Notazione
Nel corso di questo articolo utilizzeremo le seguenti notazioni:

- Consideriamo $0 \in \mathbb{R}^+$;
- Avendo già definito k, quando denotiamo le soluzioni di un'equazione con

$$w = kq,\ q \in \mathbb{Z}$$

questo sta a significare:

$$\begin{cases} \forall q \in \mathbb{Z},\ kq\ risolve\ l'equazione \\ \forall w'\ soluzione\ dell'equazione\ \exists q' \in \mathbb{Z}\ t.c.\ w' = kq' \end{cases}.$$

1 Studio dell'equazione diofantea $ax + by + cz = d$

Risolubilità dell'equazione

In questo paragrafo studieremo l'esistenza di soluzioni intere di equazioni della forma $ax + by + cz = d$ con $a, b, c, d \in \mathbb{Z}$

Proposition 1.

$$\exists\ x, y, z \in \mathbb{Z} \mid ax + by + cz = d \iff (a, b, c)|d$$

Proof. $\implies$

$$ax + by + cz = d \Leftrightarrow (a, b, c)\left(\frac{a}{(a, b, c)}x + \frac{b}{(a, b, c)}y + \frac{c}{(a, b, c)}z\right) = d$$

Ma

$$\frac{a}{(a, b, c)}, \frac{b}{(a, b, c)}, \frac{c}{(a, b, c)} \in \mathbb{Z} \Rightarrow \frac{a}{(a, b, c)} + \frac{b}{(a, b, c)} + \frac{c}{(a, b, c)} \in \mathbb{Z} \Leftrightarrow \frac{d}{(a, b, c)} \in \mathbb{Z} \Leftrightarrow (a, b, c)|d$$

$\impliedby$ *(Metodo costruttivo, impiegabile per trovare x, y, z soluzioni particolari)*

Per il teorema di Bézout $\forall\ a, b, \alpha \in \mathbb{Z}\ \exists\ x, y \in \mathbb{Z} \mid ax + by = (a, b)\alpha$ dunque sostituisco e ottengo $(a, b)\alpha + cz = d$ che, ancora per il teorema di Bézout, ha soluzione se e solo se $((a, b), c)|d \Leftrightarrow (a, b, c)|d$. □

Esplicitazione delle soluzioni intere

Proposition 2. *Tutte e sole le soluzioni intere dell'equazione $ax + by + cz = d$ possono essere trovate sommando ad una terna di soluzioni particolari (x_0, y_0, z_0) le soluzioni intere dell'equazione omogenea associata $ax + by + cz = 0$:*

Proof. $\implies$

$$\forall\ x_0, y_0, z_0, x_1, y_1, z_1\ \in \mathbb{Z} \mid ax_0 + by_0 + cz_0 = d \wedge ax_1 + by_1 + cz_1 = d \implies$$

Sottraendo membro a membro

$$0 = a(x_0 - x_1) + b(y_0 - y_1) + c(z_0 - z_1)$$

E dunque la terna $((x_0 - x_1), (y_0 - y_1), (z_0 - z_1))$ è soluzione dell'equazione omogenea associata. Allora due qualsasi soluzioni dell'equazione differiscono per una soluzione dell'equazione omogenea associata.

$\Longleftarrow$

$$\forall\ x_0, y_0, z_0, x_a, y_a, z_a\ \in \mathbb{Z} \mid ax_0 + by_0 + cz_0 = d\ \wedge\ ax_a + by_a + cz_a = 0 \Rightarrow$$

Sommando membro a membro

$$d = a(x_0 + x_a) + b(y_0 + y_a) + c(z_0 + z_a)$$

E dunque la terna $((x_0 + x_a), (y_0 + y_a), (z_0 + z_a))$ è ancora soluzione dell'equazione.

□

Trovare una soluzione particolare

Per trovare una soluzione particolare possiamo procedere in questo modo:
per il teorema di Bézout $\forall\ a, b, \alpha \in \mathbb{Z}\ \exists\ x, y \in \mathbb{Z} \mid ax + by = \alpha(a, b)$ dunque posso considerare i primi due addendi come un unico termine, e sostituendo ottengo $\alpha(a, b) + cz = d$.
A questo punto posso applicare l'algoritmo di Euclide per ottenere

$$(\alpha_0, z_0)\ t.c.\ \alpha_0(a, b) + cz_0 = d.$$

Posso adesso sostiturire il valore di α trovato nell'equazione $ax + by = \alpha_0(a, b)$ e, applicando nuovamente l'algoritmo di Euclide, trovo

$$(x_0, y_0)\ t.c.\ ax_0 + by_0 = \alpha_0(a, b).$$

La terna di valori (x_0, y_0, z_0) soddisfa dunque l'equazione.

Trovare le soluzioni dell'equazione omogenea associata

Definiamo

$$Z_0(a, b, c) = \{z \in \mathbb{Z}\ t.c.\ \exists x, y \in \mathbb{Z}\ t.c.\ ax + by + cz = 0\}$$

Proposition 3.

$$Z_0(a, b, c) = \left\{\ z \in \mathbb{Z}\ t.c.\ z = \frac{(a, b)}{(a, b, c)}\alpha,\ \alpha \in \mathbb{Z}\right\}.$$

Proof.
Possiamo sostituire, grazie al teorema di Bézout, $ax + by$ con $(a, b)k,\ k \in \mathbb{Z}$. Otteniamo così:

$$cz + (a, b)k = 0.$$

Ma

$$\exists k \in \mathbb{Z}\ t.c.\ cz + (a, b)k = 0 \Leftrightarrow z = \frac{(a, b)}{(a, b, c)}\alpha,\ \alpha \in \mathbb{Z}.$$

□

This project has been funded with support from the European Commission in its Lifelong Learning Programme (510028-LLP-1-2010-1-IT-COMENIUS-CMP). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

A questo punto troviamo x e y in funzione di $z \in Z_0(a,b,c)$:

$$ax + by = -cz \;\Leftrightarrow\; ax + by = -c\frac{(a,b)}{(a,b,c)}\alpha.$$

Date x_c e y_c soluzioni dell'equazione

$$ax + by = -c\frac{(a,b)}{(a,b,c)},$$

allora αx_c e αy_c sono soluzioni di

$$ax + by = -c\frac{(a,b)}{(a,b,c)}\alpha,$$

infatti

$$ax_c\alpha + by_c\alpha = \alpha(ax_c + by_c) = -c\frac{(a,b)}{(a,b,c)}\alpha.$$

Allora trovo, attraverso l'algoritmo di Euclide, x_c e y_c che risolvono $ax + by = -c\frac{(a,b)}{(a,b,c)}$, dal momento che $(a,b)\ |c\frac{(a,b)}{(a,b,c)}\ \forall c \in \mathbb{Z}$.
Dunque posso sommare alla soluzione particolare così ottenuta le soluzioni dell'equazione omogenea associata $ax + by = 0$, ottenendo

$$\begin{cases} x = \alpha x_c + \frac{b}{(a,b)}t \\ y = \alpha y_c - \frac{a}{(a,b)}t \end{cases} \quad t \in \mathbb{Z}$$

Dunque le soluzioni dell'equazione omogenea $ax + by + cz = 0$ sono tutte e sole quelle della forma

$$\begin{cases} x = x_c\alpha + \frac{b}{(a,b)}t \\ y = y_c\alpha - \frac{a}{(a,b)}t \\ z = \frac{(a,b)}{(a,b,c)}\alpha \end{cases} \quad \alpha, t \in \mathbb{Z}$$

Nota: x_c e y_c dipendono soltanto dai valori di a, b, c e sono costanti.

Dunque, data comunque un'equazione della forma $ax + by + cz = d$ con $a, b, c, d \in \mathbb{Z}$ *t.c.* $(a,b,c)|d$, tutte e sole le soluzioni $x, y, z \in \mathbb{Z}$ sono quelle della forma

$$\begin{cases} x = x_0 + x_c\alpha + \frac{b}{(a,b)}t \\ y = y_0 + y_c\alpha - \frac{a}{(a,b)}t \\ z = z_0 + \frac{(a,b)}{(a,b,c)}\alpha \end{cases} \quad \alpha, t \in \mathbb{Z}$$

2 Studio del $min(x + y + z)$ soluzioni naturali dell'equazione

In questa sezione tratteremo il caso con $a, b, c, d \in \mathbb{N}$ e $x, y, z \in \mathbb{N} \cup \{0\}$.

Studio preliminare del caso con 2 incognite

Se ci troviamo nel caso di un'equazione della forma $ax + by = d;\quad a, b, d \in \mathbb{N}\ ;\quad x, y \in \mathbb{N} \cup \{0\}$
e siamo interessati tovare il minimo di $(x + y)$ con x, y soluzioni naturali dell'equazione, possiamo procedere in questo modo:

Possiamo supporre senza perdita di generalità $b > a$

Se consideriamo l'insieme

$$\mathbb{Y}(a,b,d) = \{y \in \mathbb{N} \cup \{0\} \quad t.c.\ \exists\ x \in \mathbb{N} \cup \{0\} \quad t.c.\ ax + by = d\}\,.$$

A questo punto:

- Se $\mathbb{Y}(a,b,d) = \emptyset \implies \nexists x, y \in \mathbb{N} \cup \{0\}$ *t.c.* $ax + by = d$
- Se $\mathbb{Y}(a,b,d) \neq \emptyset$ allora:

Lemma 2.1. $\mathbb{Y}(a,b,d)$ *è limitato superiormente.*

Proof.
Dimostriamo che $\lfloor \frac{d}{b} \rfloor$ è maggiorante dell'insieme $\mathbb{Y}(a,b,d)$.
Se per assurdo esistesse

$$y_e \in \mathbb{Y}(a,b,d) \text{ t.c. } y_e > \frac{d}{b}, \Rightarrow \exists x_e \in \mathbb{N} \cup \{0\} \text{ t.c. } ax_e + by_e = d \Rightarrow$$

$$ax_e = d - by_e < d - b\frac{d}{b} = 0 \Rightarrow ax_e < 0.$$

Ma $a \in \mathbb{N} \wedge x_e \in \mathbb{N} \cup \{0\}$, dunque questo è assurdo.
Allora

$$\forall y \in \mathbb{Y}(a,b,d), \ y \leq \frac{d}{b} \Rightarrow$$

dal momento che $y \in \mathbb{N} \cup \{0\}$,

$$y \leq \lfloor \frac{d}{b} \rfloor.$$

□

Posso percio considerare $max\mathbb{Y}(a,b,d)$. Per ipotesi $\exists x_0 \in \mathbb{N} \cup \{0\}$ *t.c.* $ax_0 + bmax\mathbb{Y}(a,b,d) = d$

Theorem 1. $min\{x + y \text{ t.c. } x, y \in \mathbb{N} \cup \{0\} \wedge ax + by = d\} = max\mathbb{Y}(a,b,d) + x_0$

Proof.

$$\forall y' \in \mathbb{Y}(a,b,d) \text{ t.c. } y' \neq \max \mathbb{Y}(a,b,d) \ \exists x' = x'(y') \in \mathbb{N} \cup \{0\} \text{ t.c. } ax' + by' = d$$

Definisco $max\mathbb{Y}(a,b,d) - y' = k$; $k > 0$ per la massimalita' di $max\mathbb{Y}(a,b,d)$.

$$\Rightarrow ax_0 + bmax\mathbb{Y}(a,b,d) = d = ax' + by' \Rightarrow ax_0 - ax' = b(y' - max\mathbb{Y}(a,b,d))$$

$$\Rightarrow ax_0 - ax' = -bk \Rightarrow x_0 - x' = -\frac{b}{a}k.$$

Dunque

$$x' + y' > x_0 + max\mathbb{Y}(a,b,d) \Leftrightarrow x' - x_0 > max\mathbb{Y}(a,b,d) - y' \Leftrightarrow \frac{b}{a}k > k \Leftrightarrow \frac{b}{a} > 1$$

che è vero per ipotesi.

□

Dunque e' ben definita la funzione $\rho : \mathbb{N}^3 \longmapsto \mathbb{N} \cup \{-1\}$ come segue:

$$\rho(a,b,d) = \begin{cases} -1 & \text{se } \mathbb{Y}(a,b,d) = \emptyset \\ max\mathbb{Y}(a,b,d) + x_0 & \text{se } \mathbb{Y}(a,b,d) \neq \emptyset \end{cases}$$

Calcolare esplicitamente $\rho(a,b,d)$

Sappiamo che le soluzioni dell'equazione $ax + by = d$:

- Non esistono se $(a,b) \not| d$ e dunque $\mathbb{Y}(a,b,d) = \emptyset$
- Se $(a,b)|d$ sono tutte e sole quelle della forma

$$\begin{cases} x = x_0 + \frac{b}{(a,b)}t \\ y = y_0 - \frac{a}{(a,b)}t \end{cases} \quad t \in \mathbb{Z}$$

Con x_0, y_0 coefficienti ricavati grazie all'algoritmo di Euclide.

Lemma 1. *Sia* $\mathbb{Y}_{\mathbb{Z}}(a,b,d) = \{y \in \mathbb{Z} \text{ t.c. } \exists x \in \mathbb{Z} \text{ t.c. } ax+by=d\}$.
Allora

$$\forall h \in \mathbb{Z}\ \exists! y_h \in \mathbb{Y}_{\mathbb{Z}}(a,b,d) \text{ t.c. } y_h \in [h - \frac{a}{(a,b)} + 1, h]$$

Proof.
Abbiamo dimostrato che

$$\exists y_0 \in \mathbb{Z} \text{ t.c. } \mathbb{Y}_{\mathbb{Z}}(a,b,d) = \left\{ y \in \mathbb{Z} \text{ t.c. } y = y_0 - \frac{a}{(a,b)}t,\ t \in \mathbb{Z} \right\}.$$

Per il Teorema di divisione euclidea:

$$\exists!\ t_0, k \in \mathbb{Z} \text{ t.c. } h - y_0 = \frac{a}{(a,b)}t_0 + k,\ 0 \le k < \frac{a}{(a,b)};$$

$$h - k = y_0 + \frac{a}{(a,b)}t_0;$$

Allora

$$h - \frac{a}{(a,b)} + 1 \le h - k \le h\ \wedge\ h - k \in \mathbb{Y}_{\mathbb{Z}}(a,b,d).$$

Abbiamo dimostrato che l'intervallo contiene almeno un elemento di $\mathbb{Y}_{\mathbb{Z}}(a,b,d)$, dimostriamo che non può contenerne altri. Infatti

$$\forall y_w \in \mathbb{Y}_{\mathbb{Z}}(a,b,d) \text{ t.c. } y_w \neq h-k, \exists w\mathbb{Z} \text{ t.c. } w \neq 0 \wedge\ y_w - (h-k) = w\frac{a}{(a,b)}.$$

- Se $w > 0$

  $$y_w \ge h - k + \frac{a}{(a,b)}$$

  Dato che $k < \frac{a}{(a,b)}$

  $$\Rightarrow y_w > h \Rightarrow y_w \notin [h - \frac{a}{(a,b)} + 1, h]$$

- Se $w < 0$

  $$y_w \le h - k - \frac{a}{(a,b)}$$

  Dato che $k \ge 0$

  $$\Rightarrow y_w < h - \frac{a}{(a,b)} + 1 \Rightarrow y_w \notin [h - \frac{a}{(a,b)} + 1, h]$$

Quindi

$$\forall y_w \in \mathbb{Y}_{\mathbb{Z}}(a,b,d) \text{ t.c. } y_w \neq h-k;$$

$$y_w \notin [h - \frac{a}{(a,b)} + 1, h]$$

□

Dunque $\forall h \in \mathbb{Z}$, l'intervallo $[h - \frac{a}{(a,b)} + 1, h]$ contiene uno e un sono elemento di $\mathbb{Y}_{\mathbb{Z}}(a,b,d)$.
Abbiamo dimostrato che $\forall y \in \mathbb{Y}(a,b,d),\ y < \frac{d+1}{b} \le \frac{d}{b} + 1$.

Consideriamo percio' $y_s \in \mathbb{Z}$ *t.c.* $\lfloor \frac{d}{b} \rfloor - \frac{a}{(a,b)} + 1 \le y_s \le \lfloor \frac{d}{b} \rfloor\ \wedge \exists x_s \in \mathbb{Z}$ *t.c.* $ax_s + by_s = d$.

Lemma 2.2.

- *Se* $y_s < 0$, *allora* $\mathbb{Y}(a,b,d) = \emptyset$ *e quindi* $\rho(a,b,d) = -1$
- *Se* $y_s \ge 0$, *allora* $y_s = max\mathbb{Y}(a,b,d)$ *e* $\exists x_s \in \mathbb{N} \cup \{0\}$ *t.c.* $ax_s + by_s = d$; $\quad x_s = \frac{d - by_s}{a}$.
  In questo caso $\rho(a,b,d) = x_s + max\mathbb{Y}(a,b,d)$.

Proof.

$$\forall y_t \in \mathbb{Z} \; t.c. \; y_t \neq y_s \; \wedge \; \exists x_t \in \mathbb{Z} \; t.c. \; ax_t + by_t = d; \quad y_t > y_s \veebar \; y_t < y_s$$

- Se $y_s < 0$ allora:
  - $\forall y_t \; t.c. \; y_t > y_s$ allora, per costruzione delle soluzioni, $y_t \geq y_s + \frac{a}{(a,b)} \geq \lfloor \frac{d}{b} \rfloor + 1$; dunque $y_t \notin \mathbb{Y}(a,b,d)$;
  - $\forall y_t \; t.c. \; y_t < y_s, \; y_t < 0, \; \Rightarrow y_t \notin \mathbb{Y}(a,b,d)$;

  Dunque se $y_s < 0 \Longrightarrow \mathbb{Y}(a,b,d) = \emptyset$ e $\rho(a,b,d) = -1$.
- Se $y_s > 0$ dimostriamo che $y_s \in \mathbb{Y}(a,b,d)$.
  y_s e' soluzione, dunque

  $$\exists x_s \in \mathbb{Z} \; t.c. \; ax_s + by_s = d; x_s = \frac{d - by_s}{a}.$$

  Per costruzione $y_s \leq \frac{d}{b}$, dunque

  $$x_s \geq \frac{d - b\frac{d}{b}}{a} = 0$$

  ossia $x_s \in \mathbb{N} \cup \{0\}$. Allora $y_s \in \mathbb{Y}(a,b,d)$.

  Quindi:
  - $\forall y_t > y_s$, per costruzione delle soluzioni, $y_t \geq y_s + \frac{a}{(a,b)} \geq \lfloor \frac{d}{b} \rfloor + 1$; dunque $y_t \notin \mathbb{Y}(a,b,d)$;
  - $\forall y_t < y_s, \; y_t \neq max\mathbb{Y}(a,b,d)$;

  Dunque $y_s = max\mathbb{Y}(a,b,d) \wedge \; \rho(a,b,d) = x_s + y_s$.

□

Algoritmo per il caso con 3 incognite

Data (I) $ax + by + cz = d$ equazione con $a, b, c, d \in \mathbb{N}$ di cui cerchiamo soluzioni naturali, definiamo

$$Z_Z(a,b,c,d) = \{z \in \mathbb{Z} \; t.c. \; \exists x, y \in \mathbb{Z} \; t.c. \; ax + by + cz = d\}$$

Lemma 2. *Dato z_0 soluzione particolare dell'equazione (I),*

$$Z_Z(a,b,c,d) = \left\{ \; z \in \mathbb{Z} \; t.c. \; z = z_0 + \frac{(a,b)}{(a,b,c)}\alpha, \; \alpha \in \mathbb{Z} \right\}.$$

Proof.
Possiamo sostituire, grazie al teorema di Bézout, $ax+by$ con $(a,b)k, \; k \in \mathbb{Z}$; dunque, sostituendo, ottengo:

$$cz + (a,b)k = d.$$

Ma

$$\exists k \in \mathbb{Z} \; t.c. \; cz + (a,b)k = d \Leftrightarrow \; z = z_0 + \frac{(a,b)}{(a,b,c)}\alpha, \; \alpha \in \mathbb{Z}$$

□

A questo punto possiamo definire

$$Z_N(a,b,c,d) = \{z \in \mathbb{N} \cup \{0\} \; t.c. \; \exists x, y \in \mathbb{Z} \; t.c. \; ax + by + cz = d\}.$$

Questo insieme è limitato inferiormente.
Possiamo inoltre definire

$$Z_S(a,b,c,d) = \left\{ z \in \mathbb{N} \cup \{0\} \; t.c. \; z \leq \frac{d}{c} \; \wedge \; \exists x, y \in \mathbb{Z} \; t.c. \; ax + by + cz = d \right\}$$

infatti noi siamo interessati a trovare le soluzioni $x, y, z \in \mathbb{N}$, e se

$$z > \frac{d}{c} \;\Rightarrow\; ax + by < d - \frac{d}{c}c \;\Rightarrow\; ax + by < 0,$$

ma

$$\forall a, b \in \mathbb{N} \; \nexists x, y \in \mathbb{N} \cup \{0\} \;\; t.c. \; ax + by < 0.$$

Dunque l'insieme $Z_S(a, b, c, d)$ ha cardinalità finita, dunque possiamo calcolare, in un numero finito di passaggi,

$$min(x + y + z) = min\left\{z + \rho(a, b, d - cz) \; t.c. \; z \in Z_S(a, b, c, d) \;\wedge\; \rho(a, b, d - cz) \neq -1\right\}$$

Algoritmo
Denotiamo gli elementi di Z_S che sono tutti della forma $maxZ_S(a, b, c, d) - \frac{(a,b)}{(a,b,c)}i$ con z_i , con $i \in \{0, 1, 2, ..., \xi\}$ (infatti la cardinalità di Z_S è finita), e dunque $z_i < z_h \;\Leftrightarrow\; i > h$.

Calcoliamo

$$min(x + y + z) = min\left\{z + \rho(a, b, d - cz) \; t.c. \; z \in Z_S(a, b, c, d) \;\wedge\; \rho(a, b, d - cz) \neq -1\right\} :$$

Definiamo $0 := m_p$ (che sta per "minimo parziale") .
Partendo da $i = 0$:
(1)
Calcoliamo il valore di $\rho(a, b, d - cz_i)$;

- se $\rho(a, b, d - cz_i) \neq -1$ allora:
  - Se $m_p = 0 \;\vee\; m_p > z_i + \rho(a, b, d - cz_i)$ allora ridefinisci $m_p := z_i + \rho(a, b, d - cz_i)$ e vai a (2);
  - Se $m_p \leq z_i + \rho(a, b, d - cz_i)$ allora vai a (2).
- se $\rho(a, b, d - cz_i) = -1$ allora passa a (2).

(2)

- Se $i + 1 \leq \xi$ allora ridefinisci $i := i + 1$ e vai a (1);
- Se $i + 1 > \xi$ allora
  - Se $m_p = 0$ allora non ci sono terne di soluzioni in $\mathbb{N} \cup 0$; fine.
  - Se $m_p \neq 0$ allora $m_p = min(x + y + z)$; fine.

Ottimizzazione computazionale
L'algoritmo così com'è stato definito calcola il $min(x + y + z)$ in un numero finito di passaggi. Può comunque essere utile utilizzare delle proprietà delle soluzioni per ridurre drasticamente il numero di soluzioni da ricavare.
Conviene anzitutto riordinare l'equazione in modo che risulti $a < b < c$.

Caso $x_s = 0$ Dimostriamo che, se durante l'algoritmo viene trovata una terna di soluzioni del tipo

$$\begin{cases} x = 0 \\ y = y_s \\ z = z_s \end{cases}$$

allora tutte le soluzioni (x', y', z') trovate successivamente (con $z' < z_s$) hanno valore di $x' + y' + z' > y_s + z_s$, dunque l'algoritmo può interrompersi dal momento che il minimo dell'intero insieme è uguale al minimo dell'insieme contenente gli elementi già calcolati.

Lemma 2.3. *Dati*

$$b, a \in \mathbb{R} \text{ t.c. } b > a,$$
$$k \in \mathbb{R}^+,$$
$$\mathbb{T} = \left\{(x, y) \in \mathbb{R}^{+2} \text{ t.c. } x + y \leq k\right\},$$

e data

$$f : \mathbb{T} \to \mathbb{R};\ f(x, y) = ax + by;$$
$$\implies max(f(\mathbb{T})) = kb$$

Proof.

$$x + y \leq k \ \Leftrightarrow\ x \leq k - y \ \Leftrightarrow\ ax + by \leq ak - ay + by = ak + (b - a)y$$

Ma per ipotesi $b - a > 0 \ \Rightarrow\ f(x, y)$ è crescente in y e

$$max(f(\mathbb{T})) = f(0, k) = kb$$

□

Se consideriamo

$$x', y', z' \text{ t.c. } z' < z_s \ \wedge\ ax' + by' + cz' = d,$$

possiamo dire che

$$by_s + cz_s = ax' + by' + cz';$$
$$\exists \alpha \in \mathbb{N} \text{ t.c. } z' = z_s - \frac{(a, b)}{(a, b, c)}\alpha;$$
$$by_s + cz_s = ax' + by' + cz_s - c\frac{(a, b)}{(a, b, c)}\alpha;$$
$$by_s = ax' + by' - c\frac{(a, b)}{(a, b, c)}\alpha;$$
$$by_s + c\frac{(a, b)}{(a, b, c)}\alpha = ax' + by';$$

Se per assurdo

$$x' + y' + z' \leq z_s + y_s \ \Rightarrow\ x' + y' + z_s - \frac{(a, b)}{(a, b, c)}\alpha \leq z_s + y_s \ \Rightarrow\ x' + y' \leq y_s + \frac{(a, b)}{(a, b, c)}\alpha.$$

A questo punto il lemma 2.3 implica che

$$ax' + by' \leq b(y_s + \frac{(a, b)}{(a, b, c)}\alpha) \ \Rightarrow\ ax' + by' \leq by_s + b\frac{(a, b)}{(a, b, c)}\alpha < by_s + c\frac{(a, b)}{(a, b, c)}\alpha.$$

Dunque $ax' + by'$ sarebbe allo stesso tempo minore e uguale alla stessa quantità. Assurdo.

Funzione j

Cerchiamo una funzione $j : Z_S(a, b, c, d) \to \mathbb{R}$ che abbia le seguenti caratteristiche:

- Valga $j(z_i) > j(z_h) \ \Leftrightarrow\ i > h$;
- Valga $j(z_i) < min\left\{z_h + \rho(a, b, d - cz_h) \text{ t.c. } z_h \in Z_S(a, b, c, d) \ \wedge\ \ h > i \ \wedge\ \rho(a, b, d - cz_h) \neq -1\right\}$;

In questo modo, calcolando i valori di $z_i + \rho(a, b, d - cz_i)$ partendo da z_0, procedendo aumentando l'indice i di unità in unità e calcolando parallelamente ad ogni passaggio il valore di $j(z_i)$, ottengo ad ogni passaggio una stima dal basso della somma delle soluzioni che troverò nei passaggi successivi. Dato che la funzione j è crescente, non appena

$$j(z_i) \geq min\left\{z_h + \rho(a, b, d - cz_h) \; t.c. \; z_h \in Z_S(a, b, c, d) \; \wedge \; h \leq i \; \wedge \; \rho(a, b, d - cz_h) \neq -1\right\}$$

so che non possono essere trovate soluzioni la cui somma è minore del minimo delle soluzioni già trovate.

Lemma 2.4.

$$Se \; \rho(a, b, d) \neq -1, \Longrightarrow \quad \rho(a, b, d) \geq \frac{d}{b}.$$

Proof.
Se vale $ax + by = d \Rightarrow y = \frac{d-ax}{b}$ consideriamo la funzione $f(x) : \mathbb{R}^+ \to \mathbb{R}$ definita come $f(x) = x + \frac{d-ax}{b}$ che associa ad ogni valore di x il valore di $x + y$ con y tale che $ax + by = d$. Cerchiamo il minimo di questa funzione. La funzione é strettamente crescente poichè $f'(x) = 1 - \frac{a}{b} > 0$ dato che $a < b$. Allora

$$min\left\{x + y \; t.c. \; x, y \in \mathbb{R}^+ \wedge ax + by = d\right\} = f(0) = \frac{d}{b}$$

D'altra parte

$$min\left\{x + y \; t.c. \; x, y \in \mathbb{R}^+ \wedge ax + by = d\right\} \leq min\left\{x + y \; t.c. \; x, y \in \mathbb{N} \cup \{0\} \wedge ax + by = d\right\} = \rho(a, b, d)$$

dato che $\mathbb{N} \cup \{0\} \subset \mathbb{R}$. □

Dunque $\forall z_i \in Z_S(a, b, c, d)$,

$$\rho(a, b, d - cz_i) \geq \frac{d - cz_i}{b}$$

.

Dunque definiamo

$$j(z_i) = \frac{d - cz_i}{b} + z_i.$$

Sappiamo dunque che se $\rho(a, b, d - cz_i) \neq -1$ allora:

$$j(z_i) \leq z_i + \rho(a, b, d - cz_i)$$

Inoltre dimostriamo che, se $k > h \implies j(z_k) > j(z_h)$.
Infatti, se

$$k > h \; \Rightarrow \; z_k < z_h \; \Rightarrow \exists \lambda \in \mathbb{N} \; t.c. \; \; z_k = z_h - \lambda; \implies$$

$$j(z_k) = j(z_h - \lambda) = \frac{d - c(z_h - \lambda)}{b} + z_h - \lambda \; = \; \frac{d - cz_h}{b} + z_h + \frac{c}{b}\lambda - \lambda > \frac{d - cz_h}{b} + z_h = j(z_h) \Leftrightarrow \; (\frac{c}{b} - 1)\lambda > 0$$

che è vero perché, per ipotesi, $c > b$.

Quindi,

$$\forall i > h \; t.c. \; \rho(a, b, d - cz_i) \neq -1, \;\; j(z_h) < j(z_i) \leq z_i + \rho(a, b, d - cz_i);$$

Dunque la funzione è minorante di tutte le somme delle soluzioni successive.

Battista Ludovico e Pisanu Federico Giuseppe