0.1 Complementi sulle Congruenze

Teorema 0.1.1. *(Divisione Euclideo) Per ogni coppia di numeri interi* $a, b \in \mathbb{Z},\ b \neq 0$ *esistono interi* $q, r \in \mathbb{Z}$ *tali che*

$$a = qb + r \quad \textit{ed} \quad 0 \leq r < |b|.$$

q *ed* r *sono univocamente determinati*.

q è il ***quoziente*** della divisione di a per b ed r è il ***resto*** della divisione. Nel caso in cui $r = 0$ diremo che b ***divide*** a e scriveremo $b|a$. Se b non divide a, allora $b \nmid a$.

Dim. Possiamo supporre, senza restrizioni, che sia anche $b \neq \pm 1$. Si consideri l'insieme

$$R = \{a - nb \mid n \in \mathbb{Z},\ a - nb \geq 0\}.$$

Tale insieme è non vuoto, infatti: per $a = n$ si ha $a - nb = a(1 - b) \neq 0$, poichè $a - ab = 0$ fornirebbe $b = 1$. Analogamente, per $a = -n$ si ottiene $a(1 + b) \neq 0$. Una delle due quantità deve essere maggiore di 0.
Essendo R un sottinsieme non vuoto di $\mathbb{N}$, esso ammette minimo r.
Si ha quindi $r = a - qb$, p.q. $q \in \mathbb{Z}$, ed anche $r \leq |b|$. Se fosse infatti $s = r - |b| \geq 0$, allora

$$s = a - qb - |b| = a - (q + \frac{|b|}{b})b \in R,$$

che non è possibile. Supponiamo poi che sia contemporaneamente

$$a = qb + r \quad \text{ed} \quad a = q'b + r' \quad \text{con} \quad 0 \leq r, r' < |b|.$$

Allora $r - r' = (q' - q)b$, quindi

$$|r - r'| = |q' - q||b| < |b|,$$

da cui $|q' - q| < 1$. Deve essere $|q' - q| = 0$. Segue $q = q'$ ed anche $r = r'$ □

Teorema 0.1.2. *(Identità di Bezout) Siano $a, b \in \mathbb{Z}$ numeri interi non nulli tali che $b \nmid a$ e $a \nmid b$. Allora esistono $x, y \in \mathbb{Z}$ tali che*

$$M.C.D.(a, b) = xa + yb.$$

Corollario 0.1.3. *$a, b \in \mathbb{Z}$ sono primi tra loro se e solo se esistono interi $x, y \in \mathbb{Z}$ tali che*

$$1 = xa + yb.$$

Dim. Una impicazione è ovvia. Viceversa, se vale $1 = xa + yb$, supponiamo $d = MCD(a, b)$, allora $a = a'd$ e $b = b'd$. Da

$$1 = xa'd + yb'd$$

segue $d|1$ e quindi $d = 1$.

Esempio 0.1.4. *Calcoliamo il massimo comun divisore tra $a = 66$ e $b = 28$ con un procedimento di divisioni successive che terminano al minimo resto non nullo:*

$$66 = 2 \cdot 28 + 10$$
$$28 = 2 \cdot 10 + 8$$
$$10 = 1 \cdot 8 + 2$$

Allora

$$2 = 10 - 1 \cdot 8 =$$
$$= 10 - 1 \cdot (28 - 2 \cdot 10) =$$
$$= 3 \cdot 10 - 1 \cdot 28 =$$
$$= 3 \cdot (66 - 2 \cdot 28) - 1 \cdot 28 =$$
$$= 3 \cdot 66 + (-7) \cdot 28$$

così $M.C.D.(66, 28) = x66 + y28 = 3 \cdot 66 + (-7) \cdot 28 = 2$.

Nel seguito indicheremo con $\mathbb{Z}_n$ l'anello commutativo con unità delle classi di resto modulo un intero positivo n. Esplicitamente

$$\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n-1]\},$$

ove, per due interi $a, b \in \mathbb{Z}$, si intende

$$[a] = [b] \Leftrightarrow a \equiv_n b \Leftrightarrow a - b = kn, \ k \in \mathbb{Z}.$$

Proposizione 0.1.5. *Dati numeri interi $a, b, c, m, n \in \mathbb{Z}$, con $m, n > 0$, si ha:*

1. $a \equiv_n b \Leftrightarrow a + c \equiv_n b + c$, *cioè* $[a] = [b] \Rightarrow [a + c] = [b + c]$
2. $a \equiv_n b \Leftrightarrow ac \equiv_n bc$, *cioè* $[a] = [b] \Rightarrow [ac] = [bc]$
3. $a \equiv_n b \Leftrightarrow am \equiv_{nm} bm$
4. $a \equiv_{nm} b \Rightarrow a \equiv_n b$
5. $a \equiv_n b, a \equiv_m b \Leftrightarrow a \equiv_{m.c.m(n,m)} b$

Dim. La prova delle cinque affermazioni segue dalla definizione di congruenza (mod n) e si lascia al lettore come esercizio. □

Abbiamo già notato che, ad es., in $\mathbb{Z}_6$ esistono elementi non nulli che moltiplicati tra loro danno come risultato lo zero: $[2][3] = [0]$. Elementi di questo tipo in un anello si chiamano *divisori dello zero*. Se K è un campo, esso non può contenere divisori dello zero, infatti, se $x, y \in K$, con $y \neq 0$, tali che $xy = 0$, allora

$$x = xyy^{-1} = 0y^{-1} = 0.$$

Proposizione 0.1.6. *Una classe di resto non nulla $[a] \in \mathbb{Z}_n$ è invertibile se e solo se $MCD(a, n) = 1$.*

Dim. Si ha che:

$$\text{esiste } [c] \in \mathbb{Z}_n \text{ tale che } [a] \cdot [c] = [1] \Leftrightarrow$$

$$\Leftrightarrow [ac] = [1] \Leftrightarrow ac - 1 = nk \Leftrightarrow$$

$$\Leftrightarrow 1 = ac - nk \Leftrightarrow MCD(a, n) = 1.$$

Teorema 0.1.7. *L'anello $\mathbb{Z}_n$ è un campo se e solo se n è un numero primo.*

Dim. Se n è primo allora ogni $[a] \neq [0]$ in $\mathbb{Z}_n$ è invertibile per la Proposizione predente, infatti $MCD(a, n) = 1$, essendo $a < n$.

Viceversa, sia $\mathbb{Z}_n$ un campo. Se n non fosse primo si potrebbe scrivere $n = rs$ con $0 < r, s < n$, allora

$$[0] = [n] = [rs] = [r][s] \quad \text{con} \quad [r], [s] \neq [0],$$

ovvero $\mathbb{Z}_n$ conterrebbe divisori dello zero.

Ci poniamo ora il problema della risoluzione di una equazione della forma

$$ax \equiv_n b.$$

Proposizione 0.1.8. *L'equazione data ammette una soluzione se e solo se* $M.C.D.(a, n)|b$.

Dim. Infatti, se $u \in \mathbb{Z}$ è tale che $au \equiv_n b$, allora

$$au - b = kn \Leftrightarrow b = au + kn.$$

Allora ogni divisore comune di a e n divide anche b.
Viceversa, poniamo $d = M.C.D.(a, n)$, possiamo quindi scrivere

$$a = a'd, \quad b = b'd, \quad n = n'd.$$

L'equazione di partenza si riscrive come

$$a'dx \equiv_{n'd} b'd$$

e questa, per la Prop.1.5 equivale a

$$a'x \equiv_{n'} b',$$

ed essendo $M.C.D.(a', n') = 1$ si risolve facilmente poichè $[a']$ è invertibile in $\mathbb{Z}_{n'}$: posto $[c] = [a']^{-1}$, segue $x \equiv_{n'} b'c$, così le soluzione dell'equazione di partenza sono tutti gli interi della forma

$$x = b'c + kn', \quad \text{per} \quad k \in \mathbb{Z}.$$

□

Esempio 0.1.9. *Sia data l'equazione*

$$6x \equiv_{14} 8.$$

Questa è risolubile poichè $M.C.D.(6,14) = 2$*, che divide* 8*. L'equazione data equivale alla*

$$3x \equiv_7 4.$$

Si ha $[5] = [3]^{-1}$ *in* $\mathbb{Z}_7$*, allora*

$$[x] = [4][5] = [20] = [6]$$

così

$$x = 6 + 7k,\ k \in \mathbb{Z}.$$

Consideriamo ora un sistema di equazioni del tipo

$$\begin{cases} b_1 x \equiv_{n_1} c_1 \\ b_2 x \equiv_{n_2} c_2 \end{cases}$$

che pone il problema di trovare soluzioni comuni alle due congruenze. Naturalmente queste devono essere entrambe risolubili, cioè si deve avere

$$M.C.D.(b_i, n_i) | c_i, \quad i = 1, 2.$$

Se

$$x = a_1 + kn_1 \quad \text{e} \quad x = a_2 + kn_2$$

sono le soluzioni delle due equazioni, allora siamo alla ricerca di quegli interi x tali che

$$\begin{cases} x \equiv_{n_1} a_1 \\ x \equiv_{n_2} a_2 \end{cases}$$

quindi il primo sistema si riduce a quest'ultimo.
Supponiamo dapprima $M.C.D.(n_1, n_2) = 1$. Allora esistono interi $y, z \in \mathbb{Z}$ per cui

$$1 = yn_1 + zn_2.$$

Moltiplicando entrambi i membri dell'uguaglianza per $a_2 - a_1$ si ottiene

$$a_2 - (a_2 - a_1)zn_2 = a_1 + (a_2 - a_1)yn_1.$$

Se u è il valore comune dei due membri, segue allora

$$\begin{cases} u \equiv_{n_1} a_1 \\ u \equiv_{n_2} a_2 \end{cases}$$

e si è trovata una soluzione del sistema di partenza.
Tutte le altre soluzioni del sistema sono gli interi della forma

$$s = u + kn_1n_2,\ k \in \mathbb{Z}.$$

Infatti, se s è della forma sopra, allora

$$s \equiv_{n_1n_2} u \Rightarrow s \equiv_{n_1} u,$$

$$s \equiv_{n_1n_2} u \Rightarrow s \equiv_{n_2} u,$$

e, per la Prop. 1.5, anche

$$s \equiv_{n_1} a_1,$$

$$s \equiv_{n_2} a_2.$$

Viceversa, se s è soluzione, si vede subito dalle relazioni precedenti che

$$s \equiv_{n_1} u,$$

$$s \equiv_{n_2} u,$$

quindi l'asserto, ancora per la Prop. 1.5.

Esempio 0.1.10. *Sia dato il sistema*

$$\begin{cases} x \equiv_{10} 3 \\ x \equiv_{23} 4 \end{cases}$$

Si ha $M.C.D.(10, 23) = 1$ *e l'dentità di Bezout*

$$1 = 7 \cdot 10 + (-3) \cdot 23,$$

quindi una soluzione è

$$u = a_2 - (a_2 - a_1)zn_2 = 4 - (4 - 3)(-3)23 = 73,$$

mentre la soluzione generale si ottiene come

$$s = u + kn_1n_2 = 73 + k230,$$

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

In generale si ha:

Teorema 0.1.11. *Il sistema*

$$\begin{cases} x \equiv_{n_1} a_1 \\ x \equiv_{n_2} a_2 \end{cases}$$

ammette soluzioni se e solo se $M.C.D.(n_1, n_2) = d$ *divide* $a_2 - a_1$.
Posto

$$d = yn_1 + zn_2,$$

una soluzione è

$$u = a_1 - czn_2, \quad \textit{ove} \quad a_2 - a_1 = cd,$$

mentre la soluzione generale è

$$s = u + k \cdot m.c.m.(n_1, n_2).$$

Esempio 0.1.12. *Sia dato il sistema*

$$\begin{cases} x \equiv_8 1 \\ x \equiv_{10} 5 \end{cases}$$

$M.C.D.(8, 10) = 2$ *e* $2 \mid a_2 - a_1 = 5 - 1$. *Quindi il sistema è risolubile*.
Si ha $c = 2,\ d = 2,\ 2 = (-1) \cdot 8 + 1 \cdot 10$. *Segue*

$$u = 5 - 2 \cdot 10 = -15.$$

Essendo $m.c.m.(8, 10) = 40$, *risulta*

$$s = -15 + 40k.$$