è primo e 8 ha MCD che sarà d=1 allora $d|c$ quindi 1 divide qualunque intero di 3.

Algoritmo di Euclide

Teniamo a mente sempre la nostra traccia: $8x + 13y = 3$

Possiamo anche ottenere una soluzione particolare usando l'**algoritmo di Euclide esteso** (trova u, v tali che $8u + 13v = mcd(8, 13) = 1$). Poi moltiplichiamo per 3.

Ecco i passi (Euclide + retro-sostituzione):

13 = 8\cdot1 + 5 → 5 = 13 - 8\cdot1
8 = 5\cdot1 + 3   → 3 = 8 - 5
5 = 3\cdot1 + 2   → 2 = 5 - 3
3 = 2\cdot1 + 1   → 1 = 3 - 2

Ora risaliamo esprimendo 1 come combinazione di 8 e 13:

$1 = 3 - 2$
Ma $2 = 5 - 3 \Rightarrow 1 = 3 - (5 - 3) = 2 \cdot 3 - 5$
E $3 = 8 - 5 \Rightarrow 1 = 2(8 - 5) - 5 = 2 \cdot 8 - 3 \cdot 5$
E $5 = 13 - 8 \Rightarrow 1 = 2 \cdot 8 - 3(13 - 8) = 2 \cdot 8 - 3 \cdot 13 + 3 \cdot 8 = 5 \cdot 8 - 3 \cdot 13$

Quindi abbiamo
$1 = 5 \cdot 8 + (-3) \cdot 13.$

Moltiplichiamo per 3:
$3 = 15 \cdot 8 + (-9) \cdot 13.$

Quindi $(x, y) = (15, -9)$ è una soluzione particolare. (È equivalente a quella trovata prima: $15 = 2 + 13$, e $-9 = -1 - 8$; sono la stessa "famiglia".)

Come modus operandi di questo esercizio vi è qui un esempio fornito da Dott. Sblendorio:

"Pasted image 20250911115704.png" could not be found.

Una volta trovati x_0 e y_0 si esegue la formula:
$x_0 + \frac{b}{d} * t, y_0 + \frac{a}{d} * t$

Adesso bisogna sostituire i valori moltiplicandoli per i valori di a e b nelle giuste posizioni, come mostrato.
Così troveremo tutte le possibili soluzioni dell'equazione.

Relazioni di Equivalenza – Appunti

1. Definizione di Relazione

Sia A un insieme. Una **relazione** R su A è un sottoinsieme del prodotto cartesiano $A \times A$, cioè un insieme di coppie ordinate (x,y) con $x, y \in A$.

Scriviamo xRy quando $(x, y) \in R$.

2. Relazioni di equivalenza

Una relazione R su un insieme A si dice **relazione di equivalenza** se soddisfa **tutte e tre** queste proprietà:

1. **Riflessiva**: $\forall x \in A,\ xRx$. (Ogni elemento è in relazione con sé stesso).
2. **Simmetrica**: $\forall x, y \in A,\ xRy \implies yRx$. (Se x è in relazione con y, allora anche y con x).
3. **Transitiva**: $\forall x, y, z \in A,\ (xRy \wedge yRz) \implies xRz$. (Se x è in relazione con y e y con z, allora anche x con z).
   Se una relazione è di equivalenza, essa suddivide l'insieme A in **classi di equivalenza** (cioè sottoinsiemi disgiunti i cui elementi sono equivalenti fra loro).

3. La relazione proposta

Definiamo la relazione su $\mathbb{Z}$:
$xRy \iff 3 \mid (8x + 13y)$.
Qui "$3 \mid m$" significa che **3 divide** m, cioè esiste $k \in \mathbb{Z}$ con m=3k.

4. Dimostrazione che R è una relazione di equivalenza

4.1 Riflessività

Prendiamo un qualsiasi $x \in \mathbb{Z}$:
$8x + 13x = 21x = 3(7x)$
Quindi 3 divide sempre $8x + 13x$.
Conclusione: xRx. Riflessività provata.

4.2 Simmetria

Vogliamo dimostrare che se xRy, allora yRx

Passo 1 – Introduzione al "modulo"
Quando scriviamo
$a \bmod m$
intendiamo il **resto della divisione di a per m**.

- a è un numero intero qualsiasi,
- m è un intero positivo (si chiama **modulo**),
- il risultato è il resto della divisione euclidea di a per m.

Lavorare **modulo 3** significa guardare i **resti della divisione per 3**.
Scriviamo:
$a \equiv b \pmod 3 \quad \iff \quad 3 \mid (a-b).$
Esempi:

- $10 \equiv 1 \pmod 3$ (perché 10-1=9 è multiplo di 3).
- $22 \equiv 1 \pmod 3$.
- $21 \equiv 0 \pmod 3$.

Passo 2 – Riduzione dei coefficienti
Notiamo che:
$8 \equiv 2 \pmod 3, \quad 13 \equiv 1 \pmod 3.$
Quindi:
$8x + 13y \equiv 2x + y \pmod 3.$

Passo 3 – Applicazione
Se xRy, allora:

$8x + 13y \equiv 0 \pmod 3 \iff 2x + y \equiv 0 \pmod 3.$
Da questo segue:
$y \equiv -2x \pmod 3.$

Ma $-2 \equiv 1 \pmod 3$, quindi:
$y \equiv x \pmod 3.$

Passo 4 – Scambio dei ruoli
Se $y \equiv x \pmod 3$, allora:
$8y + 13x \equiv 2y + x \equiv 2x + x = 3x \equiv 0 \pmod 3.$

Quindi yRx.
Simmetria dimostrata.

4.3 Transitività

Supponiamo che xRy e yRz.

$xRy \iff 2x + y \equiv 0 \pmod 3,$
$yRz \iff 2y + z \equiv 0 \pmod 3.$

Dal primo: $y \equiv -2x \equiv x \pmod 3$.
Dal secondo: $z \equiv -2y \equiv y \pmod 3$.

Conclusione: $x \equiv y \equiv z \pmod 3$.

Quindi:
$2x + z \equiv 2x + x = 3x \equiv 0 \pmod 3,$
e dunque xRz.

Transitività dimostrata.

5. Conclusione

La relazione R è **riflessiva**, **simmetrica** e **transitiva**.
Quindi è una **relazione di equivalenza**.