I NUMERI INTERI

ALBERTO CANONACO

26 settembre 2018

0. Preliminari

Indichiamo con $\mathbb{N} = \{0, 1, \dots\} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ gli insiemi dei numeri naturali, interi, razionali, reali e complessi. Richiamiamo qui brevemente alcune proprietà aritmetiche di questi insiemi numerici, che si assumono già note.

Su $\mathbb{C}$ sono definite le operazioni di somma e prodotto

$$\begin{aligned} +\colon \mathbb{C} \times \mathbb{C} &\to \mathbb{C} & \times\colon \mathbb{C} \times \mathbb{C} &\to \mathbb{C} \\ (a, b) &\mapsto a + b & (a, b) &\mapsto a \times b = a \cdot b = ab \end{aligned}$$

che verificano le seguenti proprietà per ogni $a, b, c \in \mathbb{C}$:

associatività della somma: $a + (b + c) = (a + b) + c$;
commutatività della somma: $a + b = b + a$;
elemento neutro della somma: $a + 0 = a$;
inverso additivo o opposto: esiste $-a \in \mathbb{C}$ tale che $-a + a = 0$;
associatività del prodotto: $a(bc) = (ab)c$;
commutatività del prodotto: $ab = ba$;
elemento neutro del prodotto: $a1 = a$;
inverso (moltiplicativo): se $a \neq 0$, esiste $a^{-1} \in \mathbb{C}$ tale che $a^{-1}a = 1$;
distributività: $a(b + c) = ab + ac$.

Si dice allora che $\mathbb{C}$ è un *campo*.

Ciascuno dei sottoinsiemi di $\mathbb{C}$ indicati sopra è chiuso rispetto a somma e prodotto (cioè, se A è uno tra $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $a, b \in A$, allora $a + b, ab \in A$). Inoltre $\mathbb{Q}$ e $\mathbb{R}$ verificano tutte le proprietà elencate sopra (dunque sono anche loro campi). Invece $\mathbb{Z}$ verifica tutte le proprietà tranne quella dell'inverso moltiplicativo (solo 1 e -1 hanno un inverso moltiplicativo in $\mathbb{Z}$), e viene allora detto *anello commutativo*.[1] Infine, $\mathbb{N}$ verifica tutte le proprietà tranne quelle degli inversi (solo 0 ha un opposto in $\mathbb{N}$).

Osservazione 0.1. Ci sono altre proprietà ben note che potranno essere usate in seguito, ma che non sono state qui ricordate perché sono conseguenze formali di quelle elencate (come si vedrà studiando gli anelli). Per esempio, si ha $a0 = 0$ per ogni elemento a di un anello (e quindi non avrebbe senso richiedere l'esistenza dell'inverso moltiplicativo anche per 0), e $ab = 0$ implica $a = 0$ o $b = 0$ in un campo (e quindi anche in un suo sottoinsieme).

Osservazione 0.2. Anche se non seguiamo questo approccio, è bene sapere che è possibile, partendo da pochi assiomi fondamentali di teoria degli insiemi, definire rigorosamente sia i vari insiemi numerici, che le operazioni di

[1] La parola commutativo si riferisce alla commutatività del prodotto.

somma e prodotto su di essi, e dimostrare che effettivamente valgono le proprietà richiamate sopra. In particolare, si può definire $\mathbb{N}$ assiomaticamente (vedi l'Osservazione 0.3). Si costruisce poi $\mathbb{Z}$ a partire da $\mathbb{N}$ "aggiungendo formalmente gli opposti" (il che implica tra l'altro che ogni intero è della forma $a - b := a + (-b)$ con $a, b \in \mathbb{N}$). Analogamente, si costruisce $\mathbb{Q}$ a partire da $\mathbb{Z}$ "aggiungendo formalmente gli inversi (degli interi non nulli)" (il che implica tra l'altro che ogni razionale è della forma $\frac{a}{b} := ab^{-1}$ con $a, b \in \mathbb{Z}$ e $b \neq 0$). La costruzione di $\mathbb{R}$ a partire da $\mathbb{Q}$ ha invece motivazioni più analitico-topologiche che algebriche. Infine, si costruisce $\mathbb{C}$ a partire da $\mathbb{R}$ "aggiungendo formalmente $\sqrt{-1}$".

Si useranno liberamente anche ben note proprietà delle relazioni di disuguaglianza tra numeri reali. In particolare, $\leq$ (e analogamente $\geq$) definisce su $\mathbb{R}$ (e quindi anche su ogni sottoinsieme di $\mathbb{R}$) una relazione d'ordine[2] totale.[3] Tale relazione "si comporta bene" rispetto alle operazioni di somma e prodotto, nel senso che per ogni $a, b, c \in \mathbb{R}$ si ha:

- $a \leq b$ (rispettivamente $a < b$) implica $a + c \leq b + c$ (rispettivamente $a + c < b + c$);
- $a \leq b$ e $c \geq 0$ (rispettivamente $a < b$ e $c > 0$) implica $ac \leq bc$ (rispettivamente $ac < bc$);
- $a \leq b$ e $c \leq 0$ (rispettivamente $a < b$ e $c < 0$) implica $ac \geq bc$ (rispettivamente $ac > bc$).

$(\mathbb{N}, \leq)$ ha anche l'importante proprietà di essere un insieme *ben ordinato*: questo significa che ogni sottoinsieme non vuoto A di $\mathbb{N}$ ammette minimo, cioè esiste (necessariamente unico) un elemento $\min(A) \in A$ tale che $\min(A) \leq a$ per ogni $a \in A$. Il fatto che $\mathbb{N}$ sia ben ordinato è anche detto *principio di buon ordinamento* (o *del minimo intero*) dei numeri naturali. Esso è essenzialmente equivalente al *principio di induzione*, secondo il quale, se $A \subseteq \mathbb{N}$ soddisfa:

- $0 \in A$;
- $n \in A$ implica $n + 1 \in A$;

allora $A = \mathbb{N}$.

Osservazione 0.3. Per la definizione assiomatica dei numeri naturali si usano di solito gli *assiomi di Peano*, che possono essere enunciati dicendo che $\mathbb{N}$ è un insieme dotato di una funzione $s \colon \mathbb{N} \to \mathbb{N}$ tale che:

- s è iniettiva;
- esiste $0 \in \mathbb{N}$ tale che $0 \neq s(n)$ per ogni $n \in \mathbb{N}$ (quindi s non è suriettiva);
- vale il principio di induzione, riformulato con $s(n)$ al posto di $n + 1$.

Partendo da tali assiomi è facile vedere che per ogni $n \in \mathbb{N} \setminus \{0\}$ esiste (unico) $m \in \mathbb{N}$ tale che $n = s(m)$. Si possono allora definire univocamente somma e prodotto su $\mathbb{N}$ tali che:

---

[2] Questo significa che valgono le proprietà riflessiva ($a \leq a$ per ogni $a \in \mathbb{R}$), antisimmetrica ($a \leq b$ e $b \leq a$ implica $a = b$ per ogni $a, b \in \mathbb{R}$) e transitiva ($a \leq b$ e $b \leq c$ implica $a \leq c$ per ogni $a, b, c \in \mathbb{R}$).

[3] Questo significa che $a \leq b$ o $b \leq a$ (quindi vale esattamente uno tra $a < b$, $a = b$ e $a > b$) per ogni $a, b \in \mathbb{R}$.

- $a + 0 = a$ e $a + s(b) = s(a + b)$ per ogni $a, b \in \mathbb{N}$;
- $a0 = 0$ e $as(b) = ab + a$ per ogni $a, b \in \mathbb{N}$.

Si dimostra poi che tali operazioni soddisfano le proprietà richiamate all'inizio. Analogamente, si dimostra che si può definire univocamente una relazione d'ordine (totale) su $\mathbb{N}$ tale che $n < s(n)$ per ogni $n \in \mathbb{N}$, e che in questo modo $\mathbb{N}$ risulta effettivamente ben ordinato. D'altra parte, è anche facile dimostrare che, se $\mathbb{N}$ è un insieme ben ordinato che soddisfa gli altri assiomi di Peano, e per ogni $n \in \mathbb{N} \setminus \{0\}$ esiste $m \in \mathbb{N}$ tale che $n = s(m)$ e $m < n$, allora vale anche il principio di induzione.

Introduciamo ora alcune notazioni che useremo spesso anche in seguito. Dati $A, B \subseteq \mathbb{Z}$, poniamo

$$A + B := \{a + b : a \in A, b \in B\} \subseteq \mathbb{Z}, \qquad -A := \{-a : a \in A\} \subseteq \mathbb{Z}.$$

Nel caso in cui $A = \{a\}$ sia costituito da un solo elemento, scriveremo anche $a + B$ invece di $\{a\} + B$.

A partire dal principio di buon ordinamento è facile dimostrare che, più in generale, se $A \subseteq \mathbb{Z}$ è non vuoto e limitato inferiormente (cioè esiste $k \in \mathbb{Z}$ tale che $k \leq a$ per ogni $a \in A$), allora esiste $\min(A)$: infatti si vede subito che $-k + A \subseteq \mathbb{N}$ e $\min(A) = k + \min(-k + A)$. Analogamente, se $A \subseteq \mathbb{Z}$ è non vuoto e limitato superiormente (cioè esiste $k \in \mathbb{Z}$ tale che $a \leq k$ per ogni $a \in A$), allora esiste il massimo di A (cioè un elemento $\max(A) \in A$ tale che $a \leq \max(A)$ per ogni $a \in A$): risulta in effetti che $-A$ è limitato inferiormente e $\max(A) = -\min(-A)$.

1. Divisibilità e divisione con resto

Definizione 1.1. Dati $a, b \in \mathbb{Z}$, si dice che a *divide* b (o che a è un *divisore* di b, o che b è *divisibile* per a, o che b è un *multiplo* di a) se esiste $c \in \mathbb{Z}$ tale che $b = ac$. Si usa la notazione $a \mid b$ se a divide b e $a \nmid b$ se a non divide b.

Indicheremo con

$$a\mathbb{Z} := \{an : n \in \mathbb{Z}\} \subseteq \mathbb{Z}$$

l'insieme dei multipli di a. Dunque, per definizione, $a \mid b$ se e solo se $b \in a\mathbb{Z}$.

È molto facile vedere che, per ogni $a, b, c \in \mathbb{Z}$, valgono le seguenti proprietà (che d'ora in poi saranno usate liberamente):

- $1 \mid a$ e $a \mid 0$;
- $0 \mid a$ se e solo se $a = 0$;
- $a \mid a$;
- $a \mid b$ se e solo se $(-a) \mid b$ se e solo se $a \mid (-b)$;
- se $a \mid b$ e $b \mid c$, allora $a \mid c$;
- se $a \mid b$ e $a \mid c$, allora $a \mid (mb + nc)$ per ogni $m, n \in \mathbb{Z}$;
- se $a \mid b$, allora $ac \mid bc$, e il viceversa vale se $c \neq 0$;
- se $a \mid b$ e $b \neq 0$, allora $|a| \leq |b|$;
- se $a \mid b$ e $b \mid a$, allora $|a| = |b|$.

Teorema 1.2. *Dati $a, b \in \mathbb{Z}$ con $b \neq 0$, esistono unici $q, r \in \mathbb{Z}$ tali che $a = qb + r$ e $0 \leq r < |b|$. Si dice che q è il* quoziente *e r il* resto *della divisione di a per b.*

Dimostrazione. Poiché $a = qb + r$ se e solo se $a = (-q)(-b) + r$, l'enunciato è vero per (a, b) se e solo se è vero per $(a, -b)$. Si può quindi supporre $b > 0$.

Dimostriamo prima l'esistenza di q e r. Sia

$$A = \{n \in \mathbb{N} : n = a - cb \text{ per qualche } c \in \mathbb{Z}\} \subseteq \mathbb{N}$$

e osserviamo che $A \neq \emptyset$. Infatti, prendendo per esempio $c = -|a|$, si ha (tenendo conto che $b \geq 1$)

$$n = a - cb = a + |a|b \geq a + |a| \geq 0,$$

dunque $n \in A$. Poniamo allora $r := \min(A)$ e sia $q \in \mathbb{Z}$ tale che $r = a - qb$ (un tale q esiste perché $r \in A$). Per definizione si ha quindi $a = qb + r$ e $r \geq 0$, e resta da dimostrare che $r < b$. Supponiamo per assurdo che $r \geq b$: si avrebbe $0 \leq r - b = a - (q + 1)b \in A$ e $r - b < r$, contraddicendo la minimalità di r.

Dimostriamo ora l'unicità di q e r. Sia dunque $a = qb + r = q'b + r'$ con $q, r, q', r' \in \mathbb{Z}$ tali che $0 \leq r, r' < b$, e dimostriamo che $q = q'$ e $r = r'$. Si ha infatti $r - r' = (q' - q)b$, da cui segue che $b \mid (r - r')$. D'altra parte, $|r - r'| < b$ perché

$$-b < -r' \leq r - r' \leq r < b,$$

e quindi $r - r' = 0$ (cioè $r = r'$). Infine, anche $q - q' = 0$ (cioè $q = q'$) perché $(q' - q)b = r - r' = 0$ e $b \neq 0$. □

Osservazione 1.3. Con la notazione del Teorema 1.2, è chiaro che $r = 0$ se e solo se $b \mid a$, e in quel caso $q = \frac{a}{b}$.

Esempio 1.4. Se $b = 10$ e $a \geq 0$, il resto r della divisione di a per 10 è l'ultima cifra (nell'ordinaria scrittura in base 10) di a. Quindi, per esempio, $r = 2$ se $a = 32 = 3 \cdot 10 + 2$. Si noti che invece $r = 8$ se $a = -32 = -4 \cdot 10 + 8$.

2. Massimo comun divisore

Definizione 2.1. Il *massimo comun divisore* di $a, b \in \mathbb{Z}$ è

$$\mathrm{mcd}(a, b) := \begin{cases} \max\{n \in \mathbb{Z} : n \mid a,\ n \mid b\} & \text{se } (a, b) \neq (0, 0) \\ 0 & \text{se } (a, b) = (0, 0). \end{cases}$$

Osservazione 2.2. Se $(a, b) \neq (0, 0)$, l'insieme

$$D(a, b) := \{n \in \mathbb{Z} : n \mid a,\ n \mid b\}$$

è non vuoto (in ogni caso $1 \in D(a, b)$) e limitato superiormente (da $|a|$ se $a \neq 0$ o da $|b|$ se $b \neq 0$). Dunque esiste $\max D(a, b)$ e $\mathrm{mcd}(a, b)$ risulta ben definito. D'altra parte, $D(0, 0) = \mathbb{Z}$, che non ha massimo: è quindi necessario dare una definizione ad hoc per $\mathrm{mcd}(0, 0)$. Si noti inoltre che $\mathrm{mcd}(a, b) \in \mathbb{N}$ per ogni $a, b \in \mathbb{Z}$ e $\mathrm{mcd}(a, b) = 0$ se e solo se $a = b = 0$. È anche chiaro che $\mathrm{mcd}(a, b) = \mathrm{mcd}(b, a) = \mathrm{mcd}(a, -b)$ e

$$\mathrm{mcd}(a, b) = \mathrm{mcd}(a, b + ac) \tag{2.1}$$

per ogni $a, b, c \in \mathbb{Z}$ (quest'ultima uguaglianza segue dal fatto che $D(a, b) = D(a, b + ac)$, come è facile verificare). Infine si ha

$$\mathrm{mcd}(a, 0) = |a|, \tag{2.2}$$

dato che $D(a, 0) = \{n \in \mathbb{Z} : n \mid a\}$.

Teorema 2.3. *Per ogni $a, b \in \mathbb{Z}$ si ha*

$$a\mathbb{Z} + b\mathbb{Z} = \mathrm{mcd}(a, b)\mathbb{Z}.$$

In particolare, se $(a, b) \neq (0, 0)$, $\mathrm{mcd}(a, b)$ è il minimo intero positivo che si può scrivere come $am + bn$ per qualche $m, n \in \mathbb{Z}$.

Dimostrazione. Poniamo $d := \mathrm{mcd}(a, b)$.

Se $a = b = 0$, allora $d = 0$ e l'uguaglianza da dimostrare è ovvia.

Se $(a, b) \neq (0, 0)$ (dunque $d > 0$), sia $d' := \min\{c \in a\mathbb{Z} + b\mathbb{Z} : c > 0\}$ (si noti che tale minimo esiste perché $|a|, |b| \in a\mathbb{Z} + b\mathbb{Z}$ e almeno uno dei due è positivo). Se dimostriamo che $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$, allora

$$d' = \min\{c \in d\mathbb{Z} : c > 0\} = d,$$

il che dimostrerebbe anche l'ultima affermazione. L'inclusione $a\mathbb{Z} + b\mathbb{Z} \subseteq d\mathbb{Z}$ segue subito dal fatto che $d \mid a$ e $d \mid b$ per definizione di d. Per ottenere $d\mathbb{Z} \subseteq a\mathbb{Z} + b\mathbb{Z}$ basta verificare che $d \in a\mathbb{Z} + b\mathbb{Z}$ (se $d = am + bn \in a\mathbb{Z} + b\mathbb{Z}$, anche $dc = amc + bnc \in a\mathbb{Z} + b\mathbb{Z}$ per ogni $c \in \mathbb{Z}$), e in effetti dimostriamo direttamente che $d = d'$.

Dato che $d' \in a\mathbb{Z} + b\mathbb{Z} \subseteq d\mathbb{Z}$, si ha $d \mid d'$, e quindi $d \leq d'$. Resta allora da dimostrare che $d' \leq d$, e per questo basta verificare $d' \mid a$ e $d' \mid b$ (sempre ricordando che $d = \mathrm{mcd}(a, b)$). Per questo, dimostriamo più in generale che $d' \mid c$ per ogni $c \in a\mathbb{Z} + b\mathbb{Z}$. Infatti, per il Teorema 1.2 esistono (unici) $q, r \in \mathbb{Z}$ tali che $c = qd' + r$ e $0 \leq r < d'$. Per ipotesi esistono $m, n, m', n' \in \mathbb{Z}$ tali che $c = am + bn$ e $d' = am' + bn'$, da cui segue che

$$r = c - qd' = am + bn - q(am' + bn') = a(m - qm') + b(n - qn') \in a\mathbb{Z} + b\mathbb{Z}.$$

Essendo d' il minimo intero positivo di $a\mathbb{Z} + b\mathbb{Z}$, deve essere $r = 0$. Allora $c = qd'$, per cui $d' \mid c$. □

Osservazione 2.4. Per ogni $a, b \in \mathbb{Z}$ esistono dunque sempre $m, n \in \mathbb{Z}$ che verificano l'uguaglianza

$$am + bn = \mathrm{mcd}(a, b), \tag{2.3}$$

detta *identità di Bézout*.

Corollario 2.5. *Per ogni $a, b \in \mathbb{Z}$ l'intero $d = \mathrm{mcd}(a, b) \in \mathbb{N}$ verifica le seguenti condizioni:*

(1) *$d \mid a$ e $d \mid b$;*
(2) *se $c \mid a$ e $c \mid b$ (con $c \in \mathbb{Z}$), allora $c \mid d$.*

Viceversa, se $d \in \mathbb{N}$ verifica (1) e (2), allora $d = \mathrm{mcd}(a, b)$.

Dimostrazione. È chiaro per definizione che $d = \mathrm{mcd}(a, b)$ verifica (1) (anche se $a = b = 0$), mentre (2) vale perché $d \in a\mathbb{Z} + b\mathbb{Z}$ per il Teorema 2.3.

Viceversa, supponiamo che $d \in \mathbb{N}$ verifichi (1) e (2). Se $a = b = 0$, allora $0 \mid a$ e $0 \mid b$, dunque $0 \mid d$ per (2), da cui $d = 0$. Se invece $(a, b) \neq (0, 0)$, (1) implica $0 < d \leq \mathrm{mcd}(a, b)$ e (2) (con $c = \mathrm{mcd}(a, b)$) implica $\mathrm{mcd}(a, b) \mid d$, e quindi $\mathrm{mcd}(a, b) \leq d$. □

Definizione 2.6. Due interi a e b si dicono *coprimi* o *primi tra loro* se $\mathrm{mcd}(a, b) = 1$.

Corollario 2.7. *Due interi a e b sono coprimi se e solo se esistono $m, n \in \mathbb{Z}$ tali che $am + bn = 1$.*

Dimostrazione. Se $\mathrm{mcd}(a,b) = 1$, esistono $m, n \in \mathbb{Z}$ tali che $am + bn = 1$ per (2.3). Viceversa, se esistono $m, n \in \mathbb{Z}$ tali che $am + bn = 1$, chiaramente $(a,b) \neq (0,0)$ e 1 è il minimo intero positivo che si può scrivere in questa forma, dunque $\mathrm{mcd}(a,b) = 1$ per il Teorema 2.3. □

Proposizione 2.8. *Siano $a, b, c \in \mathbb{Z}$ tali che $a \mid bc$. Se $\mathrm{mcd}(a,b) = 1$, allora $a \mid c$.*

Dimostrazione. Per (2.3) esistono $m, n \in \mathbb{Z}$ tali che $am + bn = 1$, e moltiplicando per c si ottiene $c = acm + bcn$. Allora $a \mid c$, dato che $a \mid a$ e $a \mid bc$. □

Proposizione 2.9. *Per ogni $a, b, c \in \mathbb{Z}$ si ha*

$$\mathrm{mcd}(ac, bc) = |c|\mathrm{mcd}(a,b).$$

Dimostrazione. Si può chiaramente supporre $c \geq 0$, e, posto $d := \mathrm{mcd}(a,b)$, va dimostrato che $\mathrm{mcd}(ac, bc) = dc$. A tal fine, mostriamo che dc verifica le condizioni del Corollario 2.5. Ovviamente $dc \in \mathbb{N}$ e vale (1) (cioè $dc \mid ac$ e $dc \mid bc$) perché $d \mid a$ e $d \mid b$. D'altra parte, per (2.3) esistono $m, n \in \mathbb{Z}$ tali che $d = am + bn$, da cui $dc = acm + bcn$. Ne segue che, se $k \in \mathbb{Z}$ è tale che $k \mid ac$ e $k \mid bc$, allora $k \mid dc$, cioè anche (2) è soddisfatta. □

Corollario 2.10. *Siano $(a,b) \neq (0,0)$ e $d := \mathrm{mcd}(a,b)$. Allora*

$$\mathrm{mcd}\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

Dimostrazione. Essendo $d > 0$, per la Proposizione 2.9 abbiamo

$$d = \mathrm{mcd}(a,b) = \mathrm{mcd}\left(d\frac{a}{d}, d\frac{b}{d}\right) = d\mathrm{mcd}\left(\frac{a}{d}, \frac{b}{d}\right),$$

da cui segue subito la tesi. □

3. Minimo comune multiplo

Definizione 3.1. Il *minimo comune multiplo* di $a, b \in \mathbb{Z}$ è

$$\mathrm{mcm}(a,b) := \begin{cases} \min\{n > 0 \,:\, a \mid n,\ b \mid n\} & \text{se } a \neq 0 \text{ e } b \neq 0 \\ 0 & \text{se } a = 0 \text{ o } b = 0. \end{cases}$$

Osservazione 3.2. L'insieme $\{n > 0 \,:\, a \mid n,\ b \mid n\}$ (contenuto in $\mathbb{N}$) è non vuoto se e solo se $a \neq 0$ e $b \neq 0$ (nel qual caso contiene $|ab|$), dunque $\mathrm{mcm}(a,b)$ risulta ben definito. È anche ovvio per definizione che $\mathrm{mcm}(a,b) \in \mathbb{N}$ per ogni $a, b \in \mathbb{Z}$ e $\mathrm{mcm}(a,b) = 0$ se e solo se $a = 0$ o $b = 0$. È inoltre chiaro che $\mathrm{mcm}(a,b) = \mathrm{mcm}(b,a)$ e $\mathrm{mcm}(a,b) = \mathrm{mcm}(a,-b)$.

Teorema 3.3. *Per ogni $a, b \in \mathbb{Z}$ si ha*

$$a\mathbb{Z} \cap b\mathbb{Z} = \mathrm{mcm}(a,b)\mathbb{Z}.$$

In altre parole, i multipli comuni di a e di b sono i multipli di $\mathrm{mcm}(a,b)$.

Dimostrazione. Si può chiaramente supporre $a \neq 0$ e $b \neq 0$, e dunque $m := \mathrm{mcm}(a,b) > 0$. Se $c \in m\mathbb{Z}$, cioè $m \mid c$, allora, tenendo conto che $a \mid m$ e $b \mid m$ per definizione di m, si ha anche $a \mid c$ e $b \mid c$, cioè $c \in a\mathbb{Z} \cap b\mathbb{Z}$. Viceversa, se $c \in a\mathbb{Z} \cap b\mathbb{Z}$, per il Teorema 1.2 esistono (unici) $q, r \in \mathbb{Z}$ tali che $c = qm + r$ e $0 \leq r < m$. Dato che $a \mid c$ e $a \mid m$, $a \mid r = c - qm$, e analogamente $b \mid r$. Per definizione di m, deve essere allora $r = 0$, e perciò $c = qm \in m\mathbb{Z}$. □

Corollario 3.4. *Per ogni $a, b \in \mathbb{Z}$ l'intero $m = \mathrm{mcm}(a, b) \in \mathbb{N}$ verifica le seguenti condizioni:*

(1) *$a \mid m$ e $b \mid m$;*
(2) *se $a \mid c$ e $b \mid c$ (con $c \in \mathbb{Z}$), allora $m \mid c$.*

Viceversa, se $m \in \mathbb{N}$ verifica (1) e (2), allora $m = \mathrm{mcm}(a, b)$.

Dimostrazione. È chiaro per definizione che $m = \mathrm{mcm}(a, b)$ verifica (1) (anche se $a = 0$ o $b = 0$), mentre (2) è una riformulazione dell'inclusione $a\mathbb{Z} \cap b\mathbb{Z} \subseteq m\mathbb{Z}$, che vale per il Teorema 3.3.

Viceversa, supponiamo che $m \in \mathbb{N}$ verifichi (1) e (2). Se $a = 0$ o $b = 0$, (1) implica $m = 0$. Se invece $a \neq 0$ e $b \neq 0$, (2) (con $c = \mathrm{mcm}(a, b) > 0$) implica $0 < m \mid \mathrm{mcm}(a, b)$, e quindi $m \leq \mathrm{mcm}(a, b)$, e (1) implica $\mathrm{mcm}(a, b) \leq m$. □

Proposizione 3.5. *Per ogni $a, b, c \in \mathbb{Z}$ si ha*

$$\mathrm{mcm}(ac, bc) = |c|\mathrm{mcm}(a, b).$$

Dimostrazione. Si può chiaramente supporre $c > 0$, e, posto $m := \mathrm{mcm}(a, b)$, va dimostrato che $\mathrm{mcm}(ac, bc) = mc$. A tal fine, mostriamo che mc verifica le condizioni del Corollario 3.4. Ovviamente $mc \in \mathbb{N}$ e vale (1) (cioè $ac \mid mc$ e $bc \mid mc$) perché $a \mid m$ e $b \mid m$. D'altra parte, se $k \in \mathbb{Z}$ è tale che $ac \mid k$ e $bc \mid k$, allora $c \mid k$, e, posto $k' := \frac{k}{c}$, si ha $a \mid k'$ e $b \mid k'$. Questo implica (sempre per il Corollario 3.4) che $m \mid k'$, e perciò $mc \mid k'c = k$, cioè anche (2) è verificata. □

Corollario 3.6. *Per ogni $a, b \in \mathbb{Z}$ si ha*

$$\mathrm{mcd}(a, b)\mathrm{mcm}(a, b) = |ab|.$$

Dimostrazione. Il risultato è ovvio se $a = 0$ o $b = 0$, e si può allora supporre $a, b > 0$. Posto $d := \mathrm{mcd}(a, b) > 0$, $a' := \frac{a}{d}$ e $b' := \frac{b}{d}$, per il Corollario 2.10 si ha $\mathrm{mcd}(a', b') = 1$. Poiché $\mathrm{mcm}(a, b) = dm'$ (dove $m' := \mathrm{mcm}(a', b')$) per la Proposizione 3.5, la tesi diventa $d^2m' = d^2a'b'$, e quindi basta dimostrare che $m' = a'b'$. Chiaramente $a' \mid a'b'$ e $b' \mid a'b'$, cioè $a'b'$ soddisfa (1) del Corollario 3.4. Se poi $a' \mid c$ e $b' \mid c$, posto $c' := \frac{c}{b'}$, si ha $a' \mid c = b'c'$, e dunque $a' \mid c'$ per la Proposizione 2.8. Si conclude allora che $a'b' \mid c'b' = c$, cioè anche (2) è verificata. □

4. Numeri primi e fattorizzazione unica

Definizione 4.1. Un intero $n > 1$ è un *numero primo* se gli unici divisori positivi di n sono 1 e n.

Osservazione 4.2. Anche se 1 è l'unico divisore positivo di 1, ci sono buoni motivi per non considerare 1 un numero primo. Uno di questi è che altrimenti non varrebbe l'unicità della fattorizzazione di un intero positivo come prodotto di numeri primi (vedi il Teorema 4.4).

Proposizione 4.3. *Per un intero $n > 1$ le seguenti condizioni sono equivalenti:*

(1) *n è un numero primo;*
(2) *se $n \mid ab$ (con $a, b \in \mathbb{Z}$), allora $n \mid a$ o $n \mid b$.*

Dimostrazione. Se n è primo e $n \mid ab$, risulta $\mathrm{mcd}(n,a) = 1$ o $\mathrm{mcd}(n,a) = n$ (essendo in ogni caso un divisore positivo di n). Se $\mathrm{mcd}(n,a) = n$, allora $n \mid a$, mentre se $\mathrm{mcd}(n,a) = 1$, la Proposizione 2.8 mostra che $n \mid b$.

Viceversa, se n non è primo, per definizione esistono interi $1 < a, b < n$ tali che $n = ab$. Allora $n \mid ab$, ma $n \nmid a$ e $n \nmid b$. □

Teorema 4.4 (Teorema fondamentale dell'aritmetica)**.** *Ogni intero positivo si può scrivere in modo unico (a meno dell'ordine) come prodotto (finito) di numeri primi. In altre parole, per ogni intero $n > 0$ esistono $k \in \mathbb{N}$ e dei numeri primi (non necessariamente distinti) $p_1, \dots, p_k$ tali che $n = \prod_{i=1}^{k} p_i$; dati inoltre $l \in \mathbb{N}$ e altri numeri primi $q_1, \dots, q_l$ tali che $n = \prod_{i=1}^{l} q_i$, si ha $l = k$ ed esiste una funzione biunivoca $\sigma\colon \{1, \dots, k\} \to \{1, \dots, k\}$ tale che $q_i = p_{\sigma(i)}$ per ogni $i = 1, \dots, k$.*

Dimostrazione. Dimostriamo prima che ogni intero positivo è un prodotto di numeri primi. Supponiamo per assurdo che non sia così: esiste allora il minimo intero positivo n che non è prodotto di numeri primi. Essendo 1 un prodotto (vuoto) di numeri primi, deve essere $n > 1$. Inoltre n non è primo (ogni numero primo è il prodotto di un solo numero primo, cioè sè stesso), per cui esistono due interi $1 < a, b < n$ tali che $n = ab$. Ora, per definizione di n, a e b sono prodotti di numeri primi, e quindi anche $n = ab$ lo è, il che è assurdo.

Procediamo per assurdo anche per dimostrare l'unicità della fattorizzazione di ogni intero positivo come prodotto di primi. Supponiamo dunque che esistano degli interi positivi con almeno due fattorizzazioni distinte (anche a meno dell'ordine), e sia n minimo con questa proprietà. Chiaramente $n > 1$, dato che 1 si può ottenere solo come prodotto vuoto di numeri primi. Se

$$n = \prod_{i=1}^{k} p_i = \prod_{i=1}^{l} q_i$$

sono due fattorizzazioni distinte di n, deve essere allora $k, l > 0$. Dato che $q_l \mid n$, segue induttivamente dalla Proposizione 4.3 che esiste $i \in \{1, \dots, k\}$ tale che $q_l \mid p_i$, e, a meno di riordinare $p_1, \dots, p_k$, si può supporre $i = k$. Essendo p_k primo, $q_l \mid p_k$ implica $q_l = p_k$, e quindi $n' := \frac{n}{p_k} = \frac{n}{q_l}$ ammette le due fattorizzazioni seguenti:

$$n' = \prod_{i=1}^{k-1} p_i = \prod_{i=1}^{l-1} q_i.$$

Poiché $n' < n$, tali fattorizzazioni coincidono (a meno dell'ordine) per definizione di n. Ciò chiaramente implica che anche le due date fattorizzazioni di n coincidono, il che è assurdo. □

Osservazione 4.5. È anche facile fornire un algoritmo finito (anche se non il più veloce, soprattutto per interi abbastanza grandi) per trovare esplicitamente la fattorizzazione di un dato intero $n > 0$. Se infatti n non è divisibile per nessun intero nell'intervallo $[2, \sqrt{n}]$ (in effetti basta limitarsi ai numeri primi tra tali interi), allora n è primo. Altrimenti il più piccolo divisore trovato è il più piccolo primo p che compare nella fattorizzazione di n, e si

continua ripetendo la stessa procedura con $\frac{n}{p}$ al posto di n (e chiaramente non è più necessario controllare la divisibilità per i numeri minori di p).

Corollario 4.6. *I numeri primi sono infiniti.*

Dimostrazione. Supponiamo per assurdo che $p_1, \ldots, p_k$ siano tutti i numeri primi. Per il Teorema 4.4, $n := 1 + \prod_{i=1}^{k} p_i$ è un prodotto (non vuoto, essendo $n > 1$) di numeri primi, quindi, in particolare, esiste un numero primo p tale che $p \mid n$. D'altra parte, per ipotesi esiste $j \in \{1, \ldots, k\}$ tale che $p = p_j$. Ne segue che $p \mid \prod_{i=1}^{k} p_i$, ma allora anche $p \mid (n - \prod_{i=1}^{k} p_i) = 1$, il che è impossibile. □

Dato un intero $a > 0$, segue dal Teorema 4.4 che per ogni numero primo p esiste unico $\alpha_p \in \mathbb{N}$ tale che solo un numero finito di α_p non è nullo e

$$a = \prod_{p \text{ primo}} p^{\alpha_p}$$

(si noti che $p^{\alpha_p} = 1$ se $\alpha_p = 0$, per cui in tale prodotto infinito solo un numero finito di fattori sono rilevanti). Dato un altro intero $b > 0$ che si scriva analogamente come $b = \prod_{p \text{ primo}} p^{\beta_p}$, è immediato verificare che $ab = \prod_{p \text{ primo}} p^{\alpha_p + \beta_p}$ e

$$a \mid b \iff \alpha_p \leq \beta_p \text{ per ogni } p \text{ primo}. \tag{4.1}$$

Vale inoltre il seguente ben noto risultato.

Proposizione 4.7. *Se $a = \prod_{p \text{ primo}} p^{\alpha_p}$ e $b = \prod_{p \text{ primo}} p^{\beta_p}$, allora*

$$\mathrm{mcd}(a, b) = \prod_{p \text{ primo}} p^{\min\{\alpha_p, \beta_p\}} \qquad e \qquad \mathrm{mcm}(a, b) = \prod_{p \text{ primo}} p^{\max\{\alpha_p, \beta_p\}}.$$

Dimostrazione. Sia, per ogni p primo, $\delta_p := \min\{\alpha_p, \beta_p\}$ e $d := \prod_{p \text{ primo}} p^{\delta_p}$. Per dimostrare che $\mathrm{mcd}(a, b) = d$ basta verificare che d soddisfa (1) e (2) del Corollario 2.5. Poiché $\delta_p \leq \alpha_p$ e $\delta_p \leq \beta_p$ per ogni p primo, (4.1) implica che $d \mid a$ e $d \mid b$, cioè (1) vale. Se poi $c \mid a$ e $c \mid b$, deve essere $c \neq 0$, e si può supporre $c > 0$. Posto $c = \prod_{p \text{ primo}} p^{\gamma_p}$ (con $\gamma_p \in \mathbb{N}$), segue ancora da (4.1) che $\gamma_p \leq \alpha_p$ e $\gamma_p \leq \beta_p$, e dunque $\gamma_p \leq \delta_p$, per ogni p primo. Di nuovo (4.1) permette di concludere che $c \mid d$, cioè anche (2) vale. Ciò dimostra la formula per $\mathrm{mcd}(a, b)$, e quella per $\mathrm{mcm}(a, b)$ si dimostra in modo del tutto analogo, usando il Corollario 3.4 invece del Corollario 2.5. □

Osservazione 4.8. Alcuni dei risultati visti in precedenza relativi a massimo comun divisore e minimo comune multiplo (come la Proposizione 2.9, il Corollario 2.10, la Proposizione 3.5 e il Corollario 3.6) si possono dimostrare più facilmente usando la Proposizione 4.7. È anche vero che dalla Proposizione 4.7 segue subito la Proposizione 2.8 e quindi la Proposizione 4.3, ma è importante osservare che è stato necessario fornire una dimostrazione di quest'ultimo risultato che non dipendesse dall'unicità della fattorizzazione perché esso è servito proprio per dimostrare il Teorema 4.4.

5. Algoritmo di Euclide

Come vedremo, dati $a, b \in \mathbb{Z}$, può essere utile conoscere un metodo non solo per calcolare $\mathrm{mcd}(a, b)$ (e quindi $\mathrm{mcm}(a, b)$, grazie al Corollario 3.6), ma anche per trovare esplicitamente due interi m e n che verificano (2.3). Chiaramente, ricordando (2.2), la soluzione di entrambi i problemi è banale se $a = 0$ o $b = 0$, per cui possiamo assumere $a, b > 0$. È allora sempre possibile trovare le fattorizzazioni di a e b (vedi l'Osservazione 4.5) e poi calcolare $\mathrm{mcd}(a, b)$ utilizzando la Proposizione 4.7. Ciò non è però di grande aiuto per trovare m e n che soddisfano (2.3). Il cosiddetto *algoritmo di Euclide* permette di risolvere tale problema e allo stesso tempo fornisce un metodo alternativo per calcolare $\mathrm{mcd}(a, b)$, che non richiede la conoscenza delle fattorizzazioni di a e b (ha anche il vantaggio di essere molto più veloce se a e b sono grandi e difficili da fattorizzare).

Per descrivere l'algoritmo di Euclide poniamo intanto

$$r_0 := a, \qquad r_1 := b.$$

Per $i \geq 1$ e se $r_i \neq 0$, definiamo poi induttivamente dei nuovi interi q_i e r_{i+1} facendo la divisione con resto di r_{i-1} per r_i. Più precisamente, se $r_i \neq 0$, per il Teorema 1.2 esistono unici $q_i, r_{i+1} \in \mathbb{Z}$ tali che

$$r_{i-1} = q_i r_i + r_{i+1}, \qquad 0 \leq r_{i+1} < r_i.$$

Non potendo esistere una successione infinita e strettamente decrescente di interi positivi, deve esistere $k \geq 1$ tale che $r_k > 0$ e $r_{k+1} = 0$. Risulta allora

$$\mathrm{mcd}(a, b) = r_k.$$

Infatti, per $1 \leq i \leq k$ si ha

$$\mathrm{mcd}(r_{i-1}, r_i) = \mathrm{mcd}(q_i r_i + r_{i+1}, r_i) = \mathrm{mcd}(r_i, r_{i+1} + q_i r_i) = \mathrm{mcd}(r_i, r_{i+1})$$

grazie a (2.1), da cui si deduce induttivamente che

$$\mathrm{mcd}(a, b) = \mathrm{mcd}(r_0, r_1) = \mathrm{mcd}(r_k, r_{k+1}) = \mathrm{mcd}(r_k, 0) = r_k,$$

tenendo conto di (2.2).

È inoltre facile trovare induttivamente per $0 \leq i \leq k$ degli interi m_i e n_i tali che $am_i + bn_i = r_i$. Infatti, si può ovviamente scegliere $m_0 = 1$, $n_0 = 0$, $m_1 = 0$ e $n_1 = 1$. Se poi $1 \leq i < k$ e sono già stati trovati m_j e n_j per $0 \leq j \leq i$, l'uguaglianza

$$\begin{aligned} r_{i+1} = r_{i-1} - q_i r_i &= am_{i-1} + bn_{i-1} - q_i(am_i + bn_i) \\ &= a(m_{i-1} - q_i m_i) + b(n_{i-1} - q_i n_i) \end{aligned}$$

implica che si può scegliere $m_{i+1} := m_{i-1} - q_i m_i$ e $n_{i+1} := n_{i-1} - q_i n_i$. È allora chiaro che $m := m_k$ e $n := n_k$ verificano (2.3).

Esempio 5.1. Se $a = r_0 = 806$ e $b = r_1 = 299$, si trova

$$\begin{aligned} 806 &= 2 \cdot 299 + 208 && (q_1 = 2,\ r_2 = 208), \\ 299 &= 1 \cdot 208 + 91 && (q_2 = 1,\ r_3 = 91), \\ 208 &= 2 \cdot 91 + 26 && (q_3 = 2,\ r_4 = 26), \\ 91 &= 3 \cdot 26 + 13 && (q_4 = 3,\ r_5 = 13), \\ 26 &= 2 \cdot 13 + 0 && (q_5 = 2,\ r_6 = 0), \end{aligned}$$

e dunque $\mathrm{mcd}(806, 299) = r_5 = 13$. Inoltre

$$\begin{aligned} m_0 &= 1, & n_0 &= 0, \\ m_1 &= 0, & n_1 &= 1, \\ m_2 &= m_0 - q_1 m_1 = 1, & n_2 &= n_0 - q_1 n_1 = -2, \\ m_3 &= m_1 - q_2 m_2 = -1, & n_3 &= n_1 - q_2 n_2 = 3, \\ m_4 &= m_2 - q_3 m_3 = 3, & n_4 &= n_2 - q_3 n_3 = -8, \\ m_5 &= m_3 - q_4 m_4 = -10, & n_5 &= n_3 - q_4 n_4 = 27, \end{aligned}$$

per cui $m = m_5 = -10$ e $n = n_5 = 27$ verificano $806(-10) + 299 \cdot 27 = 13$.

6. Soluzioni intere di $ax + by = c$

Dati $a, b, c \in \mathbb{Z}$, il Teorema 2.3 implica che l'equazione

$$ax + by = c \tag{6.1}$$

ammette soluzioni intere x e y se e solo se $d := \mathrm{mcd}(a, b) \mid c$. Assumendo dunque che $d \mid c$, è naturale chiedersi quali siano tutte le soluzioni di tale equazione e come sia possibile trovarle. Il problema è banale se $a = b = 0$, perché in quel caso $d = 0$, quindi $c = 0$ e (x, y) è soluzione per ogni $x, y \in \mathbb{Z}$. Supponiamo perciò $(a, b) \neq (0, 0)$ (e quindi $d > 0$). È facile trovare esplicitamente una soluzione particolare (x_0, y_0) di (6.1): per esempio, si possono prima trovare $m, n \in \mathbb{Z}$ tali che $am + bn = d$ (eventualmente usando l'algoritmo di Euclide, come spiegato nella Sezione 5), e poi porre $x_0 := m\frac{c}{d}$, $y_0 := n\frac{c}{d}$. Per trovare tutte le altre soluzioni conviene semplificare l'equazione dividendo tutti i coefficienti per d. Infatti, posto $a' := \frac{a}{d}$, $b' := \frac{b}{d}$ e $c' := \frac{c}{d}$, (si noti che per ipotesi $a', b', c' \in \mathbb{Z}$), è chiaro che le soluzioni intere di (6.1) coincidono con le soluzioni intere di

$$a'x + b'y = c'. \tag{6.2}$$

Il vantaggio di questa nuova equazione è che $\mathrm{mcd}(a', b') = 1$, grazie al Corollario 2.10. Assumendo che (x_0, y_0) sia una soluzione particolare di (6.2), si può allora dimostrare che un'altra coppia di interi (x, y) è soluzione di (6.2) se e solo se esiste $k \in \mathbb{Z}$ tale che

$$\begin{cases} x = x_0 + b'k \\ y = y_0 - a'k. \end{cases} \tag{6.3}$$

In effetti, è immediato verificare che ogni coppia (x, y) di questa forma è soluzione. Viceversa, se (x, y) è soluzione, si ha

$$a'x + b'y = c' = a'x_0 + b'y_0,$$

per cui $a'(x - x_0) = b'(y_0 - y)$. Essendo $(a', b') \neq (0, 0)$, possiamo supporre per esempio $a' \neq 0$. Dall'ultima uguaglianza segue che $a' \mid b'(y_0 - y)$, e quindi $a' \mid (y_0 - y)$ per la Proposizione 2.8. Ciò significa che esiste $k \in \mathbb{Z}$ tale che $y_0 - y = a'k$, cioè la seconda uguaglianza in (6.3) è soddisfatta. Inoltre $x - x_0 = \frac{b'(y_0 - y)}{a'} = b'k$, cioè anche la prima uguaglianza in (6.3) è soddisfatta. Si è quindi dimostrato il risultato seguente, riformulato in termini dei coefficienti dell'equazione di partenza.

Proposizione 6.1. *Dati $a, b, c \in \mathbb{Z}$, l'equazione* (6.1) *ha soluzioni intere se e solo se* $\mathrm{mcd}(a, b) \mid c$. *In questo caso, assumendo che* $(a, b) \neq (0, 0)$ *e che* (x_0, y_0) *sia una soluzione particolare, le soluzioni sono tutte e sole della forma*

$$\begin{cases} x = x_0 + \frac{bk}{\mathrm{mcd}(a,b)} \\ y = y_0 - \frac{ak}{\mathrm{mcd}(a,b)} \end{cases}$$

con $k \in \mathbb{Z}$.

7. Congruenze

Definizione 7.1. Dati $a, b, n \in \mathbb{Z}$, si dice che a è *congruo* a b *modulo* n e si scrive

$$a \equiv b \mod n \qquad \text{o} \qquad a \equiv b \pmod{n}$$

se $n \mid (a - b)$.

Dato che $a \equiv b \mod n$ se e solo se $a \equiv b \mod -n$ e che $a \equiv b \mod 0$ se e solo se $a = b$, nel seguito supporremo sempre $n > 0$.

Proposizione 7.2. *La congruenza modulo* n *è una relazione di equivalenza su* $\mathbb{Z}$.

Dimostrazione. La relazione è riflessiva, cioè $a \equiv a \mod n$ per ogni $a \in \mathbb{Z}$, perché $n \mid (a - a) = 0$.

La relazione è simmetrica, cioè $a \equiv b \mod n$ implica $b \equiv a \mod n$ per ogni $a, b \in \mathbb{Z}$, perché $n \mid (a - b)$ implica $n \mid (b - a) = -(a - b)$.

La relazione è transitiva, cioè $a \equiv b \mod n$ e $b \equiv c \mod n$ implica $a \equiv c \mod n$ per ogni $a, b, c \in \mathbb{Z}$, perché $n \mid (a - b)$ e $n \mid (b - c)$ implica $n \mid (a - c) = (a - b) + (b - c)$. □

Per ogni $a \in \mathbb{Z}$ spesso si indica con $\bar{a}$ o $[a]$ (o anche $[a]_n$ se ci possono essere dubbi su n) la classe di congruenza modulo n di a. Per definizione

$$\bar{a} = \{b \in \mathbb{Z} : a \equiv b \mod n\} = \{a + kn : k \in \mathbb{Z}\} = a + n\mathbb{Z}.$$

Si indica con $\mathbb{Z}/n\mathbb{Z}$ l'insieme quoziente di $\mathbb{Z}$ rispetto alla congruenza modulo n. Tautologicamente si ha $\mathbb{Z}/n\mathbb{Z} = \{\bar{a} : a \in \mathbb{Z}\}$. Per ottenere una descrizione più interessante di $\mathbb{Z}/n\mathbb{Z}$ è utile il seguente risultato.

Lemma 7.3. *Dati* $a, b \in \mathbb{Z}$, *si ha* $a \equiv b \mod n$ *se e solo se* a *e* b *hanno lo stesso resto della divisione per* n.

Dimostrazione. Siano $q, r, q', r' \in \mathbb{Z}$ (che esistono unici per il Teorema 1.2) tali che $a = qn + r$ e $b = q'n + r'$ con $0 \leq r, r' < n$. Se $r = r'$, allora $n \mid (a - b) = (q - q')n$, cioè $a \equiv b \mod n$. Viceversa, se $a \equiv b \mod n$, cioè $a - b = kn$ per qualche $k \in \mathbb{Z}$, allora

$$qn + r = a = b + (a - b) = q'n + r' + kn = (q' + k)n + r',$$

da cui segue $r = r'$ (e $q = q' + k$) per l'unicità di r (e di q). □

Corollario 7.4. $\#\mathbb{Z}/n\mathbb{Z} = n$ *e* $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$.

Proposizione 7.5. *Le operazioni*

$$+\colon \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \qquad \times\colon \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$
$$(\bar{a}, \bar{b}) \mapsto \overline{a+b} \qquad (\bar{a}, \bar{b}) \mapsto \overline{ab}$$

sono ben definite e rendono $\mathbb{Z}/n\mathbb{Z}$ un anello commutativo.

Dimostrazione. Se $a, a', b, b' \in \mathbb{Z}$ sono tali che $\bar{a} = \overline{a'}$ e $\bar{b} = \overline{b'}$, per definizione esistono $h, k \in \mathbb{Z}$ tali che $a' = a + hn$ e $b' = b + kn$. Allora

$$a' + b' = a + b + (h + k)n, \qquad a'b' = ab + (ak + bh + hkn)n,$$

il che dimostra che $\overline{a' + b'} = \overline{a + b}$ e $\overline{a'b'} = \overline{ab}$.

Una volta dimostrata la buona definizione, la verifica di ciascun assioma di anello commutativo per $\mathbb{Z}/n\mathbb{Z}$ segue facilmente dal fatto che il corrispondente assioma vale per $\mathbb{Z}$. Dimostriamo per esempio la proprietà distributiva, lasciando il resto per esercizio. Per ogni $a, b, c \in \mathbb{Z}$ si ha

$$\bar{a}(\bar{b} + \bar{c}) = \bar{a}(\overline{b + c}) = \overline{a(b + c)} = \overline{ab + ac} = \overline{ab} + \overline{ac} = \bar{a}\bar{b} + \bar{a}\bar{c},$$

dove l'uguaglianza centrale segue dalla proprietà distributiva in $\mathbb{Z}$ e le altre dalle definizioni di somma e prodotto in $\mathbb{Z}/n\mathbb{Z}$. □

Osservazione 7.6. Se $n > 1$ non è un numero primo, esistono $a, b \in \mathbb{Z}$ tali che $\bar{a} \neq \bar{0} \neq \bar{b}$ ma $\bar{a}\bar{b} = \bar{0}$: per esempio, basta scegliere $1 < a, b < n$ tali che $ab = n$. Questo non succede se invece n è primo, perché in quel caso $\overline{ab} = \bar{a}\bar{b} = \bar{0}$ implica $n \mid ab$, quindi $n \mid a$ (cioè $\bar{a} = \bar{0}$) o $n \mid b$ (cioè $\bar{b} = \bar{0}$) per la Proposizione 4.3. In effetti, come vedremo nell'Osservazione 8.4, è anche vero che $\mathbb{Z}/n\mathbb{Z}$ è un campo se n è primo.

8. Soluzioni di congruenze polinomiali

Dato un intero $n > 0$ e una funzione polinomiale $f\colon \mathbb{Z} \to \mathbb{Z}$ (cioè della forma $f(x) = \sum_{i=0}^{d} c_i x^i$ con $d \in \mathbb{N}$ e $c_0, \ldots, c_d \in \mathbb{Z}$) è sempre possibile risolvere la congruenza

$$f(x) \equiv 0 \mod n \tag{8.1}$$

(cioè determinare tutti gli $x \in \mathbb{Z}$ che la verificano). Poiché $f(x)$ si ottiene da x con operazioni di somma e prodotto, segue infatti facilmente dalla Proposizione 7.5 che, se $x \equiv y \mod n$, allora $f(x) \equiv f(y) \mod n$. Se ne deduce che f induce una funzione ben definita

$$\overline{f}\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$
$$\bar{x} \mapsto \overline{f(x)}$$

e che $\overline{f}(\bar{x}) = \sum_{i=0}^{d} \overline{c_i}\bar{x}^i$ se $f(x) = \sum_{i=0}^{d} c_i x^i$. Alla luce del Corollario 7.4, per risolvere (8.1) basta dunque trovare le soluzioni intere nell'intervallo $[0, n-1]$ (cosa che si può sempre fare, in mancanza di meglio semplicemente calcolando $f(x)$ per $x = 0, \ldots, n-1$):[4] se $x_1, \ldots, x_k$ sono tali soluzioni (ovviamente per qualche $0 \leq k \leq n$), si avrà poi che $x \in \mathbb{Z}$ è soluzione di

[4] Al posto di $\{0, \ldots, n-1\}$ si può usare qualsiasi altro insieme di rappresentanti delle classi di congruenza modulo n. Per semplificare i calcoli è spesso più comodo usare per esempio gli interi nell'intervallo $(-\frac{n}{2}, \frac{n}{2}]$.

(8.1) se e solo se $x \equiv x_i \mod n$ per qualche $i = 1, \dots, k$. Si noti anche che $\overline{x_1}, \dots, \overline{x_k}$ sono le soluzioni dell'equazione

$$\overline{f}(\overline{x}) = \overline{0} \tag{8.2}$$

in $\mathbb{Z}/n\mathbb{Z}$. Ciò mostra che risolvere (8.1) è essenzialmente equivalente a risolvere (8.2), anche se va evidenziato che le soluzioni non sono le stesse (nel primo caso sono elementi di $\mathbb{Z}$, nel secondo di $\mathbb{Z}/n\mathbb{Z}$).

Esempio 8.1. Se $n = 6$ e $f(x) = x^3 + 3x + 2$, si trova che $6 \mid f(1), f(4)$ e $6 \nmid f(0), f(2), f(3), f(5)$. Dunque in questo caso le soluzioni di (8.1) sono $x \equiv 1, 4 \mod 6$ (che si possono scrivere più semplicemente come $x \equiv 1 \mod 3$)[5] e le corrispondenti soluzioni di (8.2) sono $\overline{x} = \overline{1}, \overline{4}$ in $\mathbb{Z}/6\mathbb{Z}$.

Osservazione 8.2. Per quanto detto finora è essenziale che f sia una funzione polinomiale, perché altrimenti in generale non è vero che $x \equiv y \mod n$ implica $f(x) \equiv f(y) \mod n$.

Mostriamo infine come si possa procedere più velocemente per trovare le soluzioni di (8.1) almeno quando f è data da un polinomio di primo grado (o da una costante). Cambiando leggermente notazione, dati $a, b \in \mathbb{Z}$, vogliamo dunque risolvere

$$ax \equiv b \mod n. \tag{8.3}$$

Dato $x \in \mathbb{Z}$, per definizione (8.3) è verificata se e solo se esiste $y \in \mathbb{Z}$ tale che $ax + ny = b$. Segue allora dalla Proposizione 6.1 che esiste una soluzione se e solo se $\mathrm{mcd}(a, n) \mid b$, e che in questo caso, se x_0 è una soluzione particolare (che si può trovare come spiegato nella Sezione 6), le soluzioni di (8.3) sono tutte e sole della forma

$$x \equiv x_0 \mod \frac{n}{\mathrm{mcd}(a, n)}.$$

Si noti che quindi, se $\mathrm{mcd}(a, n) \mid b$, ci sono $\mathrm{mcd}(a, n)$ soluzioni di $\overline{a}\overline{x} = \overline{b}$ in $\mathbb{Z}/n\mathbb{Z}$, cioè

$$\left\{ \overline{x_0 + \frac{ni}{\mathrm{mcd}(a, n)}} \,:\, 0 \leq i < \mathrm{mcd}(a, n) \right\}.$$

Esempio 8.3. La congruenza

$$6x \equiv 15 \mod 21$$

ha soluzione perché $\mathrm{mcd}(6, 21) = 3 \mid 15$, e la soluzione è unica modulo $\frac{21}{\mathrm{mcd}(6,21)} = 7$. Si trova facilmente che per esempio 6 è una soluzione particolare, dunque tutte le soluzioni sono $x \equiv 6 \mod 7$. Ci sono invece 3 soluzioni di $\overline{6}\overline{x} = \overline{15}$ in $\mathbb{Z}/21\mathbb{Z}$, cioè $\overline{x} = \overline{6}, \overline{13}, \overline{20}$.

Osservazione 8.4. Se $\mathrm{mcd}(a, n) = 1$ esiste dunque sempre una soluzione di (8.3) (ed è unica modulo n). In particolare, se n è primo e $\overline{a} \neq \overline{0}$, la condizione $\mathrm{mcd}(a, n) = 1$ è verificata, e si ottiene allora (prendendo $b = 1$) che esiste $x \in \mathbb{Z}$ tale che $\overline{a}\overline{x} = \overline{1}$. Ciò dimostra che $\mathbb{Z}/n\mathbb{Z}$ è un campo se n è primo.

[5] È facile vedere che, in generale, il più piccolo intero positivo n' tale che le soluzioni si possono scrivere modulo n' risulta sempre un divisore di n (eventualmente $n' = n$).

9. Sistemi di congruenze

Dati due interi $m, n > 0$ e due funzioni polinomiali $f, g\colon \mathbb{Z} \to \mathbb{Z}$, vediamo ora come si possono trovare le soluzioni del sistema di congruenze

$$\begin{cases} f(x) \equiv 0 \mod m \\ g(x) \equiv 0 \mod n \end{cases} \tag{9.1}$$

(dovrebbe essere poi chiaro come trattare induttivamente il caso di più di due congruenze). Come spiegato nella Sezione 8, si possono trovare separatamente le soluzioni $x \equiv \overline{a_1}, \dots, \overline{a_h} \mod m'$ (con m' divisore positivo di m) della prima congruenza e le soluzioni $x \equiv \overline{b_1}, \dots, \overline{b_k} \mod n'$ (con n' divisore positivo di n) della seconda. Si avrà allora che le soluzioni di (9.1) sono date dall'unione delle soluzioni di ciascuno dei sistemi

$$\begin{cases} x \equiv a_i \mod m' \\ x \equiv b_j \mod n' \end{cases}$$

per $i = 1, \dots, h$ e $j = 1, \dots, k$. Per risolvere un sistema di questo tipo sarà utile il seguente risultato.

Lemma 9.1. *Dati $s, t \in \mathbb{Z}$, si ha $s \equiv t \mod m$ e $s \equiv t \mod n$ se e solo se $s \equiv t \mod \operatorname{mcm}(m, n)$.*

Dimostrazione. Si tratta di dimostrare che $s - t \in m\mathbb{Z}$ e $s - t \in n\mathbb{Z}$ se e solo se $s - t \in \operatorname{mcm}(m, n)\mathbb{Z}$, ma questo è vero per il Teorema 3.3. □

Proposizione 9.2. *Dati $a, b \in \mathbb{Z}$, il sistema*

$$\begin{cases} x \equiv a \mod m \\ x \equiv b \mod n \end{cases} \tag{9.2}$$

ha soluzione se e solo se $\operatorname{mcd}(m, n) \mid (b - a)$, e in questo caso la soluzione è unica modulo $\operatorname{mcm}(m, n)$.

Dimostrazione. Per definizione, $x \in \mathbb{Z}$ è soluzione di (9.2) se e solo se esistono $y, z \in \mathbb{Z}$ tali che

$$\begin{cases} x = a + my \\ x = b - nz. \end{cases}$$

Dunque (9.2) ha soluzione se e solo se esistono $y, z \in \mathbb{Z}$ tali che $a + my = b - nz$, cioè $my + nz = b - a$, e per la Proposizione 6.1 quest'ultima equazione ha soluzione se e solo se $\operatorname{mcd}(m, n) \mid (b - a)$. In questo caso, indicando con x_0 una soluzione particolare di (9.2) (che si può trovare come $x_0 = a + my_0 = b - nz_0$ a partire da una soluzione particolare (y_0, z_0) di $my + nz = b - a$), $x \in \mathbb{Z}$ è pure soluzione di (9.2) se e solo se $x \equiv x_0 \mod m$ e $x \equiv x_0 \mod n$. Per il Lemma 9.1 questo succede se e solo se $x \equiv x_0 \mod \operatorname{mcm}(m, n)$. □

Dato che $\operatorname{mcm}(m, n) = mn$ se $\operatorname{mcd}(m, n) = 1$ (per il Corollario 3.6), otteniamo in particolare il seguente famoso risultato.

Corollario 9.3 (Teorema cinese del resto)**.** *Se $mcd(m, n) = 1$, il sistema (9.2) ha soluzione per ogni $a, b \in \mathbb{Z}$, e la soluzione è unica modulo mn.*

Osservazione 9.4. Il teorema cinese del resto può essere enunciato in modo equivalente dicendo che la funzione (che è sempre ben definita, dato che $m, n \mid mn$)

$$\begin{aligned} \mathbb{Z}/mn\mathbb{Z} &\to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ [x]_{mn} &\mapsto ([x]_m, [x]_n) \end{aligned}$$

è biunivoca se $\mathrm{mcd}(m, n) = 1$.

È infine importante osservare che spesso può essere utile spezzare una congruenza in un sistema di due o più congruenze con moduli più piccoli (e quindi di solito più semplici da risolvere). Più precisamente, se $n = n_1 n_2$ con $\mathrm{mcd}(n_1, n_2) = 1$ e $f\colon \mathbb{Z} \to \mathbb{Z}$ è una funzione polinomiale, segue dal Lemma 9.1 che le soluzioni di $f(x) \equiv 0 \mod n$ coincidono con le soluzioni del sistema

$$\begin{cases} f(x) \equiv 0 \mod n_1 \\ f(x) \equiv 0 \mod n_2 \end{cases}$$

(che può essere risolto con il procedimento descritto sopra). In particolare, se $n = \prod_{i=1}^{k} p_i^{e_i}$ con $p_1, \ldots, p_k$ primi distinti e $e_1, \ldots, e_k > 0$, le soluzioni cercate sono le soluzioni del sistema

$$\begin{cases} f(x) \equiv 0 \mod p_1^{e_1} \\ \quad \vdots \\ f(x) \equiv 0 \mod p_k^{e_k}. \end{cases}$$

Per risolvere una congruenza polinomiale ci si può dunque sempre ricondurre al caso in cui il modulo è una potenza di un numero primo.

Esempio 9.5. Le soluzioni di

$$x^4 + 3x + 9 \equiv 0 \mod 63$$

coincidono con quelle del sistema

$$\begin{cases} x^4 + 3x + 9 \equiv 0 \mod 9 \\ x^4 + 3x + 9 \equiv 0 \mod 7. \end{cases}$$

Si vede facilmente che le soluzioni della prima congruenza sono $x \equiv 0 \mod 3$ e quelle della seconda $x \equiv -1 \mod 7$. Si trova allora che le soluzioni cercate sono $x \equiv 6 \mod 21$.