Matematica di Base

Giovanna Carnovale

November 25, 2003

1 I numeri naturali

L'insieme dei numeri naturali, che denoteremo con $\mathbb{N}$, è, intuitivamente, l'insieme degli elementi 0, 1, 2, ... Sull'insieme $\mathbb{N}$ abbiamo la relazione $\leq$ con $0 \leq 1 \leq 2 \leq 3 \cdots$. Scriveremo $x < y$ se $x \leq y$ e $x \neq y$. L'insieme $\mathbb{N}$ è totalmente ordinato rispetto a $\leq$. Infatti $\leq$ è una relazione riflessiva, transitiva, antisimmetrica, e vale la tricotomia ovvero: per ogni x, $y \in \mathbb{N}$ allora si verifica una ed una sola delle tre possibilità:

$$x < y; \quad x = y; \quad x > y.$$

Dato un sottoinsieme S di $\mathbb{N}$ diremo che m è un elemento di minimo per S se $m \in S$ e $m \leq x$, per ogni $x \in S$. Denoteremo tale elemento con $\min S$. Un'importante proprietà di $\mathbb{N}$ è *il buon ordinamento*: *ogni sottoinsieme non vuoto S di $\mathbb{N}$ possiede un elemento minimo.*

Sull'insieme dei numeri naturali possiamo effettuare le operazioni di somma e di prodotto nel modo noto. La costruzione dell'insieme $\mathbb{N}$, del suo ordinamento e delle sue operazioni, può essere data in modo costruttivo (vedi note di Silvio Valentini). Le operazioni di somma e prodotto godono delle seguenti proprietà:

1. $a + b = b + a$ per ogni a, $b \in \mathbb{N}$ (proprietà commutativa della somma);
2. $(a + b) + c = a + (b + c)$ per ogni a, b, $c \in \mathbb{N}$ (proprietà associativa della somma);
3. $0 + a = a$ per ogni $a \in \mathbb{N}$ (esistenza dell'elemento neutro per la somma);
4. $(ab)c = a(bc)$ per ogni a, b, $c \in \mathbb{N}$ (proprietà associativa del prodotto);
5. $a(b+c) = ab+ac$ per ogni a, b, $c \in \mathbb{N}$ (proprietà distributiva del prodotto rispetto alla somma);
6. $1a = a$ per ogni $a \in \mathbb{N}$ (esistenza dell'elemento neutro per il prodotto);
7. $ab = ba$ per ogni a, $b \in \mathbb{N}$ (proprietà commutativa del prodotto);
8. dati a, $b \in \mathbb{N}$, se $ab = 0$ allora $a = 0$ e/o $b = 0$.
9. dato a, $b \in \mathbb{N}$, se $ab = 1$ allora $a = b = 1$.

10. per ogni $a, b \in \mathbb{N}$, $a \geq b$ se e solo se $a + c \geq b + c$ per ogni $c \in \mathbb{N}$ (compatibilità dell'ordine con la somma);

11. per ogni $a, b \in \mathbb{N}$, $a > b$ se e solo se $ac > bc$ per ogni $c \in \mathbb{N} \setminus \{0\}$ (compatibilità dell'ordine con il prodotto).

1.1 Divisibilità e massimo comun divisore

1.1.1 Divisibilità in $\mathbb{N}$

In questa sezione introdurremo il concetto di divisibilità e di massimo comun divisore di due numeri naturali non nulli. Daremo inoltre due algoritmi per calcolare il massimo comun divisore.

Definizione 1.1 *Dati $a, b \in \mathbb{N}$ diremo che a divide b (in formule, $a|b$) se esiste $k \in \mathbb{N}$ tale che $ak = b$.*

Ad esempio, $4|12$ perché esiste 3 tale che $4 \cdot 3 = 12$.

Esercizio 1.2 *Dimostrare che la relazione data da $|$ è una relazione transitiva su $\mathbb{N} \setminus \{0\}$.*

Soluzione: Dobbiamo dimostrare che se $a|b$ e $b|c$ allora $a|c$. Se $a|b$ e $b|c$ allora esistono l, k in $\mathbb{N}$ per i quali $al = b$ e $bk = c$. Allora $a(lk) = (al)k = bk = c$ quindi $a|c$. □

Esercizio 1.3 *Dimostrare che la relazione $|$ è una relazione antisimmetrica su $\mathbb{N} \setminus \{0\}$.*

Soluzione: Dobbiamo dimostrare che se, per $a \neq 0$, $b \neq 0$ si hanno $a|b$ e $b|a$ allora $a = b$. Se $a|b$ e $b|a$ allora esistono l, k in $\mathbb{N}$ per i quali $al = b$ e $bk = a$. Vogliamo allora dimostrare che $l = 1$ e $k = 1$. Dalle uguaglianze ottenute per a e b si ottiene: $a(lk) = (al)k = bk = a$. Quindi $a(lk) - a = 0$ ovvero $a(lk) - a(1) = a(lk - 1) = 0$. Allora, poiché $a \neq 0$, si ha $lk = 1$, ovvero $l = k = 1$. Pertanto $b = al = a \cdot 1 = a$. □

Definizione 1.4 *Un elemento $p \in \mathbb{N}$ è detto un numero primo se soddisfa le seguenti proprietà:*

- $p \neq 1$
- *se $x \in \mathbb{N}$ è tale che $x|p$ allora $x = 1$ oppure $x = p$.*

Si hanno i seguenti risultati:

1. Ogni elemento non nullo di n di $\mathbb{N}$ si può scrivere come prodotto di (potenze di) numeri primi $n = p_1^{e_1} \cdots p_k^{e_k}$. Tale scrittura è unica a meno dell'ordine in cui compaiono i fattori (Teorema fondamentale dell'aritmetica o teorema della fattorizzazione unica).

2. I numeri primi sono infiniti.

Dati m, $n \in \mathbb{N}$, con fattorizzazione

$$m = p_1^{e_1} \cdots p_k^{e_k}, \quad n = q_1^{f_1} \cdots q_s^{f_s}$$

si deduce che $m|n$ se e solo se

- $\{p_1, \ldots, p_k\} \subset \{q_1, \ldots, q_s\}$ e
- $f_j \geq e_i$ se $q_j = p_i$.

Vale a dire: $m|n$ se e solo se

- tutti i divisori primi di m sono anche divisori di n e
- se p compare nella fattorizzazione di m con esponente e, allora p compare nella fattorizzazione di n con esponente $f \geq e$.

1.1.2 Massimo comun divisore

Definizione 1.5 *Dati a, $b \in \mathbb{N}$ non entrambi nulli, l'elemento $d \in \mathbb{N}$ è detto un* massimo comun divisore *di a e b se*

1. *$d|a$ e $d|b$;*
2. *se $z|a$ e $z|b$ per qualche $z \in \mathbb{N}$, allora $z|d$.*

Ad esempio 12 è massimo comun divisore di 252 e 60. Infatti, 12 divide sia 60 che 252, i divisori di $60 = 2^3 \cdot 3 \cdot 5$ sono i numeri della forma $2^a \cdot 3^b \cdot 5^c$ con $a \leq 3$, $b \leq 1$ e $c \leq 1$, i divisori di $252 = 2^2 \cdot 3^2 \cdot 7$ sono i numeri della forma $2^s \cdot 3^t \cdot 7^r$ con $s \leq 2$, $t \leq 2$ ed $r \leq 1$. Quindi gli elementi che dividono sia 60 che 252 sono tutti e soli i numeri della forma $2^x 3^y$ con $x \leq 2$ e $y \leq 1$. Tali numeri sono tutti divisori di $12 = 2^2 \cdot 3$.

Esercizio 1.6 *Dimostrare che dati qualsiasi a, $b \in \mathbb{N}$ non nulli, il loro massimo comun divisore è unico.*

Soluzione: Se avessi d_1 e d_2 massimi comuni divisori, allora avrei $d_1|d_2$ (utilizzo la prima proprietà del massimo comun divisore applicata a d_1 e la seconda aaplicata a d_2) e $d_2|d_1$ (utilizzo la prima proprietà del massimo comun divisore applicata a d_2 e la seconda applicata a d_1). Pertanto $d_1 = d_2$. □

Denoteremo il massimo comun divisore dei due numeri a e b con il simbolo $MCD(a, b)$.

Ispirati dall'esempio appena visto, osserviamo che, $MCD(m, n)$ è il prodotto delle potenze di tutti i primi p che compaiono sia nella scomposizione di m che nella scomposizione di n, con esponente il minimo tra l'esponente di p nella scomposizione di m e l'esponente di p nella scomposizione di n.

Esercizio 1.7 *Calcolare il massimo comun divisore di* 144 *e* 9 *e dimostrare che è un massimo comun divisore.*

Esercizio 1.8 *Calcolare il massimo comun divisore di* 84 *e* 15 *e dimostrare che è un massimo comun divisore.*

Esercizio 1.9 *Siano dati* $a, b \in \mathbb{N}$ *con* $a|b$. *Dimostrare che* $MCD(a, b) = a$.

1.1.3 Divisione con il resto

Abbiamo introdotto il concetto di divisibilità: ora vorremmo vedere cosa si può fare quando due numeri interi non sono uno divisore dell'altro.

Proposizione 1.10 *Dati* $a \neq 0$ *e* b *in* $\mathbb{N}$, *esitono sempre* $q, r \in \mathbb{N}$ *tali che* $0 \leq r < a$ *e* $b = aq + r$.

Dimostrazione: Se $b < a$ allora $b = 0a + b$ quindi possiamo prendere $q = 0$ ed $r = b < a$.
Sia ora $a \leq b$. Consideriamo l'insieme

$$S = \{n \in \mathbb{N} \mid n = b - ak \text{ per qualche } k \in \mathbb{N}\},$$

(Attenzione: non tutti i numeri di questa forma sono in $\mathbb{N}$, noi consideriamo *solo* i numeri nonnegativi di questa forma). Poiché $b \geq a$, $b - 1 \cdot a = b - a \in S$, che quindi non è vuoto. Per il buon ordinamento di $\mathbb{N}$, l'insieme S ammette quindi un elemento minimo m che si potrà scrivere come $m = b - ak$ per un certo k. Se prendiamo $q = k$ e $m = r$, per dimostrare l'enunciato è sufficiente mostrare che $m < a$. Se per assurdo avessimo $m \geq a$, allora $0 \leq m - a < m$ con $m - a \in S$ perché $m - a = b - a(q + 1)$. Ciò è impossibile perché m è l'elemento minimo di S. L'assurdo deriva dall'aver supposto che pertanto $m \geq a$, pertanto l'enunciato è dimostrato. □

I numeri q ed r sono detti *quoziente* e *resto* della divisione.

Esercizio 1.11 *Calcolare quoziente e resto della divisione di* b *per* a *quando:*

1. $b = 17$, $a = 3$;
2. $b = 45$, $a = 3$;
3. $b = 0$, $a = 123$.

1.1.4 L'algoritmo di Euclide

Abbiamo già visto un algoritmo per calcolare il massimo comun divisore di due numeri naturali, tramite fattorizzazione dei due numeri dati. L'algoritmo di scomposizione di un numero nei suoi fattori primi è però piuttosto lungo. Introdurremo ora un nuovo algoritmo, molto meno complesso, per calcolare il massimo comun divisore di due numeri naturali, basato sulla divisione con il resto ed il principio di buon ordinamento. Tale algoritmo prende il nome di *Algoritmo di Euclide.*

Dati due numeri $a \leq b$, interi positivi, se $a = b$ allora $MCD(a, b) = MCD(a, a) = a$.
Se invece $a \neq b$ allora $a < b$ ed esistono q_1, $r_1 \in \mathbb{N}$ con $0 \leq r_1 < a$ tali che

$$b = aq_1 + r_1.$$

Se $r_1 = 0$, allora $a|b$ e $MCD(a, b) = a$.
Se $r_1 \neq 0$, allora esistono q_2, $r_2 \in \mathbb{N}$ con $0 \leq r_2 < r_1$ tali che

$$a = q_2 r_1 + r_2$$

(divisione di a per r_1).
Se $r_2 = 0$ allora r_1 è il MCD di a e b. Infatti, $r_1|a$ perché $r_1 q_2 = a$ e $b = (q_2 r_1)q_1 + r_1 = r_1(q_2 q_1 + 1)$, cioè $r_1|b$. Sia $z \in \mathbb{N}$ con $zm = a$ e $zn = b$ un divisore comune di a e di b. Allora

$$zn = b = (zm)q_1 + r_1, \text{ quindi } r_1 = (n - mq_1)z$$

cioè $z|r_1$. Quindi $MCD(a, b) = r_1$ e ci si ferma.
Se invece $r_2 \neq 0$, allora esistono q_3, $r_3 \in \mathbb{N}$, con $0 \leq r_3 < r_2$ per i quali

$$r_1 = q_3 r_2 + r_3$$

(divisione di r_1 per r_2).
Se $r_3 = 0$ allora, come sopra si dimostra che $r_2 = MCD(a, b)$.
Se invece $r_3 \neq 0$, iteriamo il procedimento dividendo r_2 per r_3, e cosi via. Il procedimento ha termine per il principio del buon ordinamento perché $a > r_1 > r_2 > \cdots$. L'ultimo resto non nullo ottenuto per divisioni successive è il massimo comun divisore di a e b.

Esempio 1.12 *Calcolare mediante l'algoritmo di Euclide il massimo comun divisore di* 74 *e* 14.
Abbiamo

$$74 = 14 \cdot 5 + 4$$

quindi $q_1 = 14$ *e* $r_1 = 4 \neq 0$.

$$14 = 4 \cdot 3 + 2$$

quindi $q_2 = 3$ *e* $r_2 = 2 \neq 0$.

$$4 = 2 \cdot 2 + 0$$

quindi $q_3 = 2$ *e* $r_3 = 0$. *L'ultimo resto non nullo, cioè* 2 *è* $MCD(74, 14)$.

Esercizio 1.13 *Calcolare, utilizzando l'algoritmo di Euclide, il MCD delle coppie di numeri degli esercizi della sezione precedente.*

2 I numeri interi

Nell'insieme dei naturali non possiamo sempre calcolare "la differenza" di due numeri. Infatti $b-a \in \mathbb{N}$ se e solo se $b \geq a$. In termini formali, questo vuol dire che l'equazione

$$X + a = b$$

ha soluzione in $\mathbb{N}$ se e solo se $b \geq a$. Introduciamo allora l'insieme $\mathbb{Z}$ dei numeri interi, ovvero l'insieme dei numeri: 0, ± 1, ± 2, ..., con le operazioni note.

Tale insieme numerico può essere costruito come l'insieme delle classi di equivalenza di coppie di elementi di $\mathbb{N}$ rispetto alla seguente relazione di equivalenza:

$$(a,\, b) \sim (c,\, d), \qquad \text{se } a + d = b + c$$

con somma e prodotto definiti come segue:

$$[(a,\, b)] + [(r,\, s)] = [(a + r,\, b + s)], \quad [(a,\, b)][(r,\, s)] = [(ar + bs, as + br)].$$

Con questa descrizione, al numero positivo a corrisponderà la classe alla quale appartiene la coppia $(a,\, 0)$ mentre al numero negativo b corrisponderà la classe della coppia $(0,\, -b)$.

Esercizio 2.1 *Verificare che la relazione introdotta $\sim$ è una relazione di equivalenza sull'insieme delle coppie di elementi di $\mathbb{N}$. Verificare che le operazioni di somma e prodotto sono ben definite (cioè non dipendono dalla scelta del rappresentante).*

In $\mathbb{Z}$, con le operazioni di somma e prodotto introdotte, *tutte* le equazioni del tipo $X + a = b$, con a e $b \in \mathbb{Z}$ ammettono la soluzione $b + (-a) = b - a \in \mathbb{Z}$.

Come l'insieme $\mathbb{N}$, anche $\mathbb{Z}$ è un insieme totalmente ordinato, con ordinamento dato da da $\leq$: diremo che $x \leq y$ se e solo se $y - x \geq 0$, o, alternativamente, se $y - x$ corisponde alla classe di equivalenza di una coppia della forma $(a,\, b)$ con $a,\, b \in \mathbb{N}$ e $a \geq b$. Tuttavia, $\mathbb{Z}$ non ha la proprietà del buon ordinamento: ad esempio, l'insieme $S = \{x \in \mathbb{Z} \mid x \leq 5\}$ non possiede un elemento minimo.
La somma, il prodotto e l'ordinamento in $\mathbb{Z}$ godono delle seguenti proprietà:

1. $a + b = b + a$ per ogni $a,\, b \in \mathbb{Z}$ (proprietà commutativa della somma);
2. $(a + b) + c = a + (b + c)$ per ogni $a,\, b,\, c \in \mathbb{Z}$ (proprietà associativa della somma);
3. $0 + a = a$ per ogni $a \in \mathbb{Z}$ (esistenza dell'elemento neutro per la somma);
4. per ogni $a \in \mathbb{Z}$ esiste $b = (-a) \in \mathbb{Z}$ tale che $a + b = 0$ (esistenza dell'elemento opposto);
5. $a(b + c) = ab + ac$ per ogni $a,\, b,\, c \in \mathbb{Z}$ (proprietà distributiva);
6. $(ab)c = a(bc)$ per ogni $a,\, b,\, c \in \mathbb{Z}$ (proprietà associativa del prodotto);

7. $1a = a$ per ogni $a \in \mathbb{Z}$ (esistenza dell'elemento neutro per il prodotto);

8. dati a, $b \in \mathbb{Z}$, se $ab = 0$ allora $a = 0$ oppure $b = 0$ ($\mathbb{Z}$ è privo di divisori dello zero);

9. dati a, $b \in \mathbb{Z}$, se $ab = 1$ allora $a = b = 1$ oppure $a = b = -1$ (gli elementi invertibili di $\mathbb{Z}$ sono solo ± 1);

10. $ab = ba$ per ogni a, $b \in \mathbb{Z}$ (proprietà commutativa del prodotto);

11. per ogni $a, b \in \mathbb{Z}$, $a \geq b$ se e solo se $a + c \geq b + c$ per ogni $c \in \mathbb{Z}$ (compatibilità dell'ordine con la somma).

Osservazione 2.2 *La compatibilità dell'ordine con il prodotto in $\mathbb{Z}$ non vale nella stessa forma in cui vale per $\mathbb{N}$. Si ha invece la seguente regola: Per ogni a, $b \in \mathbb{Z}$, $a \geq b$ se e solo se $ac \geq bc$ per ogni $c \in \mathbb{Z}$ con $c > 0$, mentre $ac \leq bc$ per ogni $c \in \mathbb{Z}$ con $c < 0$. Ad esempio, $3 \geq -5$ mentre $-6 = (-2)3 \leq (-2)(-5) = 10$.*

Osservazione 2.3 *Dalla compatibilità dell'ordine con la somma segue che, se x, $y \geq 0$ allora $x + y \geq 0$. Infatti se $x \geq 0$ ed $y \geq 0$ allora $x + y \geq 0 + y \geq 0$. Segue inoltre che in questo caso $x + y > 0$ se e solo se almeno un elemento tra x ed y è strettamente positivo.*

Esercizio 2.4 *Dimostrare per induzione che se $x_1, \ldots, x_k \geq 0$, allora $x_1 + \cdots + x_k \geq 0$.*

Esercizio 2.5 *Dimostrare che per ogni $x \in \mathbb{Z}$, $x^2 \geq 0$.*

2.1 Divisibilità e Massimo comun divisore

In questa sezione descriveremo il concetto di divisibilità e di massimo comun divisore in $\mathbb{Z}$. Per il calcolo pratico, ci baseremo su quanto accade in $\mathbb{N}$.

2.1.1 Divisibilità

Definizione 2.6 *Dati a, $b \in \mathbb{Z}$ diremo che a divide b (in formule, $a|b$) se esiste $k \in \mathbb{Z}$ tale che $ak = b$.*

Ad esempio, $-4|12$ perché esiste $-3 \in \mathbb{Z}$ tale che $(-4) \cdot (-3) = 12$.

Esercizio 2.7 *Dimostrare che dati a, $b \in \mathbb{Z}$, $a|b$ se e solo se $-a|b$. Dimostrare che dati a, $b \in \mathbb{Z}$, $a|b$ se e solo se $a| - b$.*

Esercizio 2.8 *Dimostrare che dati a, $b \in \mathbb{Z}$, se $a|b$ e $b|a$ allora $a = \pm b$.*

Definizione 2.9 *Un elemento $p \in \mathbb{Z}$ è detto un numero primo se soddisfa le seguenti proprietà:*

- $p \neq \pm 1$

- *se $x \in \mathbb{Z}$ è tale che $x|p$ allora $x = \pm 1$ oppure $x = \pm p$.*

Segue dalla definizione di numero primo che p è primo se e solo se $-p$ è primo e che se p è primo e $p > 0$ allora p è primo in $\mathbb{N}$. Pertanto anche i numeri primi in $\mathbb{Z}$ sono infiniti. Anche per $\mathbb{Z}$ vale il teorema della fattorizzazione unica:

Teorema 2.10 *Ogni elemento non nullo z di $\mathbb{Z}$ si può scrivere come prodotto di (potenze di) numeri primi positivi per ± 1 ovvero $n = \pm p_1^{e_1} \cdots p_k^{e_k}$. Tale scrittura è unica a meno dell'ordine in cui compaiono i fattori.*

Anche in $\mathbb{Z}$ abbiamo un criterio di divisibilità: dati due elementi m ed n di $\mathbb{Z}$, con fattorizzazione

$$m = \pm p_1^{e_1} \cdots p_k^{e_k}, \quad n = \pm q_1^{f_1} \cdots q_s^{f_s}$$

$m|n$ se e solo se

- $\{p_1, \ldots, p_k\} \subset \{q_1, \ldots, q_s\}$ e
- $f_j \geq e_i$ se $q_j = p_i$.

2.1.2 Massimo comun divisore

Anche nel caso di $\mathbb{Z}$ abbiamo il concetto di massimo comun divisore.

Definizione 2.11 *Dati $a, b \in \mathbb{Z}$ non entrambi nulli, l'elemento $d \in \mathbb{Z}$ è detto un* massimo comun divisore *di a e b se*

1. *$d|a$ e $d|b$;*
2. *se $z|a$ e $z|b$ per qualche $z \in \mathbb{Z}$, allora $z|d$.*

Ad esempio -13 è massimo comun divisore di 39 e -52. Infatti, -13 divide sia $39 = 3 \cdot 13$ che $-52 = -4 \cdot 13$; i divisori di 39 sono gli interi della forma $\pm 3^a \cdot 13^b$ con $a \leq 1$, $b \leq 1$, i divisori di $-52 = -2^2 \cdot 13$ sono i numeri della forma $\pm 2^s \cdot 13^t$ con $s \leq 2$, $t \leq 1$. Quindi gli elementi che dividono sia 39 che -52 sono solo 13 e -13, che sono divisori di -13. □

Esercizio 2.12 *Dimostrare che dati qualsiasi $a, b \in \mathbb{Z}$ non nulli, il loro massimo comun divisore è unico a meno del segno.*

Denoteremo con $MCD(a, b)$ il massimo comun divisore *positivo* dei numeri a e b. Dalla simmetria nel ruolo di a e di b nella definizione di massimo comun divisore segue che $MCD(a, b) = MCD(b, a)$.

Esercizio 2.13 *Dimostrare che per ogni $a, b \in \mathbb{Z}$ non nulli, $MCD(a, b) = MCD(-a, b) = MCD(a, -b) = MCD(-a, -b)$.*

Esercizio 2.14 *Calcolare il massimo comun divisore positivo di -288 e 18 e dimostrare che è un massimo comun divisore.*

Dato $a \in \mathbb{Z}$, chiameremo *modulo o valore assoluto di* a, l'elemento $|a| \in \mathbb{N}$ così definito:

$$|a| = \begin{cases} a & \text{se } a \geq 0, \\ -a & \text{se } a < 0. \end{cases}$$

Il modulo di un numero intero si comporta bene rispetto al prodotto ed alla somma: $\forall a, b \in \mathbb{Z}$, si ha

- $|ab| = |a|\,|b|$;
- $|a + b| \leq |a| + |b|$.

La seconda disuguaglianza diviene un'uguaglianza se e solo se a e b hanno lo stesso segno.
Anche in $\mathbb{Z}$ possiamo effettuare la divisione con il resto:

Proposizione 2.15 *Dati $a \neq 0$ e b in $\mathbb{Z}$, possiamo sempre trovare $q \in \mathbb{Z}$ ed $r \in \mathbb{Z}$ con $0 \leq r < |a|$ per i quali $b = aq + r$.*

Dimostrazione: Si dimostra come nel caso di $\mathbb{N}$ utilizzando il principio di buon ordinamento di $\mathbb{N}$. □

Osservazione 2.16 *Il quoziente di una divisione tra due interi non è necessariamente uguale (a meno del segno) al quoziente della divisione in $\mathbb{N}$ dei moduli dei numeri dati: ad esempio*

$$12 = 3 \cdot 5 + 2; \ \textit{mentre} \ -12 = (-3) \cdot 5 + 3.$$

Ciò è conseguenza del fatto che abbiamo richiesto che il resto della divisione sia sempre non negativo.

Una volta dimostrata la possibilità di eseguire la divisione con un resto non negativo tra due numeri in $\mathbb{Z}$, osserviamo che l'algoritmo di Euclide per il calcolo del massimo comun divisore di due numeri in $\mathbb{N}$ funziona anche per il calcolo del massimo comun divisore di due elementi in $\mathbb{Z}$. Per come è costruita la divisione con il resto in $\mathbb{Z}$ l'algoritmo fornirà il massimo comun divisore positivo dei numeri dati. Per evitare difficoltà con i segni, possiamo comunque utilizzare il contenuto dell'Esercizio 2.13 e calcolare il massimo comun divisore di due numeri positivi con l'algoritmo di Euclide in $\mathbb{N}$.

Esercizio 2.17 *Calcolare $MCD(127, -12)$ con l'algoritmo di Euclide.*

2.2 Congruenze ed insiemi quoziente

Una relazione di equivalenza $\equiv$ su un insieme S dotato di un'operazione $*$ è detta congruenza se "rispetta l'operazione", ovvero se $a \equiv b$ e $c \equiv d$ implicano $a * c \equiv b * d$. Dato un insieme numerico S dotato di somma e prodotto ed una congruenza $\equiv$, l'insieme quoziente Q, cioè l'insieme i cui elementi sono le classi di equivalenza rispetto a $\equiv$, è naturalmente dotato di somma e prodotto indotte da quelle di S. Le operazioni $[a] + [b] = [a + b]$ e $[a] \cdot [b] = [ab]$ sono infatti ben definite, cioè non dipendono dalla scelta del rappresentante della classe. Ciò è una conseguenza della compatibilità tra $\equiv$ e le operazioni.

2.2.1 Un'esempio importante di congruenza

Sia $n \in \mathbb{Z}$ positivo fissato e siano a, $b \in \mathbb{Z}$. Diremo che

$$a \equiv b \mod n \quad \text{se} \quad n|(a-b) \text{ in } \mathbb{Z}.$$

Proposizione 2.18 *La relazione $\equiv$ è una relazione di equivalenza su $\mathbb{Z}$. Essa rispetta sia la somma che il prodotto in $\mathbb{Z}$.*

Dimostrazione: La relazione $\equiv$ è riflessiva perché $a \equiv a \mod n$. Infatti n divide $a - a = 0$ perché $n0 = 0$.
Essa è simmetrica (cioè se $a \equiv b \mod n$ allora $b \equiv a \mod n$) perché se $a \equiv b \mod n$, allora $n|(a-b)$ cioè esiste $k \in \mathbb{Z}$ tale che $nk = (a-b)$. Pertanto $n(-k) = b - a$ e $b \equiv a \mod n$.
Essa è transitiva (cioè se $a \equiv b \mod n$ e $b \equiv c \mod n$ segue che $a \equiv c \mod n$) perché se $a \equiv b \mod n$ e $b \equiv c \mod n$, allora $n|(a-b)$ ed $n|(b-c)$ quindi esistono l, m tali che $nl = (a-b)$, $nm = (b-c)$. Pertanto $n(l+m) = nl+nm = a-b+b-c = a-c$, quindi $n|(a-c)$ e $a \equiv c \mod b$.
La relazione rispetta l'operazione di prodotto in $\mathbb{Z}$: se $a \equiv b \mod n$ e $c \equiv d \mod n$ allora $n|(a-b)$ ed $n|(c-d)$. Esistono dunque l, $m \in \mathbb{Z}$ tali che $ln = a-b$, $mn = c-d$. L'elemento $ac-bd = ac-ad+ad-bd = a(c-d)+d(a-b)$ quindi $n|(ac-bd)$ perché $ac-bd = amn+dln = n(am+dl)$. Pertanto $ac \equiv bd \mod n$.

La verifica che la relazione rispetti anche l'operazione di somma è analoga alla precedente ed è lasciata al lettore per esercizio. □

Esercizio 2.19 *Verificare se le seguenti congruenze sono vere o false:*

1. $3 \equiv 1 \mod 12$;
2. $144 \equiv 36 \mod 12$;
3. $147 \equiv 7 \mod 12$;
4. $125 \equiv 4 \mod 11$.

Data una congruenza della forma $aX \equiv b \mod n$, con a, $b \in \mathbb{Z}$, $n \in \mathbb{Z}$, $n > 0$ ed X un'incognita, diremo che essa ammette soluzione se esiste $k \in \mathbb{Z}$ tale che $n|(ak-b)$. Le soluzioni di tali congruenze non esistono sempre e se esistono, non sono uniche: se k è una soluzione, allora anche tutti gli interi della forma $k+mn$ con $m \in \mathbb{Z}$ (cioè *tutti* gli elementi appartenenti alla classe di equivalenza dell'elemento k) sono soluzioni.

Il seguente risultato offre un'analisi dell'esistenza di soluzioni per tali congruenze ed una stima di esse. Non daremo una dimostrazione per limiti di spazio ma il risultato è illustrato con due esempi.

Proposizione 2.20 *La congruenza $aX \equiv b \mod n$ ha soluzione se e soltanto se $MCD(a, n)$ divide b. Se ciò si verifica, allora la congruenza ha esattamente $MCD(a, n)$ soluzioni non congruenti tra loro.*

Esempio 2.21 *Analizzare l'esistenza di soluzioni in $\mathbb{Z}$ della congruenza $4X \equiv 14 \mod 8$.*

Soluzione: Osserviamo che se esiste $k \in \mathbb{Z}$ tale che $8|(4k-14)$, cioè se esistono k ed $s \in \mathbb{Z}$ tali che $8s = 4k - 14$ allora $8s - 4k = 4(2s-k) = 14$. Ciò è assurdo perché $4 = MCD(4,8)$ non è un divisore di 14.

Esempio 2.22 *Analizzare l'esistenza di soluzioni in $\mathbb{Z}$ della congruenza $4X \equiv 8 \mod 14$.*

Soluzione: La congruenza ammette soluzioni se e solo se esiste $k \in \mathbb{Z}$ tale che $14|4z-8$, cioè se e solo se esistono k, $s \in \mathbb{Z}$ tali che $4(z-2) = 14s$. Ciò è equivalente all'esistenza di k, $s \in \mathbb{Z}$ tali che $2(z-2) = 7s$ (dividendo tutto per 2). Per risolvere la congruenza data risolviamo la congruenza:

$$2X \equiv 4 \mod 7.$$

Cerchiamo un numero $m \in \mathbb{Z}$ tra 1 e 6 tale che $2m \equiv 1 \mod 7$, ovvero un inverso, modulo 7, del coefficiente della X. Nel nostro caso $m = 4$. Moltiplicando entrambi i membri per 4 otteniamo

$$1 \cdot X \equiv m \cdot 2X \equiv m \cdot 4 \equiv 16 \equiv 2 \mod 7$$

perché $16 = 2 \cdot 7 + 2 \equiv 2 \mod 7$. Perciò $X \equiv 2 \mod n$, cioè 2 e tutti gli interi congrui a 2 modulo 7 sono soluzioni della congruenza. Essi sono, gli elementi dell'insieme

$$\{k \in \mathbb{Z} \mid k = 2 + 7l,\ l \in \mathbb{Z}\}$$

Tale insieme coincide con l'unione delle due classi di equivalenza modulo 14 (una corrisponde agli l pari, l'altra agli l dispari)

$$\{k \in \mathbb{Z} \mid k = 2 + 14j,\ j \in \mathbb{Z}\} \cup \{k \in \mathbb{Z} \mid k = 9 + 14j,\ j \in \mathbb{Z}\}.$$

Esercizio 2.23 *Analizzare l'esistenza di soluzioni delle seguenti congruenze. Nel caso in cui la congruenza ammetta soluzioni, descriverle tutte.*

1. $9X \equiv 11 \mod 36$;
2. $16X \equiv 6 \mod 30$;
3. $11X \equiv 2 \mod 10$.

2.2.2 L'insieme quoziente $\mathbb{Z}/n\mathbb{Z}$

Abbiamo un'altra caratterizzazione della relazione di congruenza introdotta:

Proposizione 2.24 *Dato $n \in \mathbb{Z}$ positivo, allora $a \equiv b \mod n$ se e solo se a e b hanno lo stesso resto nella divisione per n.*

Dimostrazione: Sia $a \equiv b \mod n$ e sia $a = nq_1 + r_1$, $b = nq_2 + r_2$, con $0 \leq r_1 < n$, ed $0 < r_2 < n$. Se per assurdo $r_1 \neq r_2$, allora $r_1 < r_2$ oppure $r_2 < r_1$. Trattiamo il caso in cui $r_1 < r_2$, l'altro caso è analogo e lasciato al lettore. Abbiamo allora

$$(b-a) = n(q_2 - q_1) + (r_2 - r_1) \text{ ed } nk = b - a \text{ per qualche } k \in \mathbb{Z}.$$

Allora n divide anche $r_2 - r_1$ perché $n(k - q_2 + q_1) = r_2 - r_1$. D'altra parte $r_2 - r_1 < n - r_1 < n$. Ciò è assurdo, quindi i due resti devono coincidere.

Viceversa, se $a = nq_1 + r$ e $b = nq_2 + r$, allora $a - b = n(q_1 - q_2)$ quindi $a \equiv b \mod n$. □

Tale risultato ci permette di individuare *tutti* gli elementi congruenti ad un numero dato, ovvero le classi di equivalenza, che chiameremo *classi resto modulo* n, e di contarle.

Proposizione 2.25 *L'insieme quoziente $\mathbb{Z}/n\mathbb{Z}$ rispetto alla relazione di equivalenza $\equiv \mod n$ ha esattamente n elementi. Essi sono rappresentati dagli elementi $0, 1, \ldots, n-1$ di Z.*

Dimostrazione: L'enunciato è conseguenza del risultato precedente: i numeri interi da 0 ad $n-1$ non sono congrui tra di loro. D'altra parte per ogni elemento $z \in \mathbb{Z}$ esiste $r \in \{0, \ldots, n-1\}$ tale che $z = nq + r$ con $q \in \mathbb{Z}$, quindi $z \equiv r \mod n$. Perciò ogni elemento di $\mathbb{Z}$ appartiene alla classe di equivalenza di uno ed uno solo di questi elementi. □

Descriviamo ora alcuni esempi di questi insiemi quoziente:

Esempio 2.26 *Se $n = 2$, avremo esattamente 2 classi resto, quella dei numeri pari, o congrui a 0 modulo 2, e quella dei numeri dispari, congrui a 1 modulo 2. Il prodotto in $\mathbb{Z}/2\mathbb{Z}$ sarà allora:*

$$[0] \cdot [0] = [0], \quad [0] \cdot [1] = [0] = [1] \cdot [0], \quad [1] \cdot [1] = [1]$$

e la somma sarà data da:

$$[0] + [0] = [0], \quad [0] + [1] = [1] = [1] + [0], \quad [1] + [1] = [0].$$

Esempio 2.27 *Se $n = 6$, avremo esattamente 6 classi, corrispondenti ai possibili resti della divisione per 6. Descriviamo il risultato di alcune operazioni nell'insieme quoziente $\mathbb{Z}/6\mathbb{Z}$:*

$$[3] + [3] = [0], \quad [3] + [4] = [1], \quad [2] \cdot [5] = [4]$$

$$[2] \cdot [3] = [0], \quad [4] \cdot [2] = [2], \quad [5] \cdot [5] = [1]$$

Esercizio 2.28 *Descrivere gli elementi di $\mathbb{Z}/4\mathbb{Z}$. Calcolare $[2] \cdot [2]$, $[2] \cdot [3]$, $[2] + [3]$ e $[3] + [3]$. Dire se secondo voi esiste $[k] \in \mathbb{Z}/4\mathbb{Z}$ tale che $[k] \cdot [2] = [1]$. Dire se secondo voi esiste $[k] \in \mathbb{Z}/4\mathbb{Z}$ tale che $[k] \cdot [3] = [1]$.*

Esercizio 2.29 *Verificare quali proprietà della somma e del prodotto in $\mathbb{Z}$ valgono ancora in $\mathbb{Z}/n\mathbb{Z}$.*

3 I numeri razionali

Abbiamo visto che in $\mathbb{Z}$ tutte le equazioni della forma $X + a = b$ con a e b in $\mathbb{Z}$ ammettono soluzione. D'altra parte, le equazioni della forma $aX = b$ con $a \neq 0$ ammettono soluzione in $\mathbb{Z}$ se e soltanto se $a|b$, per definizione di divisore. Introduciamo allora l'insieme $\mathbb{Q}$ dei numeri razionali. Gli elementi di questo insieme hanno la forma: $\pm\frac{m}{n}$ con $m \in \mathbb{N}$ ed $n \in \mathbb{N}$, con le operazioni note di somma e prodotto.

L'insieme $\mathbb{Q}$ può essere costruito come insieme quoziente per la relazione di equivalenza definita sugli elementi di $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ come segue:

$$(m,\, n) \sim (r,\, s), \qquad \text{se e solo se} \qquad ms = rn.$$

Le operazioni di somma e prodotto sono definite in tale caso come:

$$[(m,\, n)] + [(r,\, s)] = [(ms + nr,\, ns)], \qquad [(m,\, n)] \cdot [(r,\, s)] = [(mr,\, ns)].$$

La "frazione" $\frac{m}{n}$ corrisponderà allora alla classe della coppia $(m,\, n)$.

Esercizio 3.1 *Verificare che $\sim$ è una relazione di equivalenza. Verificare che le operazioni di somma e prodotto sono ben definiti sull'insieme quoziente, ovvero non dipendono dalla scelta del rappresentante della classe di equivalenza.*

Tutte le equazioni del tipo $aX = b$, con $a \neq 0$ e $b \in \mathbb{Q}$ ammettono soluzione in $\mathbb{Q}$, ovvero: se $a = \frac{m}{n} \in \mathbb{Q} \setminus \{0\}$ e se $b = \frac{r}{s} \in \mathbb{Q}$ allora la soluzione è $a^{-1}b = \frac{nr}{ms}$.

Anche $\mathbb{Q}$ è un insieme totalmente ordinato, con ordinamento dato da da $\leq$. Diremo che $x \leq 0$ se esso corrisponde alla classe di una coppia $(a,\, b)$ con $a,\, b \in \mathbb{Z}$ e $ab \leq 0$. Diremo allora che $x \leq y$ se $x - y \leq 0$. Poiché $\mathbb{Q}$ contiene $\mathbb{Z}$, che non gode della proprietà del buon ordinamento, neanche $\mathbb{Q}$ gode di tale proprietà.

Osservazione 3.2 *Neanche l'insieme $\mathbb{Q}^+$ dei numeri razionali positivi, che è un insieme ordinato, gode della proprietà di buon ordinamento. E' sufficiente osservare che $\mathbb{Q}^+$ stesso non possiede un minimo. Se per assurdo esistesse un minimo $r \in \mathbb{Q}^+$, allora $r \leq x$ per ogni $x \in \mathbb{Q}^+$. Ma $\frac{1}{2}r \leq r$, $\frac{1}{2}r \neq r$ e $\frac{1}{2}r \in \mathbb{Q}^+$, assurdo.*

La somma, il prodotto e l'ordinamento in $\mathbb{Q}$ godono delle seguenti proprietà:

1. $a + b = b + a$ per ogni $a,\, b \in \mathbb{Q}$ (proprietà commutativa della somma);
2. $(a + b) + c = a + (b + c)$ per ogni $a,\, b,\, c \in \mathbb{Q}$ (proprietà associativa della somma);
3. $0 + a = a$ per ogni $a \in \mathbb{Q}$ (esistenza dell'elemento neutro per la somma);
4. per ogni $a \in \mathbb{Q}$ esiste $b = (-a) \in \mathbb{Q}$ tale che $a + b = 0$ (esistenza dell'elemento opposto);
5. $a(b + c) = ab + ac$ per ogni $a,\, b,\, c \in \mathbb{Q}$ (proprietà distributiva);

6. $(ab)c = a(bc)$ per ogni a, b, $c \in \mathbb{Q}$ (proprietà associativa del prodotto);
7. $ab = ba$ per ogni a, $b \in \mathbb{Q}$ (proprietà commutativa del prodotto);
8. $1a = a$ per ogni $a \in \mathbb{Q}$ (esistenza dell'elemento neutro per il prodotto);
9. dati a, $b \in \mathbb{Q}$, se $ab = 0$ allora $a = 0$ oppure $b = 0$ ($\mathbb{Q}$ è privo di divisori dello zero);
10. Per ogni $a \in \mathbb{Q} \setminus \{0\}$ esiste $b \in \mathbb{Q}$ tale che $ab = 1$ (tutti gli elementi *non nulli* di $\mathbb{Q}$ sono invertibili);
11. per ogni a, $b \in \mathbb{Q}$, $a \geq b$ se e solo se $a + c \geq b + c$ per ogni $c \in \mathbb{Q}$ (compatibilità dell'ordine con la somma);
12. Per ogni x, $y \in \mathbb{Q}$ con $x < y$ esiste $z \in \mathbb{Q}$ con $x < z < y$ (proprietà di densità di $\mathbb{Q}$);
13. per ogni $a \in \mathbb{Q}$ con $a \neq 0$, $a > 0$ se e solo se $a^{-1} > 0$;
14. per ogni a, $b \in \mathbb{Q}$, $a \geq b$ se e solo se $ac \geq bc$ per ogni $c \in \mathbb{Q}$ con $c > 0$;
15. per ogni a, $b \in \mathbb{Q}$, $a \geq b$ se e solo se $ac \leq bc$ per ogni $c \in \mathbb{Q}$ con $c < 0$;
16. per ogni a, $b \in \mathbb{Q}$ con $0 < a < b$ si ha: $0 < b^{-1} < a^{-1}$.

Esercizio 3.3 *Dimostrare che la proprietà 13 è conseguenza della proprietà 14.*

L'insieme $\mathbb{Q}$ è numerabile, cioè può essere messo in biezione con i numeri naturali. Un possibile metodo è il seguente: se posso numerare l'insieme dei razionali non negativi $\mathbb{Q}^+$, allora posso numerare tutto $\mathbb{Q}$ perché se q_n con $n \in \mathbb{N}$ è una enumerazione di $\mathbb{Q}^+$, allora 0, q_1, $-q_1$, q_2, $-q_2, \ldots$ è una enumerazione di $\mathbb{Q}$. Pertanto è sufficiente risolvere il problema per $\mathbb{Q}^+$. A questo punto, scriviamo i numeri razionali positivi in una tabella infinita scrivendo sulla prima riga tutti i razionali con denominatore 1, sulla seconda quelli con denominatore 2, etc. I razionali con denominatore fissato sono numerabili.

$$\begin{array}{ccccccccc}
\frac{1}{1} & & \frac{2}{1} & & \frac{3}{1} & & \frac{4}{1} & & \cdots \\
& \swarrow & & \swarrow & & \swarrow & & \swarrow & \\
\frac{1}{2} & & \frac{2}{2} & & \frac{3}{2} & & \frac{4}{2} & & \cdots \\
& \swarrow & & \swarrow & & \swarrow & & \swarrow & \\
\frac{1}{3} & & \frac{2}{3} & & \frac{3}{3} & & \frac{4}{3} & & \cdots \\
& \swarrow & & \swarrow & & \swarrow & & \swarrow & \\
\cdots & \cdots & \cdots & \cdots & \cdots & & & &
\end{array}$$

Alcuni razionali appariranno più volte ma se posso enumerare gli elementi di questa tabella, posso enumerare gli elementi di $\mathbb{Q}^+$ che ne formano un sottoinsieme. Ora, una enumerazone degli elementi di questa tabella si ottiene scrivendo prima $\frac{1}{1}$, poi $\frac{2}{1}$, poi seguendo le frecce fino alla prima colonna, ripartendo successivamente dal primo elemento non ancora scritto della prima riga. In modo analogo si dimostra che ogni famiglia numerabile di insiemi numerabili è numerabile.

3.1 Scrittura n-adica

Di solito scriviamo i numeri in forma decimale, o in base 10. Ad esempio $72523 = 7 \cdot 10^4 + 2 \cdot 10^3 + 5 \cdot 10^2 + 2 \cdot 10^1 + 3 \cdot 10^0$. Tuttavia si può scegliere di scrivere i numeri in altre basi naturali, ad esempio, lo stesso numero in base 11 è scritto come 4 10 5 4 0 perché è uguale a $4 \cdot 11^4 + 10 \cdot 11^3 + 5 \cdot 11^2 + 4 \cdot 11^1 + 0 \cdot 11^0$. Ciò si ottiene dividendo successivamente per 11

$$72523 = 11 \cdot 6593 = 11(11 \cdot 599 + 4) = 11^2 \cdot 599 + 4 \cdot 11 =$$

$$= 11^2(54 \cdot 11 + 5) + 4 \cdot 11 = 54 \cdot 11^3 + 5 \cdot 11^2 + 4 \cdot 11 =$$

$$11^3(4 \cdot 11 + 10) + 5 \cdot 11^2 + 4 \cdot 11.$$

In generale possiamo affermare che

Proposizione 3.4 *Fissato $n \in N$, $n \neq 0, 1$, ogni $m \in \mathbb{N}$, $m \neq 0$ può essere scritto in modo unico nella forma $m = m_k n^k + m_{k-1} n^{k-1} + \cdots + m_1 n^1 + m_0 n^0$ con $m_k \neq 0$ e $0 \leq m_j < n$ per ogni j.*

La somma ed il prodotto in base n-adica si possono calcolare con le solite tecniche.

Esercizio 3.5 *Scrivere il numero* 45123 *in base* 7 *ed in base* 4. *Scrivere in forma decimale il numero che in forma* 5*-adica si scrive come* 43241.

Esercizio 3.6 *Scrivere i numeri* 3040; 121; 256; 65 *in forma* 2*-adica (=binaria).*

Esercizio 3.7 *Verificare l'unicità di scrittura enunciata nella Proposizione 3.4.*

Finora ci siamo occupati dell'espressione n-adica di numeri interi. Tuttavia, possiamo anche scrivere in forma n-adica numeri razionali, separando con una virgola i coefficienti delle potenze non negative di n da quelle negative:

$$234,56 = 2 \cdot n^2 + 3 \cdot n^1 + 4 \cdot n^0 + 5 \cdot n^{-1} + 6 \cdot n^{-2} =$$

$$\frac{2 \cdot n^4 + 3 \cdot n^3 + 4 \cdot n^2 + 5 \cdot n^1 + 6 \cdot n^0}{n^2} \in \mathbb{Q}.$$

In questo caso non avremo sempre una scrittura "pulita", ad esempio non tutti i razionali hanno una scrittura decimale finita in senso stretto: $\frac{10}{3} = 3,33333\ldots = 3,\bar{3}$; $\frac{12}{7} = 1,714285714285\ldots = 1,\overline{714285}$; $\frac{12002}{990} = 12,1232323\ldots = 12,1\overline{23}$ mentre $\frac{2}{5} = 0,4 = 0,4\overline{0}$.

E' però vero che tutti i numeri razionali hanno una scrittura decimale *periodica* ovvero tale che da un certo punto in poi dopo la virgola lo stesso blocco di cifre sarà ripetuto infinite volte. Ciò è una conseguenza dell'algoritmo di divisione. Infatti le cifre decimali si ottengono, come abbiamo visto, per divisioni successive: $\frac{12}{7} = \frac{7 \cdot 1 + 5}{7} = 1 + \frac{5}{7} = \cdots$ I possibili resti di successive divisioni per il denominatore della frazione devono essere tutti minori della cifra al denominatore stesso. Pertanto dopo un numero finito di passaggi, i resti si ripeteranno.

4 I numeri reali

Anche per i numeri razionali esistono equazioni algebriche che non ammettono soluzione, ad esempio $X^2 = 2$ non ha soluzione in $\mathbb{Q}$. Infatti, se per assurdo esistessero m, $n \in \mathbb{Z}$ tali che $\frac{m^2}{n^2} = 2$, allora avremmo $2n^2 = m^2$. Scomponendo in fattori primi entrambi i membri, 2 apparirebbe con esponente dispari nell'espressione a sinistra e con esponente pari nell'espressione a destra, impossibile per l'unicità della fattorizzazione in $\mathbb{Z}$. Cerchiamo allora un insieme di numeri nei quali esistano, ad esempio, numeri x tali che $x^n = p$ per ogni coppia di numeri positivi n e p. Un insieme che soddisfi questa proprietà è dato dall'insieme $\mathbb{R}$ dei numeri reali. I suoi elementi possono essere descritti come "espansioni decimali infinite", ad esempio $-\sqrt{2} = -1,414213542\ldots$ dove l'espansione decimale non ha termine.

Proposizione 4.1 *L'insieme $\mathbb{R}$ non è numerabile.*

Dimostrazione: (idea) Se lo fosse, avremmo anche una enumerazione dei numeri reali compresi tra 0 e 10: $r_0 = r_{00}, r_{01}\ldots$; $r_1 = r_{10}, r_{11}\ldots$; $\ldots$; $r_k = r_{k0}r_{k1}\ldots$; $\ldots$. Prendiamo allora il numero x avente scrittura decimale $x_0, x_1\ldots$ costruita in modo che la cifra k-esima sia *diversa* dalla cifra k-esima di r_k. Il numero x non può avere scrittura uguale a nessuno degli r_k perché ha cifra k-esima diversa. Si può dimostrare cheè possibile costruire x in modo tale che non sia uguale a nessuno dei numeri precedenti, pertanto la enumerazione data non può essere una enumerazione dei numeri reali compresi ta 0 e 10. □

Per definire la somma ed il prodotto di due numeri reali non possiamo utilizzare un algoritmo o una formula come nel caso dei naturali, degli interi o dei razionali. Per descrivere la somma ed il prodotto in modo rigoroso sarebbe necessario utilizzare il concetto di *limite*, che sarà trattato più avanti in questo corso. Intuitivamente, possiamo vedere $-\sqrt{2}$ come limite della successione approssimante

$$x_0 = -1;\ x_1 = -1,4;\ x_2 = -1,41;\ x_3 = -1,414;$$

$$x_4 = -1,4142;\ x_5 = -1,41421;\ldots$$

Utilizzando questa visione intuitiva, la somma ed il prodotto di due numeri reali

$$r = \sum_{k=-\infty}^{M} a_k 10^k = a_M a_{M-1}\cdots a_0, a_{-1}a_{-2}\ldots$$

$$s = \sum_{k=-\infty}^{N} b_k 10^k = b_N b_{N-1}\cdots b_0, b_{-1}b_{-2}\ldots$$

saranno i numeri reali che sono limite delle successioni $(r+s)_n$ ed $(rs)_n$:

$$(r+s)_n = a_M a_{M-1}\cdots a_0, \cdots a_{-n} + b_N b_{N-1}\cdots b_0, \cdots b_{-n};$$

$$(rs)_n = (a_M a_{M-1} \cdots a_0, \cdots a_{-n})(b_N b_{N-1} \cdots b_0, \cdots b_{-n})$$

cioè saranno i limiti delle somme e prodotti *approssimati* alla n-esima cifra decimale.

Tali operazioni soddisfano le seguenti proprietà:

1. $a + b = b + a$ per ogni a, $b \in \mathbb{R}$ (proprietà commutativa della somma);
2. $(a + b) + c = a + (b + c)$ per ogni a, b, $c \in \mathbb{R}$ (proprietà associativa della somma);
3. $0 + a = a$ per ogni $a \in \mathbb{R}$ (esistenza dell'elemento neutro per la somma);
4. per ogni $a \in \mathbb{R}$ esiste $b = (-a) \in \mathbb{R}$ tale che $a + b = 0$ (esistenza dell'elemento opposto);
5. $a(b + c) = ab + ac$ per ogni a, b, $c \in \mathbb{R}$ (proprietà distributiva);
6. $(ab)c = a(bc)$ per ogni a, b, $c \in \mathbb{R}$ (proprietà associativa del prodotto);
7. $ab = ba$ per ogni a, $b \in \mathbb{R}$ (proprietà commutativa del prodotto);
8. $1a = a$ per ogni $a \in \mathbb{R}$ (esistenza dell'elemento neutro per il prodotto);
9. dati a, $b \in \mathbb{R}$, se $ab = 0$ allora $a = 0$ oppure $b = 0$ ($\mathbb{R}$ è privo di divisori dello zero);
10. per ogni $a \in \mathbb{R} \setminus \{0\}$ esiste $b \in \mathbb{R}$ tale che $ab = 1$, (tutti gli elementi *non nulli* di $\mathbb{R}$ sono invertibili).

E' definita inoltre un'applicazione iniettiva $j\colon \mathbb{Q} \to \mathbb{R}$ data dall'espansione decimale dei numeri razionali. Come abbiamo visto precedentemente, l'immagine della funzione j è contenuta nell'insieme dei reali con scrittura decimale periodica.

Proposizione 4.2 *L'immagine della funzione $j\colon \mathbb{Q} \to \mathbb{R}$ consiste di tutti e soli gli elementi di $\mathbb{R}$ che ammettono scrittura decimale periodica.*

Dimostrazione: Sia $x = a_N \cdots a_0, a_{-1} \cdots a_{-k}\overline{b_1 b_2 \cdots b_l}$. Allora il numero $10^l x$ ha scrittura decimale periodica con stesso periodo $\overline{b_1 b_2 \cdots b_l}$ di x e con stesso numero k di cifre comprese tra la virgola ed il periodo. Pertanto $(10^l x - x) = (10^l - 1)x$ è un numero che ha scrittura decimale finita ed è della forma

$$(10^l - 1)x = a_N 10^{N+l} + \cdots + c_0 10^0 + c_{-1} 10^{-1} \cdots c_{-k} 10^{-k}$$

$$= \frac{a_N 10^{N+l+k} + \cdots + c_0 10^k + c_{-1} 10^{k-1} \cdots c_{-k}}{10^k}$$

quindi

$$x = \frac{a_N 10^{N+l+k} + \cdots + c_0 10^k + c_{-1} 10^{k-1} \cdots c_{-k}}{10^k (10^l - 1)} \in \mathbb{Q}. \ \square$$

Osservazione 4.3 *A scritture decimali distinte non sempre corrispondono numeri razionali distinti: ad esempio* $0,\bar{9} = 1$. *Infatti se* $x = 0,\bar{9}$ *allora, come nella dimostrazione della proposizione, abbiamo* $10x - x = 9,\bar{9} - 0,\bar{9} = 9$ *quindi* $9x = 9$ *pertanto* $x = 1$.

Esercizio 4.4 *Scrivere in forma di frazione i numeri aventi scrittura decimale* $12,3\overline{45}$ *e* $31,4\overline{839}$.

Anche l'insieme dei numeri reali è totalmente ordinato da una relazione che indicheremo con $\leq$. Dati $x, y \in \mathbb{R}$ diremo che $x \leq y$ se $x = y$ oppure $x < y$, dove la relazione $<$ può essere descritta, in termini di espansione decimale, come segue: un elemento $x \in \mathbb{R}$ è positivo ($x > 0$) se la sua espansione decimale ha segno $+$ e negativo $x < 0$ se la sua espansione decimale ha segno $-$. I numeri negativi sono minori di tutti i numeri positivi. Se $x, y > 0$ con $x \neq 0$ allora sia r l'esponente della più elevata potenza di 10 tale che le scritture di x ed y presentino cifre diverse. Allora $x < y$ se il termine r-esimo dell'espansione decimale di x è minore del termine r-esimo dell'espansione decimale di y. Se $x, y < 0$ allora $x < y$ se e solo se $-x > -y > 0$.

Possiamo riassumere le proprietà di compatibilità tra l'ordinamento e le operazioni in $\mathbb{R}$ come segue.

1. per ogni $a, b \in \mathbb{R}$, $a \geq b$ se e solo se $a + c \geq b + c$ per ogni $c \in \mathbb{R}$ (compatibilità dell'ordine con la somma);
2. se $x > 0$ allora $x^{-1} > 0$;
3. se $x < 0$ allora $x^{-1} < 0$;
4. per ogni $x, y \in \mathbb{R}$, $x \geq y$ se e solo se $xz \geq yz$ per ogni $z \in \mathbb{R}$ con $z > 0$;
5. per ogni $x, y \in \mathbb{R}$, $x \geq y$ se e solo se $xz \leq yz$ per ogni $z \in \mathbb{R}$ con $z < 0$;
6. per ogni $x, y \in \mathbb{R}$ tali che $0 < x < y$, si ha: $0 < y^{-1} < x^{-1}$.

Esercizio 4.5 *Dire quali delle suddette proprietà sono conseguenza delle altre.*

Esercizio 4.6 *Siano* $x, y \in \mathbb{R}$ *tali che* $x > 0$, $y < 0$. *Determinare l'ordine tra* 0, x^{-1} *e* y^{-1}.

Esercizio 4.7 *Dimostrare che, dati* $x_1, \ldots, x_k \in \mathbb{R}$,

1. $x_1 \cdots x_k = 0$ *se e solo se almeno un* $x_j = 0$;
2. $x_1 \cdots x_k > 0$ *se un numero pari di* x_j *è negativo;*
3. $x_1 \cdots x_k < 0$ *se un numero dispari di* x_j *è negativo.*

Anche per i numeri reali possiamo introdurre il concetto di modulo: dato $a \in \mathbb{R}$ il modulo o valore assoluto di a è

$$|a| = \begin{cases} a & \text{se } a \geq 0, \\ -a & \text{se } a < 0. \end{cases}$$

Il modulo soddisfa le proprietà:

1. per ogni $x \in \mathbb{R}$, $|x| \geq 0$;
2. per ogni $x \in \mathbb{R}$, $|x| = 0$ se e solo se $x = 0$;
3. per ogni x, $y \in \mathbb{R}$, $|xy| = |x||y|$;
4. per ogni x, $y \in \mathbb{R}$, $|x + y| \leq |x| + |y|$;

Esercizio 4.8 *Calcolare il modulo dei seguenti numeri reali:*

1. $x = \frac{\sqrt{5}}{2} - \sqrt{3}$;
2. $y = \sqrt{10} - \sqrt{12} + \sqrt{2}$;
3. $z = \frac{2}{7} - \sqrt{6} + 0,04$;
4. $w = 2\pi - 6$.

4.1 Maggioranti, minoranti, estremi superiori ed inferiori

Definizione 4.9 *Un sottoinsieme $S \subset \mathbb{R}$ si dice* limitato superiormente *se ammette maggioranti, ovvero se esistono elementi $x \in \mathbb{R}$ tali che $x \geq s$ per ogni $s \in S$.*
Un sottoinsieme $S \subset \mathbb{R}$ si dice limitato inferiormente *se ammette minoranti, ovvero se esistono elementi $x \in \mathbb{R}$ tali che $x \leq s$ per ogni $s \in S$.*

Attenzione: non è richiesto che i minoranti appartengano all'insieme S.

Esempio 4.10 *Tutti i sottoinsiemi di $\mathbb{R}$ con un numero finito di elementi sono limitati sia superiormente che inferiormente. L'intervallo $[2, 34) = \{x \in \mathbb{R} \mid 2 \leq x < 34\}$ è limitato superiormente ed inferiormente. L'intervallo $(-\infty, 34) = \{x \in \mathbb{R} \mid x < 34\}$ è limitato superiormente ma non inferiormente.*

Definizione 4.11 *Un sottoinsieme $S \subset \mathbb{R}$ ammette un minimo se esiste un elemento $m \in S$ tale che $m \leq s$ per ogni $s \in S$. Un sottoinsieme $S \subset \mathbb{R}$ ammette un massimo se esiste un elemento $m \in S$ tale che $m \geq s$ per ogni $s \in S$.*

Esempio 4.12 *Tutti i sottoinsiemi di $\mathbb{R}$ con un numero finito di elementi ammettono sia massimo che minimo. L'intervallo $[2, 34) = \{x \in \mathbb{R} \mid 2 \leq x < 34\}$ ammette un minimo, che è 2, ma non ammette massimo perché 34 non appartiene all'insieme. L'intervallo $(-\infty, 34) = \{x \in \mathbb{R} \mid x < 34\}$ non ammette né minimo né massimo.*

La relazione d'ordine soddisfa inoltre le seguenti proprietà:

1. L'insieme dei maggioranti M di un qualsiasi sottoinsieme S non vuoto di $\mathbb{R}$ limitato superiormente ammette un minimo, (completezza ordinale di $\mathbb{R}$);

2. Per ogni $x, y \in \mathbb{R}$ con $x < y$ esiste $z \in \mathbb{Q}$ con $x < z < y$ (proprietà di densità di $\mathbb{Q}$ in $\mathbb{R}$);

3. ogni elemento di $\mathbb{R}$ è il minimo dell'insieme dei maggioranti di un insieme di numeri razionali.

4. per ogni $x, y \in \mathbb{R}$, $x > 0$ esiste $n \in \mathbb{N}$ tale che $nx > y$ (Postulato di Archimede);

5. per ogni $x, y \in \mathbb{R}$ con $x > 0$ esiste un unico $m \in \mathbb{Z}$ tale che $mx \leq y < (m+1)x$.

Osservazione 4.13 *La proprietà di completezza ordinale non vale per i razionali: ad esempio l'insieme $S = \{x \in \mathbb{Q} \mid x^2 < 3\}$ è limitato superiormente ed inferiormente (2 è un maggiorante e -2 è un minorante) ma l'insieme $M_{\mathbb{Q}}$ dei maggioranti di S in $\mathbb{Q}$ non ammette minimo. L'insieme $M_{\mathbb{R}}$ dei maggioranti di S in $\mathbb{R}$ ammette invece il minimo $\sqrt{3}$.*

Grazie alla proprietà di completezza ordinale dei reali, possiamo introdurre i concetti di *estremo superiore* ed *estremo inferiore*. Dato un sottoinsieme $S \neq \emptyset$ limitato superiormente, il suo estremo superiore $\sup S$ è l'elemento minimo dell'insieme dei suoi maggioranti, in formule:

$$\sup S = \min\{x \in \mathbb{R} \mid x \geq s,\ \forall s \in S\}.$$

Analogamente, dato un sottoinsieme $S \neq \emptyset$ limitato inferiormente, il suo estremo inferiore $\inf S$ è l'elemento massimo dell'insieme dei suoi minoranti, in formule:

$$\inf S = \max\{x \in \mathbb{R} \mid x \leq s,\ \forall s \in S\}.$$

Esempio 4.14 *Sia S l'intervallo $[2, 34) = \{x \in \mathbb{R} \mid 2 \leq x < 34\}$. Allora $\sup S = 34$ ed $\inf S = \min S = 2$. Sia L l'intervallo $(-\infty, 34) = \{x \in \mathbb{R} \mid x < 34\}$. Allora $\sup L = 34$ mentre l'estremo inferiore di L non è definito perché L non è limitato inferiormente. (Alcuni autori scrivono in questo caso che l'estremo inferiore di L è $-\infty$).*

Esempio 4.15 *Verificare se l'insieme*

$$S = \left\{ y \in \mathbb{R} \mid y = \frac{2x-1}{x},\ x \geq 2 \right\}$$

è limitato superiormente e se lo è, calcolare $\sup S$. L'insieme S è dotato di massimo?

Soluzione: Gli elementi di S sono tutti e soli gli elementi della forma $2 - \frac{1}{x}$ con $x \geq 2$. Poiché $x > 0$ avremo che $\frac{1}{x} > 0$ quindi $-\frac{1}{x} < 0$ e $2 - \frac{1}{x} < 2$. Perciò 2 è un maggiorante di S ed S è limitato superiormente. Sia M l'insieme dei suoi maggioranti. Il suo minimo m è 2. Infatti,$m \leq 2$ perché $2 \in S$ e se avessimo $m < 2$, avremmo $m = 2 - z$ per qualche $z \in \mathbb{R}$, $z > 0$. Sia allora $x_0 = \max\left\{\frac{2}{z}, 2\right\}$. Allora $x_0 \geq 2$, $x_0 \geq \frac{2}{z}$ quindi $\frac{1}{x_0} \leq \frac{z}{2}$ e $-\frac{1}{x_0} \geq -\frac{z}{2}$

e $2 - \frac{1}{x_0} \geq 2 - \frac{z}{2} > 2 - z = m$. Avremmo quindi trovato un elemento di S strettamente maggiore di un suo maggiorante, assurdo. L'assurdo deriva dall'aver supposto $\sup S < 2$.

Esercizio 4.16 *Sia* $S = \{y \in \mathbb{R} \mid y = \frac{1}{x},\ x \in \mathbb{R},\ x > 3\}$. *Dire se* S *è limitato inferiormente e/o superiormente ed in caso affermativo, calcolare* $\inf S$, $\sup S$. *Dire inoltre se* S *ammette un minimo e/o un massimo.*

Soluzione: Se $0 < 3 < x$, allora $0 < y = \frac{1}{x} < \frac{1}{3}$ per ogni $y \in S$. Quindi 0 appartiene all'insieme Min dei minoranti di S e $\frac{1}{3}$ appartiene all'insieme Mag dei maggioranti di S. Ne segue che sono definiti sia $\sup S$ che $\inf S$.
Affermo che $0 = \inf S$. Poché 0 appartiene all'insieme Min se per assurdo $0 \neq \max Min$, avrei che $\max Min = t$ con $t > 0$. Per tale t deve valere $0 < t < \frac{1}{3}$, altrimenti avrei $t \geq \frac{1}{3} > \frac{1}{4} \in S$ mentre t è un minorante di S. Quindi, prendendo $\bar{x} = \frac{2}{t} = 2 \cdot \frac{1}{t} > 3$ (posso farlo perché t non è nullo) ho che $\frac{1}{\bar{x}} \in S$ e che $\frac{1}{\bar{x}} = \frac{t}{2} < t$, assurdo perché avevo supposto che $t \in Min$. L'assurdo deriva dall'aver supposto che $infS \neq 0$. Tale estremo inferiore non è un minimo di S perché $0 \notin S$.

Affermo ora che $supS = \frac{1}{3}$. Sicuramente $\frac{1}{3} \in Mag$, quindi $\min Mag \leq \frac{1}{3}$. Supponiamo per assurdo che tale minimo sia $l \in \mathbb{R}$ con l strettamente minore di $\frac{1}{3}$. Sicuramente $l > 0$ altrimenti avrei $l \leq 0 \leq y$ per ogni $y \in S$. Allora so che esiste $q \in \mathbb{Q} \subset \mathbb{R}$ tale che $l < q < \frac{1}{3}$. Ponendo $x_0 = \frac{1}{q} > 3$ ottengo che $q \in S$ e $q > l$ quindi $l \notin Mag$, assurdo. L'assurdo deriva dall'aver supposto che l'elemento minimo di Mag fosse strettamente minore di $\frac{1}{3}$. Quindi $\sup S = \frac{1}{3}$, che non è un minimo perché non appartiene ad S ($3 \not> 3$).

Esercizio 4.17 *Sia* S *come nell'Esempio 4.15. Dire se* S *è limitato inferiormente e, in caso affermativo, calcolare* $\inf S$. *Dire inoltre se* S *ammette un minimo. Cosa succede se prendiamo*

$$S' = \left\{ y \in \mathbb{R} \mid y = \frac{2x-1}{x},\ x > 2 \right\}$$

5 Richiami di trigonometria

Dato un punto P nel piano cartesiano, esso è individuato dalle sue coordinate, ovvero dalla sua ascissa e la sua ordinata, oppure da altri due dati: la sua distanza dall'origine degli assi O e l'angolo orientato θ che la retta passante per O e per P forma con l'asse delle ascisse. In particolare, se prendiamo il punto P sul disco di centro O e raggio 1, le sue coordinate dipenderanno solo dall'angolo θ. Chiameremo $\cos\theta$ e $\sin\theta$ rispettivamente l'ascissa e l'ordinata del punto P.

Esempio 5.1 *Dalla definizione di* $\sin\theta$ *e* $\cos\theta$ *segue che* $\sin\pi = 0$, $\cos\pi = -1$, $\sin\frac{\pi}{3} = \frac{\sqrt{3}}{2}$, $\cos\frac{5\pi}{4} = -\frac{\sqrt{2}}{2}$.

Per quanto abbiamo appena visto, cos e sin possono essere viste come funzioni da $\mathbb{R}$ in $\mathbb{R}$. Dalla definizione segue inoltre che l'immagine delle funzioni seno e

coseno è l'intervallo $[-1,\,1] = \{x \in \mathbb{R} \mid -1 \leq x \leq 1\}$. Tali funzioni sono legate tra loro da una serie di relazioni:

$$\sin(\theta) = \sin(\pi - \theta), \quad \text{per ogni } \theta \in \mathbb{R};$$

$$\cos(\theta) = \cos(-\theta), \quad \text{per ogni } \theta \in \mathbb{R};$$

$$\sin(\theta) = \sin(\theta + 2k\pi) \quad \text{per ogni } \theta \in \mathbb{R},\, k \in \mathbb{Z};$$

$$\cos(\theta) = \cos(\theta + 2k\pi) \quad \text{per ogni } \theta \in \mathbb{R} \text{ e } k \in \mathbb{Z};$$

che derivano da come abbiamo definito le funzioni seno e coseno;

$$\sin^2(\theta) + \cos^2(\theta) = 1, \quad \text{per ogni } \theta \in \mathbb{R}$$

che segue dal Teorema di Pitagora;

$$\sin(\theta + \eta) = \sin(\theta)\cos(\eta) + \sin(\eta)\cos(\theta) \quad \text{per ogni } \eta, \theta \in \mathbb{R};$$

$$\cos(\theta + \eta) = \cos(\theta)\cos(\eta) - \sin(\eta)\sin(\theta) \quad \text{per ogni } \eta, \theta \in \mathbb{R}.$$

Altre funzioni trigonometriche sono:

- $\tan\theta = \frac{\sin\theta}{\cos\theta}$, la funzione tangente, definita per $\theta \neq \frac{\pi}{2} + 2k\pi$. Essa è il coefficiente angolare m della retta di equazione $y = mx$ e passante sia per O che per il punto di coordinate $(\cos\theta, \sin\theta)$;
- $\cot\theta = \frac{\cos\theta}{\sin\theta}$, la funzione cotangente, definita per $\theta \neq k\pi$.

Esempio 5.2 *Calcolare il valore della funzione seno nel punto* $-\frac{\pi}{12}$.
Soluzione: Poiché $-\frac{1}{12} = \frac{1}{4} - \frac{1}{3}$, avremo

$$\sin\left(-\frac{\pi}{12}\right) = \sin\left(\frac{\pi}{4} - \frac{\pi}{3}\right)$$

Per la formula del seno della somma di due angoli tale numero è uguale a:

$$\begin{aligned}
&\sin\left(\frac{\pi}{4}\right)\cos\left(-\frac{\pi}{3}\right) + \sin\left(-\frac{\pi}{3}\right)\cos\left(\frac{\pi}{4}\right) \\
&= \sin\left(\frac{\pi}{4}\right)\cos\left(\frac{\pi}{3}\right) - \sin\left(\frac{\pi}{3}\right)\cos\left(\frac{\pi}{4}\right) \\
&= \frac{\sqrt{2}}{2}\cdot\frac{1}{2} - \frac{\sqrt{3}}{2}\cdot\frac{\sqrt{2}}{2} = \frac{\sqrt{2}-\sqrt{6}}{4}.
\end{aligned}$$

Esempio 5.3 *Calcolare per quali* $z \in \mathbb{R}$ *si ha* $\cos z = \frac{\sqrt{3}}{2}$ *e* $\sin z = -\frac{1}{2}$.

Soluzione: Poiché il coseno è positivo ed il seno è negativo, l'angolo si trova nel quarto quadrante. Il triangolo avente vertici nei punti O, P di coordinate $\left(\frac{\sqrt{3}}{2}, -\frac{1}{2}\right)$ e Q di coordinate $\left(\frac{\sqrt{3}}{2}, \frac{1}{2}\right)$ è equilatero (tutti i lati hanno lunghezza 1). L'asse delle ascisse biseca l'angolo $P\hat{O}Q$ che ha ampiezza $\frac{\pi}{3}$. L'angolo tra la retta passante per O e Q e l'asse delle ascisse avrà quindi ampiezza $\frac{\pi}{6}$. Poichè cerchiamo un angolo nel quarto quadrante, $z = -\frac{\pi}{6}$ è una soluzione. Tutte le altre soluzioni sono della forma $z = -\frac{\pi}{6} + 2k\pi$, con $k \in \mathbb{Z}$.

Esercizio 5.4 *Calcolare il valore delle seguenti funzioni trigonometriche nei seguenti punti:*

1. $\sin x$, $x = \frac{\pi}{6}$;
2. $\cos x$, $x = \frac{19\pi}{12}$;
3. $\tan x$, $x = \frac{19\pi}{12}$ *(usare la parte precedente);*
4. $\cot x$, $x = \frac{43\pi}{6}$.

Esercizio 5.5 *Calcolare tutti gli angoli x per i quali* $\cos x = -\frac{\sqrt{2}}{2}$ *e* $\sin x = -\frac{\sqrt{2}}{2}$.

6 Funzioni ed applicazioni

Nelle note di Silvio Valentini

7 I numeri complessi

Non tutte le equazioni del tipo $ax^2 + bX + c = 0$ con $a \neq 0$, $a, b, c \in \mathbb{R}$ ammettono soluzione in $\mathbb{R}$. Ad esempio, $X^2 + c = 0$ ammette soluzione se e solo se $c \leq 0$. Per tale motivo si è introdotto un altro insieme numerico, l'insieme $\mathbb{C}$ dei numeri complessi. I suoi elementi sono della forma $z = a + ib$ con $a, b \in \mathbb{R}$ ed i è un numero tale che $i^2 = -1$. Il numero reale a è detto *parte reale* di z, mentre b è detto *parte immaginaria* di z. Identificheremo il numero complesso con parte immaginaria nulla $z = a + 0i$, con il numero reale a, cioè con la sua parte reale.
In $\mathbb{C}$ possiamo definire operazioni di somma e prodotto utilizzando il prodotto in $\mathbb{R}$ e le regole: $i^2 = -1$, $ia = ai$ se $a \in \mathbb{R}$. Avremo allora:

$$(a + ib) + (c + id) = (a + c) + i(b + d)$$

$$(a + ib)(c + id) = ac + iad + ibc + i^2bd = (ac - bd) + i(ad + bc).$$

Tali operazioni godono delle seguenti proprietà:

1. $a + b = b + a$ per ogni $a, b \in \mathbb{C}$ (proprietà commutativa della somma);
2. $(a + b) + c = a + (b + c)$ per ogni $a, b, c \in \mathbb{C}$ (proprietà associativa della somma);
3. $0 + a = a$ per ogni $a \in \mathbb{C}$ (esistenza dell'elemento neutro per la somma, $0 = 0 + i0$);
4. per ogni $a \in \mathbb{C}$ esiste $b = (-a) \in \mathbb{C}$ tale che $a + b = 0$ (esistenza dell'elemento opposto);
5. $a(b + c) = ab + ac$ per ogni $a, b, c \in \mathbb{C}$ (proprietà distributiva);

6. $(ab)c = a(bc)$ per ogni a, b, $c \in \mathbb{C}$ (proprietà associativa del prodotto);

7. $ab = ba$ per ogni a, $b \in \mathbb{C}$ (proprietà commutativa del prodotto);

8. $1a = a$ per ogni $a \in \mathbb{C}$ (esistenza dell'elemento neutro per il prodotto $1 = 1 + i0$);

9. dati a, $b \in \mathbb{C}$, se $ab = 0$ allora $a = 0$ e/o $b = 0$ ($\mathbb{C}$ è privo di divisori dello zero);

10. Per ogni $z \in \mathbb{C} \setminus \{0\}$ esiste $w \in \mathbb{C}$ tale che $zw = 1$ (tutti gli elementi *non nulli* di $\mathbb{C}$ sono invertibili).

L'ultima proprietà enunciata segue dalla seguente osservazione: se $z = a+ib$ allora $z(a - ib) = (a + ib)(a - ib) = a^2 + b^2$ è un numero reale non negativo, ed, essendo somma di due numeri non negativi, esso è 0 se e soltanto se $a = b = 0$, ovvero se e soltanto se $z = 0$. Se $z \neq 0$ avremo

$$z\frac{(a - ib)}{(a^2 + b^2)} = (a + ib)\left(\frac{a}{(a^2 + b^2)} - i\frac{b}{(a^2 + b^2)}\right) = 1$$

quindi z è invertibile.

Motivati da questa osservazione, osserviamo che, ad ogni un numero complesso $z = a + ib$, possiamo associare il numero complesso $\bar{z} = a - ib$, detto il *coniugato* di z, ed il numero reale non negativo $|z| = \sqrt{z\bar{z}} = \sqrt{a^2 + b^2}$, detto *modulo di* z. Se $z \neq 0$, si ha:

$$z^{-1} = \frac{\bar{z}}{|z|^2}.$$

Esempio 7.1 *Il coniugato dell'elemento* $z = \frac{\sqrt{3}}{8} - i\frac{1}{8}$ *è* $\bar{z} = \frac{\sqrt{3}}{8} + i\frac{1}{8}$*; il modulo di* z *è*

$$|z| = \sqrt{\frac{3}{64} + \frac{1}{64}} = \sqrt{\frac{4}{64}} = \sqrt{\frac{1}{16}} = \frac{1}{4}$$

e l'inverso di z *è*

$$z^{-1} = \frac{\bar{z}}{|z|^2} = \frac{\frac{\sqrt{3}}{8} + i\frac{1}{8}}{\frac{1}{16}} = \frac{\frac{\sqrt{3}}{8}}{\frac{1}{16}} + i\frac{\frac{1}{8}}{\frac{1}{16}} = 2\sqrt{3} + 2i.$$

Il modulo di un numero complesso, ed il complesso coniugato godono delle seguenti proprietà:

1. $\overline{(x \pm y)} = \overline{x} \pm \overline{y}$ per ogni x, $y \in \mathbb{C}$, ovvero il coniugato della somma (rispettivamente della differenza) è la somma (rispettivamente la differenza) dei coniugati;

2. $\overline{(xy)} = \overline{x}\,\overline{y}$ per ogni x, $y \in \mathbb{C}$, ovvero il coniugato del prodotto è il prodotto dei coniugati;

3. $\overline{(\bar{z})} = z$ per ogni $z \in \mathbb{C}$, ovvero il coniugato del coniugato di un numero complesso coincide con il numero dato;

4. dato $z \in \mathbb{C}$, z è reale se e solo se $z = \bar{z}$.

5. $|z| \in \mathbb{R}$ e $|z| \geq 0$ per ogni $z \in \mathbb{C}$ (il modulo è sempre un numero reale non negativo);

6. $|z| = 0$ se e soltanto se $z = 0 + i0$;

7. $|z| = |\bar{z}|$ per ogni $z \in \mathbb{C}$ (il modulo di un numero complesso coincide con il modulo del suo coniugato);

8. $|zw| = |z||w|$ (il modulo del prodotto è uguale al prodotto dei moduli);

9. $z^2 = |z|^2$ se e soltanto se $z \in \mathbb{R}$;

10. Se $z \in \mathbb{R}$, allora $|z|$ coincide con il valore assoluto precedentemente introdotto su $\mathbb{R}$.

Esercizio 7.2 *Verificare le proprietà del coniugio e del modulo per un numero complesso $z = a + ib$.*

Esercizio 7.3 *Esprimere nella forma $a + ib$ con $a, b \in \mathbb{R}$ i seguenti numeri complessi:*

1. $(3 - i)(5 + 2i)$;
2. $(3 + 4i)\overline{(2 - i)}$;
3. $\frac{1}{(2-2i)}$;
4. $\frac{(2-9i)}{(5+i)}$;

Il modulo ed il coniugato di un numero complesso hanno un'interpretazione geometrica. Possiamo infatti identificare i numeri complessi con i punti del piano cartesiano, che in questo caso chiameremo piano di Gauss, ponendo il numero complesso $z = a + ib$ nel punto del piano di ascissa a e di ordinata b. Allora $|z|$ è la distanza di z dall'origine, mentre $\bar{z}$ si ottiene riflettendo il punto z rispetto all'asse delle ascisse. L'angolo che la retta passante per 0 e z forma con l'asse delle ascisse è detto *l'argomento* di z. Tale angolo è determinato a meno di multipli di 2π. Chiameremo *argomento principale* di z, l'argomento θ di z tale che $0 \leq \theta < 2\pi$.

Come si determina tale angolo? Osserviamo che, se $z = a+ib$, allora $z' = \frac{z}{|z|}$ ha modulo 1, e si trova sulla retta passante per 0 e per z (il rapporto tra la sua ordinata e la sua ascissa è uguale al rapporto tra l'ordinata e l'ascissa di z). Quindi z' si trova sulla circonferenza di raggio 1 ed ha lo stesso argomento, che chiameremo θ, di z. Dalle nozioni di trigonometria ricaviamo che

$$\frac{a}{|z|} + i\frac{b}{|z|} = \frac{z}{|z|} = z' = \cos\theta + i\sin\theta$$

perciò, uguagliando ascisse tra loro ed ordinate tra loro, abbiamo:

$$\frac{a}{|z|} = \cos\theta, \qquad \frac{b}{|z|} = \sin\theta$$

quindi l'argomento principale θ di z è l'angolo compreso tra 0 e 2π con coseno e seno dati dalle formule soprastanti. Grazie all'identificazione dei punti del piano cartesiano con gli elementi di $\mathbb{C}$, possiamo osservare che un numero complesso z non nullo è completamente determinato dal suo modulo $|z|$ ed un suo argomento $\theta = \arg(z)$: Si ha inoltre:

$$z = |z|(\cos\theta + i\sin\theta).$$

Tale espressione viene detta *forma polare di z*.

Esercizio 7.4 *Scrivere in forma polare i seguenti numeri complessi:*

1. $z = 2\sqrt{3} - 2i$;
2. $w = \frac{(4-4i)}{(\sqrt{3}-i)}$;
3. $y = -5 + 5i$;

La forma polare di un numero complesso "si comporta bene rispetto al prodotto": se $z = |z|(\cos\theta + i\sin\theta)$ e $w = |w|(\cos\eta + i\sin\eta)$, allora avremo

$$zw = |z||w|(\cos\theta + i\sin\theta)(\cos\eta + i\sin\eta)$$

$$= |z||w|((\cos\theta\cos\eta - \sin\theta\sin\eta) + i(\sin\theta\cos\eta + \cos\theta\sin\eta)).$$

Dalle formule del seno e del coseno della somma di due angoli, otteniamo:

$$zw = |z||w|(\cos(\theta+\eta) + i\sin(\theta+\eta))$$

ovvero: il prodotto di due numeri complessi è il numero complesso avente per modulo il prodotto dei moduli dei numeri dati e per argomento la somma degli argomenti dei numeri dati. In particolare, da questa formula deduciamo facilmente la forma polare dell'inverso di un numero complesso $z \neq 0$: si ha

$$zz^{-1} = |z||z^{-1}|(\cos(\arg(z) + \arg(z^{-1})) + i\sin(\arg(z) + \arg(z^{-1}))) =$$

$$= 1 = |1|(\cos 0 + i\sin 0)$$

perciò $|z^{-1}| = |z|^{-1}$ e $\arg(z^{-1}) = -\arg(z)$.

Esercizio 7.5 *Verificare che* $\arg(\bar{z}) = -\arg z$ *per ogni* $z \neq 0$.

Un'ulteriore conseguenza della formula del prodotto in forma polare è la formula di de Moivre per la potenza di un numero complesso: dato $z \in \mathbb{C}$ ed $n \in \mathbb{N}$, si può calcolare la potenza n-esima di z, overo $\underbrace{z \cdots z \cdots z}_{n \text{ volte}}$

$$z^n = |z|^n(\cos(n \arg z) + i \sin(n \arg z)).$$

Utilizzando sia la formula di de Moivre che la forma polare dell'inverso, possiamo anche calcolare le potenze *negative* di un numero complesso $z \neq 0$:

$$z^{-n} = |z|^{-n}(\cos(n \arg z) - i \sin(n \arg z)).$$

Per quest'ultima uguaglianza abbiamo usato il fatto che $z^{-n} = (z^{-1})^n$ e che $\cos(-\theta) = \cos\theta$.

Esercizio 7.6 *Si calcolino, utilizzando la formula di De Moivre, i seguenti numeri complessi:*

1. $(-5 + 5i)^6$;
2. $(\sqrt{3} - i)^{10}$;
3. $3(\cos 10^\circ - i \sin 10^\circ)^3$;
4. $(5 + 5\sqrt{3})^{-3}$.

Osserviamo che, se $z = a + i0$, allora in $\mathbb{C}$ possiamo sempre estrarre la radice quadrata di z: infatti se $a > 0$, avremo $(\pm\sqrt{a})^2 = a$, se $a = 0$ avremo $0^2 = 0$, se $a < 0$ allora $-a > 0$ e $(i\sqrt{-a})^2 = (-i\sqrt{-a})^2 = a$. Osserviamo che in questo caso, le radici di $z = a + i0$ sono reali, oppure complesse e coniugate. In realtà si può dire molto di più perché la formula di de Moivre può essere utilizzata anche per calcolare le radici n-esime di un numero complesso z. Per ogni numero naturale non nullo n possiamo calcolare tutti i numeri $w \in \mathbb{C}$ tali che $w^n = z$. Infatti, data la forma polare di un numero complesso fissato $z = |z|(\cos\theta + i \sin\theta)$ se w è un numero complesso tale che $w^n = z$, allora la sua forma polare $w = |w|(\cos\alpha + i \sin\alpha)$ deve essere tale che

- $|w|^n = |z|$
- $n\alpha = \theta + 2k\pi$ per qualche $k \in \mathbb{Z}$ (ricordate che l'argomento di un numero complesso è determinato solo a meno di multipli interi di 2π).

Pertanto $|w| = |z|^{\frac{1}{n}}$ e $\alpha = \frac{\theta}{n} + \frac{2k\pi}{n}$, con $k \in \mathbb{Z}$. Ora, osserviamo che, prendendo $k = 0, 1, \ldots, n-1$, i numeri:

$$w_k = |z|^{\frac{1}{n}} \left(\cos\left(\frac{\theta}{n} + \frac{2k\pi}{n}\right) + i \sin\left(\frac{\theta}{n} + \frac{2k\pi}{n}\right)\right)$$

sono tutti diversi tra loro. Pertanto esistono almeno n radici n-esime distinte del numero z. D'altra parte, qualsiasi altro intero l può essere scritto come $l = mn + r$ (divisione con il resto in $\mathbb{Z}$) con $r = 0, 1, \ldots, n-1$. Quindi $\frac{2l\pi}{n} = \frac{(2mn\pi)+2r\pi}{n} = \frac{2r\pi}{n} + 2m\pi$ con $m \in \mathbb{Z}$. Ne segue che

$$w_l = |z|^{\frac{1}{n}} \left(\cos\left(\frac{\theta}{n} + \frac{2l\pi}{n}\right) + i \sin\left(\frac{\theta}{n} + \frac{2l\pi}{n}\right)\right) = w_r.$$

Ne deduciamo che le radici n-esime di z coincidono con tutti e soli i numeri complessi che si possono scrivere nella forma

$$w_k = |z|^{\frac{1}{n}} \left(\cos\left(\frac{\theta}{n} + \frac{2k\pi}{n}\right) + i \sin\left(\frac{\theta}{n} + \frac{2k\pi}{n}\right)\right), \quad k = 0, 1, \ldots, n-1.$$

In particolare, per ogni numero complesso non nullo z e per ogni numero naturale n non nullo, z ha esattamente n radici n-esime in $\mathbb{C}$.

Esercizio 7.7 *Si determinino tutti i numeri complessi tali che:*

1. $w^3 = i$;
2. $z^5 = \frac{(2-2\sqrt{3}i)}{(3-i)}$;
3. $y^3 = 1 - i$.

Esercizio 7.8 *Calcolare le radici quadrate di un numero della forma $z = a + i0$ già descritte in precedenza, utilizzando la formula delle radici n-esime.*

Come conseguenza della formula sulle radici n-esime, sappiamo che è possibile estrarre la radice quadrata di un qualsiasi numero complesso ponendo $n = 2$ nella formula. Questo vuol dire che, *tutte le equazioni di secondo grado $aX^2 + bX + c = 0$ con coefficienti in $\mathbb{C}$ ($a \neq 0$), hanno soluzioni in $\mathbb{C}$*. Infatti, utilizzando la formula delle soluzioni

$$y_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

poiché in $\mathbb{C}$ è sempre possibile estrarre la radice quadrata di un elemento, tali soluzioni saranno sempre elementi di $\mathbb{C}$.

Esercizio 7.9 *Calcolare le soluzioni dell'equazione: $iX^2 - X + \frac{\sqrt{3}}{4} = 0$.*
(Soluzioni: $w_1 = \frac{\sqrt{6}}{4} + i\left(\frac{\sqrt{2}-2}{4}\right)$, $w_2 = -\frac{\sqrt{6}}{4} - i\left(\frac{\sqrt{2}+2}{4}\right)$).

In realtà vale un teorema molto più forte:

Teorema 7.10 *(Teorema fondamentale dell'algebra) Tutte le equazioni algebriche della forma $a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 = 0$ con $a_n \neq 0$ e $n \neq 0$ ammettono soluzione in $\mathbb{C}$.*

8 Polinomi

Sia S l'insieme $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ oppure $\mathbb{C}$.
Un polinomio a coefficienti in S nell'indeterminata X è un'espressione della forma

$$p(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$$

con $a_i \in S$ (gli a_i sono detti i *coefficienti di* $p(X)$). Il polinomio nullo è il polinomio che ha tutti i coefficienti nulli e lo denoteremo con 0. Il grado di un polinomio non nullo $p(X)$ è il massimo numero n per il quale $a_n \neq 0$ (cioè l'esponente della potenza più alta di X che compare con coefficiente non nullo) e sarà denotato con $\deg(p(X))$. Un polinomio di grado zero è anche detto polinomio costante. Denoteremo con il simbolo 1 il polinomio costante con $a_0 = 1$.

Denoteremo con $S[X]$ l'insieme dei polinomi a coefficienti nell'insieme S. In $S[X]$ possiamo introdurre operazioni di somma e prodotto: dati

$$p(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 = \sum_{j=0}^{n} a_j X^j$$

$$q(X) = b_m X^m + b_{m-1} X^{m-1} + \cdots + b_1 X + b_0 = \sum_{j=0}^{m} b_j X^j$$

avremo

$$p + q = \sum_{j=0}^{\max\{m,\, n\}} (a_j + b_j) X^j$$

$$pq = \sum_{j=0}^{n+m} \left(\sum_{k=0}^{j} a_k b_{j-k} \right) X^j$$

(qui se $k > m$, $b_k = 0$ ed analogamente per a_j). Tali operazioni godono delle seguenti proprietà:

1. $p + q = q + p$ per ogni p, $q \in S[X]$ (proprietà commutativa della somma);
2. $(p + q) + r = p + (q + r)$ per ogni p, q, $r \in S[X]$ (proprietà associativa della somma);
3. $0 + p = p$ per ogni $p \in S[X]$ (esistenza dell'elemento neutro per la somma);
4. dato $p \in S[X]$ esiste $q = -p \in S[X]$ tale che $q + p = 0$ (esistenza dell'elemento opposto);
5. $(pq)r = p(qr)$ per ogni p, q, $r \in S[X]$ (proprietà associativa del prodotto);
6. $p(q + r) = pq + pr$ per ogni p, q, $r \in S[X]$ (proprietà distributiva);
7. $pq = qp$ per ogni p, $q \in S[X]$ (proprietà commutativa del prodotto);
8. $1a = a$ per ogni $p \in S[X]$ (esistenza dell'elemento neutro per il prodotto);
9. $\deg(p + q) = \max(\deg p, \deg q)$ per ogni p, $q \in S[X]$ p, $q \neq 0$;
10. $\deg(pq) = \deg(p) + \deg(q)$ per ogni p, $q \in S[X]$, p, $q \neq 0$;
11. Dati p, $q \in S[X]$, se $pq = 0$ allora $p = 0$ e/o $q = 0$ ($S[X]$ è privo di divisori dello 0);

12. $p(X)q(X) = 1$ se e solo se $p(X) = p_0$, $q(X) = q_0$ hanno grado 0 e $p_0 q_0 = 1$ in S.

Anche in $S[X]$ è possibile effettuare la divisione con il resto:

Proposizione 8.1 *Dati f, $g \in S[X]$ con $S = \mathbb{C}, \mathbb{R}, \mathbb{Q}$ esistono sempre due polinomi q, r con $r = 0$ oppure $\deg r < \deg g$ per i quali $f = gq + r$.*

Esempio 8.2 *Calcolare quoziente e resto dei due polinomi $f = 3X^3 - 2X^2 + X + 4$ e $g = X^2 - 1$ in $\mathbb{Q}[X]$.*

Soluzione: Costruiamo, termine per termine il polinomio q, a partire dal grado più alto:

$$\begin{array}{l|l} 3X^3 - 2X^2 + X + 4 & X^2 - 1 \\ \hline & 3X + \cdots \end{array}$$

Abbiamo posto $3X$ perché $\tilde{f} = f - (3X)g = f - 3X^3 + 3X$ ha grado minore o uguale a 2, e quindi abbiamo "diminuito" il grado di f.

$$\begin{array}{llll|l} 3X^3 & -2X^2+ & X+ & 4 & X^2 - 1 \\ \hline 3X^3 & & -3X & & 3X + \cdots \end{array}$$

Qui abbiamo scritto sotto f, il polinomio $(3X)g$ incolonnato in modo da avere termini dello stesso grado nella stessa colonna. Ora *sottraiamo* alla riga corrispondente ad f la riga corrispondente a $(3X)g$:

$$\begin{array}{llll|l} 3X^3 & -2X^2+ & X+ & 4 & X^2 - 1 \\ \hline 3X^3 & & -3X & & 3X - 2 \\ & -2X^2 & +4X & +4 & \end{array}$$

e ripetiamo l'operazione. Abbiamo aggiunto un -2 perché $\tilde{f} - (-2)g$ ha grado minore o uguale ad 1. Scriviamo ora sotto la riga del polinomio $\tilde{f} = f - (3X)g$ il polinomio $(-2)g$.

$$\begin{array}{llll|l} 3X^3 & -2X^2+ & X+ & 4 & X^2 - 1 \\ \hline 3X^3 & & -3X & & 3X - 2 \\ & -2X^2 & +4X & +4 & \\ & -2X^2 & & +2 & \end{array}$$

e sottraiamo alla riga del polinomio $\tilde{f}$ il polinomio $(-2)g$ ottenendo $f-(3X-2)g$:

$$\begin{array}{llll|l} 3X^3 & -2X^2+ & X+ & 4 & X^2 - 1 \\ \hline 3X^3 & & -3X & & 3X - 2 \\ & -2X^2 & +4X & +4 & \\ & -2X^2 & & +2 & \\ & & 4X & +2 & \end{array}$$

Ora $q = 3X - 2$ ed $r = 4X + 2$.

Diremo che il polinomio g divide il polinomio f se il resto della divisione di f per g è 0. In tal caso diremo anche che g è un *fattore* di f.

Esercizio 8.3 *Calcolare quoziente e resto della divisione di f per g con*

1. $f = 6X^5 - 12X^3 + X-$, $g = 2X^3 - 3$ *in* $\mathbb{Q}[X]$;
2. $f = 6X^5 - 12X^3 + X-$, $g = 2X + 1$ *in* $\mathbb{Q}[X]$;
3. $f = X^3 - \sqrt{2}X + 1$, $g = X - \sqrt{3}$ *in* $\mathbb{R}[X]$;
4. $f = X^2 - iX + 2$, $g = \sqrt{3}X - 2i$ *in* $\mathbb{C}[X]$.

Ad un elemento $f = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in S[X]$ possiamo associare la *funzione polinomiale*

$$\begin{array}{rccc} \psi_f\colon & S & \longrightarrow & S \\ & z & \mapsto & a_nz^n + a_{n-1}z^{n-1} + \cdots + a_1z + a_0 \end{array}$$

Se $f = g \in S[X]$, allora la funzione ψ_f è uguale alla funzione ψ_g, vale a dire, per ogni $z \in S$, $\psi_f(z) = \psi_g(z)$. Se $f \in S[X]$ è un polinomio costante a_0, allora ψ_f è la funzione costante che associa a tutti i valori di S il valore a_0. Infine, per ogni coppia f, $g \in S[X]$ e per ogni $z \in S$ si ha: $\psi_{f+g}(z) = \psi_f(z) + \psi_g(z)$; $\psi_{fg}(z) = (\psi_f(z))(\psi_g(z))$.
Una *radice* di $f = a_0 + a_1X + \cdots + a_nX^n \in S[X]$ è un elemento $z \in S$ per il quale $\psi_f(z) = 0$. Sfruttando la divisione con il resto otteniamo il seguente risultato, noto come Teorema di Ruffini:

Teorema 8.4 *Sia $f \in S[X]$ non nullo e sia $z \in S$. Allora z è una radice di S se e soltanto se $(X - z)$ è un fattore di f.*

Dimostrazione: La divisione con il resto di f per $(X - z)$ dà

$$f = q(X - z) + r$$

con $r = 0$ oppure $\deg r < \deg(X - z) = 1$, cioè $r = r_0$ è un polinomio costante oppure è 0.
Se z è una radice di f, allora la funzione $\psi_f = \psi_{q(X-z)+r_0} = \psi_q\psi_{(X-z)} + \psi_{r_0}$ si annulla in z, ovvero $\psi_q(z)(z - z) + r_0 = r_0 = 0$, quindi il resto della divisione di f per $(X - z)$ è nullo ed $(X - z)$ divide f.
Se $(X - z)$ divide f allora $f = (X - z)q$, quindi $\psi_f = \psi_{(X-z)q} = \psi_{(X-z)}\psi_q$. Calcolando il valore di questa funzione in z vediamo che z è una radice di f. □

Il teorema di Ruffini ci aiuta nella ricerca delle radici di polinomi di grado superiore al secondo, se ne conosciamo almeno una radice, come nel seguente esempio:

Esempio 8.5 *Calcolare le radici reali del polinomio: $f = X^3 - 3X^2 - 13X + 15$.*

Soluzione: Poiché la somma dei coefficienti di questo polinomio è zero, 1 è una radice di f. Per il teorema di Ruffini $f = (X - 1)q$ per qualche polinomio $q \in \mathbb{R}[X]$. L'algoritmo di divisione ci fornisce $f = (X - 1)(X^2 - 2X - 15)$. Con la formula di risoluzione delle equazioni di secondo grado troviamo altre due radici: -3 e 5.

Esercizio 8.6 *Trovare le radici reali dei polinomi:* $f = X^3 - 6X^2 - 9X + 14$ *e* $g = X^3 - 10X^2 - 23X - 12$.

Come conseguenza del Teorema di Ruffini e della formula del grado di un prodotto di polinomi abbiamo il seguente corollario:

Corollario 8.7 *Ogni polinomio di grado n ha al più n radici.*

In particolare, una conseguenza del Teorema di Ruffini e del Teorema fondamentale dell'algebra (ogni polinomio non costante di $\mathbb{C}[X]$ ha una radice in $\mathbb{C}$) è il seguente Teorema:

Teorema 8.8 *Ogni elemento* f *di* $\mathbb{C}[X]$ *ammette una fattorizzazione del tipo* $f = c_0(X - c_1)\cdots(X - c_n)$ *dove i* $c_j \in \mathbb{C}$ *per* $j > 0$ *sono tutti e soli gli zeri di* f.

9 Disuguaglianze

Esercizio 9.1 *Determinare per quali valori reali valgono le seguenti disuguaglianze:*

1. $-3X + 6 > 0$;
2. $49X^2 - 14X + 1 < 0$;
3. $2X^2 + 2X - 12 \geq 0$;
4. $4X^2 - 25 < 0$;
5. $X^2 + 4X - 5 \leq 0$.

Soluzione:

1. $-3X + 6 = 3(-X + 2) > 0$ se e solo se $-X + 2 > 0$ se e solo se $X - 2 < 0$ se e solo se $X < 2$. Pertanto questa disuguaglianza è vera per ogni $z \in \mathbb{R}$ tale che $z < 2$.

2. Verifico se esistono numeri reali tali che $49X^2 - 14X + 1 = 0$. Con la formula delle soluzioni di un'equazione di secondo grado trovo le due soluzioni reali e coincidenti $\frac{2}{7}$. Pertanto

$$49X^2 - 14X + 1 = 49\left(x - \frac{2}{7}\right)\left(x - \frac{2}{7}\right) = 49\left(x - \frac{2}{7}\right)^2 \geq 0$$

   perché è un quadrato. Pertanto non esiste alcun valore reale per il quale $49X^2 - 14X + 1 < 0$.

3. Verifico se esistono numeri reali tali che $2X^2 + 2X - 12 = 0$. Con la formula delle soluzioni di un'equazione di secondo grado trovo le soluzioni $x = -3$ ed $x = 2$. Pertanto $2X^2 + 2X - 12 = 2(X + 3)(X - 2)$. Sostituendo ad X il valore reale z, otterremo un valore non negativo se $(z + 3) \geq 0$ e $(z - 2) \geq 0$, oppure se $(z + 3) \leq 0$ e $(z - 2) \leq 0$. La primo coppia di disuguaglianze si verifica se $z \geq \max\{2, -3\} = 2$, la seconda si verifica se $z \leq \min\{2, -3\} = -3$. Pertanto $2z^2 + 2z - 12 \geq 0$ per $z \geq 2$ o $z \leq -3$.

4. L'espressione si decompone come prodotto: $4X^2 - 25 = (2X - 5)(2X + 5)$. Sostituendo ad X il valore reale z, otterremo un valore negativo se $(2z - 5) < 0$ e $(2z + 5) > 0$, oppure se $(2z - 5) > 0$ e $(2z + 5) < 0$. La prima coppia di disuguaglianze è verificata se $z < \frac{5}{2}$ e $z > -\frac{5}{2}$, la seconda coppia di disuguaglianze non è mai verificata. Pertanto $4z^2 - 25 < 0$ per tutti i valori $z \in \mathbb{R}$ tali che $-\frac{5}{2} < z < \frac{5}{2}$.

5. Verifico se esistono numeri reali tali che $X^2 + 4X - 5 = 0$. Con la formula delle soluzioni di equazioni di secondo grado trovo le soluzioni $x = -5$ ed $x = 1$. Pertanto $X^2 + 4X - 5 = (X - 1)(X + 5)$. Sostituendo ad X il valore reale z, otterremo $(z - 1)(z + 5) \leq 0$ se $(z - 1) \leq 0$ e $(z + 5) \geq 0$ oppure se $(z - 1) \geq 0$ e $(z + 5) \leq 0$. La prima coppia di disuguaglianze è verificata se $-5 \leq z \leq 1$ mentre la seconda coppia di disuguaglianze non è mai verificata. Pertanto $X^2 + 4X - 5 \leq 0$ per tutti i valori reali z tali che $-5 \leq z \leq 1$.

Esercizio 9.2 *Determinare per quali valori $x \in \mathbb{R}$ valgono le seguenti disuguaglianze:*

1. $-5X + 2 > 0$;
2. $4X^2 - 12X + 9 \leq 0$;
3. $X^2 + X - 6 \geq 0$;
4. $3X^2 + 7 < 0$;
5. $X^2 + 4X - 5 \leq 0$.