h 08:45

Lezione 14

Alessandro Ardizzoni

Funzioni tra insiemi di classi di resto

Esercizio

Stabilire se la funzione $f : \mathbb{Z}_n \to \mathbb{Z}_n,\ \overline{a} \mapsto \overline{a^2}$ *sia ben definita.*

<u>SOLUZIONE</u>. Sappiamo che f è ben definita se manda elementi uguali del dominio in elementi uguali del codominio, cioé se $\forall a, b \in \mathbb{Z},\ \overline{a} = \overline{b} \Rightarrow \overline{a^2} = \overline{b^2}$. Equivalentemente dobbiamo capire se $n \mid a - b \Rightarrow n \mid a^2 - b^2$. Questo è vero. Infatti $a^2 - b^2 = (a+b)(a-b)$ e quindi $n \mid a - b \Rightarrow n \mid (a+b)(a-b)$.

Esercizio

Stabilire se la funzione $f : \mathbb{Z}_n \to \mathbb{Z}_n,\ \overline{a} \mapsto \overline{2^a}$ *sia ben definita.*

<u>SOLUZIONE</u>. Similmente a sopra, per vedere che f è ben definita basta capire se $\forall a, b \in \mathbb{Z},\ \overline{a} = \overline{b} \Rightarrow \overline{2^a} = \overline{2^b}$. Notiamo però che $\overline{0} = \overline{n}$ ma $\overline{2^0} \neq \overline{2^n}$ in generale. Infatti se fosse $\overline{2^0} = \overline{2^n}$ si avrebbe $n \mid 2^n - 2^0 = 2^n - 1$ ma questo non è sempre vero, ad esempio se $n \neq 0$ è pari non può dividere $2^n - 1$ che è dispari. Quindi f non è sempre ben definita.

Esercizio

Dimostrare che la funzione $f : \mathbb{Z}_6 \to \mathbb{Z}_3,\ [a]_6 \mapsto [a]_3$ *è ben definita.*

SOLUZIONE. Notiamo che qui la notazione con le parentesi quadre per le classi di resto è utile per non confondere una classe del dominio con una del codominio. Ora f è ben definita se $\forall a, b \in \mathbb{Z},\ [a]_6 = [b]_6 \Rightarrow [a]_3 = [b]_3$ cioé se $6 \mid a - b \Rightarrow 3 \mid a - b$. Siccome $3 \mid 6$ questo è vero. Infatti:
$6 \mid a - b \Rightarrow \exists k, a - b = 6k \Rightarrow a - b = 3(2k) \Rightarrow 3 \mid a - b$.

Esercizio

Dimostrare che la funzione $f : \mathbb{Z}_5 \to \mathbb{Z}_3, [a]_5 \mapsto [a]_3$ *non è ben definita.*

SOLUZIONE. f è ben definita se $\forall a, b \in \mathbb{Z},\ [a]_5 = [b]_5 \Rightarrow [a]_3 = [b]_3$ cioé se $5 \mid a - b \Rightarrow 3 \mid a - b$. Siccome i multipli di 5 non sono sempre multipli di 3, ci aspettiamo che questo non sia vero. In effetti basta scegliere $a = 5$ e $b = 0$ perché l'implicazione sia falsa.

Gli esercizi precedenti anticipano il seguente risultato.

Proposizione

Siano $m, n \in \mathbb{N}$*. Allora la funzione*

$$f : \mathbb{Z}_m \to \mathbb{Z}_n, \quad [a]_m \mapsto [a]_n$$

è ben definita se e solo se $n \mid m$*.*

Proof.

Notiamo che $m \mid m - 0$ e quindi $m \equiv_m 0$, da cui $[m]_m = [0]_m$. Pertanto, se f è ben definita, si avrà $f([m]_m) = f([0]_m)$, cioé $[m]_n = [0]_n$. Questo vuol dire $m \equiv_n 0$ cioé $n \mid m - 0$ e quindi $n \mid m$ come richiesto.

Viceversa, supponiamo $n \mid m$. Dobbiamo dimostrare che f è ben definita cioé che, per ogni a, b, si ha $[a]_m = [b]_m \Rightarrow [a]_n = [b]_n$ cioé $m \mid a - b \Rightarrow n \mid a - b$. Siccome $n \mid m$ questo è vero. □

Il prossimo obiettivo è dimostrare che le classi di resto si possono sommare e moltiplicare. Per farlo occorre definire le relative operazioni.

Operazioni sulle classi di resto

Vogliamo ora mostrare che in $\mathbb{Z}_n$ possiamo introdurre una somma ed una moltiplicazione. Per farlo abbiamo bisogno del seguente risultato.

Proposizione

Se $a, b, a', b' \in \mathbb{Z}$ sono tali che $a \equiv_n a'$ e $b \equiv_n b'$ allora

$$a + b \equiv_n a' + b' \qquad e \qquad ab \equiv_n a'b'.$$

Proof.

Sappiamo che $a \equiv_n a'$ cioé $n \mid (a - a')$. Quindi $\exists k \in \mathbb{Z}$ tale che $a = a' + kn$. Similmente $\exists s \in \mathbb{Z}$ tale che $b = b' + sn$. Ma allora

$$a+b = (a'+kn)+(b'+sn) = (a'+b')+(k+s)n \Rightarrow n \mid (a+b)-(a'+b') \Rightarrow a+b \equiv_n a'+b';$$

$$ab = (a'+kn)(b'+sn) = a'b' + (a's+kb'+ksn)n \Rightarrow n \mid ab - a'b' \Rightarrow ab \equiv_n a'b'.$$

$\square$

Somma di classi.

Definiamo l'addizione in $\mathbb{Z}_n$ come l'operazione

$$+ : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n, \ (\overline{a}, \overline{b}) \mapsto \overline{a+b}.$$

Perchè questa sia una funzione occorre che elementi uguali del dominio vengano mandati in elementi uguali del codominio cioé che, $\forall a, b \in \mathbb{Z}$,

$$(\overline{a}, \overline{b}) = (\overline{a'}, \overline{b'}) \Rightarrow \overline{a+b} = \overline{a'+b'} \quad \text{cioé che}$$

$$\overline{a} = \overline{a'} \ \wedge \ \overline{b} = \overline{b'} \Rightarrow \overline{a+b} = \overline{a'+b'}.$$

Ora due classi sono uguali se i rispettivi rappresentanti sono in relazione. Pertanto l'implicazione da dimostrare diventa

$$a \equiv_n a' \ \wedge \ b \equiv_n b' \Rightarrow a+b \equiv_n a'+b'.$$

Questo lo abbiamo appena dimostrato nella proposizione precedente. Sapendo ora che l'addizione è ben definita, possiamo indicare l'immagine della coppia $(\overline{a}, \overline{b})$ con il simbolo $\overline{a}+\overline{b}$ e chiamarla somma delle classi $\overline{a}$ e $\overline{b}$ in $\mathbb{Z}_n$. Quindi:

$$\overline{a}+\overline{b} := \overline{a+b} \qquad \text{o equivalentemente} \qquad [a]_n + [b]_n := [a+b]_n.$$

Prodotto di classi.

Definiamo la moltiplicazione in $\mathbb{Z}_n$ come l'operazione

$$\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n, (\overline{a},\ \overline{b}) \mapsto \overline{ab}.$$

Perchè questa sia una funzione occorre che elementi uguali del dominio vengano mandati in elementi uguali del codominio cioé che, $\forall a, b \in \mathbb{Z}$,

$$(\overline{a}, \overline{b}) = (\overline{a'}, \overline{b'}) \Rightarrow \overline{ab} = \overline{a'b'} \quad \text{cioé che}$$
$$\overline{a} = \overline{a'} \ \wedge \ \overline{b} = \overline{b'} \Rightarrow \overline{ab} = \overline{a'b'}.$$

Ora due classi sono uguali se i rispettivi rappresentanti sono in relazione. Pertanto l'implicazione da dimostrare diventa

$$a \equiv_n a' \ \wedge \ b \equiv_n b' \Rightarrow ab \equiv_n a'b'.$$

Questo lo abbiamo dimostrato nella proposizione precedente.
Essendo ora la moltiplicazione ben definita, possiamo indicare l'immagine della coppia $(\overline{a}, \overline{b})$ con il simbolo $\overline{a} \cdot \overline{b}$ e chiamarla prodotto delle classi $\overline{a}$ e $\overline{b}$ in $\mathbb{Z}_n$. Quindi:

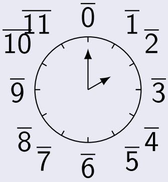
$$\overline{a} \cdot \overline{b} := \overline{ab} \qquad \text{o equivalentemente} \qquad [a]_n \cdot [b]_n := [ab]_n.$$

Aritmetica modulare

L'aritmetica modulare è lo studio delle proprietà del prodotto e della somma in $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}\}$.

Aritmetica dell'orologio

Notiamo che in $\mathbb{Z}_{12} = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{11}\}$ la somma funziona esattamente come tra le ore dell'orologio. Se sono le 11 e aggiungiamo 3 ore arriviamo alle 2: allo stesso modo $\overline{11} + \overline{3} = \overline{11+3} = \overline{14} = \overline{2}$ perché $14 \equiv_{12} 2$.
Ogni 12 ore ritorno all'ora da cui sono partito così come $\overline{a+12} = \overline{a}$.



Possiamo pensare a $\mathbb{Z}_n$ come ad un orologio suddiviso in n ore.
Per questo l'aritmetica modulare a volte è detta aritmetica dell'orologio.

Peculiarità dell'aritmetica modulare

La somma ed il prodotto in $\mathbb{Z}_n$ presentano delle peculiarità.
Ad esempio in $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$:

- La somma di classi di numeri positivi può fare zero:

$$\overline{2} + \overline{2} = \overline{2+2} = \overline{4} = \overline{0}.$$

- Il prodotto di classi diverse da $\overline{0}$ può fare $\overline{0}$:

$$\overline{2} \cdot \overline{2} = \overline{2 \cdot 2} = \overline{4} = \overline{0}.$$

  Quindi NON vale la legge di annullamento del prodotto.

- NON vale la cancellazione:

$$\overline{2} \cdot \overline{2} = \overline{2} \cdot \overline{0} \not\Rightarrow \overline{2} = \overline{0} \quad (\text{perché } \overline{2} \neq \overline{0}).$$

  Quindi non è sempre possibile dividere per classi diverse da $\overline{0}$.

Peculiarità a parte, vedremo che $\mathbb{Z}_n$ eredita da $\mathbb{Z}$ diverse proprietà.

Quando n è piccolo, può essere utile rappresentare la somma ed il prodotto di $\mathbb{Z}_n$ mediante Tavole di Cayley. Ad esempio, per $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

Tavola additiva

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

Tavola moltiplicativa

Queste tavole ci portano a queste conclusioni:

- Facendo i conti caso per caso si vede che l'addizione e la moltiplicazione sono associative.
- La simmetria delle tavole mostra che l'addizione e la moltiplicazione sono commutative.
- Nella tavola additiva la riga rossa e la colonna blu si riproducono accanto e sotto $\overline{0}$. Allora $\overline{0}$ è l'elemento neutro dell'addizione (lo zero). Similmente $\overline{1}$ è l'elemento neutro della moltiplicazione (l'unità).
- Siccome $\overline{0}$ compare almeno una volta in ogni riga ed ogni colonna della tavola additiva, allora ogni elemento di $\mathbb{Z}_3$ ha un inverso rispetto all'addizione (un opposto). Non potendo dire lo stesso per $\overline{1}$ nella tavola moltiplicativa, allora non tutti gli elementi hanno un inverso moltiplicativo.

Esercizio (per casa...sarà un QUIZ del prossimo tutorato)

Provare a scrivere le tabelle moltiplicativa ed additiva per $\mathbb{Z}_4$.

Vediamo che, per ogni $n \in \mathbb{N} \setminus \{0\}$, si ha che $\mathbb{Z}_n$ ha le stesse proprietà descritte nel caso particolare considerato sopra.

Proprietà della somma

- Associativa: $(\overline{a}+\overline{b})+\overline{c} = \overline{a+b}+\overline{c} = \overline{(a+b)+c} = \overline{a+(b+c)} = \overline{a}+\overline{b+c} = \overline{a}+(\overline{b}+\overline{c})$.
- Commutativa: $\overline{a}+\overline{b} = \overline{a+b} = \overline{b+a} = \overline{b}+\overline{a}$.
- Ha uno zero: $\overline{a}+\overline{0} = \overline{a+0} = \overline{a}$
- C'è un opposto: $\overline{-a}+\overline{a} = \overline{-a+a} = \overline{0}$. L'elemento $\overline{-a}$ è detto opposto di $\overline{a}$ e si indica con il simbolo $-\overline{a}$.

Proprietà del prodotto

- Associativa: $(\overline{a}\cdot\overline{b})\cdot\overline{c} = \overline{a\cdot b}\cdot\overline{c} = \overline{(a\cdot b)\cdot c} = \overline{a\cdot(b\cdot c)} = \overline{a}\cdot\overline{b\cdot c} = \overline{a}\cdot(\overline{b}\cdot\overline{c})$.
- Commutativa: $\overline{a}\cdot\overline{b} = \overline{a\cdot b} = \overline{b\cdot a} = \overline{b}\cdot\overline{a}$.
- Ha un'unità: $\overline{a}\cdot\overline{1} = \overline{a\cdot 1} = \overline{a}$.
- Un elemento $\overline{a}$ è invertibile se esiste un elemento $\overline{b}$ tale che $\overline{a}\cdot\overline{b} = \overline{1}$. In tal caso $\overline{b}$ è detto un suo inverso moltiplicativo.

NB: non tutte le classi sono invertibili. Ad esempio $\forall a \in \mathbb{Z}$ si ha che

$$\overline{0} \cdot \overline{a} = \overline{0 \cdot a} = \overline{0} \neq \overline{1}$$

e quindi non esiste un inverso moltiplicativo di $\overline{0}$.

Proprietà distributiva

- $\overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot \overline{b+c} = \overline{a \cdot (b+c)} = \overline{a \cdot b + a \cdot c} = \overline{a \cdot b} + \overline{a \cdot c} = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}.$

Per quanto visto sopra possiamo lavorare con le classi di resto come se fossero nei numeri tenendo però presenti le eccezioni (peculiarità) viste prima.

Osservazione

Per quanto visto sopra, $(\mathbb{Z}_n, +)$ e $(\mathbb{Z}_n, \cdot)$ sono monoidi commutativi.

Criteri di divisibilità

Consideriamo un numero positivo:

$$\mathbf{23015} = \boxed{2} \cdot 10^4 + \boxed{3} \cdot 10^3 + \boxed{0} \cdot 10^2 + \boxed{1} \cdot 10^1 + \boxed{5} \cdot 10^0.$$

I numeri $2, 3, 0, 1, 5$ sono detti cifre e si dice che il numero è espresso in notazione decimale. Ci sono altre notazioni utilizzate in matematica come, ad esempio, la notazione binaria, ma ora non vogliamo parlare di questo. In generale, un $N \in \mathbb{N} \setminus \{0\}$ lo possiamo esprimere in notazione decimale come

$$N = c_n c_{n-1} \dots c_2 c_1 c_0$$

per certi $c_0, c_1, \dots c_n \in \{0, 1, \dots 9\}$, intendendo

$$N = \boxed{c_n} \cdot 10^n + \boxed{c_{n-1}} \cdot 10^n + \cdots \boxed{c_2} \cdot 10^2 + \boxed{c_1} \cdot 10^1 + \boxed{c_0} \cdot 10^0.$$

Sfruttando l'aritmetica modulare possiamo dimostrare i criteri di divisibilità noti.

Teorema

Consideriamo un numero $N > 0$ scritto in notazione decimale nella forma $N = c_k c_{k-1} \dots c_2 c_1 c_0$. Valgono allora le seguenti proprietà.

- $2 \mid N \Leftrightarrow 2 \mid c_0$.
- $3 \mid N \Leftrightarrow 3 \mid (c_k + c_{k-1} + \cdots + c_2 + c_1 + c_0)$.
- $5 \mid N \Leftrightarrow 5 \mid c_0$.
- $11 \mid N \Leftrightarrow 11 \mid ((-1)^k c_k + (-1)^{k-1} c_{k-1} + \cdots + c_2 - c_1 + c_0)$.

DIMOSTRAZIONE. Per definizione, abbiamo

$$N = c_k \cdot 10^k + c_{k-1} \cdot 10^{k-1} + \cdots + c_2 \cdot 10^2 + c_1 \cdot 10^1 + c_0.$$

Per come sono definiti somma e prodotto in $\mathbb{Z}_n$ otteniamo

$$\begin{aligned} \overline{N} &= \overline{c_k \cdot 10^k + c_{k-1} \cdot 10^{k-1} + \cdots + c_2 \cdot 10^2 + c_1 \cdot 10^1 + c_0} \\ &= \overline{c_k \cdot 10^k} + \overline{c_{k-1} \cdot 10^{k-1}} + \cdots + \overline{c_2 \cdot 10^2} + \overline{c_1 \cdot 10^1} + \overline{c_0} \\ &= \overline{c_k} \cdot \overline{10}^k + \overline{c_{k-1}} \cdot \overline{10}^{k-1} + \cdots + \overline{c_2} \cdot \overline{10}^2 + \overline{c_1} \cdot \overline{10}^1 + \overline{c_0}. \end{aligned}$$

Pertanto

$$\overline{N} = \overline{c_k} \cdot \overline{10}^k + \overline{c_{k-1}} \cdot \overline{10}^{k-1} + \cdots + \overline{c_2} \cdot \overline{10}^2 + \overline{c_1} \cdot \overline{10}^1 + \overline{c_0}.$$

Dimostreremo che $\overline{N} = \overline{M}$ per un M più semplice e a questo punto

$$\boxed{n \mid N} \Leftrightarrow \overline{N} = \overline{0} \Leftrightarrow \overline{M} = \overline{0} \Leftrightarrow \boxed{n \mid M}.$$

Se $n = 2$, allora $\overline{10} = \overline{0}$, perché $10 \equiv_2 0$, e quindi

$$\begin{aligned}\overline{N} &= \overline{c_k} \cdot \overline{10}^k + \overline{c_{k-1}} \cdot \overline{10}^{k-1} + \cdots + \overline{c_2} \cdot \overline{10}^2 + \overline{c_1} \cdot \overline{10}^1 + \overline{c_0} \\ &= \overline{c_k} \cdot \overline{0}^k + \overline{c_{k-1}} \cdot \overline{0}^{k-1} + \cdots + \overline{c_2} \cdot \overline{0}^2 + \overline{c_1} \cdot \overline{0}^1 + \overline{c_0} = \overline{\underbrace{c_0}_{M}}\end{aligned}$$

Se $n = 3$, allora $\overline{10} = \overline{1}$, perché $10 \equiv_3 1$, e quindi

$$\begin{aligned}\overline{N} &= \overline{c_k} \cdot \overline{10}^k + \overline{c_{k-1}} \cdot \overline{10}^{k-1} + \cdots + \overline{c_2} \cdot \overline{10}^2 + \overline{c_1} \cdot \overline{10}^1 + \overline{c_0} \\ &= \overline{c_k} \cdot \overline{1}^k + \overline{c_{k-1}} \cdot \overline{1}^{k-1} + \cdots + \overline{c_2} \cdot \overline{1}^2 + \overline{c_1} \cdot \overline{1}^1 + \overline{c_0} \\ &= \overline{c_k} + \overline{c_{k-1}} + \cdots + \overline{c_2} + \overline{c_1} + \overline{c_0} = \overline{\underbrace{c_k + c_{k-1} + \cdots + c_2 + c_1 + c_0}_{M}}.\end{aligned}$$

Se $n = 5$, allora $\overline{10} = \overline{0}$ e quindi $\overline{N} = \overline{c_0}$ come nel caso $n = 2$.
Se $n = 11$, allora $\overline{10} = \overline{-1}$ e quindi

$$\begin{aligned}
\overline{N} &= \overline{c_k} \cdot \overline{10}^k + \overline{c_{k-1}} \cdot \overline{10}^{k-1} + \cdots + \overline{c_2} \cdot \overline{10}^2 + \overline{c_1} \cdot \overline{10}^1 + \overline{c_0} \\
&= \overline{c_k} \cdot \overline{-1}^k + \overline{c_{k-1}} \cdot \overline{-1}^{k-1} + \cdots + \overline{c_2} \cdot \overline{-1}^2 + \overline{c_1} \cdot \overline{-1}^1 + \overline{c_0} \\
&= \overline{\underbrace{(-1)^k c_k + (-1)^{k-1} c_{k-1} + \cdots + c_2 - c_1 + c_0}_{M}}.
\end{aligned}$$

Esercizio (per casa)

Stabilire un criterio di divisibilità per 99.

Esempio

Consideriamo il numero 123456.

- Esso è divisibile per 2 perché ha come ultima cifra 6 che è divisibile per 2.
- Non è divisibile per 5 perché ha come ultima cifra 6 che non lo è.
- É divisibile per 3 perché ha come somma delle cifre $1+2+3+4+5+6=21$ che è divisibile per 3.
- Non è divisibile per 11 perché $-1+2-3+4-5+6=3$ non lo è.

In effetti si vede che

$$123456 = 2^6 \cdot 3 \cdot 643.$$

Il massimo comun divisore

Consideriamo $a, b \in \mathbb{Z}$.
Se uno dei due è non nullo, diciamo a, consideriamo l'insieme

$$D := \{d \in \mathbb{N} \ : \ d \mid a \wedge d \mid b\}.$$

Sicuramente $1 \mid a \wedge 1 \mid b$ e quindi $D \neq \emptyset$.
Inoltre, se $d \in D$, poiché $a \neq 0$, otteniamo $d \leq |a|$ e quindi

$$D \subseteq I_{|a|} = \{1, 2, \ldots, |a| - 1, |a|\}$$

che è un insieme finito. Esiste allora $\max(D)$.
Questo numero naturale è detto il massimo comun divisore di a e b e si indica con

$$\mathrm{MCD}(a, b) := \max\{d \in \mathbb{N} \ : \ d \mid a \wedge d \mid b\}.$$

Includiamo poi anche il caso $a = b = 0$ definendo

$$\mathrm{MCD}(0, 0) := 0.$$

In questo modo abbiamo definito $\mathrm{MCD}(a, b) \in \mathbb{N}$, per ogni $a, b \in \mathbb{Z}$.

Notiamo i seguenti fatti per ogni $a, b \in \mathbb{Z}$

1. Chiaramente $\mathrm{MCD}(a, b) = \mathrm{MCD}(b, a)$.
2. Siccome $d \mid a \Leftrightarrow d \mid -a$ e $d \mid b \Leftrightarrow d \mid -b$ (Lezione 13), è chiaro che
$$\mathrm{MCD}(a, b) = \mathrm{MCD}(-a, b) = \mathrm{MCD}(a, -b) = \mathrm{MCD}(-a, -b).$$
3. Poiché il MCD è positivo, otteniamo $\mathrm{MCD}(a, 0) = |a| = \mathrm{MCD}(0, a)$.

MCD e Teorema della divisione

Consideriamo $a, b \in \mathbb{Z}$ con $b \neq 0$. Per il Teorema della divisione, esistono $q, r \in \mathbb{Z}$ tali che $a = q \cdot b + r$ e $0 \leq r < |b|$. Vediamo che

$$\mathrm{MCD}(a, b) = \mathrm{MCD}(b, r) \qquad \text{cioè che}$$

l'MCD tra dividendo e divisore è uguale all'MCD tra divisore e resto. Basta provare l'uguaglianza dei seguenti insiemi (e quindi dei loro massimi).

$$\{d \in \mathbb{N} \text{ tale che } d \mid a \text{ e } d \mid b\} = \{d \in \mathbb{N} \text{ tale che } d \mid b \text{ e } d \mid r\}.$$

$\subseteq$). Se $d \mid a$ e $d \mid b$, allora $d \mid (a - bq) = r$.
$\supseteq$). Se $d \mid b$ e $d \mid r$, allora $d \mid (bq + r) = a$.

Nel seguito sottolineiamo dividendo, divisore e resto che sono i termini coinvolti quando si applica l'osservazione precedente.

Esempio

Prendiamo $a = 40$ e $b = 36$. Vogliamo scrivere $\underline{a} = q \cdot \underline{b} + \underline{r}$. Nel nostro caso 36 sta nel 40 una volta con resto di 4, cioé

$$\underline{40} = 1 \cdot \underline{36} + \underline{4}.$$

Dall'osservazione precedente otteniamo $\mathrm{MCD}(a, b) = \mathrm{MCD}(b, r)$ cioé

$$\mathrm{MCD}(40, 36) = \mathrm{MCD}(36, 4).$$

Chiaramente il secondo MCD è più semplice da calcolare del primo perché abbiamo sostituito 40 con un numero più piccolo.
Questo fatto è alla base dell'algoritmo Euclideo della divisione.

L'algoritmo Euclideo serve a calcolare il massimo comun divisore tra due numeri interi $a, b \in \mathbb{Z}$.
Se $b = 0$ sappiamo che $\mathrm{MCD}(a,b) = |a|$ e abbiamo finito.
Se $b \neq 0$, si applica ripetutamente il Teorema della divisione:

Passo	divisione	resto
0)	$a = q_0 b + r_0$	$0 \leq r_0 < \lvert b \rvert$
1)	$b = q_1 r_0 + r_1$	$0 \leq r_1 < \lvert r_0 \rvert = r_0$
2)	$r_0 = q_2 r_1 + r_2$	$0 \leq r_2 < \lvert r_1 \rvert = r_1$
...		
n)	$r_{n-2} = q_n r_{n-1} + \boxed{r_n}$	$0 \leq r_n < \lvert r_{n-1} \rvert = r_{n-1}$
$n+1$)	$r_{n-1} = q_{n+1} r_n + 0$	$r_{n+1} = 0$

Dopo ogni passo il resto si riduce: $0 \leq \cdots < r_n < \cdots < r_2 < r_1 < r_0 < |b|$.
Ad un certo punto troveremo un n per cui $r_{n+1} = 0$ come sopra. Allora

$$\begin{aligned}\mathrm{MCD}(a,b) &= \mathrm{MCD}(b,r_0) = \mathrm{MCD}(r_0,r_1) = \mathrm{MCD}(r_1,r_2) = \cdots \\ &= \mathrm{MCD}(r_{n-1},r_n) = \mathrm{MCD}(r_n,r_{n+1}) = \mathrm{MCD}(r_n,0) = |r_n| = r_n.\end{aligned}$$

In definitiva l'ultimo resto non nullo trovato è proprio $\mathrm{MCD}(a,b)$.

Esercizio

Calcolare $\mathrm{MCD}(40,37)$.

<u>SOLUZIONE</u>. Applichiamo l'algoritmo prendendo $a = 40$ e $b = 37$.

0)	$\underline{40} = 1 \cdot \underline{37} + \underline{3}$
1)	$\underline{37} = 12 \cdot \underline{3} + \boxed{\underline{1}}$
2)	$\underline{3} = 3 \cdot \underline{1} + \underline{0}.$

Pertanto $\mathrm{MCD}(40,37) = \mathrm{MCD}(37,3) = \mathrm{MCD}(3,1) = \mathrm{MCD}(1,0) = 1$.

Esercizio

Calcolare $\mathrm{MCD}(40,-37)$.

<u>SOL</u>. Sappiamo che $\mathrm{MCD}(40,-37) = \mathrm{MCD}(40,37) = 1$ (come sopra).
Possiamo quindi ridurci al calcolo dell'MCD di numeri positivi.

Esercizio

Calcolare $\mathrm{MCD}(37,40)$.

<u>SOL</u>. Sappiamo che $\mathrm{MCD}(37,40) = \mathrm{MCD}(40,37) = 1$ (come sopra).
Possiamo quindi ridurci ad avere il dividendo maggiore del divisore.