Interi e Congruenze

Giovanna Carnovale

November 3, 2011

1 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 messo in corrispondenza biunivoca con l'insieme delle classi di equivalenza di coppie di elementi di $\mathbb{N}$ rispetto alla seguente relazione di equivalenza:

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

In altre parole, esiste un'applicazione biettiva f tra l'insieme $\mathbb{Z}$ e l'insieme quoziente $\mathbb{N} \times \mathbb{N}/\sim$. L'applicazione è data da

$$\begin{array}{rl} f\colon \mathbb{Z} & \to \mathbb{N} \times \mathbb{N}/\sim \\ z & \mapsto \begin{cases} (z, 0) & \text{se } z \geq 0 \\ (0, -z) & \text{se } z < 0. \end{cases} \end{array}$$

Se dotiamo $\mathbb{N} \times \mathbb{N}/\sim$ di somma e prodotto definiti come segue:

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

la biezione f soddisferà le relazioni $f(z+z') = f(z)+f(z')$ e $f(zz') = f(z)\cdot f(z')$ per ogni $z, z' \in \mathbb{Z}$.

Esercizio 1.1 *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 definiti non dipendono dalla scelta dei rappresentanti.*

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 1.2 *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 1.3 *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 1.4 *Dimostrare per induzione che se $x_1, \ldots, x_k \geq 0$, allora $x_1 + \cdots + x_k \geq 0$.*

Esercizio 1.5 *Dimostrare che per ogni $x \in \mathbb{Z}$, $x^2 \geq 0$.*

1.1 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 $\mathbb{N}$.

1.1.1 Divisibilità

Definizione 1.6 *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 1.7 *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 1.8 *Dimostrare che dati $a, b \in \mathbb{Z}$, se $a|b$ e $b|a$ allora $a = \pm b$.*

Definizione 1.9 *Un elemento $p \in \mathbb{Z}$ è detto un numero primo se soddisfa le seguenti proprietà:*

- $p \neq 0, \pm 1$
- *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 1.10 *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

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

1.1.2 Massimo comun divisore

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

Definizione 1.11 *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 1.12 *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 1.13 *Dimostrare che per ogni a, $b \in \mathbb{Z}$ non nulli, $MCD(a, b) = MCD(-a, b) = MCD(a, -b) = MCD(-a, -b)$.*

Esercizio 1.14 *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 1.15 *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 1.16 *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*

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

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 1.13 e calcolare il massimo comun divisore di due numeri positivi con l'algoritmo di Euclide in $\mathbb{N}$.

Osserviamo inoltre che, applicando l'algoritmo di Euclide agli interi a e b e percorrendolo a ritroso, tutti i resti non nulli che si ottengono possono essere scritti nella forma $r_i = m_i a + n_i b$ con $m_i, n_i \in \mathbb{Z}$. Ad esempio, $r_1 = b - aq_1$ quindi $m_1 = -q_1$ e $n_1 = 1$; inoltre $r_2 = a - q_2 r_1 = a - q_2(b - aq_1) = (1 + q_1 q_2)a - q_2 b$ quindi $m_2 = (1 + q_1 q_2)$ ed $n_2 = -q_2$ e così via. In particolare

Il massimo comun divisore di a e b può essere sempre scritto nella forma $MCD(a, b) = ma + nb$ per qualche $n, m \in \mathbb{Z}$. Tale ugualglianza è detta *uguaglianza di Bézout.*

Esercizio 1.17 *Calcolare $MCD(127, -12)$ con l'algoritmo di Euclide e determinare m, $n \in \mathbb{Z}$ tali che $MCD(127, -12) = m(127) + n(-12)$.*

1.2 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.

1.2.1 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 1.18 *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 1.19 *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. $125 \equiv 4 \mod 11$.

La classe di equivalenza di un elemento $a \in \mathbb{Z}$ rispetto alla relazione di congruenza modulo n ha la forma:

$$[a] = \{z \in \mathbb{Z} \mid z = a + nl \text{ per qualche } l \in \mathbb{Z}\}$$

ad esempio, se $n = 5$ ed $a = 0$ avremo

$$[0] = \{z \in \mathbb{Z} \mid z = 5l \text{ per qualche } l \in \mathbb{Z}\}$$

cioè la classe di 0 modulo 5 è data dall'insieme dei multipli di 5 in $\mathbb{Z}$.

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 1.20 *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.*

Osservazione 1.21 *Dati $m, a, n, b \in \mathbb{Z}$ con n diverso da 0 ed $a, m \not\equiv 0 \mod n$, un elemento $z \in \mathbb{Z}$ è soluzione dell'equazione*

$$aX \equiv b \mod n \tag{1.1}$$

se e soltanto se è soluzione dell'equazione

$$amX \equiv bm \mod nm \tag{1.2}$$

perché se n divide $az-b$ allora mn divide $amz-bm$ e viceversa, se mn divide $amz-bm$ allora esiste $l \in \mathbb{Z}$ tale che $mnl = m(az-b)$ quindi esiste $l \in \mathbb{Z}$ tale che $nl = az-b$ cioè n divide $az-b$. Pertanto è equivalente risolvere l'equazione (1.1) *o l'equazione* (1.2).

Esempio 1.22 *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 1.23 *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 1.24 *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. $11X \equiv 2 \mod 10$.

Esercizio 1.25 *Dimostrare che se $a \not\equiv 0 \mod n$ abbiamo $MCD(a,n) = MCD(a+ln,n)$ per ogni $l \in \mathbb{Z} \setminus \{0\}$, ovvero il massimo comun divisore tra a ed n non dipende dalla scelta del rappresentante della classe di a modulo n.*

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

Abbiamo un'altra caratterizzazione della relazione di congruenza introdotta:

Proposizione 1.26 *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.

L'insieme quoziente rispetto alla relazione di equivalenza $\mod n$ su $\mathbb{Z}$ si denota con $\mathbb{Z}/n\mathbb{Z}$. Esso è dotato di un'operazione di somma e di un'operazione di prodotto date da:

$$[a] + [b] = [a + b], \quad [a] \cdot [b] = [ab]$$

per ogni coppia di classi $[a], [b] \in \mathbb{Z}/n\mathbb{Z}$.

Ci chiediamo ora quante siano le classi di equivalenza e come possiamo elencarle tutte. La seguente proposizione risponde a questa domanda.

Proposizione 1.27 *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 1.28 *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 1.29 *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 1.30 *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 1.31 *Verificare quali proprietà della somma e del prodotto in $\mathbb{Z}$ valgono ancora in $\mathbb{Z}/n\mathbb{Z}$.*

Osserviamo che risolvere una congruenza dellla forma $aX \equiv b(\mod n)$ con $a \not\equiv 0 \mod n$ fornisce o nessuna soluzione, oppure infinite soluzioni che corrispondono ad un'unione di una o più classi di equivalenza modulo n. Questo segue dalle proprietà delle congruenze. Sappiamo che esistono soluzioni se e solo se $d = MCD(a, n)$ divide b e che le soluzioni in questo caso sono d a meno di congruenza. In altre parole, possiamo dire che l'equazione $[a]X = [b]$ in $\mathbb{Z}/n\mathbb{Z}$ ha soluzioni se e solo se $d = MCD(a, n)$ divide b. (Per l'Esercizio 1.25 il numero d non dipende dalla scelta del rappresentante della classe $[a]$ scelto). Inoltre, in questo caso, le soluzioni saranno *classi* ed il numero di soluzioni in $\mathbb{Z}/n\mathbb{Z}$ è finito e pari a d. Ad esempio, se consideriamo $[4]X = [8]$ in $\mathbb{Z}/14\mathbb{Z}$ deduciamo dall'Esempio 1.22 che essa ammette 2 soluzioni, precisamente [9] e [2].

1.2.3 Il Teorema Cinese dei Resti

Ci potrebbe capitare di voler risolvere un *sistema di congruenze*, ovvero di cercare gli elementi di $\mathbb{Z}$ che soddisfino una famiglia di congruenze. Abbiamo alcuni risultati che ci garantiscono che in certi casi la soluzione esiste e ci dicono come determinare *tutte* le soluzioni.

Teorema 1.32 *Sia dato un sistema di congruenze*

$$\begin{cases} a_1X & \equiv b_1 & \mod n_1 \\ a_2X & \equiv b_2 & \mod n_2 \\ \cdots & \equiv \cdots & \\ a_rX & \equiv b_r & \mod n_r \end{cases}$$

con $a_i \not\equiv 0 \mod n_i$ e $d_i = MCD(a_i, n_i) | b_i$ per ogni $i = 1, \ldots, r$.
Sia ora $m_i = \frac{n_i}{d_i}$ per ogni $i = 1, \ldots, r$.

Se $MCD(m_i, m_j) = 1$ per ogni $i \neq j$ allora il sistema ammette soluzioni. Più precisamente, il sistema ammetterà un'unica soluzione a meno di multipli di $m = m_1 \cdots m_r$.
In particolare, se $MCD(a_i, n_i) = 1$ per ogni $i = 1, \ldots, r$, con $MCD(n_i, n_j) = 1$ per ogni $i \neq j$, allora il sistema ammette un'unica soluzione a meno di multipli di $n = n_1 \cdots n_r$.

Dimostrazione: (idea:) Poiché $a_i \not\equiv 0 \mod n_i$ e $MCD(a_i, n_i)|b_i$ per ogni $i = 1, \ldots, r$ ciascuna equazione presa singolarmente possiede una soluzione modulo n_i/d_i. Se c_i è una soluzione di $a_i X \equiv b_i \mod n_i$ allora questa equazione è equivalente all'equazione $X \equiv c_i \mod (n_i/d_i)$ ed il sistema è equivalente al sistema

$$\begin{cases} X & \equiv c_1 \mod (n_1/d_1) \\ X & \equiv c_2 \mod (n_2/d_2) \\ \cdots & \equiv \cdots \\ X & \equiv c_r \mod (n_r/d_r) \end{cases}$$

Scriviamo $m_i = (n_i/d_i)$ per comodità. Le soluzioni della prima equazione sono tutti e soli gli interi della forma $x = c_1 + l_1 m_1$ al variare di $l_1 \in \mathbb{Z}$. Sostituiamo questi valori nella seconda equazione: m_1 e c_1 sono fissati e dovremo cercare condizioni su l_1 affinché anche la seconda equazione sia verificata. Avremo $c_1 + l_1 m_1 \equiv c_2 \mod m_2$. Questa, come equazione nell'incognita l_1 è equivalente all'equazione $m_1 l_1 \equiv c_2 - c_1 \mod m_2$ che ammette un'unica soluzione c_{12} modulo m_2 perché $MCD(m_1, m_2) = 1$. Perciò $l_1 = c_{12} + l_2 m_2$ al variare di l_2 in $\mathbb{Z}$ e, sostituendo i valori di l_1 nell'espressione di x otterremo $x = c_1 + c_{12} m_1 + l_2 m_1 m_2$ che, al variare di l_2 in $\mathbb{Z}$ ci dà tutte le soluzioni simultanee delle prime due equazioni. Ora procediamo induttivamente, sostituendo questi valori di x nella terza equazione e cercando le condizioni che deve soddisfare l_2 affinché x sia anche soluzione della terza equazione, e così via. La condizione $MCD(m_i, m_j) = 1$ ci assicura che ad ogni passo l'equazione nella l_i ottenuta ha soluzione ed il procedimento mostra che le soluzioni sono uniche, al passo i, modulo $m_1 m_2 \cdots m_i$. Questa procedura ci offre anche una strategia di soluzione del sistema, che sarà unica a meno di multipli di $m_1 \cdots m_r$. Nel caso particolare in cui $d_i = MCD(a_i, n_i) = 1$ per ogni i, avremo $m_i = n_i$ per ogni i e la soluzione sarà unica modulo $n_1 \cdots n_r$. □

Attenzione! A differenza della Proposizione 1.20, che ci dice precisamente *quando* una congruenza $aX \equiv b \mod n$ ammette soluzioni, il Teorema 1.32 ci dà solo una condizione *sufficiente* a garantire l'esistenza delle soluzioni. Tale condizione non è *necessaria*, vale a dire che esistono dei casi di sistemi che ammettono soluzioni pur non soddisfacendo la condizione sui moduli del Teorema. Per tali sistemi ovviamente sono verificate le condizioni dettate dalla Proposizione 1.20. Un esempio è dato da:

$$\begin{cases} 4X & \equiv 3 \mod 5 \\ 3X & \equiv 1 \mod 5 \end{cases}$$

che non soddisfa le condizioni del teorema ma ammette le soluzioni della forma $x = 2 + 5k$ al variare di $k \in \mathbb{Z}$.

Esempio 1.33 *Consideriamo il sistema di congruenze ed illustriamo un metodo per risolverle:*

$$\begin{cases} 3X & \equiv 1 \mod 5 \\ 2X & \equiv 1 \mod 7 \\ 3X & \equiv 15 \mod 6 \end{cases}$$

Per prima cosa osserviamo che ciascuna equazione presa singolarmente soddisfa le condizioni della Proposizione 1.20 e che i moduli della tre equazioni soddisfano le condizioni del Teorema 1.32. Pertanto siamo sicuri che esistono soluzioni di questo sistema. Inoltre la terza equazione può essere semplificata riducendo prima il termine noto 15 *modulo* 6*, e poi dividendo coefficiente, modulo e termine noto per* $3 = MCD(3, 6)$*. Quest'ultimo passaggio è lecito grazie all'Osservazione 1.21. Il sistema è quindi equivalente al sistema :*

$$\begin{cases} 3X & \equiv 1 \mod 5 \\ 2X & \equiv 1 \mod 7 \\ X & \equiv 1 \mod 2 \end{cases}$$

Le soluzioni della prima equazione (risolte con il metodo già mostrato) sono date da tutti gli interi x *che si possono scrivere come* $x = 2 + 5l$ *per qualche* $l \in \mathbb{Z}$*. Ora sostituiamo questi valori di* x *nella seconda equazione, che diverrà una equazione nell'incognita* l*: Avremo:*

$2(2 + 5l) \equiv 1 \mod 7$ *le cui soluzioni sono tutte e sole le soluzioni di*
$4 + 10l \equiv 1 \mod 7$ *le cui soluzioni sono tutte e sole le soluzioni di*
$10l \equiv -3 \mod 7$ *le cui soluzioni sono tutte e sole le soluzioni di*
$3l \equiv -3 \mod 7$ *le cui soluzioni sono tutte e sole le soluzioni di*
$l \equiv -1 \mod 7$

quindi le soluzioni simultanee delle prime due equazioni sono date da tutti gli interi x *che si possono scrivere come* $x = 2 + 5l$ *con* $l = -1 + 7k$ *al variare di* $k \in \mathbb{Z}$*. In altre parole, esse sono date da tutti gli interi* x *che si possono scrivere come* $x = 2 + 5(-1 + 7k) = -3 + 35k$ *al variare di* $k \in \mathbb{Z}$*. Per cercare le soluzioni comuni a tutte e tre le equazioni del sistema dato, sostituiremo quindi questi valori di* x *nell'ultima equazione. Questo ci dirà quali condizioni dovrà soddisfare* k *affinché* x *sia soluzione anche della terza equazione. Avremo* $-3 + 35k \equiv 1 \mod 2$ *che equivale a* $35k \equiv 4 \mod 2$ *e simplificando coefficiente e termine noto modulo* 2 *avremo* $k \equiv 0 \mod 2$*, cioè* k *deve essere un multiplo di* 2*, ovvero* $k = 2t$ *per qualche* $t \in \mathbb{Z}$*. Pertanto, le soluzioni del sistema sono date da* $\{x \in \mathbb{Z} \mid x = -3 + 70t,\ t \in \mathbb{Z}\}$*.*

Esercizio 1.34 *Dire se il seguente sistema di congruenze ammette soluzione ed, in caso affermativo, trovare tutte le soluzioni:*

$$\begin{cases} 34X & \equiv 14 \mod 26 \\ 5X & \equiv 13 \mod 7 \\ 11X & \equiv 17 \mod 5 \end{cases}$$

Esercizio 1.35 *Dire se il seguente sistema di congruenze ammette soluzione ed, in caso affermativo, trovare tutte le soluzioni:*

$$\begin{cases} 34X & \equiv 14 \mod 26 \\ 5X & \equiv 13 \mod 7 \\ 12X & \equiv 17 \mod 15 \end{cases}$$