# ALGEBRA I: NUMERI INTERI, DIVISIBILITÀ E IL TEOREMA FONDAMENTALE DELL'ARITMETICA

## 1. Richiami sulle proprietà dei numeri naturali

Ho mostrato in un'altra dispensa come ricavare a partire dagli assiomi di Peano le principali strutture sull'insieme $\mathbb{N}$ dei numeri naturali. Qui mi limito a richiamare quelle che utilizzerò in seguito. Ricordo che $\mathbb{N}$ possiede un'operazione di *somma* $\mathbb{N} \times \mathbb{N} \ni (a, b) \mapsto a + b \in \mathbb{N}$ ed un'altra di *molriplicazione* $\mathbb{N} \times \mathbb{N} \ni (a, b) \mapsto a \cdot b$[1].

La somma e la moltiplicazione sono operazioni commutative ed associative, e la moltiplicazione è distributiva rispetto alla somma:

$$a + b = b + a, \qquad (a + b) + c = a + (b + c), \tag{1.1}$$

$$ab = ba, \qquad (ab)c = a(bc), \qquad a(b + c) = ab + ac, \qquad (a + b)c = ac + bc, \tag{1.2}$$

per ogni $a, b, c \in \mathbb{N}$. $0$ e $1$ sono gli elementi neutri di somma e moltiplicazione:

$$0 + a = a = a + 0, \qquad 1 \cdot a = a = a \cdot 1, \qquad 0 \cdot a = 0 = a \cdot a, \tag{1.3}$$

per ogni scelta di $a$ in $\mathbb{N}$. Vale una regola di cancellazione per la somma:

$$a + c = b + c \Rightarrow a = b, \tag{1.4}$$

ed una corrispondente per il prodotto

$$ac = bc \Rightarrow a = b \qquad \text{se } c \neq 0. \tag{1.5}$$

Una facile conseguenza della proprietà di cancellazione per il prodotto è la *legge di annullamento del prodotto*:

$$ab = 0 \Rightarrow a = 0 \text{ oppure } b = 0. \tag{1.6}$$

$\mathbb{N}$ possiede un buon ordinamento $\leq$, cioè una relazione d'ordine (totale) rispetto alla quale ogni sottoinsieme non vuoto possiede un elemento minimo. L'elemento minimo di $\mathbb{N}$ è lo $0$, e di $\mathbb{N} \setminus \{0\}$ è $1$. Le operazioni sono compatibili con l'ordinamento. In particolare, per ogni scelta di $a, b, c \in \mathbb{N}$ si ha:

$$a \leq b \Leftrightarrow a + c \leq b + c, \tag{1.7}$$

ed anche

$$a \leq b \Leftrightarrow ac \leq bc, \tag{1.8}$$

se $c \neq 0$. Di conseguenza da $a \leq c, b \leq d$ si ottiene $a + b \leq c + d$ come pure $ab \leq cd$. Poiché se $a \neq 0$, allora $1 \leq a$ abbiamo che $a \neq 0 \Rightarrow b \leq ab$. In particolare, da $ab = 1$ segue $a, b \leq 1$ e quindi $a = b = 1$. Questo fatto si può anche esprimere affermando che $1$ è l'unico elemento *invertibile* di $\mathbb{N}$. E' importante ricordare che

$$a \leq b \Leftrightarrow b = a + c \text{ per qualche } c. \tag{1.9}$$

Tale elemento $c$ è unico a causa della proprietà di cancellazione, e viene solitamente indicato con $b - a$.
E' probabilmente superfluo ricordare che $a \leq b$ si scrive anche $b \geq a$, che $a \leq b, a \neq b$ si scrive anche $a < b$ e che $a \not< b$ equivale a $a \geq b$.

**Esercizi.**

(1) Siano $a, b \leq c$. Mostrate allora che $a \leq b$ se e solo se $c - b \leq c - a$.
(2) Un sottoinsieme $X \subset \mathbb{N}$ è *limitato dall'alto* se esiste un *maggiorante* di $X$, cioè un elemento $n \in \mathbb{N}$ tale che ogni $x \in X$ soddisfi $x \leq n$. Mostrate che ogni sottoinsieme di $\mathbb{N}$ limitato dall'alto ammette elemento massimo. *[Sugg.: sfruttate l'esercizio precedente, e il buon ordinamento di $\mathbb{N}$]*
(3) Mostrate che in $\mathbb{N}$ vale la proprietà archimedea: per ogni scelta di $a, b \in \mathbb{N}$ tale che $a \neq 0$, esiste $n$ tale che $b \leq na$.

## 2. Piccolo vocabolario di strutture algebriche

In matematica, una struttura algebrica è un insieme dotato di una o più operazioni, che soddisfano opportune proprietà o *assiomi*: ad esempio, l'insieme $\mathbb{N}$ dei numeri naturali, dotato delle operazioni di somma e moltiplicazione, è una struttura algebrica. Nella pratica, si preferisce studiare strutture algebriche con caratteristiche migliori di quelle di $\mathbb{N}$ - nelle quali ad esempio sia possibile anche sottrarre e dividere elementi.

In questo paragrafo farò un elenco dei principali tipi di strutture algebriche che incontreremo durante il corso. Ricordo che un'operazione $\circ : X \times X \to X$ si dice associativa se $(x \circ y) \circ z = x \circ (y \circ z)$ per ogni $x, y, z \in X$, e commutativa se $x \circ y = y \circ x$ per ogni $x, y \in X$.

**Definizione 2.1.** Un *gruppo* è un insieme $G$ dotato di un'operazione associativa $\circ : G \times G \to G$ associativa, per la quale

- esiste un elemento $e \in G$ che soddisfa $e \circ g = g \circ e = g$ per ogni $g \in G$.
- Per ogni $g \in G$ esiste $h \in G$ tale che $g \circ h = h \circ g = e$.

[1] Spesso il punto tra i due argomenti della moltiplicazione viene dimenticato, e si scrive $ab$ invece di $a \cdot b$.

Un gruppo è *abeliano* se la sua operazione è commutativa.

Si vede facilmente che esiste al più un elemento che soddisfa la prima proprietà. Effettivamente, se $e \circ g = g \circ e = g = e' \circ g = g \circ e'$ per ogni $g \in G$, allora in particolare $e = e \circ e' = e'$. L'elemento $e$ è detto *elemento neutro* o *identità* del gruppo $G$.

Ogni elemento $h$ tale che $g \circ h = h \circ g = e$ si dice *inverso* di $g$. Ogni elemento possiede al più un inverso: in effetti se $h$ e $h'$ sono entrambi inversi di $g$, si ha: $h = h \circ e = h \circ (g \circ h') = (h \circ g) \circ h' = e \circ h' = h'$. L'inverso di $g$ in $G$ è quindi univocamente determinato, ed è solitamente indicato con la notazione $g^{-1}$.

**Esempi 2.2.** (1) L'operazione $e \circ e = e$ definisce una struttura di gruppo sull'insieme $\{e\}$.
(2) Sull'insieme $X = \{P, D\}$ definiamo un'operazione di somma tale che $P + P = P, P + D = D + P = D, D + D = P$. E' facile mostrare (fatelo!) che $+$ definisce una struttura di gruppo abeliano su $X$, la cui identità è $P$.
(3) Né l'operazione di somma né quella di prodotto definiscono una struttura di gruppo sull'insieme $\mathbb{N}$ dei numeri naturali.
(4) Sia $S_n$ l'insieme di tutte le applicazioni invertibili dell'insieme $\{1, 2, \ldots, n\}$ in se stesso. Allora l'operazione di composizione tra applicazioni definisce (mostratelo!) una struttura di gruppo non abeliano su $S_n$. $S_n$ è detto *gruppo simmetrico su $n$ elementi*.

**Definizione 2.3.** Un *anello* è un insieme $A$ dotato di un'operazione di *somma* $+ : A \times A \to A$, che vi definisce una struttura di gruppo abeliano – il cui elemento neutro è indicato con $0$; e di un'operazione associativa di moltiplicazione $\cdot : A \times A \to A$ distributiva rispetto alla somma, tale cioè che

- $a \cdot (b + c) = a \cdot b + a \cdot c$,
- $(a + b) \cdot c = a \cdot c + b \cdot c$,

per ogni scelta di $a, b, c \in A$. Un anello è *commutativo* se la moltiplicazione è commutativa, ed è *unitario* o *con unità* se $A$ possiede un elemento neutro $1 \neq 0$ rispetto alla moltiplicazione.

Si vede facilmente che $0 \cdot a = a \cdot 0 = 0$ per ogni $a \in A$. Ad esempio, $0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$, da cui si ottiene $0 = 0 \cdot a$ sommando ad entrambi i membri l'inverso di $0 \cdot a$ rispetto all'operazione di somma. Questo mostra che l'operazione di moltiplicazione non definisce mai una struttura di gruppo su un anello, perché l'elemento $0$ non può possedere un inverso moltiplicativo. L'unità $1$, se esiste, è unica. Infatti, se $1 \cdot a = a \cdot 1 = a = 1' \cdot a = a \cdot 1'$ per ogni $a \in A$, allora in particolare $1 = 1 \cdot 1' = 1'$.
Inoltre, se $-1$ indica l'inverso additivo di $1$, si ha $1 + (-1) = 0$ e quindi $0 = 0 \cdot a = (1 + (-1)) \cdot a = 1 \cdot a + (-1) \cdot a = a + (-1) \cdot a$. In modo simile si ottiene anche $(-1) \cdot a + a = 0$. In altre parole $(-1) \cdot a$ è l'inverso additivo di $a$, cioè: $-a = (-1) \cdot a$. In generale, gli anelli che saranno oggetto del nostro studio godranno di ulteriori proprietà:

**Definizione 2.4.** Un anello commutativo con unità è un *dominio d'integrità* se vale in esso la legge di annullamento del prodotto, cioè se $a \cdot b = 0$ è possibile solo quando almeno uno tra $a$ e $b$ è uguale a $0$. Un anello con unità $A$ si dice *corpo* se l'operazione di moltiplicazione definisce una struttura di gruppo sull'insieme $A \setminus \{0\}$, cioè se ogni elemento non nullo possiede un inverso moltiplicativo. Un corpo commutativo è detto *campo*.

Ogni campo è ovviamente un dominio d'integrità – mostratelo!

L'unica struttura algebrica che conosciamo finora – quella dei numeri naturali – non è un gruppo né un anello. Il nostro obiettivo è ora quello di costruire, a partire da $\mathbb{N}$, il più piccolo anello che lo contiene, e ne estende le operazione: l'anello $\mathbb{Z}$ dei numeri interi.

**Esercizi.**

(1) Una relazione d'ordine totale $\leq$ su un anello $A$ definisce una struttura di *anello ordinato* se
   - $a \leq b \iff a + c \leq b + c$,
   - $a > 0, \quad b \leq c \Rightarrow ab \leq ac$,

   per ogni $a, b, c \in A$. Mostrate che se $P = \{a \in A | a > 0\}$, allora $A$ è unione disgiunta di $P$, $-P = \{-a | a \in P\}$ e $\{0\}$, e che $x, y \in P \Rightarrow x + y, xy \in P$. [$P$ è detto *cono positivo* dell'ordinamento $\leq$]
(2) Sia $A$ un anello, e $P \subset A$ tale che $A$ sia unione disgiunta di $P$, $-P$ e $\{0\}$. Supponiamo inoltre che se $x$ e $y$ sono elementi di $P$ allora anche $x + y$ e $xy$ giacciono in $P$. Mostrate che la relazione $\leq$ definita da $x \leq y \Leftrightarrow y - x \in P \cup \{0\}$ è una relazione d'ordine totale, che definisce una struttura di anello ordinato su $A$.
(3) Sia $(A, \leq)$ un anello ordinato con unità. Mostrate che $a^2 \geq 0$ per ogni $a \in A$, e in particolare che $1 > 0$.
(4) Sia $(A, \leq)$ un anello ordinato con unità. Mostrate che $A$ non contiene elementi $a$ tali che $a^2 = -1$.
(5) Sia $(A, \leq)$ un anello ordinato con unità, e $a \in A$ un elemento invertibile, tale cioè che esista un elemento $a^{-1} \in A$ con la proprietà che $a \cdot a^{-1} = a^{-1} \cdot a = 1$. Mostrate che $a > 0 \Leftrightarrow a^{-1} > 0$.
(6) Sia $F$ un *campo ordinato*, cioè un campo con una struttura di anello ordinato. Mostrate che se $x, y \in F$ soddisfano $x, y > 0$, allora $x < y \Leftrightarrow y^{-1} < x^{-1}$.

## 3. Costruzione dell'anello dei numeri interi (facoltativo)

A lezione non ho costruito i numeri interi a partire dai numeri naturali. Abbiamo intenzione di presentare una costruzione molto simile più tardi nel corso: quella di campo delle frazioni di un dominio d'integrità. Per completezza di esposizione, vi riporto comunque la costruzione di $\mathbb{Z}$.

Nelle lezioni, ho dato per buone le principali proprietà algebriche di $\mathbb{Z}$, e cioè il fatto che sia un dominio d'integrità e possieda una struttura d'ordine compatibile con le operazioni. All'inizio del prossimo paragrafo riassumerò le proprietà di $\mathbb{Z}$ che verranno utilizzate in seguito.

3.1. **I numeri interi come classi di equivalenza.** Sull'insieme $\mathbb{N} \times \mathbb{N}$ consideriamo la relazione $(a, b) \sim (c, d) \Leftrightarrow a + d = b + c$.

**Proposizione 3.1.** *La relazione $\sim$ è di equivalenza.*

*Dimostrazione.* La relazione $\sim$ è riflessiva: $(a, b) \sim (a, b)$ dal momento che $a + b = b + a$. E' anche simmetrica: $(a, b) \sim (c, d)$ se $a + d = b + c$, mentre $(c, d) \sim (a, b)$ se $c + b = d + a$; comunque $a + d = d + a$ e $b + c = c + b$. La relazione è infine transitiva: se $(a, b) \sim (c, d)$ e $(c, d) \sim (e, f)$, allora si ha $a+d = b+c, c+f = d+e$, da cui sommando membro a membro si ottiene $(a + d) + (c + f) = (b + c) + (d + e)$. Sfruttando la commutatività e l'associatività della somma, e cancellando $c + d$ da entrambi i membri, si ottiene $a + f = b + e$, cioè $(a, b) \sim (e, f)$. □

**Definizione 3.2.** L'insieme $\mathbb{Z}$ dei numeri interi è il quoziente $(\mathbb{N} \times \mathbb{N})/\sim$.

L'idea intuitiva della definizione appena data è quella di dare alla coppia $(a, b)$ il significato $a - b$. La relazione di equivalenza introdotta è quella che garantisce l'uguaglianza di tali differenze. L'interesse di $\mathbb{Z}$ sta nel fatto di poter definire operazioni analoghe a quelle di $\mathbb{N}$.

3.2. **Buona definizione delle operazioni di somma e prodotto su $\mathbb{Z}$.**

**Proposizione 3.3.** *Le assegnazioni*

$$[(a, b)] + [(c, d)] = [(a + c, b + d)], \qquad [(a, b)] \cdot [(c, d)] = [(ac + bd, ad + bc)]$$

*danno operazioni ben definite sull'insieme $\mathbb{Z}$.*

*Dimostrazione.* Stiamo definendo delle operazioni su un insieme quoziente: dobbiamo quindi sincerarci che siano *ben definite*, che non dipendano cioè dalla scelta dei rappresentanti delle classi di equivalenza. Questo è immediato per la somma: da $(a, b) \sim (a', b')$ e $(c, d) \sim (c', d')$ si ricava $a + b' = a' + b, c + d' = c' + d$. Sommando membro a membro si ottiene $a+c+b'+d' = a'+c'+b+d$, cioe $(a+c, b+d) \sim (a'+c', b'+d')$. La verifica per la moltiplicazione è invece più laboriosa, e la facciamo in due passi.

Sostituiamo prima $(a, b) \sim (a', b')$ e verifichiamo che $(ac + bd, ad + bc) \sim (a'c + b'd, a'd + b'c)$. Questo accade se $ac + bd + a'd + b'c = ad + bc + a'c + b'd$ cioè se $(a + b')c + (a' + b)d = (a' + b)c + (a + b')d$: questo segue facilmente da $a + b' = a' + b$. Se a questo punto sostituiamo $(c, d)$ con l'elemento $(c', d')$ appartenente alla stessa classe di $\sim$-equivalenza, verifichiamo alla stessa maniera che $(a'c+b'd, a'd+b'c) \sim (a'c' + b'd', a'd' + b'c')$ utilizzando il fatto che $c + d' = c' + d$. □

**Proposizione 3.4.** *Le operazioni di somma e moltiplicazione appena definite sono commutative ed associative, e la moltiplicazione è distributiva rispetto alla somma.*

*Dimostrazione.* La commutatività di entrambe le operazioni e l'associatività della somma sono di immediata e facile verifica. Per quanto riguarda l'associatività del prodotto abbiamo:

$$([(a, b)] \cdot [(c, d)]) \cdot [(e, f)] = [(ac + bd, ad + bc)] \cdot [(e, f)] = [((ac + bd)e + (ad + bc)f, (ac + bd)f + (ad + bc)e)],$$

mentre

$$[(a, b)] \cdot ([(c, d)] \cdot [(e, f)]) = [(a, b)] \cdot [(ce + df, cf + de)] = [(a(ce + df) + b(cf + de), a(cf + de) + b(ce + df))],$$

e si vede subito che i due risultati coincidono utilizzando le proprietà di commutatività, associatività e distributività delle due operazioni. La distributività si controlla alla stessa maniera. Ad esempio si ha:

$$[(a, b)] \cdot ([(c, d)] + [(e, f)]) = [(a, b)] \cdot [(c + e, d + f)] = [(a(c + e) + b(d + f), a(d + f) + b(c + e))]$$

mentre

$$[(a, b)] \cdot [(c, d)] + [(a, b)] \cdot [(e, f)] = [(ac + bd, ad + bc)] + [(ae + bf, af + be)] = [(ac + bd + ae + bf, ad + bc + af + be)],$$

che sono chiaramente uguali. □

3.3. **Proprietà delle operazioni di $\mathbb{Z}$.**

**Lemma 3.5.** *Gli elementi $[(0, 0)]$ e $[(1, 0)]$ sono gli elementi neutri rispetto alla somma e al prodotto di $\mathbb{Z}$ rispettivamente.*

*Dimostrazione.* Si mostra facilmente che

$$[(0, 0)] + [(a, b)] = [(a, b)] = [(a, b)] + [(0, 0)],$$

e che

$$[(1, 0)] \cdot [(a, b)] = [(1 \cdot a + 0 \cdot b, 1 \cdot b + 0 \cdot a)] = [(a, b)] = [(a \cdot 1 + b \cdot 0, a \cdot 0 + b \cdot 1)] = [(a, b)] \cdot [(1, 0)].$$

□

**Lemma 3.6.** *Comunque si scelgano $a, b \in \mathbb{N}$, l'elemento $[(b, a)]$ è inverso di $[(a, b)]$ rispetto all'operazione di somma.*

*Dimostrazione.* Si ha: $[(a, b)] + [(b, a)] = [(a + b, a + b)]$, e si vede subito che $(a + b, a + b) \sim (0, 0)$. □

**Teorema 3.7.** *$(\mathbb{Z}, +, \cdot)$ è un anello commutativo con unità.*

*Dimostrazione.* Abbiamo verificato che $+$ è un'operazione commutativa ed associativa dotata di elemento neutro $[(0,0)]$ rispetto alla quale ogni elemento possiede un inverso, pertanto $(\mathbb{Z},+)$ è un gruppo abeliano.

Inoltre l'operazione di moltiplicazione $\cdot$ è commutativa ed associativa, distribuisce rispetto alla somma e possiede l'elemento neutro $[(1,0)]$. □

Nell'uso comune di $\mathbb{Z}$ utilizzeremo una notazione diversa da quella finora sfruttata per indicare le classi di equivalenza: abbiamo già visto come $[(a,a)] = [(0,0)]$ sia l'elemento neutro rispetto alla somma. Se $a \neq b$, allora esattamente una tra $a < b$ e $b < a$ sarà valida. Nel primo caso $(a,b) \sim (0, b-a)$, mentre nel secondo $(a,b) \sim (a-b, 0)$. Pertanto oltre a $[(0,0)]$, gli elementi di $\mathbb{Z}$ sono solo del tipo $[(a,0)]$ oppure $[(0,a)]$, con $a \neq 0$.

**Lemma 3.8.** *Si hanno $(a,0) \sim (b,0)$ e $(0,a) \sim (0,b)$ se e solo se $a = b$. Inoltre $(a,0) \sim (0,b)$ se e solo se $a = b = 0$.*

*Dimostrazione.* Immediata. □

Possiamo quindi concludere che gli elementi $[(0,0)]$ e $[(a,0)], [(0,a)], a \neq 0$ sono tutti distrinti in $\mathbb{Z}$, e che ogni elemento di $\mathbb{Z}$ è di tale tipo. La notazione che utilizzeremo[2] per tali elementi è: $\underline{0} = [(0,0)], \underline{a} = [(a,0)], \underline{-a} = [(0,a)]$. Il numero naturale $a$ è detto *valore assoluto* sia dell'elemento $[(a,0)]$ che dell'elemento $[(0,a)]$. Il valore assoluto di $x \in \mathbb{Z}$ si indica con $|x|$.

**Proposizione 3.9.** *$\underline{0}$ e $\underline{1}$ sono gli elementi neutri rispetto alla somma e al prodotto di $\mathbb{Z}$. Inoltre se $a, b \in \mathbb{N}$, si ha:*

- $\underline{a} + \underline{b} = \underline{a+b}$, $\underline{-a} + \underline{-b} = \underline{-(a+b)}$.
- $\underline{a} + \underline{-b} = \begin{cases} \underline{a-b} & \text{se } b \leq a \\ \underline{-(b-a)} & \text{se } a < b. \end{cases}$
- $\underline{a} \cdot \underline{b} = \underline{ab}$, $\underline{a} \cdot \underline{-b} = \underline{-(ab)}$, $\underline{-a} \cdot \underline{-b} = \underline{ab}$.

E' importante osservare come gli elementi $\underline{a}$, con $a \in \mathbb{N}$, si sommmino e si moltiplichino esattamente come i corrispondenti elementi di $\mathbb{N}$. Possiamo considerare quindi $\mathbb{Z}$ come un'*ampliamento* dell'insieme dei numeri naturali ad un insieme con una struttura di anello. Si osservi come $|xy| = |x||y|$.

**Corollario 3.10.** *Siano $x, y \in \mathbb{Z}$. Se $xy = 0$, allora $x = \underline{0}$ oppure $y = \underline{0}$.*

*Dimostrazione.* Segue da (1.6), sfruttando le regole di moltiplicazione della proposizione precedente, oppure utilizzando la moltiplicatività del valore assoluto, notando che $|x| = 0 \Rightarrow x = 0$. □

Possiamo finalmente concludere:

**Teorema 3.11.** *L'anello $(\mathbb{Z},+,\cdot)$ è un dominio di integrità.*

3.4. **Struttura d'ordine su $\mathbb{Z}$.** Una delle strutture intrinseche dell'insieme dei numeri naturali era data dalla relazione d'ordine. Si può estendere anch'essa all'anello $\mathbb{Z}$.

**Definizione 3.12.** $[(a,b)] \leq [(c,d)] \Leftrightarrow a + d \leq b + c$

**Proposizione 3.13.** *$\leq$ è una relazione d'ordine totale su $\mathbb{Z}$.*

*Dimostrazione.* La relazione $\leq$ è riflessiva: in effetti $a+b \leq b+a$. E' inoltre antisimmetrica: da $[(a,b)] \leq [(c,d)]$, $[(c,d)] \leq [(a,b)]$ seguono $a + d \leq b + c$ e $b + c \leq a + d$. Ma allora per antisimmetria di $\leq$ su $\mathbb{N}$ si ottiene $a + d = b + c$, cioè $[(a,b)] = [(c,d)]$.

Infine, è transitiva: da $a+d \leq b+c$ e $c+f \leq d+e$ si ottiene, sommando membro a membro, $a+d+c+f \leq b+c+d+e$, da cui cancellando $c+d$ si ha $a+f \leq b+e$, cioè $[(a,b)] \leq [(e,f)]$. Tale relazione d'ordine è totale, in quando è definita per mezzo della relazione di ordine totale già definita su $\mathbb{N}$. □

**Proposizione 3.14.** *Siano $a, b$ elementi di $\mathbb{N}$. Allora:*

- *$\underline{a} \leq \underline{b}$ se e solo se $a \leq b$,*
- *$\underline{-a} \leq \underline{b}$ per ogni $a, b$,*
- *$\underline{-a} \leq \underline{-b}$ se e solo se $b \leq a$.*

*Osservazione* 3.15. $\leq$ è di ordine totale su $\mathbb{Z}$, ma non è un buon ordinamento, infatti $\mathbb{Z}$ non ammette elemento minimo. Si osservi anche come la relazione d'ordine $\leq$ sugli elementi del tipo $\underline{a}$, con $a \in \mathbb{N}$, coincida con la relazione d'ordine definita sui corrispondenti elementi di $\mathbb{N}$. Con l'identificazione precedentemente data di $\mathbb{N}$ con un sottoinsieme di $\mathbb{Z}$, la relazione definita su $\mathbb{Z}$ estende allora quella già costruita su $\mathbb{N}$.

**Esercizi.**

(1) Sia $X \subset \mathbb{Z}$ un sottoinsieme non vuoto *limitato dal basso*, che possiede cioè un elemento $n \in \mathbb{Z}$ tale che $n \leq x$ per ogni $x \in X$. Mostrate che $X$ possiede un elemento minimo. *[Sugg.: osservate che un traslato di $X$ è completamente contenuto in $\mathbb{N}$]*

(2) Mostrate che se $a, b \in \mathbb{Z}$ soddisfano $ab = 1$, allora $a = b = 1$ oppure $a = b = -1$. In altre parole i soli due elementi invertibili di $\mathbb{Z}$ sono $\pm 1$.

[2] Stiamo momentaneamente sottolineando gli elementi per distinguerli dai corrispondenti elementi di $\mathbb{N}$, ma in generale eviteremo questo segno grafico, quando non ci siano rischi di confusione.

(3) Mostrate che $\leq$ definisce una struttura di anello ordinato su $\mathbb{Z}$.
(4) Sia $\preceq$ una relazione d'ordine che definisca una struttura di anello ordinato su $\mathbb{Z}$. Mostrare che $a \geq 0 \Rightarrow a \succeq 0$. Concludere che le relazioni $\preceq$ e $\leq$ coincidono, cioè che $\mathbb{Z}$ possiede un'unica struttura di anello ordinato.

## 4. Divisione euclidea e teorema fondamentale dell'aritmetica

4.1. **Divisione euclidea in $\mathbb{N}$ e in $\mathbb{Z}$.** Ricordiamo che $\mathbb{Z}$ è un dominio d'integrità dotato di una struttura di anello ordinato. Gli elementi $\geq 0$ sono chiusi rispetto alle operazioni e costituiscono una copia dell'insieme dei numeri naturali. Gli unici elementi invertibili di $\mathbb{Z}$ sono $1$ e $-1$.

Una struttura importante dell'anello dei numeri interi è l'esistenza della cosiddetta divisione euclidea. La dimostriamo prima per i numeri naturali, ed immediatamente dopo per tutti i numeri interi.

**Proposizione 4.1.** *Siano $a, b \in \mathbb{N}$, $b \neq 0$. Allora esistono $q, r \in \mathbb{N}$ tali che $a = qb + r$, con $0 \leq r < b$.*

*Dimostrazione.* Sia $X = \{n \in \mathbb{N} \mid nb > a\}$. L'insieme $X$ contiene $a + 1$ ed è pertanto non vuoto. In effetti $b \neq 0$ e quindi $b \geq 1$. Di conseguenza $ab \geq a$. Ma allora $(a+1)b = ab + b \geq a + b > a$. Inoltre $0$ non appartiene all'insieme $X$, in quando $0 \cdot b = 0 \not> a$.

Per la proprietà di buon ordinamento dei numeri naturali, $X$ possiede un elemento minimo (diverso da $0$) che possiamo indicare con $q + 1$. In altre parole $q \notin X, q + 1 \in X$. Questo significa che $(q+1)b > a$, ma $qb \not> a$, cioè $qb \leq a$; riassumendo: $qb \leq a < (q+1)b = qb + b$.

Sottraendo da tutti e tre i membri la quantità $qb$ si ottiene $0 \leq a - qb < b$. Se indichiamo $r = a - qb$, abbiamo $a = qb + r$, con $0 \leq r < b$. □

**Teorema 4.2.** *Siano $a, b \in \mathbb{Z}$, $b \neq 0$. Allora esistono $q, r \in \mathbb{Z}$ tali che $a = qb + r, 0 \leq r < |b|$.*

*Dimostrazione.* Intanto, è sufficiente dimostrare l'enunciato quando $b > 0$. In effetti, se $a = qb + r$, allora chiaramente $a = (-q)(-b) + r$.

Se anche $a \geq 0$, basta invocare la proposizione precedente. Se invece $a < 0$, allora $-a > 0$ e quindi $-a = qb + r$, da cui $a = -qb - r = (-q)b - r$. Se $r = 0$, abbiamo concluso. Se invece $0 < r < b$, allora $-qb - r = -qb - b + b - r = (-q - 1)b + (b - r)$ e $r' = b - r$ soddisfa $0 < r' < b$. □

*Osservazione* 4.3. Gli elementi $q, r$ che compaiono nell'enunciato del teorema precedente sono univocamente determinati da $a$ e $b$, anche se non avremo mai bisogno di tale fatto.

4.2. **Divisibilità e massimo comun divisore.**

**Definizione 4.4.** Siano $a, b \in \mathbb{Z}$. Si dice che $a$ *divide* $b$, e si scrive $a|b$, quando esiste $q \in \mathbb{Z}$ tale che $b = qa$.

Se $a|b$, si dice equivalentemente che $b$ è un multiplo di $a$. La relazione di divisibilità gode di alcune ovvie proprietà:

**Proposizione 4.5.** *Valgono le seguenti proprietà:*

(1) $a|a$ *per ogni* $a \in \mathbb{Z}$; *(riflessività)*
(2) *se* $a|b$ *e* $b|c$ *allora* $a|c$; *(transitività)*
(3) *se* $a|b$ *allora* $a|bc$ *per ogni* $c \in \mathbb{Z}$;
(4) *se* $a|b$ *e* $a|c$, *allora* $a|\, b + c$;
(5) *se* $a|b$ *e* $b|a$ *allora* $a = \pm b$; *(anti-simmetria a meno di invertibili)*
(6) $a|0$ *per ogni* $a \in \mathbb{Z}$;
(7) $0|a \Rightarrow a = 0$;
(8) $1|a$ *per ogni* $a \in \mathbb{Z}$;
(9) $a|1$ *se e solo se* $a$ *è invertibile in* $\mathbb{Z}$.

*Dimostrazione.* Tutte le dimostrazioni sono molto semplici. Un cenno per ognuna: (1) $a = 1 \cdot a$; (2) $b = qa, c = rb \Rightarrow c = (qr)a$; (3) è una riformulazione di (2); (4) $b = qa, c = ra \Rightarrow b + c = (q + r)a$; (5) $b = qa, a = rb \Rightarrow a = (qr)a$. Se $a = 0$, allora anche $b = 0$. Se $a \neq 0$, allora $qr = 1$; (6) $0 = 0 \cdot a$; (7) $q \cdot 0 = 0$; (8) $a = a \cdot 1$; (9) $a|1$ se e solo se esiste $x \in \mathbb{Z}$ tale che $ax = 1$. □

*Osservazione* 4.6. Una conseguenza immediata della proposizione precedente è che se $d$ divide sia $a$ che $b$ divide ogni numero intero della forma $ha + kb$, $h, k \in \mathbb{Z}$. Un'altro aspetto da sottolineare è che la relazione di divisibilità, sull'insieme $\mathbb{N}$, è riflessiva antisimmetrica e transitiva, ed è quindi una relazione d'ordine.

Una delle strutture algebriche fondamentali dell'anello dei numeri interi è l'esistenza del massimo comun divisore. In generale si è soliti definire massimo comun divisore di due interi il più grande divisore comune. Questo ha lo svantaggio di non permettere la definizione del massimo comun divisore di $0$ e $0$. In effetti, tutti gli interi dividono $0$, e non esiste un massimo elemento di $\mathbb{Z}$. La definizione che segue ha il vantaggio di fornire un massimo comun divisore (uguale a $0$) anche per la coppia $(0, 0)$. Ha purtroppo la fastidiosa controindicazione di non garantire l'esistenza, e nemmeno l'unicità, del massimo comun divisore.

**Definizione 4.7.** Siano $a, b \in \mathbb{Z}$. Un elemento $d \in \mathbb{Z}$ si dice *massimo comun divisore* di $a$ e $b$ se $d|a, d|b$ ed ogni elemento $e \in \mathbb{Z}$ che soddisfa $e|a, e|b$ soddisfa anche $e|d$.

*Osservazione* 4.8. Se $d$ e $d'$ sono entrambi massimi comuni divisori di $a$ e $b$, allora vale sia $d|d'$ che $d'|d$. Abbiamo visto come questo accada soltanto quando $d = \pm d'$. Pertanto il massimo comun divisore in $\mathbb{Z}$ è unico a meno di un segno. Se $d$ è un massimo comun divisore di $a$ e $b$, scriveremo impropriamente $MCD(a, b) = d$.

Ad esempio $MCD(26, -39) = 13$ significherà che esistono massimi comuni divisori di 26 e $-39$, e che 13 è uno di essi: in particolare che $\pm 13$ sono gli unici massimi comuni divisori di 26 e $-39$. In pratica, quando avremo bisogno di indicare il massimo comun divisore di due numeri, utilizzeremo sempre il valore non negativo tra i due disponibili.

Utilizzeremo in seguito anche la notazione più compatta $(a, b)$ al posto di $MCD(a, b)$. Dalla definizione segue immediatamente che $MCD(a, b) = MCD(b, a)$[3] per ogni scelta di $a, b \in \mathbb{Z}$.

**Lemma 4.9.** *Il massimo comun divisore soddisfa le seguenti proprietà:*

(1) $MCD(0, 0) = 0$;
(2) $MCD(a, 0) = a$ *per ogni* $a \in \mathbb{Z}$;
(3) *Siano* $a, b, q, r \in \mathbb{Z}$ *tali che* $a = bq + r$. *Allora, se esiste* $MCD(b, r)$ *esiste anche* $MCD(a, b)$ *e si ha* $MCD(a, b) = MCD(b, r)$.

*Dimostrazione.* (1) ovvio, poiché ogni intero divide 0, e 0 è l'unico intero con la proprietà di essere diviso da tutti gli altri.
(2) i divisori comuni di $a$ e 0 sono esattamente quelli di $a$. Tra tali elementi, $\pm a$ sono quelli con la proprietà di essere divisibili tra tutti gli altri.
(3) Se $d$ divide sia $a$ che $b$, allora divide anche $qb$, ed anche $a - qb = r$, quindi ogni divisore comune di $a$ e $b$ è anche un divisore comune di $b$ ed $r$. Viceversa, se $d$ divide sia $b$ che $r$, allora divide anche $qb$ e la somma $qb + r = a$. Pertanto ogni divisore comune di $b$ ed $r$ è anche un divisore comune di $a$ e $b$. Questo mostra che se tra i divisori comuni di $b$ ed $r$ esiste un elemento che è diviso da tutti gli altri, lo stesso è vero per $a$ e $b$, e tale elemento è lo stesso (a meno del segno). □

Il lemma appena dimostrato suggerisce una possibile strategia per trovare il massimo comun divisore di due numeri interi $a, b$. Eseguire la divisione euclidea $a = bq + r$ e sostituire la coppia $(a, b)$ con quella $(b, r)$. Questo ha il vantaggio di rendere il secondo elemento della coppia più piccolo (in valore assoluto) di quello della coppia precedente: infatti $0 \leq r < |b|$. Reiterando questa procedura al più $|b|$ passi, otterremo una coppia del tipo $(n, 0)$ che possiede certamente un massimo comun divisore, la cui determinazione è immediata. Ad esempio, per individuare il massimo comun divisore di 1001 e 273 si può effettuare la divisione euclidea tra 1001 e 273 ottenendo

$$1001 = 3 \cdot 273 + 182 \Rightarrow MCD(1001, 273) = MCD(273, 182).$$

Possiamo quindi continuare:

$$273 = 1 \cdot 182 + 91, \qquad 182 = 2 \cdot 91 + 0,$$

per ottenere $MCD(1001, 273) = MCD(273, 182) = MCD(182, 91) = MCD(91, 0) = 91$. In effetti, $1001 = 7 \cdot 11 \cdot 13$, mentre $273 = 3 \cdot 7 \cdot 13$, per cui il loro massimo comun divisore[4] è $7 \cdot 13 = 91$.

Questa procedura può essere percorsa alla rovescia per ottenere la cosiddetta *identità di Bézout*, che esprime il massimo comun divisore di due numeri come somma di loro multipli: vediamo come.
Sappiamo che $(1001, 273) = 91$. In effetti da $273 = 1 \cdot 182 + 91$ segue $91 = 1 \cdot 273 - 1 \cdot 182$. La divisione euclidea precedente $1001 = 3 \cdot 273 + 182$ permette di ricavare $182 = 1 \cdot 1001 - 3 \cdot 273$. Sostituendo, si ottiene

$$91 = 1 \cdot 273 - 1 \cdot 182 = 1 \cdot 273 - 1 \cdot (1 \cdot 1001 - 3 \cdot 273) = -1 \cdot 1001 + 4 \cdot 273.$$

**Teorema 4.10.** $MCD(a, b)$ *esiste per ogni scelta di* $a, b \in \mathbb{Z}$. *Inoltre, se* $d = MCD(a, b)$, *allora esistono* $h, k \in \mathbb{Z}$ *tali che* $d = ha + kb$.

*Dimostrazione.* L'esistenza di $MCD(a, b)$ si dimostra per induzione (forte) su $|b|$.
La base dell'induzione è chiara, in quanto se $|b| = 0$, allora $b = 0$, e sappiamo che $MCD(a, 0)$ esiste ed è uguale ad $a$. Il passo induttivo è stato descritto sopra: se $b \neq 0$, la divisione euclidea ci garantisce l'esistenza di $q, r \in \mathbb{Z}$ tali che $a = qb + r$, $0 \leq r < |b|$. Per ipotesi induttiva, esiste $MCD(b, r)$; ma per il lemma precedente, esiste allora anche $MCD(a, b)$ e coincide con $MCD(b, r)$.

Per quanto riguarda l'identità di Bézout, fornisco varie dimostrazioni diverse, tutte istruttive. La prima, anche se non sembra, è quella data a lezione risalendo l'algoritmo euclideo.

- Per induzione su $|b|$. Se $|b| = 0$, non c'è nulla da dimostrare: $MCD(a, 0) = a$, ed effettivamente $a = 1 \cdot a + 0 \cdot b$. Il passo induttivo è facile: se $b \neq 0$ possiamo trovare $q, r \in \mathbb{Z}$ tali che $a = qb + r, 0 \leq r < |b|$. Ma allora $MCD(a, b) = MCD(b, r)$. Per ipotesi induttiva, se $d = MCD(b, r)$, possiamo trovare $h, k \in \mathbb{Z}$ tali che $d = hb + kr$. Sostituendo $r = a - qb$ si ottiene $d = hb + k(a - qb) = ka + (h - qk)b$.
- Consideriamo l'insieme $X = \{ha + kb | h, k \in \mathbb{Z}\}$. $X$ contiene $a = 1 \cdot a + 0 \cdot b$ e $b = 0 \cdot a + 1 \cdot b$, nonché $0 = 0 \cdot a + 0 \cdot b$. Inoltre soddisfa: $x \in X \Rightarrow -x \in X; x, y \in X \Rightarrow x + y \in X; x \in X, h \in \mathbb{Z} \Rightarrow hx \in X$. Con un linguaggio che sarà introdotto solo in seguito, $X$ è un *ideale* dell'anello $\mathbb{Z}$. Basta ora osservare che eseguendo la divisione euclidea su due elementi $x, y$ di $X$, anche il resto appartiene ad $X$: se $x = qy + r$, allora $r = x + (-q)y$; da $y \in X$ segue $(-q)y \in X$, e poiché anche $x \in X$, allora $r = x + (-q)y \in X$. Reiterando le divisioni euclidee a partire da $a, b \in X$, tutti i resti che si ottengono appartengono ad $X$, e quindi anche l'ultimo resto non nullo, che è il massimo comun divisore di $a$ e $b$.

[3] cioè che ogni massimo comun divisore di $a$ e $b$ è anche un massimo comun divisore di $b$ e $a$
[4] calcolato con l'usuale procedimento di fattorizzazione che **presume** la fattorizzazione unica

- Come sopra, si dimostra che $X$ è un ideale di $\mathbb{Z}$. Se $d$ è il suo minimo elemento positivo, allora ogni altro elemento di $X$ è multiplo di $d$. Infatti, eseguendo la divisione euclidea tra $x \in X$ e $d$ si ottiene $x = qd + r$, con $0 \leq r < d$, ed $r \in X$ come abbiamo già mostrato sopra. Se $r \neq 0$ si ottiene un assurdo, quindi $d$ divide ogni elemento di $X$.
  Tra gli elementi di $X$ ci sono anche $a$ e $b$, quindi $d$ è un divisore comune di $a$ e $b$. Inoltre, $d$ è automaticamente della forma $ha + kb$, quindi se $e$ divide sia $a$ che $b$, deve dividere anche $ha + kb = d$. In altre parole, $d$ è un massimo comun divisore tra $a$ e $b$.

□

Quest'ultima dimostrazione utilizza un fatto che ha la sua indipendente utilità.

**Proposizione 4.11.** *Se $d$ è un divisore di $a$ e $b$ della forma $d = ha + kb$, con $h, k \in \mathbb{Z}$, allora $d = MCD(a, b)$.*

*Dimostrazione.* Se $e$ è un divisore comune di $a$ e $b$, deve dividere anche $ha$, $kb$ e la loro somma $d = ha + kb$. □

**Corollario 4.12.** *Siano $a, b, c \in \mathbb{Z}$:*

(1) *se è possibile esprimere $1$ nella forma $ha + kb$ con $h, k \in \mathbb{Z}$, allora $MCD(a, b) = 1$;*
(2) *$MCD(ab, ac) = a \cdot MCD(b, c)$;*
(3) *se $d = MCD(a, b)$, allora $MCD(a/d, b/d) = 1$.*

*Dimostrazione.* (1) segue direttamente dalla proposizione precedente.
(2): se $d = MCD(b, c)$, allora $d = hb + kc$, ma allora $ad = h \cdot ab + k \cdot ac$. Inoltre, se $d$ divide sia $b$ che $c$, $ad$ divide chiaramente sia $ab$ che $ac$. A questo punto basta applicare la proposizione precedente.
(3) è una riformulazione di (2). □

Quando $MCD(a, b) = 1$, gli interi $a$ e $b$ si dicono *primi tra loro* o *relativamente primi* o *coprimi*. L'ultima delle affermazioni sostiene che dividendo due numeri per il loro massimo comun divisore si ottengono due risultati primi tra loro. Da questo momento in poi utilizzeremo la notazione semplificata $(a, b)$ in luogo di $MCD(a, b)$ ogni volta che non siano possibili fraintendimenti. Due numeri $a$ e $b$ saranno quindi primi tra loro se e solo se $(a, b) = 1$.

4.3. **Elementi invertibili, primi e irriducibili in $\mathbb{N}$ e in $\mathbb{Z}$.** Per poter enunciare e dimostrare il teorema di fattorizzazione unica, abbiamo bisogno di un po' di terminologia

**Definizione 4.13.**

- $a \in \mathbb{Z}$ si dice *invertibile* se $a|1$;
- $0 \neq p \in \mathbb{Z}$ non invertibile si dice *primo* se quando $p|ab$, allora $p$ divide almeno uno tra $a$ e $b$;
- $0 \neq p \in \mathbb{Z}$ non invertibile si dice *irriducibile* se quando $p = ab$, allora uno tra $a$ e $b$ è invertibile.

*Osservazioni* 4.14.

(1) Abbiamo già visto come l'unico elemento invertibile di $\mathbb{N}$ sia $1$, e vi siano esattamente due elementi invertibili in $\mathbb{Z}$: $\pm 1$.
(2) Se $p = ab$ è irriducibile, allora esattamente uno tra $a$ e $b$ è invertibile. Se fossero entrambi invertibili, infatti, anche il loro prodotto sarebbe invertibile, e questo è escluso dalla definizione.
(3) Se $p$ è irriducibile e $x$ è invertibile, allora anche $px$ è irriducibile. In effetti, se $px = ab$, allora $p = abx^{-1} = a(bx^{-1})$. Quindi $a$ è invertibile, oppure $bx^{-1}$ è invertibile, e di conseguenza $b = (bx^{-1})x$ è invertibile perché prodotto di invertibili.
(4) Se $p \in \mathbb{Z}$ non è invertibile, $q \in \mathbb{Z}$ è irriducibile e $p|q$, allora $q = px$. Di conseguenza, $x$ è invertibile e $p = qx^{-1}$ è anch'esso irriducibile. In particolare, se $p, q$ sono entrambi irriducibili, e $p|q$, allora $p = \pm q$.
(5) Se $p \in \mathbb{Z}$ è irriducibile, gli unici divisori di $p$ sono $\pm 1, \pm p$ e sono tutti e quattro distinti. Se $p \in \mathbb{N}$ è irriducibile, gli unici divisori naturali di $p$ sono $1$ e $p$, e sono distinti.

Mi aspetto che vi sia sempre stato detto che un numero naturale $p$ è primo se i suoi unici divisori naturali sono $1$ e $p$. Questa è la definizione che diamo – dopo aver richiesto che $p$ non sia invertibile – per gli interi *irriducibili*, non per quelli primi. In realtà i concetti di elemento primo ed irriducibile coincidono in $\mathbb{Z}$, e quindi anche in $\mathbb{N}$. Dimostrare questo fatto è il nostro prossimo obiettivo.

**Lemma 4.15.** *Se $a, b, c \in \mathbb{Z}$ soddisfano $a|bc$ e $(a, b) = 1$, allora $a|c$.*

*Dimostrazione.* Se $(a, b) = 1$, per l'identità di Bézout abbiamo $1 = ha + kb$ per un'opportuna scelta di $h, k \in \mathbb{Z}$. Ma allora $c = 1 \cdot c = hac + kbc$. Sia $hac$ che $kbc$ sono chiaramente multipli di $a$ – il primo lo è esplicitamente, il secondo in quanto multiplo di $bc$ – e quindi anche la loro somma è divisa da $a$. □

*Osservazione* 4.16. Senza l'ipotesi $(a, b) = 1$, l'enunciato è evidentemente falso. Ad esempio, $4|2 \cdot 6$, ma né $2$, né $6$ sono multipli di $4$.

**Proposizione 4.17.** *Un elemento $p \in \mathbb{Z}$ è primo se e solo se è irriducibile.*

*Dimostrazione.* Se $p$ è invertibile o uguale a $0$, non è né primo né irriducibile, quindi possiamo limitarci al caso di elementi non invertibili diversi da $0$.
$p$ primo $\Rightarrow$ $p$ irriducibile: se $p = ab$, allora $p$ divide $ab$. Essendo $p$ primo, possiamo supporre (a meno di scambiare $a$ e $b$) che $p$ divida $a$. Allora $a = px$ e $p = ab = pbx$. Ma allora $bx = 1$, e quindi $b$ è invertibile. Quindi le uniche fattorizzazioni di $p$ hanno un fattore invertibile, e $p$ è irriducibile.

$p$ irriducibile $\Rightarrow$ $p$ primo: se $p|ab$, dobbiamo mostrare che $p$ divide $a$ oppure $b$. Il massimo comun divisore $(a,p)$ è un divisore di $p$. Essendo $p$ irriducibile, ci sono le sole due possibilità $(a,p)=p$ oppure $(a,p)=1$. Se $(a,p)=p$, allora $p|a$; se invece $(a,p)=1$, applicando il Lemma 4.15 si ottiene $p|b$. In conclusione, $p$ è primo. □

Gli elementi primi di $\mathbb{N}$ sono detti anche *numeri primi*.

4.4. **Fattorizzazione unica in $\mathbb{N}$ e in $\mathbb{Z}$.** E' più semplice enunciare il teorema di fattorizzazione unica in $\mathbb{N}$ che in $\mathbb{Z}$. Il teorema di fattorizzazione unica in $\mathbb{N}$, meglio noto come *Teorema fondamentale dell'aritmetica* sostiene che ogni numero naturale (diverso da zero) si scrive in modo unico come prodotto di numeri primi. L'unicità della fattorizzazione consiste nel fatto che in due fattorizzazioni dello stesso numero compaiono gli stessi numeri primi, e ciascuno di essi compare lo stesso numero di volte.

L'enunciato si compone di due affermazioni: una sull'esistenza della fattorizzazione e l'altra sulla sua unicità, che dimostriamo separatamente.

**Teorema 4.18.** *Ogni $0 \neq N \in \mathbb{N}$ può essere espresso come prodotto di numeri primi.*

*Dimostrazione.* Per induzione (forte) su $N$.
La base dell'induzione $N=1$ è banale, in quanto 1 è prodotto di zero numeri primi – è il prodotto vuoto. Per quanto riguarda il passo induttivo, sia $N>1$. Se $N$ è primo, allora costituisce la propria fattorizzazione nel prodotto di un solo primo. Se invece $N$ non è primo, allora non è irriducibile, e quindi $N=ab$, con $a,b$ non invertibili. Di conseguenza, $a,b<N$. Ma allora, per ipotesi induttiva, sia $a$ che $b$ sono prodotto di numeri primi. Moltiplicando tali espressioni tra loro, si esprime $N$ come prodotto di numeri primi. □

Passiamo ora all'unicità.

**Teorema 4.19.** *Se $0 \neq N \in \mathbb{N}$ ammette le due fattorizzazioni in primi*

$$\begin{aligned} N &= p_1^{m_1} p_2^{m_2} \dots p_h^{m_h} \\ &= q_1^{n_1} q_2^{n_k} \dots q_k^{n_k}, \end{aligned}$$

*dove i $p_i$ sono numeri primi tali che $p_1 < p_2 < \dots < p_h$, i $q_j$ sono numeri primi tali che $q_1 < q_2 < \dots < q_k$, e gli esponenti $m_i, n_j$ sono tutti maggiori di 0, allora $h=k$, e $p_i = q_i, m_i = n_i$ per ogni $i = 1, \dots, h$.*

*Dimostrazione.* Per induzione su $N$. Se $N=1$ non c'è nulla da dimostrare, perché ogni divisore di 1 è invertibile, e quindi nessun primo può dividere 1. L'unica fattorizzazione in primi di 1 è quella vuota.
Sia $N>1$. Se $p_1 \neq q_1$, possiamo supporre che $p_1 < q_1$, a meno di scambiare le due fattorizzazioni. Dal momento che $p_1$ divide $N$, deve dividere almeno uno dei fattori della seconda fattorizzazione. Se $p_1|q_i$, allora $p_1 = q_i$ poiché sono entrambi irriducibili. Ma allora $p_1 < q_1 \leq q_i = p_1$, un assurdo. Quindi $p_1 = q_1$.
Se $m_1 \neq n_1$, possiamo supporre che $m_1 < n_1$, a meno di scambiare le due fattorizzazioni. Ma allora $N/p_1^{m_1}$ possiede le due fattorizzazioni

$$\begin{aligned} N/p_1^{m_1} &= p_2^{m_2} \dots p_h^{m_h} \\ &= p_1^{n_1 - m_1} q_2^{n_k} \dots q_k^{n_k}, \end{aligned}$$

con $n_1 - m_1 > 0$. Applicando l'ipotesi induttiva a $N/p_1^{m_1} < N$ ottieniamo un assurdo, poiché il primo $p_1$ compare nella seconda fattorizzazione ma non nella prima. Quindi $m_1 = n_1$. Ripetendo il ragionamento già fatto, abbiamo allora le due fattorizzazioni

$$\begin{aligned} N/p_1^{m_1} &= p_2^{m_2} \dots p_h^{m_h} \\ &= q_2^{n_k} \dots q_k^{n_k}. \end{aligned}$$

Per l'ipotesi induttiva applicata ad $N/p_1^{m_1} < N$ abbiamo che $h-1 = k-1 \Rightarrow h=k$; inoltre $p_2 = q_2, \dots, p_h = q_h$ e $m_2 = n_2, \dots, m_h = n_h$. D'altronde, sappiamo già che $p_1 = q_1, m_1 = n_1$, ed il teorema è dimostrato. □

**Teorema 4.20.** *Ogni $0 \neq N \in \mathbb{Z}$ si scrive come prodotto di un invertibile e di elementi primi di $\mathbb{Z}$. Tale fattorizzazione in primi è unica nel senso che comunque prese due fattorizzazioni di $N$, i primi che compaiono nella prima sono tutti e soli – a meno del segno – quelli che compaiono nella seconda; inoltre il numero di volte che i primi $\pm p$ compaiono (in totale) in una delle due fattorizzazioni è uguale al numero di volte che compaiono nell'altra.*

*Dimostrazione.* A meno di sostituire ogni primo nella fattorizzazione di $N$ col suo valore assoluto, il problema si riduce alla fattorizzazione unica di $|N|$ in $\mathbb{N}$. □

**Esercizi.**

(1) Calcolare con l'algoritmo euclideo il massimo comun divisore tra 233 e 144, e ricavare la corrispondente identità di Bézout.
(2) Stimare in funzione di $a$ e $b$ il numero di divisioni euclidee necessarie a calcolare il massimo comun divisore tra $a$ e $b$.
(3) Mostrare che il minimo comune multiplo di $a,b \in \mathbb{N}$ è uguale ad $ab/(a,b)$.

DIPARTIMENTO DI MATEMATICA, UNIVERSITÀ DEGLI STUDI DI ROMA – "LA SAPIENZA"
*E-mail address*: dandrea@mat.uniroma1.it