UNIVERSITÀ DEGLI STUDI DI MILANO - BICOCCA

LAUREA TRIENNALE IN INFORMATICA

Marina Avitabile

Appunti del Corso di Metodi Algebrici per l'Informatica

Settembre 2022

Indice

1 Algoritmo della divisione in $\mathbb{Z}$

Indichiamo con $\mathbb{Z}$ l'insieme dei numeri interi e con $\mathbb{N}$ l'insieme dei numeri naturali (con la convenzione che $0 \in \mathbb{N}$).

Una proprietà fondamentale dell'insieme $\mathbb{Z}$ è il cosiddetto Principio del Buon Ordinamento.

Principio del Buon Ordinamento

Sia n_0 un intero e $\mathbb{Z}_{n_0} = \{z \in \mathbb{Z} | z \geq n_0\}$. Ogni sottoinsieme non vuoto X di $\mathbb{Z}_{n_0}$ ammette minimo.

In altre parole, se $\emptyset \neq X \subseteq \mathbb{Z}_{n_0}$, esiste $x_0 \in X$ tale che $x_0 \leq x$, $\forall x \in X$. Il Principio del Buon Ordinamento è equivalente al Principio di Induzione, che enunceremo in due forme (tra loro equivalenti)

Principio di Induzione

1^a Forma:

Sia $n_0 \in \mathbb{Z}$ e sia $P = P(n)$ un enunciato che ha senso per ogni intero $n \geq n_0$. Se

1. $P(n_0)$ è vero;
2. per ogni $n > n_0$, $P(n-1)$ vero implica $P(n)$ vero;

allora $P(n)$ è vero per tutti gli $n \geq n_0$.

2^a Forma:

Sia $n_0 \in \mathbb{Z}$ e sia $P = P(n)$ un enunciato che ha senso per ogni intero $n \geq n_0$. Se

1'. $P(n_0)$ è vero;

2'. per ogni $n > n_0$, $P(m)$ vero per ogni m con $n_0 \leq m < n$ implica $P(n)$ vero;

allora $P(n)$ è vero per tutti gli $n \geq n_0$.

Esempi.

1. *Dimostrare che la somma dei primi n numeri interi positivi è uguale a $\frac{n(n+1)}{2}$. Qui $P(n)$ è $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$ e $n_0 = 1$. Usiamo la 1^a forma del Principio di Induzione:*
   (a) *$P(1)$ è vero, infatti $P(1)$ è la proposizione*
   $$1 = \sum_{k=1}^{1} k = \frac{1 \cdot 2}{2}$$
   (b) *per ogni $n > 1$, $P(n-1)$ vero implica $P(n)$ vero, infatti*
   $$\sum_{k=1}^{n} k = \sum_{k=1}^{n-1} k + n = \frac{(n-1) \cdot n}{2} + n = \frac{n \cdot (n+1)}{2}$$

2. *Dimostrare che se X è un insieme di cardinalità n, l'insieme delle parti $P(X)$ ha cardinalità 2^n. Di nuovo usiamo il Principio di Induzione nella 1^a forma. Qui $P(n)$ è:* se X è un insieme di cardinalità n allora $P(X)$ ha cardinalità 2^n e $n_0 = 0$.

   (a) *$P(0)$ è vero perchè se X ha 0 elementi, allora $X = \emptyset$. D'altra parte, $P(\emptyset) = \{\emptyset\}$ dunque $P(X)$ ha cardinalità $2^0 = 1$.*

   (b) *per ogni $n > 0$, mostriamo che $P(n-1)$ vero implica $P(n)$ vero. Dunque supponendo che, se un insieme X' ha $n-1$ elementi allora $P(X')$ ha 2^{n-1} elementi, mostriamo che, se X ha n elementi, allora $P(X)$ ha n elementi. Sia $x_0 \in X$ (che certamente esiste perchè $n > 0$ quindi $X \neq \emptyset$), e poniamo $X' = X \setminus \{x_0\}$, così X' è un insieme con $n-1$ elementi. I sottoinsiemi di X sono tutti e soli i sottoinsiemi di X' e quelli che si ottengono da questi ultimi aggiungendo l'elemento x_0 a ciascuno. Poichè $|P(X')| = 2^{n-1}$ si ha $|P(X)| = 2^{n-1} + 2^{n-1} = 2^n$.*

Esercizi.

1. *Dimostrare che*
$$\sum_{k=1}^{n} k^2 = \frac{1}{6} n(n+1)(2n+1)$$
per $n \geq 1$.

2. *Dimostrare che*
$$\sum_{k=1}^{n} k^3 = \left(\frac{1}{2} n(n+1)\right)^2$$
per $n \geq 1$.

Algoritmo della Divisione

Dati n, m interi con $n > m > 0$, l'usuale algoritmo della divisione permette di determinare due interi q e r (il quoziente e il resto della divisione) tali che mq è il multiplo di m che più si avvicina a n per difetto e $r = n - mq$ misura lo scarto.

Possiamo generalizzare con il seguente teorema:

Teorema. *Siano n, $m \in \mathbb{Z}$ con $m \neq 0$. Esistono e sono univocamente determinati due interi q e r tali che sia:*

1. $n = mq + r$
2. $0 \leq r < |m|$

Dimostrazione. *Esistenza di q e r*

Supponiamo come primo caso che $n \geq 0$. Fissato arbitrariamente m procediamo per induzione su n.

Se $n = 0$ le condizioni 1) e 2) sono verificate con $q = 0 = r$ perchè $0 = 0 \cdot m + 0$.

Sia $n > 0$. Se $n < |m|$ di nuovo le condizioni 1) e 2) sono verificate con $q = 0$ e $r = n$.

Se invece $n \geq |m|$ ovvero $n > n - |m| \geq 0$, per l'ipotesi di induzione, esistono q_1 e r_1 in $\mathbb{Z}$ tali che

$$n - |m| = mq_1 + r_1$$

con $0 \leq r_1 < |m|$. Allora

$$n = mq_1 + |m| + r_1$$

e, essendo $|m| = \pm m$, si ha

$$n = m(q_1 \pm 1) + r_1$$

con $0 \leq r < |m|$. Le condizioni 1) e 2) sono verificate ponendo $q = q_1 \pm 1$ e $r = r_1$. Sia infine $n < 0$. Allora $-n > 0$ e, per quanto appena dimostrato, esistono due interi q_1 e r_1 tali che

$$-n = mq_1 + r_1 \text{ con } 0 \leq r_1 < |m|$$

Segue che

$$n = -mq_1 - r_1$$

Se $r_1 = 0$ le condizioni 1) e 2) sono verificate ponendo $q = -q_1$ e $r = 0$. Se invece $r_1 > 0$ si ha

$$\begin{aligned} n &= -mq_1 - r_1 = -mq_1 - |m| + |m| - r_1 \\ &= m(-q_1 \pm 1) + |m| - r_1 \end{aligned}$$

Le condizioni 1) e 2) sono soddisfatte ponendo $q = -q_1 - 1$ e $r = m - r_1$ se $m > 0$ e $q = -q_1 + 1$ e $r_1 = -m - r_1$ se $m < 0$.

Unicità di q e r

Sia $n = mq + r$ con $0 \leq r < |m|$ e $n = m\overline{q} + \overline{r}$ con $0 \leq \overline{r} < |m|$. Senza perdita di generalità si può supporre che $r \geq \overline{r}$ cioè $0 \leq r - \overline{r} < |m|$. Da $n = mq + r = m\overline{q} + \overline{r}$ si ha $r - \overline{r} = m(\overline{q} - q)$. Passando ai moduli si ottiene

$$|m| \cdot |\overline{q} - q| = |r - \overline{r}| = r - \overline{r} < |m|$$

quindi $|\overline{q} - q| < 1$. Ma q e $\overline{q}$ sono in $\mathbb{Z}$, dunque $\overline{q} - q \in \mathbb{Z}$ e pertanto $\overline{q} - q = 0$. Segue che anche $r - \overline{r} = 0$ ovvero $q = \overline{q}$ e $r = \overline{r}$. □

Definizione. *Gli interi q e r del teorema precedente si dicono quoziente e resto della divisione di n per m.*

Osservazione. *Dati n e m in $\mathbb{Z}$ con $m \neq 0$ esistono infinite coppie di interi x e y che soddisfano la condizione 1) del teorema precedente, cioè $n = mx + y$. Infatti, scelto comunque un intero x, basta porre $y = n - mx$. È invece unica la coppia q, r che soddisfa entrambe le condizioni 1) e 2).*

2 Massimo comun divisore e Algoritmo di Euclide

Definizione. *Siano $a, b \in \mathbb{Z}$. Se esiste $c \in \mathbb{Z}$ con $a = bc$ diciamo che b divide a e scriviamo $b \mid a$.*

Osservazione. *Se b divide a diciamo anche che a è un multiplo di b, ovvero b è un divisore (o fattore) di a. Ovviamente ± 1 e $\pm a$ sono divisori di ogni intero a. Se $b \mid a$ e $b \neq \pm 1, \pm a$ diciamo che b è un divisore proprio di a.*

Osservazione. *Se a, b sono interi non nulli si ha che $a \mid b$ e $b \mid a$ se e solo se $a = \pm b$. Infatti se $a \mid b$ e $b \mid a$ allora $a = bc$ e $b = ad$ per certi $c, d \in \mathbb{Z}$. Sostituendo una nell'altra, si ottiene $b = bcd$ da cui $cd = 1$, dunque $c = d = 1$ o $c = d = -1$*

Esercizi.

1. *Dimostrare che se $c \mid a$ e $c \mid b$ allora $c \mid a + b$*
   se $c \mid a$ e $c \mid b$ allora $c \mid a - b$
   se $c \mid a$ e $c \mid b$ allora $c \mid ax + by \quad \forall x, y \in \mathbb{Z}$
2. *Dimostrare che se $c \mid a$ allora $c \mid a + b$ se e solo se $c \mid b$*

Definizione. *Siano $a, b \in \mathbb{Z}$, entrambi diversi da zero. Si dice massimo comun divisore fra a e b ogni intero d tale che*

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

Teorema (Esistenza di un massimo comune divisore)**.** *Per ogni $a, b \in \mathbb{Z}$ con $a > 0$ e $b > 0$ esiste un massimo comun divisore d fra a e b. Esistono inoltre $x, y \in \mathbb{Z}$ tali che*

$$d = ax + by \qquad \text{Identità di Bezout}$$

Dimostrazione. Si supponga $a \geq b$ e si eseguano le divisioni successive

$$\begin{array}{lll} & a = bq_1 + r_1, & 0 \leq r_1 < b \\ \text{se } r_1 \neq 0 & b = r_1 q_2 + r_2, & 0 \leq r_2 < r_1 \\ \text{se } r_2 \neq 0 & r_1 = r_2 q_3 + r_3, & 0 \leq r_3 < r_2 \end{array}$$

e così via.

Poichè la sequenza dei resti delle divisioni successive è strettamente decrescente, dopo un numero finito di divisioni si ottiene resto $r_k = 0$.

Se $k = 1$, cioè se $r_1 = 0$, allora $b \mid a$ e un massimo comun divisore tra a e b è b.

Se $k > 1$, cioè se $r_1 \neq 0$, si ha

$$\begin{array}{rll}
(1) & a = bq_1 + r_1 & r_1 \neq 0 \\
(2) & b = r_1 q_2 + r_2 & r_2 \neq 0 \\
(3) & r_1 = r_2 q_3 + r_3 & r_3 \neq 0 \\
\vdots & \vdots & \vdots \\
(k-1) & r_{k-3} = r_{k-2} q_{k-1} + r_{k-1} & r_{k-1} \neq 0 \\
(k) & r_{k-2} = r_{k-1} q_k &
\end{array}$$

Dimostriamo che r_{k-1} è un massimo comun divisore tra a e b.

1. $r_{k-1} \mid a$ e $r_{k-1} \mid b$ Sostituendo (k) in $(k-1)$ si ha

   $$r_{k-3} = q_{k-1} q_k r_{k-1} + r_{k-1} = r_{k-1}(q_{k-1} q_k + 1)$$

   dunque $r_{k-1} | r_{k-3}$. Scriviamo per semplicità $r_{k-3} = \overline{q} r_{k-1}$. Sostituendo quest'ultima condizione in $(k-2)$ si ha

   $$\begin{aligned}
   r_{k-4} &= q_{k-2} r_{k-3} + r_{k-2} \\
   &= \overline{q} q_{k-2} r_{k-1} + q_k r_{k-1} \\
   &= r_{k-1}(\overline{q} q_{k-2} + q_k)
   \end{aligned}$$

   ovvero $r_{k-1} \mid r_{k-4}$. Procedendo in questo modo, cioè risalendo le varie divisioni, si trova che $r_{k-1} \mid b$ e $r_{k-1} \mid a$.

2. Se $c \in \mathbb{Z}$ con $c \mid a$ e $c \mid b$ allora $c \mid r_{k-1}$. Sia $a = c\overline{a}$ e $b = c\overline{b}$. Dalla (1) si ottiene

   $$r_1 = a - bq_1 = \overline{a}c - \overline{b}cq_1 = c(\overline{a} - \overline{b} q_1)$$

   quindi $c \mid r_1$. Posto $r_1 = c\overline{r_1}$ dalla (2) si ha

   $$r_2 = b - r_1 q_2 = \overline{b}c - c\overline{r_1} q_2 = c(\overline{b} - \overline{r_1} q_2)$$

   ovvero $c \mid r_2$. Procedendo in questo modo, cioè scendendo le divisioni, si ha che $c \mid r_{k-1}$. Si conclude quindi che r_{k-1} è un massimo comun divisore tra a e b. Per la seconda parte dell'enunciato, l'identità di Bezout, la (1) permette di scrivere r_1 nella forma

   $$r_1 = a \cdot 1 + b(-q_1)$$

   Sostituendo quest'ultima nella (2) si ha

   $$\begin{aligned}
   r_2 &= b - r_1 q_2 \\
   &= b - q_2(a - bq_1) \\
   &= b + bq_1 q_2 - q_2 a \\
   &= a(-q_2) + b(1 + q_1 q_2)
   \end{aligned}$$

   Procedendo in questo modo, si esprime ciascun resto come *combinazione lineare* di a e b. In particolare esistono $x, y \in \mathbb{Z}$ tali che

   $$r_{k-1} = ax + by.$$

□

Teorema. *Se d è un massimo comun divisore tra a e b, l'unico altro massimo comun divisore è $-d$.*

Dimostrazione. È ovvio che se d è un massimo comun divisore tra a e b, allora anche $-d$ lo è. Sia ora $\overline{d}$ un altro massimo comun divisore tra a e b. Dalla definizione abbiamo che

1. $d \mid a$ e $d \mid b$
2. $\forall c \in \mathbb{Z}$, se $c \mid a$ e $c \mid b$ allora $c \mid d$

e

1'. $\overline{d} \mid a$ e $\overline{d} \mid b$

2'. $\forall \overline{c} \in \mathbb{Z}$, se $\overline{c} \mid a$ e $\overline{c} \mid b$ allora $\overline{c} \mid \overline{d}$

Pensando d come $\overline{c}$ abbiamo che $d \mid \overline{d}$ e, pensando $\overline{d}$ come c, abbiamo $\overline{d} \mid d$. Segue che $\overline{d} = \pm d$. □

Per convenzione ci riferiamo al massimo comun divisore positivo tra a e b. Lo indichiamo con (a, b) e dunque è il massimo comun divisore tra a e b.

Osservazione. *È facile verificare che, per a, $b \in \mathbb{Z}$ entrambi non nulli, si ha*

$$(a, b) = (-a, b) = (a, -b) = (-a, -b)$$

Definizione. *Due interi a, b si dicono relativamente primi o coprimi se $(a, b) = 1$.*

Osservazione.

1. *Siano a, $b \in \mathbb{Z}$ e sia $d = (a, b)$. Posto $a = \overline{a}d$ e $b = \overline{b}d$ si ha $(\overline{a}, \overline{b}) = 1$ cioè $\overline{a}$ e $\overline{b}$ sono coprimi. Infatti, posto $t = (\overline{a}, \overline{b})$, abbiamo $td \mid a$ e $td \mid b$ dunque $td \mid d$ da cui $t = 1$*
2. *se $(a, b) = 1$ e $a \mid bc$ allora $a \mid c$. Infatti, poichè $(a, b) = 1$, esistono x, $y \in \mathbb{Z}$ con*

$$1 = xa + yb.$$

Moltiplicando per c si ha

$$c = xac + ybc.$$

Ma $a \mid bc$, dunque $bc = at$, sostituendo nell'uguaglianza sopra si trova

$$c = xac + ayt = a(xc + yt)$$

ovvero $a \mid c$.

Esempio. *Troviamo il massimo comun divisore tra* $a = 589$ *e* $b = 437$

$$\begin{aligned} 589 &= 437 \cdot 1 + 152 \\ 437 &= 152 \cdot 2 + 133 \\ 152 &= 133 \cdot 1 + 19 \\ 133 &= 19 \cdot 7 \end{aligned}$$

allora $(589, 437) = 19$. *Identità di Bezout:*

$$\begin{aligned} 152 &= a - b \\ 133 &= b - 152 \cdot 2 = b - (a - b) \cdot 2 = b - 2a + 2b = 3b - 2a \\ 19 &= 152 - 133 = (a - b) - (3b - 2a) = 3a - 4b \\ &= 3 \cdot 589 - 4 \cdot 437 \end{aligned}$$

3 Numeri in base b

Cominciamo con dimostrare il seguente:

Teorema. *Sia $b \in \mathbb{Z}$ con $b \geq 2$. Ogni intero $n \geq 0$ può essere scritto in uno e un solo modo nella forma*

$$n = d_k b^k + d_{k-1} b^{k-1} + \ldots + d_1 b + d_0$$

con $0 \leq d_i < b$ per ogni $i = 0 \ldots k$, $d_k \neq 0$ per $k > 0$.

Dimostrazione. Per induzione su n.

Per $n = 0$ l'asserto segue perché $n = 0 = 0 \cdot b^0$. Sia allora $n > 0$ e supponiamo vero l'asserto per ogni intero m con $0 \leq m < n$. Dividiamo n per b e troviamo

$$n = bq + r \text{ con } 0 \leq r < b$$

Poiché $q < n$, per l'ipotesi induttiva abbiamo che q può essere scritto in modo unico come

$$q = c_{k-1} b^{k-1} + c_{k-2} b^{k-2} + \ldots + c_1 b + c_0 \text{ con } 0 \leq c_i < b$$

Allora

$$n = bq + r = c_{k-1} b^k + c_{k-2} b^{k-1} + \ldots + c_1 b^2 + c_0 b + r$$

Posto $d_k = c_{k-1}$, $d_{k-1} = c_{k-2}, \ldots,$ $d_1 = c_0$, $d_0 = r$ si ha che

$$n = d_k b^k + d_{k-1} b^{k-1} + \ldots + d_1 b + d_0$$

con $0 \leq d_i < b$ per $i = 0 \ldots k$. Infine l'unicità di questa espressione segue dall'unicità di q ed r. □

Dati $b \in \mathbb{Z}$ con $b \geq 2$ e un numero naturale n tale che

$$n = d_k b^k + d_{k-1} b^{k-1} + \ldots + d_1 b + d_0$$

con $0 \leq d_i < b$ per ogni $i = 0 \ldots k$, $d_k \neq 0$ per $k > 0$, gli interi $d_0, d_1, \ldots d_k$ si dicono le *cifre* di n in base b e n si indica con la sequenza delle sue cifre in base b, ovvero con la sequenza $(d_k d_{k-1} \ldots d_0)_b$.

Conversione da base b a base 10

Dato il numero n che in base b è rappresentato dala sequenza $n = (d_k d_{k-1} \ldots d_0)_b$ vogliamo convertirlo in base 10. Conviene impostare la conversione in questo modo

$$n = (\ldots((d_k b + d_{k-1})b + d_{k-2})b + \ldots + d_1)b + d_0$$

Questo metodo comporta solo k moltiplicazioni per b e k addizioni.

Esempio.

$$\begin{aligned}(61405)_7 &= (((6 \cdot 7 + 1)7 + 4)7 + 0)7 + 5 \\ &= 14950\end{aligned}$$

Conversione da base 10 a base b

Per passare da base 10 a base b si osserva che $d_0, d_1, \ldots, d_k$ sono i resti delle divisioni

$$\begin{aligned} n &= bq + d_0, \quad 0 \le d_0 < b \\ q &= q_1 b + d_1, \quad 0 \le d_1 < b \\ q_1 &= q_2 b + d_2, \quad 0 \le d_2 < b \\ &\vdots \end{aligned}$$

e così via finchè non si ottiene quoziente nullo

Esempio.

$$\begin{aligned} 14950 &= 7 \cdot 2135 + 5 \\ 2135 &= 7 \cdot 305 + 0 \\ 305 &= 7 \cdot 43 + 4 \\ 43 &= 7 \cdot 6 + 1 \\ 6 &= 7 \cdot 0 + 6 \end{aligned}$$

dunque $14950 = (61405)_7$

Osservazione. *Il numero di cifre in base b di un intero non negativo n è*

$$k + 1 = \lfloor \log_b n \rfloor + 1 = \left\lfloor \frac{\log n}{\log b} \right\rfloor + 1$$

perché $b^k \le n < b^{k+1}$. Qui log *è il logaritmo naturale (in base e).*

4 Stime temporali

Esempio. *Supponiamo di voler sommare due numeri scritti in base 2: $n = (1111000)_2$ ed $m = (11110)_2$. Innanzitutto possiamo aggiungere degli zeri a sinistra di m, nella sua scrittura binaria, in modo che n ed m abbiano lo stesso numero di bit. Otteniamo così che $m = (0011110)_2$. Procediamo poi come siamo abituati a fare dalla scuola per la usuale somma:*

$$\begin{array}{cccccccc} & {}^{1}1 & {}^{1}1 & {}^{1}1 & 1 & 0 & 0 & 0 \\ & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ \hline 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{array}$$

Generalizziamo l'esempio. Per sommare n e m possiamo sempre assumere che n e m abbiano lo stesso numero di bit. Infatti se così non fosse, cioè se n avesse k bit e m avesse l bit, con $l < k$, basta aggiundere degli zeri a sinistra nella scrittura di m.

Per sommare n ed m, ciascuno di k bit, scriviamo n sopra m in colonna e fissiamo una colonna. Applichiamo poi la seguente procedura:

1. guardiamo il bit della prima riga e il bit della seconda riga che appartengono alla colonna fissata e guardiamo eventuali riporti sopra il primo bit;
2. se entrambi i bit sono 0 e non c'è riporto scriviamo 0 nella terza riga (in corrispondenza alla colonna fissata) e procediamo oltre, considerando la colonna successiva a sinistra di quella fissata;
3. se accade una e una sola delle seguenti eventualità:
   - entrambi i bit considerati sono 0 e c'è riporto;
   - uno dei bit considerati è 0 e l'altro è 1 e non c'è riporto

   scriviamo 1 nella terza riga e procediamo oltre (considerando la colonna successiva a sinistra di quella fissata);
4. se accade una e una sola delle seguenti eventualità:
   - entrambi i bit considerati sono 1 e non c'è riporto;
   - uno dei bit considerati è 0 e l'altro è 1 e c'è riporto

   scriviamo 0 nella terza riga, segniamo un riporto nella colonna successiva a sinistra e procediamo oltre (considerando la colonna successiva a sinistra di quella fissata);
5. se entrambi i bit considerati sono 1 e c'è riporto scriviamo 1 nella terza riga, segniamo un riporto nella colonna successiva a sinistra e procediamo oltre (considerando la colonna successiva a sinistra di quella fissata).

Eseguire questa procedura una volta si dice una operazione bit. Il tempo che un computer impiega per effettuare un calcolo è essenzialmente proporzionale al numero di operazioni bit necessarie. La costante di proporzionalità dipende dal computer usato e non tiene conto del tempo necssario

per operazioni di tipo *amministrativo* (come accedere alla memoria, copiare dati da un posto all'altro..).

Sommare due numeri di k bit richiede k operazioni bit (una per ciascuna colonna), procedendo da destra a sinistra lungo le colonne.

Occupiamoci ora della moltiplicazione. Vogliamo moltiplicare n di k bit per m di l bit.

Esempio. *Supponiamo di voler moltiplicare* $n = (10011)_2$ *per* $m = (1011)_2$.

$$\begin{array}{cccccccc} & & & 1 & 0 & 0 & 1 & 1 \\ & & & & 1 & 0 & 1 & 1 \\ \hline & & & 1 & 0 & 0 & 1 & 1 \\ & & 1 & 0 & 0 & 1 & 1 & \\ 1 & 0 & 0 & 1 & 1 & & & \\ \hline 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{array}$$

Generalizziamo l'esempio visto. Moltiplicando n per m otteniamo $l' \leq l$ righe (una per ogni bit pari a 1 nella scrittura di m) ciascuna delle quali è una copia di n traslata a sinistra di una certa distanza. Dobbiamo poi eseguire $l' - 1$ somme (si somma la prima riga alla seconda, al risultato si aggiunge la terza e così via). Le somme parziali si allungano, cioè hanno un numero di bit maggiore di k, però ciscuna somma comporta solo k operazioni bit non banali. Nel nostro esempio la somma tra la prima e la seconda riga fornisce $s = 111001$. A questo numero dobbiamo sommare la terza riga cioè il numero 10011000. Gli ultimi tre bit del risultato sono esattamente gli ultimi tre bit di s, che dunque possiamo semplicemente ricopiare. Gli altri bit del risultato si ottengono sommando 111 a 10011. In tutto le operazioni bit necessarie per la moltiplicazione sono pertanto

$$(l' - 1)k \leq (l - 1)k < lk$$

La notazione O-grande

Definizione. *Siano* $f, g : \mathbb{N}^+ \to \mathbb{R}^+$ *due funzioni definite sull'insieme dei naturali positivi a valori nei reali positivi. Diciamo che* $f \in O(g)$ *se esistono due costanti* $B > 0$, $C > 0$ *tali che per ogni* $n > B$ *si ha*

$$f(n) < Cg(n).$$

Osservazioni. *1. Se* $f \in O(g)$ *e* $g \in O(h)$ *allora* $f \in O(h)$. *Quindi se* $f \in O(g)$ *possiamo rimpiazzare* g *con una funzione che cresce più velocemente di* g. *Nella pratica però vogliamo scegliere* g *in modo che la stima sia la migliore possibile per limitare* f, *preferendo funzioni* g *che siano semplici da descrivere.*

2. Se esiste finito il limite

$$\lim_{n \to +\infty} \frac{f(n)}{g(n)}$$

allora $f \in O(g)$.

3. *Se $f(n)$ è un polinomio di grado d con coefficiente direttivo positivo, cioè se*

$$f(n) = a_d n^d + a_{d-1} n^{d-1} + \cdots + a_1 n + a_0,$$

con $a_d > 0$, allora $f \in O(n^d)$.

4. *Se $f(n)$ è la funzione che restituisce il numero di bit di n, per quanto visto in precedenza, si ha $f(n) \in O(logn)$. La stessa stima vale per qualunque altra base b.*

Concludiamo estendendo la notazione O-grande a funzioni di più variabili.

Definizione. *Siano $f, g : \mathbb{N}^+ \times \mathbb{N}^+ \times \cdots \times \mathbb{N}^+ \to \mathbb{R}^+$ due funzioni definite sulle r-ple dei naturali positivi, a valori nei reali positivi. Diciamo che $f \in O(g)$ se esistono due costanti $B > 0$, $C > 0$ tali che se $n_j > B$ per ogni $j = 1, \ldots r$ si ha*

$$f(n_1, n_2, \ldots n_r) < Cg(n_1, n_2, \ldots n_r).$$

Esempio. *Per quanto visto per somma e moltiplicazione di numeri interi positivi in base 2 abbiamo*

$$\textit{Tempo } (\textit{(k bit) + (k bit)} \in O(k)$$
$$\textit{Tempo } (\textit{(k bit)} \cdot \textit{(l bit)} \in O(kl)$$

Notiamo che per Tempo *si intende il tempo di calcolo necessario usando un ben preciso algoritmo. Se vogliamo esprimere il tempo in termini di n ed m e non delle loro cifre binarie abbiamo*

$$\textit{Tempo } (n+m) \in O(max\{\log n, \log m\})$$
$$\textit{Tempo } (n \cdot m) \in O(\log n \cdot \log m).$$

Queste stime valgono per una qualunque altra base b. Osserviamo inoltre che, per la moltiplicazione, esistono algoritmi più efficienti di quello utilizzato da noi.

5 Numeri Primi e Teorema Fondamentale dell'Aritmetica

Definizione. *Un numero intero $p \in \mathbb{Z}$ con $p > 0$ e $p \neq 1$ si dice primo se, $\forall a, b \in \mathbb{Z}$*

$$p \mid ab \to p \mid a \text{ oppure } p \mid b$$

Definizione. *Un numero intero $p \in \mathbb{Z}$ con $p > 0$ e $p \neq 1$ si dice irriducibile se, per $a \in \mathbb{Z}$*

$$a \mid p \to a \pm p \text{ oppure } a \pm 1$$

Teorema. *Sia $p \in \mathbb{Z}$ con $p > 0$ e $p \neq 1$. Allora p è primo se e solo se p è irriducibile.*

Dimostrazione.

1. p primo $\to$ p irriducibile.

   Sia $a \in \mathbb{Z}$ con $a \mid p$ così $p = ab$ per un certo $b \in \mathbb{Z}$. Ora $p \mid p$ dunque $p \mid ab$ e p è primo. Segue che $p \mid a$ oppure $p \mid b$. Se $p \mid a$, da $a \mid p$ e $p \mid a$ si ha che $a = \pm p$. Se $p \mid b$ sarà $b = pc$ per un certo $c \in \mathbb{Z}$. Da $p = ab$ si trova $p = ab = pac$ da cui $ac = 1$ e dunque $a = \pm 1$.

2. p irriducibile $\to$ p primo.

   Supponiamo che $p \mid ab$ per $a, b \in \mathbb{Z}$. Allora $ab = pq$ per un certo $q \in \mathbb{Z}$. Sia $d = (a, p)$ così $d \mid p$. Poiché p è irriducibile, abbiamo $d = 1$ oppure $d = p$. Se $d = p$ allora $p \mid a$. Se $d = 1$ per l'identità di Bezout esistono $x, y \in \mathbb{Z}$ con

   $$1 = ax + py.$$

   Moltiplicando per b abbiamo

   $$b = bax + pby$$

   da cui $p \mid b$

□

Lemma. *Sia p un numero primo. Se p divide il prodotto di $n \geq 2$ numeri interi, allora p divide almeno uno dei fattori.*

Dimostrazione. Per induzione su n. Se $n = 2$, l'enunciato è vero, dunque assumiamo $n > 2$. Supponiamo che p divida il prodotto $a_1 a_2 \dots a_n$ con $a_1, \dots, a_n \in \mathbb{Z}$. Allora $p \mid (a_1 \dots a_{n-1}) \cdot a_n$ dunque $p \mid a_1 \dots a_{n-1}$ oppure $p \mid a_n$. Nel secondo caso siamo a posto. Nel primo caso, per induzione p divide almeno un a_i, con $1 \leq i \leq n - 1$. □

Possiamo allora enunciare e dimostrare il Teorema Fondamentale dell'Aritmetica

Teorema (Teorema Fondamentale dell'Aritmetica)**.** *Ogni numero intero n, con $n \geq 2$, si può scrivere come prodotto di $s \geq 1$ numeri primi (non necessariamente distinti). Tale fattorizzazione è essenzialmente unica, nel senso che se $n = p_1 p_2 \dots p_s$ e $n = q_1 q_2 \dots q_t$, dove ogni p_i per $1 \leq i \leq s$ e ogni q_j per $1 \leq j \leq t$ è primo, allora $s = t$ e si possono ordinare i fattori in modo che sia $p_1 = q_1, \dots, p_s = q_s$.*

Dimostrazione. Esistenza della fattorizzazione

Per induzione su n. Se $n = 2$ il teorema è vero perché 2 è primo. Supponiamo il risultato vero per ogni m con $2 \leq m < n$ e dimostriamolo vero per n, con $n > 2$. Se n è primo il teorema è vero. Se n non è primo si può scrivere $n = ab$ con $1 < a, b < n$. Per induzione $a = a_1 \dots a_n$ e $b = b_1 \dots b_k$ con ciascun a_i $(1 \leq i \leq h)$ e ciascun b_j $(1 \leq j \leq k)$ numero primo. Allora $n = a_1 \dots a_n b_1 \dots b_k$ si può esprimere come prodotto di un numero finito di primi.

Unicità della fattorizzazione

Dimostriamo che la fattorizzazione è essenzialmente unica, nel senso precisato nell'enunciato. Sia quindi

$$n = p_1 p_2 \dots p_s = q_1 q_2 \dots q_t$$

dove ogni p_i $(1 \leq i \leq s)$ e ogni q_j $(1 \leq j \leq t)$. Poiché $p_1 \mid p_1 \dots p_s$ abbiamo che $p_1 \mid q_1 q_2 \dots q_t$ e dunque $p_1 | q_j$ per almeno un j con $1 \leq j \leq t$. A meno di riordinare i fattori $q_1, \dots, q_t$, possiamo assumere che $p_1 \mid q_1$ e pertanto $p_1 = q_1$. Da

$$n = p_1 p_2 \dots p_s = p_1 q_2 \dots q_t$$

segue che

$$p_2 \dots p_s = q_2 \dots q_t$$

Per induzione abbiamo $s = t$ e $p_i = q_i$ per $i = 2 \dots s$. □

Osservazione. *In modo del tutto simile a quanto visto, si può dare la definizione di numero primo e irriducibile chiedendo che $p \in \mathbb{Z}$, $p \neq 0, \pm 1$.*

Teorema (Euclide)**.** *Esistono infiniti numeri primi.*

Dimostrazione. Per assurdo supponiamo che i numeri primi siano in numero finito e sia $\{p_1, p_2, \dots, p_N\}$ l'insieme dei numeri primi. Posto $M = p_1 p_2 \dots p_N + 1$ abbiamo che $M \geq 2$ e $M \in \mathbb{Z}$. Per il teorema fondamentale dell'aritmetica, M si scompone in prodotto di fattori primi. Ma se $p_i \mid M$ allora $p_i \mid 1 = M - p_1 p_2 \dots p_N$, per ogni $i = 1 \dots N$. Assurdo. □

6 Equazioni Diofantee

Una equazione diofantea è una equazione della forma

$$ax + by = c$$

con $a, b, c \in \mathbb{Z}$ e x, y incognite, $a \neq 0$, $b \neq 0$, $c \neq 0$.

Vogliamo determinare, se esistono, soluzioni intere dell'equazione, cioè coppie

$$(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z} \quad \text{con } ax_0 + by_0 = c$$

Esempi.

1. $4x + 6y = 9$ *non ha soluzioni perchè se esistesse* $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ *con* $4x_0 + 6y_0 = 9$, *allora* $2(2x_0 + 3y_0) = 9$ *cioè* $2 \mid 9$.
2. $6x + 5y = 3$ *ha come soluzione* $(3, -3)$ *e anche* $(8, -9)$

Proposizione. *Si consideri l'equazione diofantea* $ax + by = c$ *con* $a, b, c \in \mathbb{Z}, a \neq 0, b \neq 0$, $c \neq 0$. *Condizione necessaria e sufficiente affinchè abbia soluzioni è che* (a, b) *divida* c.

Dimostrazione. Se l'equazione $ax + by = c$ ammette una soluzione $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ allora $ax_0 + by_0 = c$. Posto $d = (a, b)$ abbiamo che $d \mid ax_0 + by_0$ ovvero $d \mid c$.

Viceversa se $d \mid c$ allora $c = d\overline{c}$ per $\overline{c} \in \mathbb{Z}$. Per l'identità di Bezout esistono s, $t \in \mathbb{Z}$ tali che

$$d = as + bt$$

Moltiplico tutto per $\overline{c}$ e trovo

$$c = d\overline{c} = as\overline{c} + bt\overline{c}$$

Posto $x_0 = s\overline{c}$ e $y_0 = t\overline{c}$, $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ ed è soluzione di $ax + by = c$. □

Esempio. *Determiniamo, se esiste, una soluzione dell'equazione diofantea*

$$74x + 22y = 10$$

Calcoliamo $(74, 22)$ *con l'algoritmo delle divisioni successive:*

$$\begin{aligned} 74 &= 22 \cdot 3 + 8 \\ 22 &= 8 \cdot 2 + 6 \\ 8 &= 6 \cdot 1 + 2 \\ 6 &= 2 \cdot 3 \end{aligned}$$

$(74, 22) = 2$

Poichè $2 \mid 10$*, l'equazione ammette soluzioni.*

Identità di Bezout: $a = 74$*,* $b = 22$

$$\begin{aligned} 8 &= a - 3b \\ 6 &= b - 2 \cdot 8 = b - 2(a - 3b) = 7b - 2a \\ 2 &= 8 - 6 = a - 3b - (7b - 2a) = 3a - 10b \end{aligned}$$

Poichè $10 = 2 \cdot 5$*, moltiplico per 5 l'identità di Bezout e trovo*

$$\begin{aligned} 10 &= 15a - 50b \\ &= 15 \cdot 74 - 50 \cdot 22 \end{aligned}$$

quindi una soluzione è $(15, -50)$*.*

Come si determinano, se esistono, tutte le soluzioni di $ax + by = c$?

Proposizione. *Si consideri l'equazione diofantea* $ax + by = c$ *con* $a, b, c \in \mathbb{Z}$*,* $a \neq 0, b \neq 0, c \neq 0$*. Si supponga che, posto* $d = (a, b)$*,* $d \mid c$*. Sia* $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ *una soluzione di* $ax + by = c$*. Allora tutte e sole le soluzioni di* $ax + by = c$ *sono le coppie* $(x_k, y_k) \in \mathbb{Z} \times \mathbb{Z}$ *dove*

$$\begin{aligned} x_k &= x_0 + \overline{b}k \\ y_k &= y_0 - \overline{a}k, \quad k \in \mathbb{Z} \end{aligned}$$

con $a = \overline{a}d$ *e* $b = \overline{b}d$*.*

Dimostrazione. Per ogni $k \in \mathbb{Z}$, (x_k, y_k) è soluzione di $ax + by = c$ perchè

$$\begin{aligned} ax_k + by_k &= ax_0 + a\overline{b}k + by_0 - b\overline{a}k \\ &= ax_0 + by_0 + \frac{abk}{d} - \frac{abk}{d} \\ &= ax_0 + by_0 = c \end{aligned}$$

Viceversa sia $(\overline{x}, \overline{y})$ una soluzione di $ax + by = c$ così

$$a\overline{x} + b\overline{y} = c = ax_0 + by_0$$

da cui

$$a(\overline{x} - x_0) = b(y_0 - \overline{y})$$

Dividendo per d si ha

$$\overline{a}(\overline{x} - x_0) = \overline{b}(y_0 - \overline{y})$$

con $(\overline{a}, \overline{b}) = 1$. Poichè $\overline{a} \mid \overline{b}(y_0 - \overline{y})$ si ha $\overline{a} \mid y_0 - \overline{y}$ ovvero $y_0 - \overline{y} = k\overline{a}$ cioè $\overline{y} = y_0 - k\overline{a}$ con $k \in \mathbb{Z}$. Sostituendo in $\overline{a}(\overline{x} - x_0) = \overline{b}(y_0 - \overline{y})$, otteniamo $\overline{a}(\overline{x} - x_0) = \overline{b}\overline{a}k$ cioè $\overline{x} = x_0 + \overline{b}k$. $\square$

Esempio. *Determinare tutte le soluzioni dell'equazione diofantea* $74x+22y = 10$. *Abbiamo già visto che una soluzione è* $(15, -50)$. *Tutte le soluzioni sono le coppie* (x_k, y_k) *con*

$$x_k = x_0 + \overline{b}k = 15 + \frac{22}{2}k = 15 + 11k$$

$$y_k = y_0 - \overline{a}k = -50 - \frac{74}{2}k = -50 - 37k$$

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

7 Relazioni su un Insieme

Definizione. *Sia A un insieme non vuoto. Una relazione R su A è un sottoinsieme di $A \times A$.*

Se R è una relazione su A e $(a, b) \in R$, si scrive anche aRb.

Proprietà delle relazioni

Una relazione R su un insieme A si dice

1. riflessiva se $\forall a \in A,\ (a, a) \in R$.
2. simmetrica se $\forall a, b \in A$, se $(a, b) \in R$ allora $(b, a) \in R$.
3. antisimmetrica se $\forall a, b \in A,$ se $(a, b) \in R$ e $(b, a) \in R$ allora $a = b$.
4. transitiva se $\forall a, b, c \in A$, se $(a, b) \in R$ e $(b, c) \in R$ allora $(a, c) \in R$.

Esempi.

1. *$A = \{a, b, c, d\}$ e $R = \{(a, a), (b, b), (c, c), (d, d), (a, d), (d, c), (a, c), (c, a), (d, a), (c, d)\}$ è riflessiva, simmetrica e transitiva.*
2. *$A = \{1, 2, 3\}$ e $R = \{(1, 1), (2, 2), (1, 2), (2, 1), (2, 3)\}$.*

   R non è riflessiva perchè $(3, 3) \notin R$

   R non è simmetrica perchè $(2, 3) \in R$ ma $(3, 2) \notin R$

   R non è antisimmetrica perchè $(1, 2) \in R$, $(2, 1) \in R$, ma $1 \neq 2$.

   R non è transitiva perchè $(1, 2) \in R$, $(2, 3) \in R$ ma $(1, 3) \notin R$
3. *A insieme qualsiasi, R la relazione di uguaglianza tra elementi di A cioè*

$$(a, b) \in R \text{ se e solo se } a = b$$

   R è riflessiva: $\forall a \in A$, $(a, a) \in R$
   R è simmetrica: $\forall a, b \in A$, se $(a, b) \in R$ allora $a = b$ dunque $(b, a) \in R$
   R è antisimmetrica: $\forall a, b \in A$ se $(a, b) \in R$ e $(b, a) \in R$ allora $a = b$
   R è transitiva: $\forall a, b, c \in A$ se $(a, b) \in R$ e $(b, c) \in R$ allora $a = b$ e $b = c$ da cui $a = c$ ovvero $(a, c) \in R$.
4. *X insieme qualsiasi, $P(X)$ insieme delle parti di X. Sia R la relazione di inclusione tra i sottoinsieme di X ovvero*

$$R = \{(Y, Z) \mid Y, Z \in P(X) \text{ e } Y \subseteq Z\}.$$

   Notiamo che R è una relazione su $P(X)$. Inoltre:

   R è riflessiva: $\forall Y \in P(X)$, $Y \subseteq Y$ così $(Y, Y) \in R$

R è antisimmetrica: $\forall Y, Z \in P(X)$ se $(Y, Z) \in R$ e $(Z, Y) \in R$ allora $Y \subseteq Z$ e $Z \subseteq Y$ così $Y = Z$.

R è transitiva: $\forall Y, Z, T \in P(X)$ se $(Y, Z) \in R$ e $(Z, T) \in R$ allora $Y \subseteq Z$ e $Z \subseteq T$ così $Y \subseteq T$, ovvero $(Y, T) \in R$.

Definizione. *Una relazione R su un insieme A che sia riflessiva, simmetrica e transitiva si dice una relazione di equivalenza.*

Definizione. *Una relazione R su un insieme A che sia riflessiva, antisimmetrica e transitiva si dice una relazione d'ordine.*

Classi di Equivalenza e Insieme Quoziente

Siano A un insieme non vuoto e R una relazione di equivalenza su A. Per $a \in A$, si definisce classe di equivalenza di a l'insieme

$$[a]_R = \{b \in A \mid (a, b) \in R\}$$

Nota. *$[a]_R$ è un sottoinsieme di A*

$[a]_R \neq \emptyset$ perchè R è riflessiva dunque $(a, a) \in R$ e pertanto $a \in [a]_R$.

Esempio. *Siano $A = \{a, b, c, d\}$ e $R = \{(a, a), (b, b), (c, c), (d, d), (a, d), (d, c), (a, c), (c, a), (d, a), (c, d)\}$. Allora*

$[a]_R = \{a, d, c\}$
$[b]_R = \{b\}$
$[c]_R = \{a, d, c\} = [d]_R = [a]_R$

Definizione. *Data una relazione di equivalenza R su un insieme A non vuoto, l'insieme quoziente A/R è definito come*

$$A/R = \{[a]_R \mid a \in A\},$$

l'insieme delle classi di equivalenza di R.

Esempio. *Nell'esempio precedente risulta*

$$A/R = \{[a]_R, [b]_R\}$$

Notazione Le relazioni di equivalenza si indicano anche con il simbolo $\sim$ pertanto

R	$\sim$
$(a, b) \in R,\ aRb$	$a \sim b$
A/R	$A/\sim$

Una proprietà fondamentale delle classi di equivalenza è che due classi di equivalenza o coincidono o sono disgiunte, cioè

Proposizione. *Siano A un insieme non vuoto e R una relazione di equivalenza su A. Per ogni $a, b \in A$*

$$o\ [a]_R = [b]_R\ \textit{oppure}\ [a]_R \cap [b]_R = \emptyset$$

Dimostrazione. Supponiamo che $[a]_R \cap [b]_R \neq \emptyset$ e sia $c \in [a]_R \cap [b]_R$. Allora $(a, c) \in R$ e $(c, b) \in R$. Per transitività $(a, b) \in R$ cioè $a \in [b]_R$. Mostriamo ora che $[a]_R = [b]_R$. Per $x \in [a]_R$, $(x, a) \in R$. Ma $(a, b) \in R$. Per transitività anche $(x, b) \in R$ ovvero $x \in [b]_R$ così $[a]_R \subseteq [b]_R$. Viceversa se $y \in [b]_R$ allora $(b, y) \in R$. Ma $(a, b) \in R$ dunque $(a, y) \in R$ cioè $y \in [a]_R$. Così $[b]_R \subseteq [a]_R$. In tutto abbiamo provato che $[a]_R = [b]_R$.
Infine la proposizione

$$\text{se } [a]_R \cap [b]_R \neq \emptyset \text{ allora } [a]_R = [b]_R$$

è logicamente equivalente a

$$\text{o } [a]_R = [b]_R \text{ oppure } [a]_R \cap [b]_R = \emptyset$$

□

Partizioni

Sia A un insieme non vuoto. Una partizione $\mathcal{F}$ di A è una famiglia di sottoinsiemi di A tali che

1. ogni $X \in \mathcal{F}$ è non vuoto
2. $\bigcup_{X \in \mathcal{F}} X = A$
3. $\forall X, Y \in \mathcal{F}$ se $X \neq Y$ allora $X \cap Y = \emptyset$.

Abbiamo allora provato che ogni relazione di equivalenza R su un insieme A (non vuoto) determina una partizione di A, i cui elementi sono le classi di equivalenza (rispetto a R). Notiamo per completezza che vale anche il viceversa di questa affermazione.

Nota. *Gli elementi di A/R (insieme quoziente) sono gli elementi della partizione determinata da R su A. Passare al quoziente significa, intuitivamente, identificare tra loro elementi equivalenti in R.*

8 Congruenza Modulo n

Definizione. *Sia $n \in \mathbb{Z}$ con $n \geq 1$. Dati due interi a, b si dice che a è congruo a b modulo n ($a \equiv b \ mod \ n$) se $n \mid a - b$ cioè se esiste $k \in \mathbb{Z}$ con $a - b = nk$.*

Osservazione. *La definizione di congruenza modulo n si può estendere ai casi*

1. *$n = 0$; si ottiene che $a \equiv b \ mod \ 0$ se e solo se $a - b = 0 \cdot k$ per un $k \in \mathbb{Z}$ ovvero se e solo se $a = b$. In altre parole la congruenza modulo 0 coincide con la relazione di uguaglianza in $\mathbb{Z}$.*
2. *$n < 0$; basta osservare che $n \mid a - b$ se e solo se $-n \mid a - b$ per concludere che $a \equiv b \ mod \ n$ se e solo se $a \equiv b \ mod \ -n$.*

Dunque non è limitativo considerare solo il caso $n > 0$.

Teorema. *Per ogni intero $n \geq 1$ la relazione di congruenza modulo n è una relazione di equivalenza su $\mathbb{Z}$. Le classi di equivalenza sono in numero di n e, indicando con $[a]_n$ la classe che contiene l'intero a, sono precisamente le classi:*

$$[0]_n, [1]_n, \ldots, [n-1]_n$$

Dimostrazione. La congruenza modulo n definisce su $\mathbb{Z}$ la relazione R data da

$$\forall a, b \in \mathbb{Z}, \ (a, b) \in R \text{ se e solo se } a \equiv b \ mod \ n$$

1. Proprietà riflessiva: $\forall a \in \mathbb{Z}, \ a \equiv a \ mod \ n$. Infatti $a - a = 0 = 0 \cdot n$
2. Proprietà simmetrica: $\forall a, b \in \mathbb{Z}, \ a \equiv b \ mod \ n$ implica $b \equiv a \ mod \ n$. Infatti $a - b = kn$ implica $b - a = (-k)n$, per $k \in \mathbb{Z}$.
3. Proprietà transitiva: $\forall a, b, c \in \mathbb{Z}, \ a \equiv b \ mod \ n$ e $b \equiv c \ mod \ n$ implicano $a \equiv c \ mod \ n$. Infatti $a - b = kn$ e $b - c = hn$ implicano, sommandole, che $a - c = (k + h)n$, con $h, \ k \in \mathbb{Z}$.

Sia ora $a \in \mathbb{Z}$. La divisione con resto fornisce $a = nq + r$ con $0 \leq r < n$. Poichè $a - r = qn$ si ha che $a \equiv r \ mod \ n$. Ciò mostra che ogni intero a è congruo, modulo n, a uno degli interi $0, \ 1, \ldots, \ n - 1$.

D'altra parte se i e j sono interi, con $0 \leq i < n$ e $0 \leq j < n$ si ha, assumendo $i \geq j$, che

$$0 \leq i - j \leq n - 1$$

e quindi $i - j = kn$ se e solo se $k = 0$, cioè $i = j$. □

Definizione. *L'insieme quoziente di $\mathbb{Z}$ rispetto alla relazione di congruenza modulo n ($n \geq 1$) si dice insieme delle classi di resti modulo n e si denota con $\mathbb{Z}_n$.*

Il nome "classi di resti"è motivato dal fatto che, per ogni $a \in \mathbb{Z}$, si ha $[a]_n = [r]_n$ dove r è il resto della divisione di a per n.

Esempi.

1. $n = 2$, $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$ *dove*

$$[0]_2 = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}$$
$$[1]_2 = \{\ldots, -5, -3, -1, 1, 3, 5, 7, \ldots\}$$

2. $n = 3$, $\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$ *dove*

$$[0]_3 = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$$
$$[1]_3 = \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\}$$
$$[2]_3 = \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\}$$

Vale la pena notare che, più in generale, si ha

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

dove

$$\begin{aligned}
[0]_n &= \{nk \mid k \in \mathbb{Z}\} \\
[1]_n &= \{1 + nk \mid k \in \mathbb{Z}\} \\
[2]_n &= \{2 + nk \mid k \in \mathbb{Z}\} \\
&\vdots \\
[n-1]_n &= \{n - 1 + nk \mid k \in \mathbb{Z}\}
\end{aligned}$$

Osservazione. *La congruenza modulo n è una relazione di equivalenza su $\mathbb{Z}$ anche nel caso $n = 0$. Come abbiamo già visto, in questo caso coincide con la relazione di uguaglianza su $\mathbb{Z}$. Le classi di equivalenza, nel caso $n = 0$, differiscono dalla descrizione generale. Infatti se $n = 0$ ogni intero a è in relazione solo con se stesso e pertanto $[a]_0 = \{a\}$. Le classi sono tante quanti gli elementi di $\mathbb{Z}$.*

Nota. *Sia $n \in \mathbb{Z}$ con $n \geq 1$ e siano a, b interi. Le seguenti affermazioni sono equivalenti:*

1. $a \equiv b \bmod n$
2. $n|a - b$
3. $a - b = nk$, *per un certo* $k \in \mathbb{Z}$
4. $a = b + nk$, *per un certo* $k \in \mathbb{Z}$
5. $a \in [b]_n$
6. $b \in [a]_n$

7. $[a]_n = [b]_n$

8. *a e b divisi per n danno lo stesso resto.*

Esercizio. *Siano $a, b, c, d \in \mathbb{Z}$ e $n \in \mathbb{Z}$ con $n \geq 1$. Si provi che, se $a \equiv b \ mod \ n$ e $c \equiv d \ mod \ n$, allora $a + c \equiv b + d \ mod \ n$ e $ac \equiv bd \ mod \ n$.*

9 Congruenze Lineari e Teorema Cinese del Resto

Si dice congruenza lineare (modulo n) ogni espressione della forma

$$ax \equiv b \; mod \; n$$

con $a, b \in \mathbb{Z}$. Si dice soluzione ogni intero c tale che

$$ac \equiv b \; mod \; n$$

Esempi. *La congruenza* $2x \equiv 3 \; mod \; 7$ *ha* $c = 5$ *come soluzione perchè* $2 \cdot 5 = 10 \equiv 3 \; mod \; 7$. *Più in generale, ogni intero della forma* $5 + 7k$ *è soluzione,* $k \in \mathbb{Z}$.

La congruenza $2x \equiv 3 \; mod \; 4$ *non ha soluzioni. Se esistesse* $c \in \mathbb{Z}$ *con* $2c - 3 = 4k$, $k \in \mathbb{Z}$, *avremmo* $3 = 2c - 4k$ *e pertanto* $2 \mid 3$, *assurdo.*

Proposizione. *Si consideri la congruenza* $ax \equiv b \; mod \; n$. *Posto* $d = (a, n)$ *sia* $a = \overline{a}d$ *e* $n = \overline{n}d$. *Allora*

1. *la congruenza* $ax \equiv b \; mod \; n$ *ammette soluzioni se e solo se* $d \mid b$
2. *se* c *è una soluzione, tutte e sole le soluzioni di* $ax \equiv b \; mod \; n$ *sono gli interi della forma*

   $$c + k\overline{n}$$

   al variare di $k \in \mathbb{Z}$. *In particolare* $ax \equiv b \; mod \; n$ *ha esattamente* d *soluzioni non congrue fra loro, modulo* n.

Dimostrazione.

1. La congruenza $ax \equiv b \; mod \; n$ ammette soluzione se e solo se esistono $c \in \mathbb{Z}$ e $k_0 \in \mathbb{Z}$ tali che

   $$ac - nk_0 = b$$

   ovvero se e solo se l'equazione diofantea $ax + ny = b$ ammette soluzione. Dalla teoria delle equazioni diofantee deduciamo che $ax \equiv b \; mod \; n$ ammette soluzioni se e solo se $d \mid b$.

2. Se c è soluzione di $ax \equiv b \; mod \; n$ allora esiste $k_0 \in \mathbb{Z}$ tale che $(c, -k_0)$ è soluzione di

   $$ax + ny = b$$

   Sappiamo che tutte e sole le soluzione di

   $$ax + ny = b$$

   sono le coppie (x_k, y_k) dove

   $$x_k = c + \frac{n}{d}k = c + \overline{n}k$$
   $$y_k = -k_0 - \frac{a}{d}k = -k_0 - \overline{a}k$$

al variare di k in $\mathbb{Z}$. In particolare tutte e sole le soluzioni di $ax \equiv b \; mod \; n$ sono della forma $c + \overline{n}k, k \in \mathbb{Z}$.

Rimane solo da provare che, tra queste, esattamente d non sono congrue modulo n. È chiaro che

$$c, c + \overline{n}, c + 2\overline{n}, \ldots, c + (d-1)\overline{n}$$

sono d soluzioni, fra loro non congrue modulo n. Infine se $c + k\overline{n}$ è una soluzione di $ax \equiv b \; mod \; n$ dividiamo k per d ottenendo $k = dq + r$ con $0 \leq r < d$. Allora

$$\begin{aligned} c + k\overline{n} &= c + qd\overline{n} + r\overline{n} \\ &= c + qn + r\overline{n} \equiv c + r\overline{n} \; mod \; n \end{aligned}$$

Poichè $0 \leq r < d$, si conclude che $c + k\overline{n}$ è congrua a una delle d soluzioni sopra elencate.

□

Esercizi.

1. *Determinare, se esistono, tutte le soluzioni della congruenza lineare*

$$35x \equiv 23 \bmod 16$$

Innanzitutto, possiamo ridurre i coefficienti modulo 16. Poiché $35 \equiv 3 \bmod 16$ *e* $23 \equiv 7 \bmod 16$ *la congruenza data equivale a*

$$3x \equiv 7 \bmod 16.$$

Poi dobbiamo calcolare $(3, 16)$ *e scrivere l'identità di Bezout. In questo caso è immediato che* $(3, 16) = 1$ *e*

$$1 = 16 \cdot 1 + 3 \cdot (-5)$$

Moltiplicando per 7 abbiamo

$$7 = 16 \cdot 7 + 3 \cdot (-35)$$

dunque

$$3 \cdot (-35) = 7 - 16 \cdot 7$$

Una soluzione è $c = -35$ *e tutte le soluzioni sono della forma*

$$-35 + 16k, k \in \mathbb{Z}.$$

Per risolvere la congruenza lineare $3x \equiv 7 \mod 16$ *abbiamo risolto l'equazione diofantea* $3x + 16y = 7$*, e poi abbiamo considerato i valori di* x *che rendono vera quest'ultima.*

2. *Determinare, se esistono, tutte le soluzioni della congruenza lineare*

$$15x \equiv 6 \bmod 18$$

Dobbiamo calcolare $(15, 18)$ *e scrivere l'identità di Bezout. Risulta* $(15, 18) = 3$ *e*

$$3 = 18 \cdot 1 + 15 \cdot (-1)$$

Poiché $3 \mid 6$ *la congruenza ammette soluzione. Moltiplicando l'identità di Bezout per 2 abbiamo*

$$6 = 18 \cdot 2 + 15 \cdot (-2)$$

Una soluzione della congruenza lineare è

$$c = -2.$$

Tutte le soluzioni sono della forma

$$-2 + \frac{18}{3}k = -2 + 6k, k \in \mathbb{Z}$$

Di queste esattamente 3 sono non congrue tra loro modulo 18, per esempio

$$-2, -2 + 6 \cdot 1, -2 + 6 \cdot 2 \text{ } cioè \text{ } -2, 4, 10$$

Passiamo ora a risolvere sistemi di congruenza.

Teorema Cinese del Resto

Siano $n_1, n_2, \ldots, n_r$ interi positivi, a due a due coprimi, e siano $b_1, b_2, \ldots, b_r$ numeri interi. Il sistema di congruenze lineari

$$\begin{cases} x \equiv b_1 \ mod \ n_1 \\ x \equiv b_2 \ mod \ n_2 \\ \vdots \\ x \equiv b_r \ mod \ n_r \end{cases}$$

è risolubile. Se c e c' sono due soluzioni, allora $c \equiv c' \ mod \ N$ dove $N = n_1 \cdot n_2 \cdots n_r = \Pi_{i=1}^{r} n_i$.

Dimostrazione. Per ogni $i = 1, 2, \ldots, r$, poniamo $N_i = N/n_i$.

Poichè $(n_i, n_j) = 1$ per $i \neq 1$ si ha che $(N_i, n_i) = 1$. (Infatti se p primo con $p \mid n_i$ e $p \mid N_i = n_1 \ldots n_{i-1} \ n_{i+1} \ldots n_r$ allora $p \mid n_i$ e $p \mid n_j$ per almeno un $j \neq i$. Ma allora avremmo $(n_i, n_j) \neq 1$). La congruenza lineare

$$N_i y \equiv 1 \ mod \ n_i$$

ammette una soluzione y_i. Posto

$$c = \sum_{i=1}^{r} N_i y_i b_i,$$

dimostriamo che c è una soluzione del sistema, cioè che $c \equiv b_j \ mod \ n_j$.

Osserviamo che, se $j \neq i$, $N_i \equiv 0 \ mod \ n_j$ e quindi $c \equiv N_j y_j b_j \ mod \ n_j$. Ma $N_j y_j \equiv 1 \ mod \ n_j$ quindi $N_j y_j b_j \equiv b_j \ mod \ n_j$.

Resta ora da dimostrare che c è l'unica soluzione del sistema, modulo N. Sia c' un'altra soluzione del sistema. Allora $c \equiv c' \ mod \ n_i$ ovvero $n_i \mid c - c'$ per ogni $i = 1 \dots r$. Poichè gli n_i sono a due a due coprimi, segue che anche N divide $c - c'$ ovvero $c \equiv c' \ mod \ N$. □

Esempio. *Consideriamo il sistema*

$$\begin{cases} x \equiv 2 \ mod \ 3 \\ x \equiv 3 \ mod \ 5 \\ x \equiv 2 \ mod \ 7 \end{cases}$$

Si ha $N = 3 \cdot 5 \cdot 7 = 105$, $N_1 = \dfrac{N}{n_1} = 5 \cdot 7 = 35$, $N_2 = \dfrac{N}{n_2} = 3 \cdot 7 = 21$, $N_3 = \dfrac{N}{n_3} = 3 \cdot 5 = 15$.

Dobbiamo risolvere le congruenze lineari

$$\begin{array}{llll} N_1 y \equiv 1 \ mod \ n_1 \longrightarrow & 35y \equiv 1 \ mod \ 3 \longrightarrow & 2y \equiv 1 \ mod \ 3 \longrightarrow & y_1 = 2 \\ N_2 y \equiv 1 \ mod \ n_2 \longrightarrow & 21y \equiv 1 \ mod \ 5 \longrightarrow & y \equiv 1 \ mod \ 5 \longrightarrow & y_2 = 1 \\ N_3 y \equiv 1 \ mod \ n_3 \longrightarrow & 15y \equiv 1 \ mod \ 7 \longrightarrow & y \equiv 1 \ mod \ 7 \longrightarrow & y_3 = 1 \end{array}$$

Si conclude allora che

$$c = \sum_{1}^{3} N_i y_i b_i = 35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 3 + 15 \cdot 1 \cdot 2 = 233$$

è una soluzione del sistema. Tale soluzione è unica a meno di multipli di 105. In particolare la minima soluzione positiva è $23 = 233 - 2 \cdot 105$.

10 Strutture algebriche. Somma e prodotto in $\mathbb{Z}_n$.

Definizione. *Dato un insieme non vuoto A, una operazione (binaria) su A è una funzione*

$$\begin{aligned} * \ : A \times A &\longrightarrow A \\ (a, b) &\longrightarrow a * b \end{aligned}$$

In altre parole una operazione (binaria) su A è una regola per associare a ogni coppia ordinata (a, b) di elementi di A, uno e un solo elemento di A. Una struttura algebrica è un insieme non vuoto A con una o più operazioni (binarie) su A.

Una operazione (binaria) si dice

- associativa: se $\forall a, b, c \in A$

$$(a * b) * c = a * (b * c)$$

- commutativa: se $\forall a, b \in A$

$$a * b = b * a$$

- dotata di elemento neutro: se esiste $e \in A \ : \ \forall a \in A$

$$a * e = a = e * a$$

Somma e Prodotto in $\mathbb{Z}_n$

Definiamo due operazioni in $\mathbb{Z}_n$ che si dicono somma e prodotto (di classi di resto):

1. somma: per $[a]_n, [b]_n \in \mathbb{Z}_n$ poniamo

$$[a]_n + [b]_n = [a + b]_n$$

2. prodotto: per $[a]_n, [b]_n \in \mathbb{Z}_n$ poniamo

$$[a]_n \cdot [b]_n = [ab]_n$$

Esempio. *In $\mathbb{Z}_5$*

$$\begin{aligned} [1]_5 + [3]_5 &= [4]_5 \\ [2]_5 \cdot [3]_5 &= [6]_5 \end{aligned}$$

Osserviamo che risulta $[1]_5 = [6]_5$ e $[3]_5 = [8]_5$ quindi $[1]_5 + [3]_5 = [6]_5 + [8]_5$. Cioè deve essere $[4]_5 = [14]_5$. In questo caso è vero e, come vediamo ora, è vero più in generale. Analogamente per la moltiplicazione.

Proposizione. *Fissato $n \in \mathbb{Z}$ con $n \geq 1$ siano $a, b, c, d \in \mathbb{Z}$, con $[a]_n = [b]_n$ e $[c]_n = [d]_n$. Allora*

$$[a]_n + [c]_n = [b]_n + [d]_n$$
$$[a]_n \cdot [c]_n = [b]_n \cdot [d]_n$$

Dimostrazione. Poichè $[a]_n = [b]_n$ e $[c]_n = [d]_n$ si ha $a = b + nk$ e $c = d + nh$ per $k, h \in \mathbb{Z}$. Allora $a + c = (b + d) + n(k + h)$ e $ac = bd + n(bh + dk + khn)$. Poichè $k + h \in \mathbb{Z}$ e $bh + dk + khn \in \mathbb{Z}$ si conclude che

$$[a + c]_n = [b + d]_n \text{ e } [ac]_n = [bd]_n$$

ovvero

$$[a]_n + [c]_n = [b]_n + [d]_n \text{ e } [a]_n[c]_n = [b]_n[d]_n$$

□

Proprietà di somma e prodotto in $\mathbb{Z}_n$

L'operazione di somma in $\mathbb{Z}_n$ gode delle proprietà:

- associativa: $\forall\ [a]_n, [b]_n, [c]_n \in \mathbb{Z}_n$

$$([a]_n + [b]_n) + [c]_n = [(a + b) + c]_n = [a + (b + c)]_n = [a]_n + ([b]_n + [c]_n)$$

- commutativa: $\forall\ [a]_n, [b]_n \in \mathbb{Z}_n$

$$[a]_n + [b]_n = [b]_n + [a]_n$$

- dotata di elemento neutro: esiste $[0]_n \in \mathbb{Z}_n : \ \forall [a]_n \in \mathbb{Z}_n$

$$[a]_n + [0]_n = [a]_n = [0]_n + [a]_n$$

- ogni elemento ha inverso: $\forall\ [a]_n \in \mathbb{Z}_n\ :\ \exists [n - a]_n \in \mathbb{Z}_n :$

$$[a]_n + [n - a]_n = [0]_n = [n - a]_n + [a]_n$$

L'operazione di prodotto in $\mathbb{Z}_n$ gode delle proprietà:

- associativa: $\forall\ [a]_n, [b]_n, [c]_n \in \mathbb{Z}_n$

$$([a]_n \cdot [b]_n) \cdot [c]_n = [(a \cdot b) \cdot c]_n = [a \cdot (b \cdot c)]_n = [a]_n \cdot ([b]_n * [c]_n)$$

- commutativa: $\forall\ [a]_n, [b]_n \in \mathbb{Z}_n$

$$[a]_n \cdot [b]_n = [b]_n \cdot [a]_n$$

- dotata di elemento neutro: esiste $[1]_n \in \mathbb{Z}_n : \forall [a]_n \in \mathbb{Z}_n$

$$[a]_n \cdot [1]_n = [a]_n = [1]_n \cdot [a]_n$$

Definizione. *Una struttura algebrica $(G, *)$ costituita da un insieme G e da un'operazione binaria $*$ su G si dice un* gruppo *se*

1. *l'operazione $*$ è associativa, cioè $\forall g, h, k \in G$, si ha $(g * h) * k = g * (h * k)$;*
2. *esiste un* elemento neutro *in G rispetto all'operazione $*$, cioè $\exists\, e \in G$ tale che $\forall g \in G$ si ha $g * e = g = e * g$.*
3. *ogni elemento di G ha* inverso *rispetto all'operazione $*$, cioè $\forall g \in G$, $\exists\, g^{-1} \in G$ con $g * g^{-1} = e = g^{-1} * g$.*

Se l'operazione $*$ in G è commutativa si dice che il gruppo G è commutativo (o abeliano).

Esempi. 1. *$(\mathbb{Z}, +)$ è un gruppo abeliano con elemento neutro 0 e inverso di a il numero intero $-a$.*

2. *$(\mathbb{Q}^*, \cdot), (\mathbb{R}^*, \cdot)$ sono gruppi abeliani con elemento neutro 1.*

3. *Sia V uno spazio vettoriale su $\mathbb{R}$, allora V rispetto alla somma di vettori è un gruppo abeliano con elemento neutro il vettore nullo e inverso di v il vettore $-v$.*

4. *$GL(n, \mathbb{R}) = \{A \in Mat(n, \mathbb{R}) \mid \det A \neq 0\}$ l'insieme delle matrici $n \times n$ a coefficienti reali con determinante diverso da zero, è un gruppo (non abeliano) rispetto all'usuale prodotto tra matrici. L'elemento neutro è la matrice identità $n \times n$. Il gruppo $GL(n, \mathbb{R})$ si dice* gruppo generale lineare.

5. *$(\mathbb{Z}_n, +)$ è un gruppo abeliano con elemento neutro $[0]_n$ e inverso di $[a]_n$ la classe $[n - a]_n$.*

11 Invertibili in $\mathbb{Z}_n$. Funzione di Eulero

Invertibili in $\mathbb{Z}_n$.

Problema. *Data $[a]_n$ in $\mathbb{Z}_n$, esiste $[b]_n$ in $\mathbb{Z}_n$ con $[a]_n[b]_n = [1]_n$?*

Osservazione. *Se $[a]_n = [0]_n$ allora, per ogni $[b]_n \in \mathbb{Z}_n$, risulta $[0]_n[b]_n = [0]_n$. Dunque se esiste $[b]_n \in \mathbb{Z}_n$ con $[0]_n[b]_n = [1]_n$ deve essere $[0]_n = [1]_n$ ovvero $1 \equiv 0 \bmod n$. L'unica possibilità è che $n = 1$. Pertanto per $n \geq 2$ non esiste alcun $[b]_n$ con $[0]_n[b]_n = [1]_n$.*

Esempi.
1. *Se $n = 7$ e $[a]_7 = [3]_7$ esiste $[b]_7 \in \mathbb{Z}_7$ con $[3]_7[b]_7 = [1]_7$. Basta prendere $[b]_7 = [5]_7$.*
2. *Se $n = 6$ e $[a]_6 = [3]_6$ non esiste alcun $[b]_6 \in \mathbb{Z}_6$ con $[3]_6[b]_6 = [1]_6$, come si può facilmente verificare.*

Definizione. *Un elemento $[a]_n$ in $\mathbb{Z}_n$ si dice* invertibile *in $\mathbb{Z}_n$ (rispetto al prodotto) se esiste $[b]_n \in \mathbb{Z}_n$ con $[a]_n[b]_n = [1]_n$.*

Un criterio per decidere quando un elemento di $\mathbb{Z}_n$ è invertibile è dato dalla seguente

Proposizione. *Siano $n > 1$ un intero e $a \in \mathbb{Z}$. La classe di resto $[a]_n$ è invertibile in $\mathbb{Z}_n$ se e solo se $(a, n) = 1$.*

Dimostrazione. Se $[a]_n$ è invertibile allora esiste $[b]_n$ in $\mathbb{Z}_n$ con $[a]_n[b]_n = [1]_n$, cioè $[ab]_n = [1]_n$. Da quest'ultima uguaglianza segue che $[ab - 1]_n = [0]_n$ cioè $n \mid ab - 1$. Scriviamo allora $ab = 1 + nk$, per un $k \in \mathbb{Z}$. Posto $d = (a, n)$ poiché $d \mid a$ e $d \mid n$ abbiamo che $\mid 1 = ab - nk$. Segue che $d = 1$.

Viceversa se $(a, n) = 1$ per l'identità di Bezout esistono $s, t \in \mathbb{Z}$ con

$$1 = as + nt.$$

Ma allora $as = 1 - nt$ cioè $as \equiv 1 \bmod n$ ovvero $[a]_n[s]_n = [1]_n$. □

Osservazione. *Se $[a]_n$ è invertibile il suo inverso è unico e si indica con $[a]_n^{-1}$.*

Esempi.
1. *In $\mathbb{Z}_{51}$ l'elemento $[13]_{51}$ è invertibile perchè $(13, 51) = 1$.*
2. *Gli invertibili in $\mathbb{Z}_8$ sono $[1]_8, [3]_8, [5]_8, [7]_8$ con inverso, rispettivamente, $[1]_8, [3]_8, [5]_8, [7]_8$.*
3. *In $\mathbb{Z}_7$ gli elementi invertibili sono $[1]_7, [2]_7, [3]_7, [4]_7, [5]_7, [6]_7$.*
4. *Generalizzando l'esempio precedente si ha che se p è un numero primo gli elementi invertibili di $\mathbb{Z}_p$ sono le classi $[1]_p, [2]_p, \ldots [p-1]_p$ ovvero tutti gli elementi di $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{[0]_p\}$.*

Funzione di Eulero

Definizione. *La funzione di Eulero* $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ *è definita da*

$\varphi(1) = 1,$

$\varphi(n) = |\{k \in \mathbb{Z} \ : \ 1 \leq k \leq n-1, \ (k,n) = 1\}|,$ *per* $n \geq 2.$

Esempio. *Sia ha* $\varphi(8) = |\{k \in \mathbb{Z} \ : \ 1 \leq k \leq 7, \ (k,8) = 1\}| = |\{1,3,5,7\}| = 4.$

Proprietà della funzione di Eulero

1. Se p è un numero primo, $\varphi(p) = p - 1$.
2. Se p è un numero primo e $m \geq 1$ un numero naturale, $\varphi(p^m) = p^m - p^{m-1} = p^{m-1}(p-1)$.
3. La funzione di Eulero è *moliplicativa* cioè per ogni $a, b \in \mathbb{N}^*$ con $(a,b) = 1$ si ha $\varphi(ab) = \varphi(a)\varphi(b)$.

Le prime due proprietà sono immediate. Dimostriamo invece la terza.

Siano r e s interi con $1 \leq r \leq a-1$ e $(r,a) = 1$ e $1 \leq s \leq b-1$ e $(s,b) = 1$. Per il Teorema Cinese del resto il sistema di congruenze

$$\begin{cases} x \equiv r \bmod a \\ x \equiv s \bmod b \end{cases}$$

ammette soluzioni e ne ammette una e una sola compresa tra 1 e $ab-1$. Sia c questa soluzione. Mostriamo che $(c, ab) = 1$. Se così non fosse, esisterebbe p numero primo con $p \mid c$ e $p \mid ab$ (basta infatti prendere come p un qualsiasi fattore primo di (c, ab)). Poiché p è primo sia ha che $p \mid a$ oppure $p \mid b$. Supponiamo che $p \mid a$. Siccome $c \equiv r \bmod a$ sarà $c = r + ah$, con $h \in \mathbb{Z}$ da cui $p \mid r = c - ah$. Ma allora p divide sia r che a contro l'ipotesi che $(r,a) = 1$. Si conclude che $(c, ab) = 1$. Poiché ogni coppia di interi r ed s come sopra dà luogo a un intero c con $1 \leq c \leq ab-1$ e $(c, ab) = 1$ abbiamo che $\varphi(a)\varphi(b) \leq \varphi(ab)$.

Viceversa sia t un intero con $1 \leq t \leq ab-1$ e $(t, ab) = 1$. Dividendo t per a otteniamo

$$t = aq + r \quad 0 \leq r < a.$$

Se fosse $r = 0$ avremmo che $a \mid t$ e, ovviamente $a \mid ab$ contro il fatto che $(t, ab) = 1$. Affermiamo che $(r,a) = 1$. Infatti, posto $d = (r,a)$, si ha che $d \mid a$ e $d \mid r$ da cui $d \mid ab$ e $d \mid t$, assurdo. Pertanto $d = 1$ e $(a,r) = 1$. Allo stesso modo si mostra che dividendo t per b e scrivendo $t = b\bar{q} + s$ con $1 \leq s \leq b-1$ deve essere $(b,s) = 1$. In tutto abbiamo che t è soluzione del sistema di congruenze

$$\begin{cases} x \equiv r \bmod a \\ x \equiv s \bmod b. \end{cases}$$

Si conclude che $\varphi(a)\varphi(b) = \varphi(ab)$.

Le proprietà della funzione di Eulero viste sopra permettono di calcolarla facilmente. Infatti per $n \geq 2$ naturale scriviamo la sua fattorizzazione

$$n = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$$

con p_i primo per $i = 1, \cdots s$, $e_i \geq 1$ e $p_i \neq p_j$ per $i \neq j$. Risulta

$$\begin{aligned} \varphi(n) &= \varphi(p_1^{e_1})\varphi(p_2^{e_2}) \cdots \varphi(p_s^{e_s}) \\ &= p_1^{e_1-1} p_2^{e_2-1} \cdots p_s^{e_s-1}(p_1 - 1)(p_2 - 1) \cdots (p_s - 1). \end{aligned}$$

Esempio. *Per* $n = 12 = 2^2 3$ *si ha* $\varphi(12) = 2^1 3^0 (2-1)(3-1) = 4$.

Osservazione. *Concludiamo questa parte con le seguenti osservazioni:*

1. $\varphi(n)$ *è uguale al numero di elementi invertibili in* $\mathbb{Z}_n$,
2. *se* p *è un primo dispari con* $p|n$ *allora* $p - 1|\varphi(n)$.

12 Piccolo Teorema di Fermat e Teorema di Eulero

Teorema (Piccolo Teorema di Fermat)**.** *Sia p un primo. Ogni intero a soddisfa la congruenza*

$$a^p \equiv a \bmod p.$$

Ogni intero a con $p \nmid a$ soddisfa la congruenza

$$a^{p-1} \equiv 1 \bmod p.$$

Dimostrazione. Supponiamo innanzitutto che $p \nmid a$. Consideriamo le classi di resto

$$[0]_p, [a]_p, [2a]_p, \dots [(p-1)a]_p.$$

Affermiamo che sono tutte distinte tra loro. Infatti se fosse $[ra]_p = [sa]_p$ per certi $0 \leq r, s \leq p-1$ avremmo (supponendo $r \geq s$) che $[(r-s)a]_p = [0]_p$ ovvero $p \mid (r-s)a$. Ma $p \nmid a$ quindi $p \mid r-s$. D'altra parte $0 \leq r-s \leq p-1$. L'unica possibilità è che $r-s=0$ ovvero $r=s$. Questo significa che l'insieme

$$\{[0]_p, [a]_p, [2a]_p, \dots [(p-1)a]_p\}$$

coincide con l'insieme

$$\{[0]_p, [1]_p, [2]_p, \dots [p-1]_p\}$$

dato che entrambi hanno esattamente p classi di resto modulo p. Poiché la classe $[0]_p$ compare in entrambi gli insiemi, sono uguali anche gli insiemi che si ottengono da quelli considerati sopra eliminando l'elemento $[0]_p$. Vale a dire che sono uguali gli insiemi

$$\{[a]_p, [2a]_p, \dots [(p-1)a]_p\}$$

e

$$\{[1]_p, [2]_p, \dots [p-1]_p\}.$$

In particolare il prodotto degli elementi $[a]_p, [2a]_p, \dots [(p-1)a]_p$ coincide con il prodotto degli elementi $[1]_p, [2]_p, \dots [p-1]_p$. Il primo prodotto è $[(p-1)!a^{p-1}]_p$ mentre il secondo prodotto è $[(p-1)!]_p$. Da $[(p-1)!a^{p-1}]_p = [(p-1)!]_p$ si ottiene $(p-1)!a^{p-1} \equiv (p-1)! \bmod p$ cioè $p \mid (p-1)!(a^{p-1}-1)$. Poiché $p \nmid (p-1)! = (p-1)(p-2)\cdots 2 \cdot 1$, si ha che $p \mid a^{p-1}-1$ ovvero

$$a^{p-1} \equiv 1 \bmod p.$$

Dimostriamo ora la congruenza $a^p \equiv a \bmod p$, per ogni intero a. Se $p \mid a$ allora $a \equiv 0 \bmod p$ e, a maggior ragione, $a^p \equiv 0 \bmod p$. Dunque la congruenza in questo caso è banalmente verificata: $a^p \equiv 0 \equiv a \bmod p$. Se invece $p \nmid a$, per quanto visto sopra, si ha $a^{p-1} \equiv 1 \bmod p$ e. per definizione di congruenza, $a \equiv a \bmod p$. Moltiplicando membro a membro si ottiene $a^p \equiv a \bmod p$. □

Una generalizzazione del Teorema di Fermat è dovuta a Eulero. Premettiamo la *formula del binomio di Newton.* Siano r ed s numeri interi. Per m numero naturale si ha la formula

$$(r+s)^m = \sum_{k=0}^{m} \binom{m}{k} r^k s^{m-k},$$

dove $\binom{m}{k}$ è il binomiale m *sopra* k, la cui formula esplicita è

$$\binom{m}{k} = \frac{m!}{k!(m-k)!}$$

Vale la pena ricordare anche che $\binom{m}{k}$ è uguale al numero di sottoinsiemi di k elementi presi da un insieme di m elementi. Sia dalla formula esplicita che dalla interpretazione insiemistica seguono subito le seguenti proprietà dei binomiali:

$$\binom{m}{0} = 1 = \binom{m}{m} \quad \text{e} \quad \binom{m}{k} = \binom{m}{m-k}$$

per $k = 0, \ldots m$. Infine osserviamo che se p è un numero primo, i binomiali $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ sono multipli di p per $k = 1, \ldots, p-1$.

La formula del binomio di Newton si può dimostrare per induzione su m.

Teorema (Teorema di Eulero)**.** *Sia $n \geq 1$ un intero e $a \in \mathbb{Z}$ con $(a, n) = 1$. Allora*

$$a^{\varphi(n)} \equiv 1 \bmod n.$$

Dimostrazione. Consideriamo prima il caso in cui n sia potenza di un numero primo cioè $n = p^m$ con p primo e $m \geq 1$. Procediamo per induzione su m. Se $m = 1$, $n = p$ e il Teorema di Eulero coincide con il Teorema di Fermat. Supponiamo allora $m \geq 2$ e il teorema vero, per ipotesi induttiva, per $m-1$ cioè supponiamo vero che

$$a^{\varphi(p^{m-1})} \equiv 1 \bmod p^{m-1}$$

per a in $\mathbb{Z}$ con $(a, p^{m-1}) = 1$. Poiché $\varphi(p^{m-1}) = p^{m-2}(p-1)$ stiamo supponendo che

$$a^{p^{m-2}(p-1)} = 1 + p^{m-1}b$$

per un $b \in \mathbb{Z}$. Elevando alla p entrambi i membri dell'uguaglianza sopra otteniamo

$$a^{p^{m-1}(p-1)} = (a^{p^{m-2}(p-1)})^p = (1 + p^{m-1}b)^p.$$

Espandiamo $(1 + p^{m-1}b)^p$ usando la formula del binomio di Newton:

$$(1 + p^{m-1}b)^p = 1 + (p^{m-1}b)^p + \sum_{k=1}^{p-1} \binom{p}{k} (p^{m-1}b)^{p-k}.$$

Ogni addendo della sommatoria, cioè ogni termine $\binom{p}{k}(p^{m-1}b)^{p-k}$, è un multiplo di p^m perché $\binom{p}{k}$ è multiplo di p e $(p^{m-1}b)^{p-k}$ è multiplo di p^{m-1}, per $k = 1, \ldots, p-1$.

Dunque

$$(1 + p^{m-1}b)^p \equiv 1 + (p^{m-1}b)^p = 1 + b^p p^m \equiv 1 \bmod p^m.$$

In tutto abbiamo provato che

$$a^{\varphi(p^m)} \equiv 1 \bmod p^m.$$

Nel caso generale sarà $n = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$ con p_i numero primo, $1 \leq i \leq r$, e $p_i \neq p_j$ per $i \neq j$. Se $a \in \mathbb{Z}$ con $(a, n) = 1$, allora si ha anche che $(a, p_i) = 1$ e dunque, per quanto visto sopra,

$$a^{\varphi(p_i^{m_i})} \equiv 1 \bmod p_i^{m_i},$$

per $i = 1, \ldots, r$.

Ma la funzione di Eulero è moltiplicativa dunque $\varphi(p_i^{m_i}) \mid \varphi(n)$ e pertanto sarà $\varphi(n) = \varphi(p_i^{m_i})t$ con $t \in \mathbb{Z}$. Allora

$$a^{\varphi(n)} = a^{\varphi(p_i^{m_i})t} = (a^{\varphi(p_i^{m_i})})^t \equiv 1^t = 1 \bmod p_i^{m_i}$$

per $i = 1, \ldots, r$.

In tutto abbiamo che $p_1^{m_1} \mid a^{\varphi(n)} - 1$, $p_2^{m_2} \mid a^{\varphi(n)} - 1, \ldots, p_r^{m_r} \mid a^{\varphi(n)} - 1$. Poiché $(p_i^{m_i}, p_j^{m_j}) = 1$ per $i \neq j$, segue che

$$n = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r} \mid a^{\varphi(n)} - 1.$$

□

13 Permutazioni

Definizione. *Sia X un insieme non vuoto. Una biiezione $f : X \longrightarrow X$ si dice una permutazione su X.*

Indichiamo con S_X l'insieme delle permutazioni su un insieme X, con operazione la composizione tra applicazioni

$$\begin{gathered} \circ : S_X \times S_X \longrightarrow S_X \\ (f, g) \longrightarrow f \circ g \end{gathered}$$

dove $(f \circ g)(a) = f(g(a))$, per ogni $a \in X$. È facile verificare che S_X è un gruppo rispetto all'operazione $\circ$, il cui elemento neutro è l'applicazione identità che fissa ogni elemento di X. Il gruppo S_X si dice il gruppo simmetrico su X. In particolare se $|X| = n$ (finito), il gruppo simmetrico S_X si indica con S_n e ha ordine $n!$. Senza perdita di generalità, si può assumere che sia $X = \{1, 2, \ldots, n\}$. Una permutazione $f \in S_n$ si può scrivere nella forma

$$f = \begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ b_1 & b_2 & \ldots & b_n \end{pmatrix}$$

con $1 \leq a_i \leq n$, $1 \leq b_i \leq n$ e $b_i = f(a_i)$. L'ordinamento della prima riga è arbitrario.

Esempio. *$n = 5$, $f \in S_5$ data da*

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix}$$

cioè $f(1) = 2$, $f(2) = 5$, $f(3) = 4$, $f(4) = 3$, $f(5) = 1$. Possiamo anche scrivere

$$f = \begin{pmatrix} 2 & 4 & 3 & 1 & 5 \\ 5 & 3 & 4 & 2 & 1 \end{pmatrix}$$

Cicli

Definizione. *Una permutazione nella forma $\begin{pmatrix} c_1 & c_2 & \ldots & c_{r-1} & c_r & c_{r+1} & \ldots & c_n \\ c_2 & c_3 & \ldots & c_r & c_1 & c_{r+1} & \ldots & c_n \end{pmatrix}$ si dice ciclo di lunghezza r (con $2 \leq r \leq n$) e si indica con $(c_1 c_2 \ldots c_r)$*

Osservazione. *Risulta $(c_1 c_2 \ldots c_r) = (c_2 c_3 \ldots c_r c_1) = \ldots = (c_r c_1 c_2 \ldots c_{r-1})$ cioé un ciclo di lunghezza r ammette r scritture diverse*

Esempio. $n = 3$

$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1, 2)$ *ciclo di lunghezza* 2. *Risulta* $(1, 2) = (2, 1)$.

$g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1, 2, 3)$ *ciclo di lunghezza* 3. *Risulta* $(1\ 2\ 3) = (2\ 3\ 1) = (3\ 1\ 2)$.

Una permutazione $f \in S_n$ muove un elemento a se $f(a) \neq a$. In caso contrario, si dice che f fissa l'elemento a. Due permutazioni $f, g \in S_n$ si dicono disgiunte se gli elementi mossi da f sono fissati da g e viceversa. Se f e g sono disgiunte si ha $f \circ g = g \circ f$.

Teorema. *Ogni permutazione di S_n, diversa dalla identità, è un ciclo oppure è il prodotto di cicli disgiunti, univocamente determinati a meno dell'ordine.* $\square$

Esempio. *Sia $f \in S_{13}$ la permutazione*

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 9 & 12 & 13 & 6 & 7 & 11 & 2 & 3 & 4 & 10 & 1 & 5 & 8 \end{pmatrix}$$

Risulta $f = (1, 9, 4, 6, 11)(2, 12, 5, 7)(3, 13, 8)$. La cifra 10 è fissata da f e pertanto non compare nella scrittura di f in prodotto di cicli disgiunti.

Esempio. *Per $n = 3$ si ha $S_3 = \{1, (12), (13), (23), (123), (132)\}$.*

Definizione. *Siano G un gruppo e $g \in G$. Il minimo intero positivo n tale che $g^n = 1_G$ (se esiste) si dice ordine (o periodo) di g. Se per nessun intero positivo k si ha $g^k = 1$ si dice che g ha ordine infinito.*

Esempi.

1. *In un gruppo qualsiasi G, l'unico elemento che ha ordine 1 è l'unità 1_G*
2. *In $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ ogni elemento non nullo ha ordine infinito.*

   Notiamo che, quando l'operazione è la somma, un elemento $g \in G$ ha ordine (finito) n se n è il minimo intero positivo tale che

   $$ng = \underbrace{g + \ldots + g}_{n \text{ volte}} = \underbrace{0}_{\text{unità di } G}$$

   Invece g ha ordine infinito se non esiste alcun intero positivo k tale che

   $$kg = \underbrace{g + \ldots + g}_{k \text{ volte}} = 0$$

3. *In $(\mathbb{R}^*, \cdot)$ gli unici elementi di ordine finito sono 1 e -1 (che hanno rispettivamente ordine 1 e 2).*
4. *Nel gruppo $(\mathbb{C}^*, \cdot)$ l'unità immaginaria i ha ordine 4 perché $i^4 = 1$ e 4 è il più piccolo intero positivo n tale che $i^n = 1$*
5. *Nel gruppo simmetrico S_n un ciclo di lunghezza r, $(c_1, c_2, \ldots, c_r)$, ha ordine r. Infatti posto $g = (c_1, c_2, \ldots, c_r)$, si ha*

   $$g = \begin{pmatrix} c_1 & c_2 & \ldots & c_r & c_{r+1} & \ldots & c_n \\ c_2 & c_3 & \ldots & c_1 & c_{r+1} & \ldots & c_n \end{pmatrix}$$

dunque

$$g^2 = \begin{pmatrix} c_1 & c_2 & \dots & c_r & c_{r+1} & \dots & c_n \\ c_3 & c_4 & \dots & c_2 & c_{r+1} & \dots & c_n \end{pmatrix}$$
$$g^3 = \begin{pmatrix} c_1 & c_2 & \dots & c_r & c_{r+1} & \dots & c_n \\ c_4 & c_5 & \dots & c_3 & c_{r+1} & \dots & c_n \end{pmatrix}$$
$$\vdots$$
$$g^r = 1 = \begin{pmatrix} c_1 & c_2 & \dots & c_n \\ c_1 & c_2 & \dots & c_n \end{pmatrix}$$

Una permutazione f di S_n che sia prodotto di t cicli disgiunti, di lunghezza $r_1, r_2, \dots, r_t$, ha ordine il minimo comune multiplo di $r_1, r_2, \dots, r_t$.

Esempio. *In S_{12} il ciclo $(7, 10, 8)$ ha ordine 3. La permutazione*

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 3 & 9 & 5 & 12 & 1 & 11 & 10 & 7 & 2 & 8 & 6 & 4 \end{pmatrix}$$
$$= (1, 3, 5)(2, 9)(4, 12)(6, 11)(7, 10, 8)$$

ha ordine $6 = m.c.m.(3, 2, 2, 2, 3)$.

Esempi. *1. In $S_3 = \{1, (12), (13), (23), (123), (132)\}$ abbiamo*

Elemento	*Ordine*
1	*1*
(12)	*2*
(13)	*2*
(23)	*2*
(123)	*3*
(132)	*3*

2. In $(\mathbb{Z}_6, +) = \{[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6\}$ abbiamo

Elemento	*Ordine*
$[0]_6$	*1*
$[1]_6$	*6*
$[2]_6$	*3*
$[3]_6$	*2*
$[4]_6$	*3*
$[5]_6$	*6*

14 Crittografia

Un sistema crittografico si può rappresentare come

$$\mathcal{P} \xrightarrow{f} \mathcal{C} \xrightarrow{f^{-1}} \mathcal{P}$$

dove

- $\mathcal{P}$ è l'insieme dei possibili messaggi elementari in chiaro, per esempio l'insieme delle lettere dell'alfabeto, tradotti in forma numerica. Possono darsi i casi: una lettera alla volta, blocchi di lettere in una volta (coppie, terne, k-ple di lettere). Il modo in cui si associano le lettere ai numeri puó non essere segreto.
- $\mathcal{C}$ è l'insieme dei messaggi crittati.
- f è una funzione che critta i messaggi.
- f^{-1} funzione inversa di f, è la funzione che decritta i messaggi.

Esempi. *Negli esempi che seguono scriviamo, per semplicità, p, c, a e b per intendere rispettivamente $[p]_N, [c]_N, [a]_N$ e $[b]_N$.*

1. *Siano $\mathcal{P} = \mathbb{Z}_N = \mathcal{C}$ e $f : \mathcal{P} \to \mathcal{C}$ la funzione definita da $f(p) = p+b$ per un qualunque $b \in \mathbb{Z}_N$. La funzione inversa di f è la funzione $f^{-1} : \mathcal{C} \to \mathcal{P}$ definita da $f^{-1}(c) = c-b$. Un caso particolare di questo esempio è il* cifrario di Cesare *che consisteva nel traslare ogni singola lettera dell'alfabeto di tre posizioni a destra (dunque la lettera A andava nella lettera D, la B nella E e così via). Si ottiene scegliendo $N = 26$ (se assumiamo di usare l'alfabeto inglese) e $b = 3$.*

2. *Una generalizzazione dell'esempio precedente si ha considerando $\mathcal{P} = \mathbb{Z}_N = \mathcal{C}$ e $f : \mathcal{P} \to \mathcal{C}$ la funzione definita da $f(p) = ap + b$ dove a è un elemento invertibile di $\mathbb{Z}_N$ mentre b è un qualunque elemento di $\mathbb{Z}_N$. L'applicazione f si dice mappa affine invertibile. L'applicazione inversa di f è la funzione $f^{-1} : \mathcal{C} \to \mathcal{P}$ definita da $f^{-1}(c) = a^{-1}c - a^{-1}b$. Per esempio, scegliamo $N = 26$, $a = 3 = b$ e supponiamo di voler crittare i messaggi $p_1 = 3$, $p_2 = 9$, $p_3 = 1$ e $p_4 = 15$. Otteniamo*

$$f(p_1) = f(3) = 3 \cdot 3 + 3 = 12 \qquad f(p_2) = f(9) = 3 \cdot 9 + 3 = 4$$
$$f(p_3) = f(1) = 3 \cdot 1 + 3 = 6 \qquad f(p_4) = f(15) = 3 \cdot 15 + 3 = 22$$

Spediamo allora i numeri $c_1 = 12$, $c_2 = 4$, $c_3 = 6$ e $c_4 = 22$. Chi riceve per decrittare i messaggi applica $f^{-1}(c) = 9c - 1$ ai messaggi cifrati ottenendo:

$$f^{-1}(c_1) = f^{-1}(12) = 9 \cdot 12 - 1 = 107 \equiv 3 \qquad f^{-1}(c_2) = f^{-1}(4) = 9 \cdot 4 - 1 = 35 \equiv 9$$
$$f^{-1}(c_3) = f^{-1}(6) = 9 \cdot 6 - 1 = 53 \equiv 1 \qquad f^{-1}(c_4) = f^{-1}(22) = 9 \cdot 15 - 1 = 197 \equiv 15.$$

I sistemi crittografici coinsiderati negli esempi si possono attaccare con l'analisi delle frequenze. La scienza che studia il modo di decifrare messaggi non essendone autorizzati si

dice crittoanalisi. Di solito in crittoanalisi si assume che l'intruso conosca la forma generale del sistema crittografico adottato e che debba invece scoprire la particolare chiave usata (nel secondo esempio l'intruso sa che f è una mappa affine invertibile e deve scoprire i valori di a e b). L'idea dell'analisi delle frequenze è questa: supponiamo che l'intruso abbia intercettato un numero sufficientemente grande di messaggi cifrati. Egli può supporre che certe lettere compaiono più frequentemente di altre. Per esempio in italiano la lettera e compare più frequentemente delle altre e certamente più frequentemente della lettera q. La lettera che compare più frequentemente nei messaggi crittati a disposizione dell'intruso corrisponderà alla lettera che compare più frequentemente nei messaggi in chiaro, analogamente la seconda lettera e così via. Nel caso f sia una mappa affine invertbile, basta conoscere l'equivalente in chiaro di due lettere per ricavare f e dunque f^{-1}.

RSA

Alice	**Bob**
Sceglie due numeri primi (dispari) p e q con $p \neq q$. Calcola $N = p \cdot q$ e $\varphi(N) = (p-1)(q-1)$. Sceglie un intero r in modo che $(\varphi(N), r) = 1$. Calcola, con l'algoritmo di Euclide, due interi s e t in modo che $rs + \varphi(N)t = 1$ Pubblica la coppia (N, r) mentre tiene ben segreti p, q, $\varphi(N)$ e s.	
	Vuole mandare ad Alice il messaggio b, dove b è un numero intero, con $0 < b < N$. Legge la coppia (N, r) che Alice ha pubblicato, e calcola il numero $a = b^r \bmod N$ e invia il numero a ad Alice.
Riceve il messaggio a da Bob e deve ricostruire il messaggio originale, cioè b. Calcola $a^s \bmod N$ e ritrova b.	

Perchè Alice riesce a ricostruire il messaggio originale di Bob? Il motivo è il Teorema di Eulero. Infatti supponiamo dapprima che sia $(b, N) = 1$. Allora

$$\begin{aligned} b = b^1 \bmod N = b^{rs+\varphi(N)t} \bmod N = b^{rs} b^{\varphi(N)t} \bmod N \\ = ((b^r)^s \mod N)((b^{\varphi(N)})^t \bmod N) = a^s \bmod N. \end{aligned}$$

Nell'ultimo passaggio abbiamo usato proprio il Teorema di Eulero, che ci assicura che $b^{\varphi(N)} \mod N = 1$, dunque anche $(b^{\varphi(N)})^t \mod N = 1$.

Se invece fosse $(b, N) \neq 1$, poiché $N = pq$ e $b < N$ abbiamo che o b è multiplo di p oppure b è multiplo di q (ma non di entrambi). Supponiamo che sia $b = kp$ con $k < q$ e k intero. Risulta $(b, q) = 1$ quindi, per il Teorema di Eulero applicato a b e q abbiamo che

$$b^{\varphi(q)} = b^{q-1} \equiv 1 \mod q.$$

A maggior ragione si ha

$$b^{\varphi(N)} = b^{(q-1)(p-1)} = (b^{q-1})^{p-1} \equiv 1 \mod q$$

da cui

$$b^{-t\varphi(N)} = (b^{\varphi N})^{-t} \equiv 1 \mod q.$$

L'ultima congruenza si scrive in $\mathbb{Z}$ come $b^{-t\varphi(N)} = 1 + qn$ per un $n \in \mathbb{Z}$. Moltiplicandola per b otteniamo $b^{1-t\varphi(N)} = b + bqn = b + nkN$. Ma $rs = 1 - \varphi(N)t$ dunque abbiamo ottenuto che $b^{rs} = b + nkN \equiv b \mod N$. Ovvero anche in questo caso abbiamo

$$a^s \mod N = (b^r)^s \mod N = b^{rs} \mod N = b$$

Supponiamo adesso che una terza persona, Carl, intercetti il messaggio a che Bob spedisce ad Alice. Se ci mettiamo nei panni di Carl la situazione è questa

Alice	**Carl**	**Bob**
(N, r)	Intercetta il messaggio a che Bob ha spedito ad Alice. Conosce la coppia (N, r) scelta da Alice, perchè Alice l'ha resa pubblica. Per ricostruire il messaggio originale b di Bob, ha bisogno di conoscere l'intero s e poi operare esattamente come fa Alice.	Spedisce il messaggio a ad Alice.
	È facile per Carl calcolare l'intero s se conosce $\varphi(N)$. Infatti Carl può applicare l'algoritmo delle divisioni successive. Quindi il problema di Carl è conoscere $\varphi(N) = (p-1)(q-1)$, ovvero conoscere p e q.	

Carl conosce $N = pq$ ma, se p e q sono numeri primi *grandi*, da questa informazione non sa ricostruire p e q.

Esempio. *Vediamo un esempio concreto di funzionamento dell'algoritmo RSA. Supponiamo innanzitutto che a ciascuna lettera dell'alfabeto sia stato associato un numero secondo lo schema seguente*

A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*
2	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*29*	*31*	*12*	*13*	*14*	*37*	*16*	*17*	*18*	*19*

U	*V*	*Z*	*Spazio*
43	*21*	*22*	*23*

Alice sceglie i numeri primi $p = 5$ *e* $q = 11$*, calcola* $N = pq = 55$*,* $\varphi(N) = \varphi(55) = 4 \cdot 10 = 40$*. Inoltre Alice sceglie un numero* r *in modo tale che* $(r, \varphi(N)) = (r, 40) = 1$*. Nel nostro esempio Alice sceglie* $r = 37$*. Poi Alice calcola, tramite l'algoritmo di Euclide, due interi* s *e* t *per i quali* $1 = 40t + 37s$*, ottenendo* $t = -12$ *e* $s = 13$*. Riporto qui i calcoli*

$40 = 37 \cdot 1 + 3$ $37 = 3 \cdot 12 + 1$ $3 = 3 \cdot 1 + 0$	$3 = 40 - 37$ $1 = 37 - 12 \cdot 3 = 37 - 12(40 - 37) = -12 \cdot 40 + 13 \cdot 37.$

Infine Alice pubblica la coppia $(N, r) = (55, 37)$*. Bob legge le informazioni rese pubbliche da Alice e le spedisce il messaggio seguente*

26	*7*	*21*	*9*	*52*	*7*	*52*	*41*	*23*	*28*	*24*	*7*	*18*	*49*	*7*

Per decifrarlo Alice considera il primo numero 26 *e calcola* $26^s \bmod N$ *cioè* $26^{13} \bmod 55$*. Si tratta quindi di calcolare* 26^{13}*, dividerlo per* 55 *e considerarne il resto. Quello che Alice ottiene è* 31*. In modo alternativo, Alice può ragionare così: da* $13 = 1 + 4 + 8$ *segue che*

$$26^{13} \bmod 55 = (26^1 \bmod 55) \cdot (26^4 \bmod 55) \cdot (26^8 \bmod 55)$$
$$26^4 \bmod 55 = 456976 \bmod 55 = 36$$
$$26^8 \bmod 55 = 208827064576 \bmod 55 = 31$$
$$26^{13} \bmod 55 = 26 \cdot 36 \cdot 31 \bmod 55 = 29016 \bmod 55 = 31.$$

Dunque decifrando 26 *otteniamo* 31 *ovvero la lettera L. Facciamo ancora un passo. Consideriamo* 7*. Alice calcola* $7^{13} \bmod 55$ *ottenenendo* 2*. Come prima, in modo alternativo,*

si poteva ragionare come segue

$$7^{13} \bmod 55 = (7^1 \bmod 55) \cdot (7^4 \bmod 55) \cdot (7^8 \bmod 55)$$
$$7^4 \bmod 55 = 2401 \bmod 55 = 36$$
$$7^8 \bmod 55 = 5764801 \bmod 55 = 31$$
$$7^{13} \bmod 55 = 7 \cdot 36 \cdot 31 \bmod 55 = 7812 \bmod 55 = 2.$$

Il messaggio inviato da Bob, alla luce di quanto abbiamo visto, diventa

L	*A*	*21*	*9*	*52*	*A*	*52*	*41*	*23*	*28*	*24*	*A*	*18*	*49*	*A*

Finite di decifrarlo.

15 Firma digitale tramite RSA

Illustriamo come il metodo RSA può essere utilizzato per la firma digitale. Alice e Bob scelgono ciascuno una propria chiave pubblica e una propria chiave privata. Supponiamo che siano

Alice	Bob	
(N_A, r_A)	(N_A, r_A)	chiave pubblica
s_A	s_B	chiave privata

le chiavi di Alice e Bob rispettivamente.

Alice sceglie come sua firma in chiaro un intero F con $F < N_A$ e $F < N_B$.

Distinguiamo due casi.

1. $N_A < N_B$

   Per firmare un suo messaggio Alice calcola prima

   $$F_A = F^{s_A} \bmod N_A$$

   e successivamente

   $$F_{A,B} = F_A^{r_B} \bmod N_B.$$

   Spedisce poi $F_{A,B}$ a Bob. Bob riceve $F_{A,B}$ da Alice, calcola

   $$F_{A,B}^{s_B} \bmod N_B = F_A$$

   e successivamente

   $$F_A^{r_A} \bmod N_A = F.$$

2. $N_B < N_A$

   Per firmare un suo messaggio Alice calcola prima

   $$F_B = F^{r_B} \bmod N_B$$

   e successivamente

   $$F_{B,A} = F_B^{s_A} \bmod N_A.$$

   Spedisce poi $F_{B,A}$ a Bob. Bob riceve $F_{B,A}$ da Alice, calcola

   $$F_{B,A}^{r_A} \bmod N_A = F_B$$

   e successivamente

   $$F_B^{s_B} \bmod N_B = F.$$

Osservazioni.

Notare che in ogni passaggio della procedura descritta sopra sia Alice che Bob sono in grado di eseguire le operazioni descritte. Inoltre solo Alice conosce la sua chiave privata s_A così come solo Bob conosce la sua chiave privata s_B.

Bob sa distinguere se deve applicare la procedura del punto 1 *o quella del punto* 2 *perchè N_A e N_B sono pubblici.*

16 Potenze modulo m

Un modo efficiente per calcolare $a^n \bmod m$ è il seguente. Scriviamo l' esponente n in base 2 ottenendo $n = (d_{k-1}, d_{k-2}, \ldots, d_1, d_0)$ ovvero $n = \sum_{i=0}^{k-1} d_i 2^i$. Costruiamo poi una tabella come segue

$(n)_2$	$c_0 = 1$
d_{k-1}	$c_1 \equiv c_0^2 \cdot a^{d_{k-1}} \bmod m$
d_{k-2}	$c_2 \equiv c_1^2 \cdot a^{d_{k-2}} \bmod m$
$\vdots$	$\vdots$
$\vdots$	$\vdots$
d_1	$c_{k-1} \equiv c_{k-2}^2 \cdot a^{d_1} \bmod m$
d_0	$c_k \equiv c_{k-1}^2 \cdot a^{d_0} \bmod m$

Risulta $a^n \equiv c_k \bmod m$.

Esempio. *Calcoliamo* $3^{90} \bmod 91$. *Scriviamo innanzitutto* 90 *in base* 2 *e risulta*

$$(90)_2 = (1011010).$$

Abbiamo

$(90)_2$	$c_0 = 1$
1	$c_1 \equiv 1^2 \cdot 3^1 = 3 \bmod 91$
0	$c_2 \equiv 3^2 \cdot 3^0 = 9 \bmod 91$
1	$c_3 \equiv 9^2 \cdot 3^1 \equiv (-10) \cdot 3 = -30 \bmod 91$
1	$c_4 \equiv (-30)^2 \cdot 3^1 \equiv -30 \bmod 91$
0	$c_5 \equiv (-30)^2 \cdot 3^0 \equiv -10 \bmod 91$
1	$c_6 \equiv (-10)^2 \cdot 3^1 \equiv 27 \bmod 91$
0	$c_7 \equiv (27)^2 \cdot 3^0 \equiv 1 \bmod 91$

Risulta $3^{90} \equiv 1 \bmod 91$.

17 Test di Primalità

Supponiamo di avere a disposizione un test che ci dica quando un numero intero positivo è primo.
Per determinare un numero primo di data grandezza il modo più semplice è il seguente. Scegliamo un intero n random della grandezza voluta. Poi

- se n è pari, consideriamo $n+1$
- se n è dispari, applichiamo il test a n, $n+2$, $n+4, \ldots$

fino a determinare il più piccolo numero primo maggiore o uguale a n.

Osservazione. *Una conseguenza del Teorema dei Numeri Primi è che mediamente otteniamo un numero primo dopo un numero di passi dell'ordine di* $\log n$.

Si tratta allora di avere a disposizione un test di primalità.
Un modo ovvio per sapere se un intero n è primo è dividerlo per $3, \ldots, \lfloor\sqrt{n}\rfloor$.

Nota. *Se* $n = ab$ *con* $a > \sqrt{n}$ *e* $b > \sqrt{n}$ *allora* $ab > n$*, assurdo.*
In particolare se n *è composto allora* n *ha un fattore primo* $p \leq \lfloor\sqrt{n}\rfloor$.
In questo modo possiamo anche fattorizzare n *se questo è composto. Senonché eseguire tutte le divisioni elencate sopra ha un costo computazionale troppo elevato.*

Vediamo un test probabilistico di primalità, cioè un test che risponde con certezza quando un intero non è primo mentre mostra che un intero è primo con una certa probabilità.
Se un intero supera una serie di test probabilistici di primalità, la probabilità di errore, cioè la probabilità che esso non sia primo, diminuisce.
Si può allora applicare un test deterministico che garantisce che il numero sia primo. I test deterministici sono molto più lenti dei test probabilistici.

Pseudoprimi (di Fermat)

Definizione. *Siano* $n > 1$ *un intero dispari e* $b \in \mathbb{Z}$ *con* $(b, n) = 1$*. Se* $b^{n-1} \equiv 1 \bmod n$ *diciamo che* n *è pseudoprimo rispetto alla base* b.

Osservazioni.

1. *La definizione è giustificata dal Piccolo Teorema di Fermat perché se* p *è primo e* $b \in \mathbb{Z}$ *con* $(b, p) = 1$ *(ovvero* $p \nmid b$*) abbiamo*
$$b^{p-1} \equiv 1 \bmod p$$
2. *Ogni intero* $n > 1$ *dispari è pseudoprimo rispetto alle basi* $b = \pm 1$*, dove per base intendiamo ogni intero* b *con* $(b, n) = 1$.
3. *Se* p *è primo allora* p *è pseudoprimo rispetto a ogni base* b.

Dato $n > 1$ dispari e $b \in \mathbb{Z}$ con $(b, n) = 1$

- se $b^{n-1} \not\equiv 1 \bmod n$ allora n <u>non</u> è primo
- se $b^{n-1} \equiv 1 \bmod n$ allora n è pseudoprimo rispetto alla base b.

Esempi. *$n = 91$ è pseudoprimo rispetto alla base $b = 3$, ma n non è pseudoprimo rispetto alla base $b = 2$.*

Dobbiamo verificare che $3^{90} \equiv 1 \bmod 91$ *mentre* $2^{90} \not\equiv 1 \bmod 91$. *Risulta* $90 = (1011010)_2$

	$c_0 = 1$
1	$c_1 = 3 \bmod 91$
0	$c_2 = 9 \bmod 91$
1	$c_3 = 81 \cdot 3 \equiv -30 \bmod 91$
1	$c_4 = 30^2 \cdot 3 \equiv -30 \bmod 91$
0	$c_5 = 30^2 \equiv -10 \bmod 91$
1	$c_6 = 10^2 \cdot 3 \equiv 27 \bmod 91$
0	$c_7 = 27^2 \equiv 1 \bmod 91$

	$c_0 = 1$
1	$c_1 = 2 \bmod 91$
0	$c_2 = 4 \bmod 91$
1	$c_3 = 16 \cdot 2 \equiv 32 \bmod 91$
1	$c_4 = 32^2 \cdot 2 \equiv 46 \bmod 91$
0	$c_5 = 46^2 \equiv 23 \bmod 91$
1	$c_6 = 23^2 \cdot 2 \equiv 57 \bmod 91$
0	$c_7 = 57^2 \equiv 64 \bmod 91$

Proprietà dei numeri pseudoprimi

Proposizione. *Per ogni intero $b > 1$ esistono infiniti numeri composti che sono pseudoprimi rispetto alla base b.*

Dimostrazione. Sia p un numero primo dispari con $p \nmid b$ e $p \nmid b^2 - 1$. Osserviamo che esistono infiniti numeri primi con queste proprietà.
Sia

$$n = \frac{b^{2p} - 1}{b^2 - 1} = \frac{(b^p)^2 - 1}{b^2 - 1} = \frac{b^p - 1}{b - 1} \cdot \frac{b^p + 1}{b + 1}$$

Ora

$$\frac{b^p - 1}{b - 1} = \underbrace{b^{p-1} + b^{p-2} + \ldots + b + 1}_{\in \mathbb{Z}} > 1$$

e

$$\begin{aligned} \frac{b^p + 1}{b + 1} &= b^{p-1} - b^{p-2} + b^{p-3} - b^{p-4} + \ldots + b^2 - b + 1 \\ &= \underbrace{b^{p-2}(b-1) + \ldots + b(b-1) + 1}_{\in \mathbb{Z}} > 1 \end{aligned}$$

quindi n è un numero composto.
Inoltre

$$n = \frac{b^{2p}-1}{b^2-1} = \frac{(b^2)^p-1}{b^2-1} = (b^2)^{p-1} + (b^2)^{p-2} + \ldots + b^2 + 1$$

da cui

$$n - 1 = (b^2)^{p-1} + (b^2)^{p-2} + \ldots + b^2$$

Segue che $n-1$ è somma di $p-1$ termini, con $p-1$ pari, che sono tutti pari se b è pari oppure tutti dispari se b è dispari.
In tutto $n-1$ è pari cioè $2 \,|\, n-1$ (e n è dispari).
Poi

$$\begin{aligned}(n-1)(b^2-1) &= n(b^2-1) - (b^2-1) = b^{2p} - 1 - b^2 + 1 \\ &= b^{2p} - b^2 = b^2(b^{2p-2} - 1)\end{aligned}$$

Per il teorema di Fermat $b^{p-1} \equiv 1 \bmod p$ e pertanto $b^{2p-2} = (b^{p-1})^2 \equiv 1^2 \equiv 1 \bmod p$, cioè $p \,|\, b^{2p-2} - 1$. Quindi $p \,|\, (n-1)(b^2-1)$ e $p \nmid b^2 - 1$ per ipotesi. Segue che $p \,|\, n-1$.
Abbiamo allora $n - 1 = 2pk$, $k \in \mathbb{Z}$ (notare che p è dispari).

Mostriamo che n è pseudoprimo rispetto alla base b.
Innanzitutto

$$n = \underbrace{(b^2)^{p-1} + (b^2)^{p-2} + \ldots + b^2}_{\text{multiplo di } b} + 1$$

dunque $(b, n) = 1$.
Poi $n(b^2-1) = b^{2p} - 1$ cioè $n \,|\, b^{2p} - 1$ ovvero $b^{2p} \equiv 1 \bmod n$. Allora

$$b^{n-1} = b^{2pk} = (b^{2p})^k \equiv 1^k = 1 \, mod \, n$$

La tesi segue dal fatto che abbiamo infinite scelte per p numero primo dispari con $p \nmid b$ e $p \nmid b^2 - 1$. □ □

Una proprietà fondamentale per i nostri scopi dei numeri pseudoprimi segue dal teorema:

Teorema. *Sia $n > 1$ un intero composto dispari. Se n non è pseudoprimo rispetto ad almeno una base b, allora n non è pseudoprimo per almeno la metà delle basi possibili viste modulo n (cioè le $\varphi(n)$ basi b con $0 < b < n$ e $(b, n) = 1$).*

Dimostrazione.

1. Se n è pseudoprimo rispetto alle basi a e b allora n è pseudoprimo rispetto alle basi ab e ab^{-1} dove b^{-1} è l'inverso di b modulo n.

Infatti $(ab, n) = 1 = (b^{-1}, n)$.
Inoltre

$$(ab)^{n-1} = a^{n-1}b^{n-1} \equiv 1 \cdot 1 = 1 \bmod n$$
$$(ab^{-1})^{n-1} = a^{n-1}(b^{n-1})^{-1} \equiv 1 \cdot 1^{-1} = 1 \bmod n$$

2. Sia $\{b_1, b_2, \ldots, b_s\}$ l'insieme di tutte le basi rispetto alle quali n è pseudoprimo, viste modulo n. Cioè l'insieme di tutti gli interi b_i con $0 < b_i < n$, $(b_i, n) = 1$ e $b_i^{n-1} \equiv 1 \bmod n$.
Consideriamo $\bar{b}b_i$ (ridotto modulo n). Risulta $(\bar{b}b_i, n) = 1$ perché $(\bar{b}, n) = 1 = (b_i, n)$.
Se n fosse pseudoprimo rispetto alla base $\bar{b}b_i$, per la parte 1) lo sarebbe anche rispetto alla base $\bar{b} = (\bar{b}b_i)b_i^{-1}$, assurdo.
Quindi n <u>non</u> è pseudoprimo rispetto all'insieme di basi

$$\{\bar{b}b_1, \bar{b}b_2, \ldots, \bar{b}b_s\}$$

Se fosse $\bar{b}b_i = \bar{b}b_j$ avremmo $(\bar{b})^{-1}(\bar{b}b_i) = (\bar{b})^{-1}(\bar{b}b_j)$ cioè $b_i = b_j$, assurdo per $i \neq j$.
Questo significa che l'insieme $\{\bar{b}b_1, \bar{b}b_2, \ldots, \bar{b}b_s\}$ ha s elementi, dunque le basi per cui n non è pseudoprimo sono almeno tante quante le basi per cui n è pseudoprimo. □

□

Test di primalità

Sia $n > 1$ un intero dispari.

1. Scegliamo un numero random b con $0 < b < n$
2. Calcoliamo $d = (b, n)$ con l'algoritmo di Euclide
   - se $d > 1$ sappiamo che n non è primo perché $d \mid n$
   - se $d = 1$ calcoliamo $b^{n-1} \bmod n$
3. Se $b^{n-1} \not\equiv 1 \bmod n$ allora n non è primo.
   Se $b^{n-1} \equiv 1 \bmod n$ allora n può essere primo.

A questo punto scegliamo un altro valore di b e ripetiamo il procedimento. Se $b^{n-1} \not\equiv 1 \bmod n$ per almeno un valore di b siamo sicuri che n è composto e ci fermiamo.
Supponiamo invece di aver applicato la procedura a k basi b_1, b_2, …, b_k e di aver trovato che n è pseudoprimo rispetto a ciascuna di esse.
Qual è la probabilità che n sia composto?
Se n è composto e $b_1^{n-1} \equiv 1 \bmod n$ vuol dire che b_1 è una base rispetto alla quale n è pseudoprimo.
Per il teorema precedente tali basi sono al più la metà delle basi possibili. Quindi la probabilità che $b_1^{n-1} \equiv 1 \bmod n$ e n è composto è $\leq \frac{1}{2}$ (a meno che n non sia pseudoprimo

rispetto a ogni possibile base).
Siccome $b_i^{n-1} \equiv 1 \bmod n$ per $i = 1 \dots k$ e gli eventi sono indipendenti, la probabilità che n sia composto nonostante passi il test per $b_1, b_2, \dots, b_k$ è $\leq \frac{1}{2^k}$ (che descresce velocemente al crescere di k). Ma esistono interi composti che sono pseudoprimi rispetto a ogni possibile base.

18 Numeri di Carmichael

Definizione. *Sia $n > 1$ un intero dispari composto. Si dice che n è un numero di Carmichael se*

$$b^{n-1} \equiv 1 \, mod \, n$$

per ogni $b \in \mathbb{Z}$ con $(b, n) = 1$

Un numero di Carmichael è dunque un numero composto che sia pseudoprimo rispetto a ogni possibile base.
I numeri di Carmichael minori di 10000 sono 561, 1105, 1729, 2465, 2821, 6601, 8911.

Caratterizzazione dei numeri di Carmichael

Proposizione. *Un numero intero $n > 1$ composto è di Carmichael se e solo se n è libero da quadrati e $p - 1 \,|\, n - 1$ per ogni divisore primo p di n.*

Dimostrazione. Scriviamo $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ con $p_1 < p_2 < \dots < p_k$ numeri primi. Per definizione n è di Carmichael se e solo se n è dispari e $b^{n-1} \equiv 1 \bmod n$ per ogni b con $0 < b < n$ e $(b, n) = 1$.

Poniamo

$$\begin{aligned} l &= m.c.m.(\varphi(p_1^{a_1}), \varphi(p_2^{a_2}), \dots, \varphi(p_k^{a_k})) \\ &= m.c.m.(p_1^{a_1-1}(p_1 - 1), p_2^{a_2-1}(p_2 - 1), \dots, p_k^{a_k-1}(p_k - 1)) \end{aligned}$$

Sia poi b con $(b, n) = 1$. Risulta $(b, p_i^{a_i}) = 1$ pertanto

$$b^{\varphi(p_i^{a_i})} \equiv 1 \bmod p_i^{a_i} \qquad i = 1 \dots k$$

Poiché l è multiplo di $\varphi(p_i^{a_i})$ abbiamo anche

$$b^{l} \equiv 1 \bmod p_i^{a_i} \qquad i = 1 \dots k$$

Segue che $b^l \equiv 1 \bmod n$.
Si può dimostrare (ma lo omettimo) che $b^r \equiv 1 \bmod n$ se e solo se $l \,|\, r$. In particolare $b^{n-1} \equiv 1 \bmod n$ se e solo se $l \,|\, n - 1$. Quindi n è di Carmichael se e solo se $n - 1$ è multiplo di $p_i^{a_i-1}(p_i - 1)$ per $i = 1 \dots k$.
Poichè $p_i \,|\, n$ si ha che $p_i \not| \, n - 1$ e quindi n è di Carmichael se e solo se

$$\begin{cases} a_i = 1 \\ p_i - 1 \,|\, n - 1 \quad \text{per } i = 1 \dots k \end{cases}$$

□ □

Inoltre vale il seguente corollario.

Corollario. *Un numero di Carmichael è prodotto di almeno tre primi distinti.*

Dimostrazione. Sia n un numero di Carmichael e supponiamo che sia $n = pq$ con $p < q$ numeri primi. Risulta

$$n - 1 = (p-1)(q-1) + (p-1) + (q-1)$$

Per la proposizione precedente $p-1 \,|\, n-1$ e $q-1 \,|\, n-1$.
Ora da $p-1 \,|\, n-1 = (p-1)(q-1)+(p-1)+(q-1)$ si ha che $p-1 \,|\, q-1$. Analogamente da $q-1 \,|\, n-1$ si ha $q-1 \,|\, p-1$. Ma allora $p-1 = q-1$ ovvero $p = q$, assurdo. □ □

Esempio. $n = 561 = 3 \cdot 11 \cdot 17$ *è un numero di Carmichael. Infatti* 561 *è libero da quadrati e*

$$2 \,|\, 560 = 280 \cdot 2$$
$$10 \,|\, 560 = 56 \cdot 10$$
$$16 \,|\, 560 = 35 \cdot 16$$

19 Anelli e campi

Definizione. *Un anello è una struttura algebrica $(A, +, \cdot)$ data da un insieme non vuoto A e due operazioni binarie $+ : A \times A \to A$ e $\cdot : A \times A \to A$ che siddisfino le seguenti proprietà:*

1. *$(A, +)$ è un gruppo abeliano (con elemento neutro 0_A).*
2. *L'operazione $\cdot$ è associativa: $\forall a, b, c \in A$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.*
3. *Valgono le leggi distributive del prodotto rispetto alla somma: $\forall a, b, c \in A$*
$$a \cdot (b + c) = a \cdot b + a \cdot b \quad e \quad (a + b) \cdot c = a \cdot c + b \cdot c.$$
4. *Esiste un elemento neutro rispetto al prodotto: $\exists 1_A \in A : \forall a \in A, 1_A \cdot a = a = a \cdot 1_A$.*

Osservazione. *Scriviamo per semplicità ab per $a \cdot b$ e 0 e 1 per 0_A e 1_A. Si può provare che per ogni $a, b \in A$ risulta*

1. *$a \cdot 0 = 0 = 0 \cdot a$,*
2. *$a(-b) - ab = (-a)b$.*

Un anello si dice commutativo se $ab = ba$ per ogni $a, b \in A$.

Esempi.

1. *$(\mathbb{Z}, +.\cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ e $(\mathbb{C}, +, \cdot)$ sono anelli commutativi.*
2. *$(\mathbb{Z}_n, +, \cdot)$ è un anello commutativo.*
3. *$(\mathrm{Mat}(2 \times 2, \mathbb{Q}), +, \cdot)$ e $(\mathrm{Mat}(2 \times 2, \mathbb{R}), +, \cdot)$ sono anelli non commutativi.*

Campi

Definizione. *Un campo K è un anello commutativo e ogni elemento non nullo di K sia invertibile (rispetto al prodotto) cioè un campo è un anello tale che*

1. *per ogni $a, b \in K$ si ha $ab = ba$*
2. *per ogni $a \in K$ con $a \neq 0$ esiste $a^{-1} \in K$*
$$a \cdot a^{-1} = 1 = a^{-1} \cdot a$$

Detto in altre parole un campo K è un anello in cui $(K^*, \cdot)$ sia un gruppo abeliano.

Esempi.

1. *$(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ e $(\mathbb{C}, +, \cdot)$ sono campi.*
2. *$(\mathbb{Z}_p, +, \cdot)$ con p primo è un campo.*
3. *Non sono campi $(\mathbb{Z}, +, \cdot)$ e $(\mathbb{Z}_n, +, \cdot)$ con n non primo.*

20 Polinomi su un campo

Sia K un campo, indichiamo con $K[x]$ l'anello dei polinomi a coefficienti in K, nell'indeterminata x. Ovvero $K[x]$ è l'insieme di tutti i polinomi

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

con $n \in \mathbb{N}$, $a_i \in K$ per ogni $i = 0 \ldots n$, con le usuali operazioni di somma e prodotto: per $p(x) = \sum_0^n a_i x^i$ e $q(x) = \sum_0^m b_j x^j$, si ha

$$p(x) + q(x) = \sum_0^{max(u,m)} (a_k + b_k)x^k$$

$$p(x)q(x) = \sum_0^{n+m} c_k x^k \text{ dove } c_k = \sum_{i+j=k} a_i b_j$$

È immediato verificare che $K[x]$ è un anello commutativo con $0_{K[x]}$ e $1_{K[x]}$ che coincidono con 0_K e 1_K (e che indicheremo semplicemente con 0 e 1).

Definizione. *Dato un polinomio non nullo $p(x)$ in $K[x]$ con*

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

e $a_n \neq 0$, l'intero non negativo n si dice grado di $p(x)$ e lo si indica con $\partial p(x)$.

Al polinomio nullo si attribusce, per convenzione, grado -1. Il coefficiente a_n si dice coefficiente direttore di $p(x)$. Se $a_n = 1$ si dice che $p(x)$ è monico.

Per l'anello $K[x]$ si può sviluppare una teoria parallela a quella sviluppata per l'anello $\mathbb{Z}$.

Teorema (Algoritmo della divisione)**.** *Siano $a(x)$, $b(x) \in K[x]$ con $b(x) \neq 0$. Esistono e sono univocamente determinati due polinomi $q(x)$, $r(x)$ in $K[x]$ tali che*

1. $a(x) = b(x)q(x) + r(x)$
2. $\partial r(x) < \partial b(x)$

Dimostrazione. Esistenza di $q(x)$ e $r(x)$

Procediamo per induzione su $n = \partial a(x)$.
Se $n = -1$ ovvero se $a(x) = 0$ il risultato è vero con $q(x) = 0 = r(x)$.
Sia allora $n \geq 0$ e scriviamo

$$a(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$
$$b(x) = b_m x^m + b_{m-1}x^{m-1} + \ldots + b_1 x + b_0$$

con $b_m \neq 0$.
Se $\partial b(x) = m > n = \partial a(x)$ il risultato è vero con $q(x) = 0$ e $r(x) = a(x)$.
Sia allora $m \leq n$. Consideriamo il polinomio

$$a'(x) = a(x) - a_n b_m^{-1} x^{n-m} b(x)$$

Risulta

$$a'(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 - a_n b_m^{-1} x^{n-m}(b_m x^m + \ldots + b_1 x + b_0)$$

dunque $\partial a'(x) \leq n - 1$.
Per induzione esistono due polinomi $q'(x)$ e $r'(x)$ in $K[x]$ tali che

$$a'(x) = b(x)q'(x) + r'(x)$$

con $\partial r'(x) < \partial b(x)$.
Poiché $a(x) = a'(x) + a_n b_m^{-1} x^{n-1} b$ abbiamo

$$\begin{aligned} a(x) &= a'(x) + a_n b_m^{-1} x^{n-m} b(x) \\ &= q'(x)b(x) + r'(x) + a_n b_m^{-1} x^{n-m} b(x) \\ &= (q'(x) + a_n b_m^{-1} x^{n-m}) b(x) + r'(x) \end{aligned}$$

Posto $q(x) = q'(x) + a_n b_m^{-1} x^{n-m}$ e $r(x) = r'(x)$, sono verificate le condizioni 1) e 2).

Unicità di $q(x)$ e $r(x)$

Supponiamo che sia $a(x) = b(x)q(x) + r(x)$ e $a(x) = b(x)q_1(x) + r_1(x)$ con $\partial r(x) < \partial b(x)$ e $\partial r_1(x) < \partial b(x)$. Allora

$$b(x)(q(x) - q_1(x)) = r_1(x) - r(x)$$

Se fosse $q(x) \neq q_1(x)$ sarebbe

$$\partial(b(x)(q(x) - q_1(x)) \geq \partial b(x)$$

e, d'altra parte, $\partial(r_1(x) - r(x)) < \partial b(x)$, assurdo. Ne segue che $q(x) = q_1(x)$ e quindi $r(x) = r_1(x)$. □ □

Definizione. *I polinomi $q(x)$ e $r(x)$ si dicono rispettivamente quoziente e resto della divisione di $a(x)$ per $b(x)$.*
Se $r(x) = 0$ si dice che $b(x)$ divide $a(x)$, ovvero che $a(x)$ è divisibile per $b(x)$, e si scrive

$$b(x) \,|\, a(x)$$

In altre parole: $b(x)$ divide $a(x)$ se e solo se esiste $c(x) \in K[x]$ tale che $a(x) = b(x)c(x)$.

Esempi.

1. *In $\mathbb{Q}[x]$ effettuiamo la divisione tra $a(x) = x^3 - 2x^2 + x - 1$ e $b(x) = 2x^2 - 5$*

$$\begin{array}{llll|l} x^3 & -2x^2 & +x & -1 & 2x^2-5 \\ \hline & & & & \\ x^3 & & -\frac{5}{2}x & & \frac{1}{2}x-1 \\ \hline & -2x^2 & +\frac{7}{2}x & -1 & \\ & +2x^2 & & +5 & \\ \hline & & \frac{7}{2}x & -6 & \end{array} \qquad q(x) = \frac{1}{2}x - 1 \qquad r(x) = \frac{7}{2}x - 6$$

2. *In $\mathbb{Z}_7[x]$ effettuiamo la divisione tra $a(x) = 2x^4 - x^2 + 1$ e $b(x) = 3x^3 - 2$ (qui stiamo scrivendo gli elementi di $\mathbb{Z}_7$ come 0, 1, 2, 3, 4, 5, 6 invece che $[0]_7$, $[1]_7$, $[2]_7$, $[3]_7$, $[4]_7$, $[5]_7$, $[6]_7$ per non appesantire la notazione).*

$$\begin{array}{llll|l} 2x^4 & -x^2 & & +1 & 3x^3-2 \\ \hline 2x^4 & & -6x & & 3x \\ \hline & -x^2 & +6x & +1 & \end{array} \qquad q(x) = 3x \qquad r(x) = -x^2 + 6x + 1 = 6x^2 + 6x + 1$$

Definizione. *Siano $a(x)$, $b(x)$ due polinomi non nulli in $K[x]$. Si dice massimo comun divisore tra $a(x)$ e $b(x)$, ogni polinomio $d(x)$ in $K[x]$ tale che*

1. *$d(x) \mid a(x)$ e $d(x) \mid b(x)$*
2. *se $c(x) \in K[x]$ con $c(x) \mid a(x)$ e $c(x) \mid b(x)$ allora $c(x) \mid d(x)$.*

Teorema (Esistenza di un massimo comun divisore)**.** *Per ogni $a(x), b(x)$ in $K[x]$ con $a(x) \neq 0$, $b(x) \neq 0$ esiste un massimo comun divisore $d(x)$ fra $a(x)$ e $b(x)$. Esistono inoltre polinomi $f(x), g(x) \in K[x]$ tali che sia*

$$d(x) = a(x)f(x) + b(x)g(x)$$

Dimostrazione. La dimostrazione è del tutto analoga a quella svolta in $\mathbb{Z}$ e consiste nell'applicazione dell'algoritmo delle divisioni successive:

$$
\begin{array}{lll}
(1) & a(x) = b(x)q_1(x) + r_1(x) & \partial r_1(x) < \partial b(x) \\
(2) & b(x) = r_1(x)q_2(x) + r_2(x) & \partial r_2(x) < \partial r_1(x) \\
(3) & r_1(x) = r_2(x)q_3(x) + r_3(x) & \partial r_3(x) < \partial r_2(x) \\
\vdots & \vdots & \\
\text{(k-1)} & r_{k-3}(x) = r_{k-2}(x)q_{k-1}(x) + r_{k-1}(x) & \partial r_{k-1}(x) < \partial r_{k-2}(x) \\
(k) & r_{k-2}(x) = r_{k-1}(x)q_k(x) &
\end{array}
$$

L'ultimo resto non nullo è un massimo comun divisore tra $a(x)$ e $b(x)$. Infine per determinare $f(x)$ e $g(x)$, si procede come in $\mathbb{Z}$. □ □

Il massimo comun divisore tra due polinomi è determinato a meno di una costante moltiplicativa non nulla.

Proposizione. *Sia $d(x)$ un massimo comun divisore tra $a(x)$ e $b(x)$. Allora $d'(x)$ è un massimo comun divisore tra $a(x)$ e $b(x)$ se e solo se $d'(x) = kd(x)$ con $k \in K^*$.*

Dimostrazione. Supponiamo che $d'(x) = kd(x)$ con $k \in K^*$. Allora $d(x) = k^{-1}d'(x)$ e, poiché $d(x) \mid a(x)$, si ha $a(x) = d(x)\overline{a}(x) = k^{-1}d'(x)\overline{a}(x)$, cioè $d'(x) \mid a(x)$.
Analogamente si prova che $d'(x) \mid b(x)$. Sia ora $c(x) \in K[x]$ con $c(x) \mid a(x)$ e $c(x) \mid b(x)$. Allora $c(x) \mid d(x)$ cioè $d(x) = c(x)q(x)$ per $q(x) \in K[x]$. Segue che $d'(x) = kd(x) = c(x)(kq(x))$ dunque $c(x) \mid d'(x)$.

Viceversa supponiamo che $d'(x)$ sia un massimo comun divisore tra $a(x)$ e $b(x)$. Allora, per la definizione di massimo comun divisore, si ha che $d(x) \mid d'(x)$ e $d'(x) \mid d(x)$, ovvero $d(x) = q_1(x)d'(x)$ e $d'(x) = q_2(x)d(x)$. Segue che $d(x) = q_1(x)q_2(x)d(x)$ e, semplificando per $d(x)$, si ha $q_1(x)q_2(x) = 1$. Allora $\partial q_1(x) = 0 = \partial q_2(x)$ e pertanto $q_2(x) = k$ con $k \in K^*$. □ □

Osservazione. *Per la proposizione precedente, esiste uno e un solo polinomio <u>monico</u> $d(x)$ che sia massimo comun divisore tra $a(x)$ e $b(x)$.*
Denoteremo tale massimo comun divisore con il simbolo $(a(x), b(x))$ e lo chiameremo il massimo comun divisore tra $a(x)$ e $b(x)$.
In particolare, se il grado del massimo comun divisore è zero, allora tale massimo comun divisore è 1. In questo caso $a(x)$ e $b(x)$ si dicono coprimi.

Esempi.

1. *Determinare il massimo comun divisore in $\mathbb{Z}_5[x]$ tra $a(x) = x^3 + x^2 + x + 1$ e $b(x) = 3x^2 + 2x + 2$.*
   Risulta

$$\begin{array}{llll|l} x^3 & +x^2 & +x & +1 & 3x^2+2x+2 \\ x^3 & +4x^2 & +4x & & \hline 2x+4 \\ \hline & 2x^2 & +2x & +1 & \\ & 2x^2 & +3x & +3 & \\ \hline & & 4x & +3 & \end{array} \qquad a(x) = b(x)(2x+4) + 4x + 3$$

$$\begin{array}{llll|l} 3x^2 & +2x & +2 & & 4x+3 \\ 3x^2 & +x & & & \hline 2x+4 \\ \hline & x & +2 & & \\ & x & +2 & & \\ \hline & // & // & & \end{array} \qquad b(x) = (4x+3)(2x+4)$$

Un massimo comun divisore tra $a(x)$ e $b(x)$ è $4x+3$, mentre $(a(x), b(x))) = x+2$. Infine

$$\begin{aligned} 4x+3 &= a(x) - b(x)(2x+4) \\ &= a(x)\cdot 1 + b(x)(3x+1) \end{aligned}$$

e

$$x+2 = a(x)\cdot 4 + b(x)(2x+4)$$

2. *Determinare il massimo comun divisore in $\mathbb{Q}[x]$ tra $a(x) = x^3+1$ e $b(x) = x^2+1$. Risulta*

$$\begin{array}{llll|l} x^3 & & & +1 & x^2+1 \\ x^3 & +x & & & \hline x \\ \hline & -x & +1 & & \end{array} \qquad a(x) = b(x)\cdot x + (-x+1)$$

$$\begin{array}{llll|l} x^2 & & & +1 & -x+1 \\ x^2 & -x & & & \hline -x-1 \\ \hline & x & +1 & & \\ & x & -1 & & \\ \hline & & 2 & & \end{array} \qquad b(x) = (-x+1)(-x-1) + 2$$

Un massimo comun divisore tra $a(x)$ e $b(x)$ è 2, pertanto $(a(x), b(x)) = 1$, ovvero $a(x)$ e $b(x)$ sono coprimi.

Inoltre

$$-x+1 = a(x)\cdot 1 + b(x)(-x)$$

$$\begin{aligned} 2 &= b(x) - (-x+1)(-x-1) \\ &= b(x) - [a(x) + b(x)(-x)](-x-1) \\ &= b(x) + [a(x) - b(x)x](x+1) \\ &= a(x)(x+1) + b(x)(1-x^2-x) \end{aligned}$$

ovvero

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

Definizione. *Sia $a(x) \in K[x]$ un polinomio di grado $n > 0$. Si dice che $a(x)$ è un polinomio primo (in $K[x]$) se ogni volta che $a(x) \mid b(x)c(x)$, con $b(x), c(x)$ in $K[x]$, si ha $a(x) \mid b(x)$ oppure $a(x) \mid c(x)$.*

Osservazione. *Se un polinomio primo $a(x)$ divide il prodotto $n \geq 2$ polinomi, segue dalla definizione (per induzione su n) che $a(x)$ divida almeno uno dei fattori.*

Definizione. *Sia $a(x) \in K[x]$ un polinomio di grado $n > 0$. Si dice che $a(x)$ è un polinomio irriducibile (in $K[x]$) se $a(x)$ è divisibile solo per i polinomi di grado 0 e per i polinomi della forma $h \cdot a(x)$ con $h \in K^*$. In caso contrario, si dice che $a(x)$ riducibile.*

Detto altrimenti: il polinomio $a(x)$ è irriducibile se e solo se è fattorizzabile soltanto come

$$a(x) = h^{-1}(ha(x)) \qquad \text{con } h \in K^*$$

Teorema. *Un polinomio $a(x)$ in $K[x]$ è irriducibile se e solo se è primo.*

Dimostrazione. Analoga a quella vista in $\mathbb{Z}$. □

Osservazione. *Si noti che la nozione di irriducibilità di un polinomio $a(x) \in K[x]$ dipende dal campo K cui appartengono i coefficienti del polinomio. Se K è un sottocampo di un campo F, si può riguardare $a(x)$ come polinomio in $F[x]$. Può accadere che $a(x)$ sia irriducibile in $K[x]$ ma riducibile in $F[x]$.*

Esempio. *Il polinomio $a(x) = x^2 - 2$ è irriducibile in $\mathbb{Q}[x]$ ma è riducibile in $\mathbb{R}[x]$ perché*

$$x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2}) \text{ in } \mathbb{R}[x]$$

Il polinomio $a(x) = x^2 + 1$ è irriducibile in $\mathbb{Q}[x]$ e in $\mathbb{R}[x]$, ma è riducibile in $\mathbb{C}[x]$ perché

$$x^2 + 1 = (x - i)(x + i) \text{ in } \mathbb{C}[x]$$

Teorema (Teorema della fattorizzazione unica)**.** *Ogni polinomio $a(x)$ in $K[x]$ di grado $n > 0$ può essere scritto come prodotto di $s \geq 1$ polinomi irriducibili (non necessariamente distinti).*
Tale fattorizzazione è essenzialmente unica, nel senso che se $a(x) = p_1(x) \cdots p_s(x) = q_1(x) \cdots q_t(x)$, dove i polinomi $p_i(x), q_j(x)$ $(1 \leq i \leq s,\ 1 \leq j \leq t)$ sono irriducibili, allora $s = t$ e si possono ordinare i fattori in modo che $p_1(x) = h_1 q_1(x), \ldots, p_s(x) = h_s q_s(x)$ con $h_i \in K^*$ $(1 \leq i \leq s)$.

Dimostrazione. Dimostriamo il teorema per induzione sul grado n del polinomio $a(x)$. Se $n = 1$, $a(x)$ è irriducibile e il teorema è vero.

Esistenza di una fattorizzazione

Sia $n > 1$. Se $a(x)$ è irriducibile, non c'è nulla da dimostrare. Se $a(x)$ è riducibile, allora

$$a(x) = b(x)c(x) \text{ con } 0 < \partial b(x), \partial c(x) < n.$$

Per induzione risulta

$$b(x) = b_1(x) \ldots b_h(x) \text{ e } c(x) = c_1(x) \ldots c_k(x)$$

dove i fattori $b_i(x)$ e $c_j(x)$ sono irriducibili $(1 \leq i \leq h,\ 1 \leq j \leq k)$. Segue che

$$a(x) = b_1(x) \ldots b_h(x) c_1(x) \ldots c_k(x)$$

è una fattorizzazione di $a(x)$ in irriducibili.

Unicità della fattorizzazione

Sia $a(x) = p_1(x) \ldots p_s(x) = q_1(x) \ldots q_t(x)$ dove i polinomi $p_i(x)$ e $q_j(x)$ sono irriducibili, $1 \leq i \leq s$, $1 \leq j \leq t$. Poiché $q_1(x)$ è irriducibile e divide il prodotto $p_1(x) \ldots p_s(x)$, divide almeno uno dei fattori. A meno di riordinare, possiamo supporre che $q_1(x) \,|\, p_1(x)$. Ma $p_1(x)$ è irriducibile dunque $p_1(x) = h_1 q_1(x)$ con $h_1 \in K^*$. Quindi

$$a(x) = h_1 q_1(x) p_2(x) \ldots p_s(x) = q_1(x) q_2(x) \ldots q_t(x)$$

da cui

$$h_1 p_2(x) \ldots p_s(x) = q_2(x) \ldots q_t(x)$$

Per induzione risulta $s = t$ e $p_i(x) = h_i q_i(x)$ con $h_i \in K^*$, $i = 2 \ldots s$. □

Corollario. *Ogni polinomio $a(x) \in K[x]$ di grado $n > 0$ si può scrivere come*

$$a(x) = k a_1(x) \ldots a_s(x)$$

dove $k \in K^*$ è il coefficiente direttore di $a(x)$ e i polinomi $a_1(x), \ldots, a_s(x)$ sono monici e irriducibili. Tale scrittura è unica a meno dell'ordine.

21 Sottogruppi normali. Ideali. Morfismi.

Sottogruppi normali di un gruppo. Omomorfismi.

Definizione. *Sia G un gruppo (con operazione $\cdot$). Un sottoinsieme H di G si dice un sottogruppo di G se H è un gruppo rispetto alla stessa operazione definita su G. In tal caso si scrive $H \leq G$.*

In altre parole, un sottoinsieme H di G è un sottogruppo di G se e solo se

1. *Chiusura: per ogni $h_1, h_2 \in H$, $h_1 h_2 \in H$.*
2. *Elemento neutro: $1_G \in H$.*
3. *Inversi: per ogni $h \in H$, $h^{-1} \in H$.*

Osservazione. *Ogni gruppo G possiede sempre due sottogruppi (detti i sottogruppi banali): G stesso e $\{1_G\}$.*

Esempi. 1. $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$.

2. *Per $n \in \mathbb{Z}$, l'insieme $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$ dei multipli interi di n è un sottogruppo di $(\mathbb{Z}, +)$. Infatti:*
   (a) *Chiusura: per ogni $nk_1, nk_2 \in \mathbb{Z}$, $nk_1 + nk_2 = n(k_1 + k_2) \in n\mathbb{Z}$.*
   (b) *Elemento neutro: $0 = n \cdot 0 \in n\mathbb{Z}$*
   (c) *Inversi (opposti): per ogni $nk \in n\mathbb{Z}$, $-nk = n(-k) \in n\mathbb{Z}$.*
3. $SL(n, \mathbb{R}) \leq GL(n, \mathbb{R})$.
4. *Per $n \geq 2$, l'insieme H delle permutazioni di S_n che fissano la cifra 1 è un sottogruppo di S_n.*

Proposizione. *Sia G un gruppo. Un sottoinsieme <u>non vuoto</u> H di G è un sottogruppo se e solo se per ogni $h_1, h_2 \in H$, $h_1 h_2^{-1} \in H$.*

Dimostrazione. Supponiamo che $H \leq G$. Per ogni $h_1, h_2 \in H$, $h_1, h_2^{-1} \in H$ perchè H contiene gli inversi dei propri elementi. Inoltre $h_1 h_2^{-1} \in H$ per la proprietà di chiusura.

Viceversa sia H un sottoinsieme non vuoto di G tale che per ogni $h_1, h_2 \in H$, $h_1 h_2^{-1} \in H$. Poichè H è non vuoto esiste $h \in H$, allora $1_G = hh^{-1} \in H$. Poi, per ogni $h \in H$, $1_G, h \in H$, dunque $1_G h^{-1} = h^{-1} \in H$. Infine per ogni $h_1, h_2 \in H$, $h_1, h_2^{-1} \in H$ dunque $h_1 (h_2^{-1})^{-1} = h_1 h_2 \in H$. □

Definizione. *Siano G un gruppo e H un sottogruppo di G. Definiamo due relazioni R_D e R_S su G ponendo per ogni $x, y \in G$:*

- *$x R_D y$ se e solo se $xy^{-1} \in H$.*
- *$x R_S y$ se e solo se $x^{-1} y \in H$.*

Le relazioni R_D e R_S sono relazioni di equivalenza. Lo proviamo per R_D e lasciamo per esercizio la verifica per R_S. Per ogni $x, y, z \in G$ si ha:

1. Riflessività: xR_Dx perchè $1_G = xx^{-1} \in H$.
2. Simmetria: se xR_Dy allora $xy^{-1} \in H$ e pertanto $(xy^{-1})^{-1} = yx^{-1} \in H$, ovvero yR_Dx.
3. Transitività: se xR_Dy e yR_Dz allora $xy^{-1} \in H$ e $yz^{-1} \in H$, dunque $(xy^{-1})(yz^{-1}) = xz^{-1} \in H$, ovvero xR_Dz.

Vediamo ora come sono fatte le classi di equivalenza di R_D. Per $x \in G$ abbiamo

$$\begin{aligned}[x]_{R_D} &= \{y \in G : yR_Dx\} = \{y \in G : yx^{-1} \in H\} = \{y \in G : \exists h \in H \text{ con } yx^{-1} = h\} \\ &= \{y \in G : \exists h \in H \text{ con } y = hx\} = \{hx : h \in H\} = Hx.\end{aligned}$$

La classe Hx si dice *laterale destro* di H in G. Analogamente si prova che le classi di equivalenza di R_S in G sono i *laterali sinistri* $xH = \{xh : h \in H\}$ di H in G.

Esempio. *Siano $G = S_3$ e $H = \{1, (1,2)\}$. Calcoliamo i laterali destri e sinistri di H in G.*

Laterali destri

$H1 = H = \{1, (1,2)\} = H(1,2)$

$H(1,3) = \{(1,3), (1,2)(1,3)\} = \{(1,3), (1,3,2)\} = H(1,3,2)$

$H(2,3) = \{(2,3), (1,2)(2,3)\} = \{(2,3), (1,2,3)\} = H(1,2,3)$

Laterali sinistri

$1H = H = \{1, (1,2)\} = (1,2)H$

$(1,3)H = \{(1,3), (1,3)(1,2)\} = \{(1,3), (1,2,3)\} = (1,2,3)H$

$(2,3)H = \{(2,3), (2,3)(1,2)\} = \{(2,3), (1,3,2)\} = (1,3,2)H$

In generale gli insiemi Hx e xH sono distinti. Per esempio se $G = S_3$ e $H = \{1, (1,2)\}$, abbiamo verificato che $H(1,3) \neq (1,3)H$.

Definizione. *Un sottogruppo N di un gruppo G si dice un sottogruppo normale se per ogni $x \in G$ risulta $xN = Nx$. In tal caso si scrive $N \lhd G$.*

Osservazione. *L'uguaglianza $xN = Nx$ è una uguaglianza di insiemi, cioe' xN e Nx sono uguali <u>come insiemi</u> e non necessariamente elemento per elemento.*

Esempi. *1. Il sottogruppo $H = \{1, (1,2)\}$ di S_3 non è un sottogruppo normale di S_3.*

2. Il sottogruppo $N = \{1, (1,2,3), (1,3,2)\}$ di S_3 è un sottogruppo normale di S_3. Infatti $1N = N = N1$. Inoltre

$$(1,2,)N = \{(1,2), (1,2)(1,2,3), (1,2)(1,3,2)\} = \{(1,2), (2,3), (1,3)\}$$

e

$$N(1,2) = \{(1,2),(1,2,3)(1,2),(1,3,2)(1,2)\} = \{(1,2),(1,3),(2,3)\},$$

dunque $(1,2)N = N(1,2)$. *Notare che non è necessario fare altre verifiche.*

3. *Sia G un gruppo commutativo. Ogni sottogruppo H di G è normale in G perchè per ogni $x \in G$, $xH = \{xh : h \in H\} = \{hx : h \in H\} = Hx$. In particolare $n\mathbb{Z}$ è un sottogruppo normale di $(\mathbb{Z}, +)$.*

L'importanza dei sottogruppi normali di un gruppo è dovuta alla costruzione che segue. Sia $N \lhd G$, consideriamo l'insieme quoziente G/N dei laterali destri (ovvero sinistri) di G, cioè $G/N = \{Nx : x \in G\}$. Definiamo una operazione binaria su G/N ponendo

$$Nx \cdot Ny = Nxy.$$

L'operazione è ben definita proprio perchè N è un sottogruppo normale. Infatti se $Nx = N\bar{x}$ e $Ny = N\bar{y}$ allora esistono $n_1, n_2 \in N$ tali che $x = n_1\bar{x}$ e $y = n_2\bar{y}$. Allora $xy = n_1\bar{x}n_2\bar{y}$. Adesso $\bar{x}n_2 \in \bar{x}N = N\bar{x}$ quindi esiste $n_3 \in N$ con $\bar{x}n_2 = n_3\bar{x}$. Allora

$$xy = (n_1\bar{x})(n_2\bar{y}) = n_1(\bar{x}n_2)\bar{y} = n_1(n_3\bar{x})\bar{y} = n\bar{x}\bar{y},$$

dove $n = n_1n_3 \in N$. Quindi se $Nx = N\bar{x}$ e $Ny = N\bar{y}$ abbiamo provato che $Nxy = N\bar{x}\bar{y}$.

L'insieme G/N con l'operazione binaria che abbiamo definito è un gruppo, *il gruppo quoziente* di G rispetto a N. Infatti:

1. Associatività: per ogni $Nx, Ny, Nz \in G/N$

$$(Nx \cdot Ny) \cdot Nz = N(xy)z = Nx(yz) = Nx \cdot (Ny \cdot Nz)$$

2. Elemento neutro: $N = N1 \in G/N$ e per ogni $Nx \in G/N$, $N \cdot Nx = N1 \cdot Nx = N1 \cdot x = Nx = Nx \cdot 1 = Nx \cdot N1 = Nx \cdot N$.
3. Inversi: per ogni $Nx \in G/N$, $Nx^{-1} \in G/N$ e

$$Nx \cdot Nx^{-1} = N = Nx^{-1} \cdot Nx.$$

Esempi. 1. *Siano $G = S_3$ e $N = \{1,(1,2,3),(1,3,2)\} \lhd S_3$, allora $S_3/N = \{N,(1,2)N\}$ e $(1,2)N \cdot (1,2)N = N$.*

2. *Siano $G = (\mathbb{Z}, +)$ e $N = n\mathbb{Z} \lhd \mathbb{Z}$. Allora*

$$\mathbb{Z}/n\mathbb{Z} = \{a + n\mathbb{Z} : a \in \mathbb{Z}\}$$

e $(a+n\mathbb{Z})+(b+n\mathbb{Z}) = (a+b)+n\mathbb{Z}$ per ogni $a, b \in \mathbb{Z}$. Si riconosce in questo esempio $\mathbb{Z}_n$ nel senso che $a + n\mathbb{Z} = [a]_n$ e $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$.

Introduciamo ora il concetto di *omomorfismo* tra gruppi.

Definizione. *Siano $(G, *)$ e $(H, \circ)$ due gruppi. Un omomorfismo da G in H è un'applicazione $\varphi : G \to H$ tale che per ogni $x, y \in G$ si abbia $\varphi(x * y) = \varphi(x) \circ \varphi(y)$. Se φ è un'applicazione iniettiva e suriettiva si dice che φ è un isomorfismo e i gruppi G e H sono isomorfi. Un isomorfismo da G in G si dice un automorfismo di G.*

Osservazione. *Sia $\varphi : G \to H$ un omomorfismo di gruppi. Allora*

1. *$\varphi(1_G) = 1_H$ come si verifica dalla definizione ponendo $x = y = 1_G$;*
2. *per ogni $x \in G$, $\varphi(x^{-1}) = \varphi(x)^{-1}$, come si verifica dalla definizione ponendo $y = x^{-1}$.*

Esempi. 1. *Siano $G = GL(n, \mathbb{R})$ e $H = (\mathbb{R}^*, \cdot)$. L'applicazione* $\det : G \to H$ *che associa a una matrice $A \in GL(n, \mathbb{R})$ il suo determinante è un omomorfismo di gruppi perchè per ogni $A, B \in GL(n, \mathbb{R})$ si ha* $\det(AB) = \det(A)\det(B)$.

2. *Siano G un gruppo e $N \lhd G$. L'applicazione $\pi : G \to G/N$ definita da $\pi(x) = Nx$ per ogni $x \in G$, è un omomorfismo di gruppi. Infatti per ogni $x, y \in G$, $\pi(xy) = Nxy = (Nx)(Ny) = \pi(x)\pi(y)$.*

Un omomorfismo di gruppi $\varphi : G \to H$ definisce due sottogruppi: $\operatorname{Ker}\varphi$, il nucleo di φ, sottogruppo di G, e $\operatorname{Im}\varphi$, l'immagine di φ, sottogruppo di H. Nucleo e immagine sono definiti da:

$$\operatorname{Ker}\varphi = \{x \in G : \varphi(x) = 1_H\} \leq G$$

e

$$\operatorname{Im}\varphi = \{\varphi(x) : x \in G\} \leq H.$$

Verifichiamo che si tratta di due sottogruppi. Per $\operatorname{Ker}\varphi$ abbiamo:

1. Chiusura: per ogni $x, y \in \operatorname{Ker}\varphi$, $\varphi(xy) = \varphi(x)\varphi(y) = 1_H \cdot 1_H = 1_H$, dunque $xy \in \operatorname{Ker}\varphi$.
2. Elemento neutro: $1_G \in \operatorname{Ker}\varphi$ perchè $\varphi(1_G) = 1_H$.
3. Inversi: per ogni $x \in \operatorname{Ker}\varphi$, $\varphi(x^{-1}) = \varphi(x)^{-1} = (1_H)^{-1} = 1_H$ dunque $x^{-1} \in \operatorname{Ker}\varphi$.

Per $\operatorname{Im}\varphi$ abbiamo:

1. Chiusura: per ogni $\varphi(x), \varphi(y) \in \operatorname{Im}\varphi$, $\varphi(x)\varphi(y) = \varphi(xy)$, dunque $\varphi(x)\varphi(y) \in \operatorname{Im}\varphi$.
2. Elemento neutro: $1_H \in \operatorname{Im}\varphi$ perchè $\varphi(1_G) = 1_H$.
3. Inversi: per ogni $\varphi(x) \in \operatorname{Im}\varphi$, $\varphi(x)^{-1} = \varphi(x^{-1})$ dunque $\varphi(x)^{-1} \in \operatorname{Im}\varphi$.

Esempio. *Consideriamo l'omomorfismo* $\det : GL(n, \mathbb{R}) \to \mathbb{R}^*$. *Il nucleo dell'omomorfismo è*

$$\operatorname{Ker}\det = \{A \in GL(n, \mathbb{R}) : \det A = 1\} = SL(n, \mathbb{R})$$

e l'immagine è tutto $\mathbb{R}^*$. *Infatti è facile verificare che l'applicazione* $\det : GL(n,\mathbb{R}) \to \mathbb{R}^*$ *è suriettiva perchè per ogni* $a \in \mathbb{R}^*$, *la matrice*

$$A = \begin{pmatrix} a & 0 \cdots 0 \\ 0 & 1 \cdots 0 \\ \vdots & \vdots \\ 0 & 0 \cdots 1 \end{pmatrix}$$

appartiene a $GL(n,\mathbb{R})$ *e* $\det A = a$.

Il nucleo di un omomorfismo non è solo un sottogruppo, ma è un sottogruppo normale.

Proposizione. *Sia* $\varphi : G \to H$ *un omomorfismo di gruppi. Il nucleo* $\operatorname{Ker}\varphi$ *è un sottogruppo normale di* G.

Dimostrazione. Posto $K = \operatorname{Ker}\varphi$, mostriamo che per ogni $x \in G$, $xK = Kx$. Facciamo vedere che $xK \subseteq Kx$. Per ogni $xk \in xK$ (quindi $k \in K$) risulta $\varphi(xkx^{-1}) = \varphi(x)\varphi(k)\varphi(x^{-1}) = \varphi(x)\varphi(x)^{-1} = 1_H$, quindi $xkx^{-1} \in K$, ovvero esiste $\bar{k} \in K$ per cui $xkx^{-1} = \bar{k}$ e pertanto $xk = \bar{k}x \in Kx$. Analogamente si mostra l'altra inclusione $Kx \subseteq xK$. □

Sia $\varphi : G \to H$ un omomorfismo di gruppi. Poichè $\operatorname{Ker}\varphi \lhd G$ possiamo considerare il gruppo quoziente $G/\operatorname{Ker}\varphi$.

Teorema (Teorema Fondamentale degli Omomorfismi)**.** *Sia* $\varphi : G \to H$ *un omomorfismo di gruppi. Il gruppo* $G/\operatorname{Ker}\varphi$ *è isomorfo a* $\operatorname{Im}\varphi$.

Dimostrazione. Posto $K = \operatorname{Ker}\varphi$ abbiamo $G/K = \{xK : x \in G\}$. Definiamo un'applicazione $\psi : G/K \to \operatorname{Im}\varphi$ ponendo $\psi(xK) = \varphi(x)$. Facciamo vedere che la definizione è ben posta. Se $xK = yK$ allora $x = yk$ per un certo $k \in K$ quindi $\varphi(x) = \varphi(yk) = \varphi(y)\varphi(k) = \varphi(y)$, ovvero se $xK = yK$ allora

$$\psi(xK) = \varphi(x) = \varphi(y) = \psi(yK).$$

L'applicazione ψ è un omomorfismo di gruppi. Infatti per ogni $xK, yK \in G/K$ si ha

$$\psi(xK \cdot yK) = \psi(xyK) = \varphi(xy) = \varphi(x)\varphi(y) = \psi(xK)\psi(yK).$$

L'applicazione ψ è iniettiva. Infatti se $\psi(xK) = \psi(yK)$ allora $\varphi(x) = \varphi(y)$ dunque $\varphi(x)\varphi(y)^{-1} = \varphi(x)\varphi(y^{-1}) = \varphi(xy^{-1}) = 1_H$ e pertanto $xy^{-1} \in K$. Allora $xK = Kx = Ky = yK$.

L'applicazione ψ è suriettiva. Infatti se $\varphi(x) \in \operatorname{Im}(\varphi)$ allora $\varphi(x) = \psi(xK)$.

□

Ideali di un anello. Omomorfismi.

Definizione. *Sia $(A, +, \cdot)$ un anello. Un sottoinsieme B di A si dice un sottoanello di A (e si scrive $B \leq A$) se B è un anello rispetto alle operazioni di A. In altre parole*

In altre parole un sottoinsieme non vuoto B di A è un sottoanello se e solo se

1. per ogni $b_1, b_2 \in B$, $b_1 - b_2 \in B$; $(B - B \subseteq B)$
2. per ogni $b_1, b_2 \in B$, $b_1 b_2 \in B$; $(B \cdot B \subseteq B)$
3. $1_A \in B$. $(1_A \in B)$

Definizione. *Sia A un anello. Un sottoinsieme non vuoto I di A si dice un ideale di A (e si scrive $I \lhd A$) se*

1. *per ogni $i_1, i_2 \in I$, $i_1 - i_2 \in I$; $(I - I \subseteq I)$*
2. *per ogni $a \in A$ e $i \in I$, $ai \in I$ e $ia \in I$; $(AI \subseteq I$ e $IA \subseteq I)$.*

Osservazione. *Notare che la prima condizione nella definizione di ideale equivale a richiedere che $(I, +)$ sia un sottogruppo di $(A, +)$. Infatti, per la caratterizzazione dei sottogruppi di un gruppo, abbiamo che un sottoinsieme non vuoto I di A è un sottogruppo di $(A, +)$ se e solo se per ogni $i_1, i_2 \in I$, $i_1 - i_2 \in I$.*

Esempi.

1. *Sia $n \in \mathbb{Z}$ fissato. L'insieme $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$ è un ideale dell'anello $\mathbb{Z}$. Infatti abbiamo già verificato che $(n\mathbb{Z}, +)$ è un sottogruppo di $(\mathbb{Z}, +)$. Poi per ogni $m \in \mathbb{Z}$ e per ogni $nk \in n\mathbb{Z}$, $m(nk) = n(mk) = (nk)m \in n\mathbb{Z}$.*
2. *Sia A un anello commutativo e $x \in A$. L'insieme $I = (x) = \{ax : a \in A\}$ dei "multipli" di x in A è un ideale di A (che si dice l'ideale* principale *generato da x). Infatti I è non vuoto perchè $x = 1_A x \in I$, per ogni $a_1 x, a_2 x \in I$, si ha $a_1 x - a_2 x = (a_1 - a_2)x \in I$ e per ogni $b \in A$ e, per ogni $ax \in I$, $b(ax) = (ba)x \in I$ e $(ax)b = (ab)x \in I$. In particolare, se $A = \mathbb{Z}$ e $x = n$, $I = (n) = n\mathbb{Z}$.*
3. *Sia $A = K[x]$ l'anello dei polinomi nell'indeterminata x a coefficienti in un campo K. Per $g(x) \in K[x]$ fissato, $I = (g(x)) = \{a(x)g(x) : a(x) \in K[x]\}$.*

Siano ora A un anello e $I \lhd A$ un ideale. Allora $(I, +)$ è un sottogruppo di $(A, +)$, necessariamente normale perchè $(A, +)$ è un gruppo commutativo. Dunque possiamo considerare il gruppo quoziente $A/I = \{a + I : a \in A\}$, dove l'operazione è definita da $(a+I)+(b+I) = (a+b)+I$. È chiaro che $(A/I, +)$ è un gruppo commutativo. Definiamo una operazione prodotto in A/I ponendo per ogni $a + I, b + I \in A/I$

$$(a + I)(a + I) = ab + I.$$

È facile verificare che la definizione è ben posta e che A/I con le operazioni ora definite è un anello, *l'anello quoziente* di A su I.

Osservazione. *Notare che se $A = \mathbb{Z}$ e $I = n\mathbb{Z}$ allora $A/I = \mathbb{Z}_n$ e ritroviamo le operazioni che abbiamo definito in precedenza su $\mathbb{Z}_n$.*

In particolare, se $A = K[x]$ e $I = (g(x))$ con $g(x) \in K[x]$ fissato, allora l'anello quoziente $K[x]/(g(x))$ è $K[x]/(g(x)) = \{f(x) + (g(x)) : f(x) \in K[x]\}$ dove $f(x) + (g(x)) = \{f(x) + g(x)q(x) : q(x) \in K[x]\}$ e per ogni $f(x), h(x) \in K[x]$ si ha

$$(f(x) + (g(x))) + (h(x) + (g(x))) = f(x) + h(x) + (g(x))$$

e

$$(f(x) + (g(x))) \cdot (h(x) + (g(x))) = f(x) + h(x) + (g(x)).$$

Definizione. *Siano A e B due anelli. Un'applicazione $\varphi : A \to B$ si dice un omomorfismo di anelli se per ogni $a_1, a_2 \in A$*

1. $\varphi(a_1 + a_2) = \varphi(a_1) + \varphi(a_2)$
2. $\varphi(a_1 \cdot a_2) = \varphi(a_1) \cdot \varphi(a_2)$.

Osservazione. *Se $\varphi : A \to B$ è un omomorfismo di anelli, dalla prima condizione della definizione segue che φ è un omomorfismo di gruppi additivi. Dunque $\varphi(0_A) = 0_B$ e $\varphi(-a) = -\varphi(a)$ per $a \in A$.*

Come nel caso dei gruppi, un omomorfismo di anelli $\varphi : A \to B$ definisce due sottoinsiemi, il nucleo e l'immagine di φ definiti da:

$$\operatorname{Ker} \varphi = \{a \in A : \varphi(a) = 0_B\} \subseteq A$$

e

$$\operatorname{Im} \varphi = \{\varphi(a) : a \in A\} \subseteq B.$$

È facile verificare che $\operatorname{Ker} \varphi$ è un ideale di A mentre $\operatorname{Im} \varphi$ è un sottonaello di B. Inoltre $A/\operatorname{Ker} \varphi$ è isomorfo a $\operatorname{Im} \varphi$.

22 Costruzione di campi

Congruenza modulo $g(x)$

Siano K un campo e $g(x) \in K[x]$ un polinomio fissato. Diciamo che due polinomi $f(x), h(x)$ in $K[x]$ sono *congrui modulo* $g(x)$, e scriviamo $f(x) \equiv h(x) \bmod g(x)$, se $g(x)|f(x) - h(x)$. Proviamo che la congruenza modulo $g(x)$ definisce una relazione di equivalenza in $K[x]$:

1. la congruenza modulo $g(x)$ è riflessiva: $\forall f(x) \in K[x]$, $f(x) \equiv f(x) \bmod g(x)$.

   Infatti $f(x) - f(x) = 0 = 0 \cdot g(x)$ dunque $g(x)|f(x) - f(x)$

2. la congruenza modulo $g(x)$ è simmetrica: $\forall f(x), h(x) \in K[x]$, se $f(x) \equiv h(x) \bmod g(x)$ allora $h(x) \equiv f(x) \bmod g(x)$.

   Infatti se $g(x)|f(x)-h(x)$ si ha $f(x)-h(x) = g(x)q(x)$ per un $q(x) \in K[x]$. Segue che $h(x) - f(x) = -g(x)q(x) = g(x)(-q(x))$ con $-q(x) \in K[x]$, ovvero $g(x)|h(x) - f(x)$.

3. R è transitiva: $\forall f(x), h(x), t(x) \in K[x]$, se $f(x) \equiv h(x) \bmod g(x)$ e $h(x) \equiv t(x) \bmod g(x)$ allora $f(x) \equiv t(x) \bmod g(x)$. Infatti se $g(x)|f(x) - h(x)$ e $g(x)|h(x) - t(x)$ si ha $f(x) - h(x) = g(x)q_1(x)$ e $h(x) - t(x) = g(x)q_2(x)$ con $q_1(x)$, $q_2(x) \in K[x]$.
   Sommando si trova $f(x) - t(x) = g(x)(q_1(x) + q_2(x))$ con $q_1(x) + q_2(x) \in K[x]$.

Vediamo ora come sono fatte le classi di equivalenza in $K[x]$ rispetto alla congruenza modulo $g(x)$. Per $f(x) \in K[x]$ si ha

$$\begin{aligned}
[f(x)]_{g(x)} &= \{h(x) \in K[x] | h(x) \equiv f(x) \bmod g(x)\} \\
&= \{h(x) \in K[x] | h(x) - f(x) = g(x)q(x) \text{ per un certo } q(x) \in K[x]\} \\
&= \{h(x) \in K[x] | h(x) = f(x) + g(x)q(x) \text{ per un certo } q(x) \in K[x]\} \\
&= \{f(x) + g(x)q(x) | q(x) \in K[x]\}
\end{aligned}$$

Osservazione. *Si noti l'analogia con la congruenza modulo n in $\mathbb{Z}$.*

$$\begin{array}{ccc}
\mathbb{Z} & \sim & K[x] \\
n & \sim & g(x) \\
[a]_n & \sim & [f(x)]_{g(x)} \\
\mathbb{Z}_n & \sim & K[x]/(g(x))
\end{array}$$

Osservazione. *Indichiamo la classe di $f(x)$ rispetto alla congruenza modulo $g(x)$ con il simbolo $[f(x)]_{g(x)}$. L'insieme quoziente, cioè l'insieme delle classi di equivalenza, si indica con $K[x]/(g(x))$*

Operazioni in $K[x]/(g(x))$

Definiamo due operazioni in $K[x]/(g(x))$, somma e prodotto, ponendo

$$[f(x)]_{g(x)} + [h(x)]_{g(x)} = [f(x) + h(x)]_{g(x)}$$
$$[f(x)]_{g(x)} \cdot [h(x)]_{g(x)} = [f(x) \cdot h(x)]_{g(x)}$$

per $f(x), h(x) \in K[x]$.

Osservazione. *Si noti ancora l'analogia con la congruenza modulo n. Anche in questo caso, definiamo somma e prodotto tra classi di equivalenza "scaricando" le operazioni sui rappresentanti delle classi.*

Si verifica facilmente che $K[x]/(g(x))$ con le operazioni di somma e prodotto scritte sopra è un anello commutativo con unità $[1]_{g(x)}$.

Osservazione. *Siano K un campo e $g(x) \in K[x]$ un polinomio fissato. Utilizzando la nozione di ideale possiamo risparmiarci le verfiche fatte fino qui. Infatti abbiamo visto che $I = (g(x))$ è un ideale di $K[x]$ e dunque l'anello quoziente $K[x]/(g(x))$ è $K[x]/(g(x)) = \{f(x) + (g(x)) : f(x) \in K[x]\}$ dove $f(x) + (g(x)) = \{f(x) + g(x)q(x) : q(x) \in K[x]\}$ e per ogni $f(x), h(x) \in K[x]$ si ha*

$$(f(x) + (g(x))) + (h(x) + (g(x))) = f(x) + h(x) + (g(x))$$

e

$$(f(x) + (g(x))) \cdot (h(x) + (g(x))) = f(x) + h(x) + (g(x)).$$

Notare che $f(x) + (g(x)) = [f(x)]_{g(x)}$.

Vediamo ora come possiamo rappresentare gli elementi del quoziente $K[x]/(g(x))$.

Teorema. *Siano K un campo e $g(x) \in K[x]$ un polinomio fissato. Se $g(x)$ ha grado $n > 0$ ogni elemento di $K[x]/(g(x))$ si può scrivere in modo unico nella forma $[r(x)]_{g(x)}$ con $\partial r(x) < n = \partial g(x)$.*

Dimostrazione. Sappiamo che $K[x]/(g(x))$ è l'insieme delle classi, dunque

$$K[x]/(g(x)) = \{[f(x)]_{g(x)} : f(x) \in K[x]\}$$

1. Dato un generico elemento $[f(x)]_{g(x)}$ in $K[x]/(g(x))$ dividiamo $f(x)$ per $g(x)$ ottenendo

   $$f(x) = g(x)q(x) + r(x)$$

   con $\partial r(x) < n = \partial g(x)$.

   Poichè $f(x) - r(x) = g(x)q(x)$ risulta $f(x) \equiv r(x) \bmod g(x)$ e pertanto $[f(x)]_{g(x)} = [r(x)]_{g(x)}$

2. Se fosse $[r(x)]_{g(x)} = [r_1(x)]_{g(x)}$ con $\partial r(x) < n$ e $\partial r_1(x) < n$, avremmo che $r(x) \equiv r_1(x)$ ovvero $g(x)|r(x) - r_1(x)$.
   Ma $\partial(r(x) - r_1(x)) < n = \partial g(x)$. L'unica possibilità è che $r(x) - r_1(x) = 0$ ovvero $r(x) = r_1(x)$. □

□

Corollario. *Se $K = \mathbb{Z}_p$ con p primo, $K[x]/(g(x))$ ha p^n elementi, dove $n = \partial g(x)$, $n > 0$.*

Dimostrazione. Per il teorema precedente ogni elemento di $K[x]/(g(x))$ si scrive in modo unico come $[r(x)]_{g(x)}$ con $\partial r(x) < n$. Le possibili scelte per $r(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1}$ con a_0, $a_1, \ldots, a_{n-1}$ in $\mathbb{Z}_p$ sono p^n. □ □

Siamo interessati al caso in cui $K[x]/(g(x))$ è un campo.

Teorema. *Siano K un campo e $g(x) \in K[x]$ un polinomio di grado $n > 0$. L'anello $K[x]/(g(x))$ è un campo se e solo se $g(x)$ è irriducibile in $K[x]$.*

Dimostrazione.

1. Sia $g(x)$ irriducibile in $K[x]$. Per mostrare che $K[x]/(g(x))$ è un campo basta mostrare che ogni elemento non nullo in $K[x]/(g(x))$ è invertibile. Sia $[f(x)]_{g(x)}$ un elemento non nullo, quindi $[f(x)]_{g(x)} \neq [0]_{g(x)}$. In particolare $g(x)$ non divide $f(x)$. Consideriamo il massimo comun divisore $(f(x), g(x))$ tra $f(x)$ e $g(x)$. Poichè $(f(x), g(x))|g(x)$ e $g(x)$ è irriducibile, deve essere $(f(x), g(x)) = 1$ oppure $(f(x), g(x)) = k \cdot g(x)$ con $k \in K^*$. Nel secondo caso avremmo che $g(x)|f(x)$ che è escluso. Quindi $(f(x), g(x)) = 1$. Per l'identità di Bezout, esistono $t(x), s(x) \in K[x]$ con

   $$1 = s(x)f(x) + t(x)g(x)$$

   Affermiamo che l'inverso di $[f(x)]_{g(x)}$ è $[s(x)]_{g(x)}$. Infatti

   $$\begin{aligned} &([f(x)]_{g(x)}) \cdot ([s(x)]_{g(x)}) \\ &= [f(x)s(x)]_{g(x)} \\ &= [1 - t(x)g(x)]_{g(x)} \\ &= [1]_{g(x)} \end{aligned}$$

   L'ultimo passaggio segue dal fatto che $[t(x)g(x)]_{g(x)} = [0]_{g(x)}$.

2. Supponiamo che $K[x]/(g(x))$ sia un campo. Se $g(x)$ fosse riducibile ammetterebbe una fattorizzazione

   $$g(x) = a(x)b(x) \in K[x]$$

   con $0 < \partial a(x) < \partial g(x)$ e $0 < \partial b(x) < \partial g(x)$. In $K[x]/(g(x))$ si ha $[a(x)]_{g(x)} \neq [0]_{g(x)}$, $[b(x)]_{g(x)} \neq [0]_{g(x)}$ e $[a(x)]_{g(x)}[b(x)]_{g(x)} = [a(x)b(x)]_{g(x)} = [g(x)]_{g(x)} = [0]_{g(x)}$. In un

campo F non posso trovare due elementi a, b con $a \neq 0_F$, $b \neq 0_F$ e $ab = 0_F$. Perché in questo caso, moltiplicando per l'inverso di a, ottengo

$$b = (aa^{-1})b = a^{-1}ab = a^{-1}(ab) = a^{-1} \cdot 0_F = 0_F.$$

Quindi se $K[x]/(g(x))$ è un campo e $g(x)$ è riducibile trovo un assurdo. Segue che $g(x)$ è irriducibile. □

□

Esempio. *Sia $K = \mathbb{R}$ il campo dei numeri reali e $g(x) = x^2 + 1$ polinomio irriducibile in $\mathbb{R}[x]$. L'anello $\mathbb{R}[x]/(x^2+1)$ è un campo. Ogni elemento di $\mathbb{R}[x]/(x^2+1)$ si scrive in modo unico come $[r(x)]_g$ con $\partial r(x) < 2 = \partial g(x)$. Quindi*

$$\mathbb{R}[x]/(x^2 + 1) = \{[bx + a]_g : a, b \in \mathbb{R}\}.$$

Calcoliamo in $\mathbb{R}[x]/(x^2 + 1)$ il prodotto $[x]_g \cdot [x]_g = [x^2]_g$. Per scrivere $[x^2]_g$ in forma standard, cioè per scriverlo nella forma $[r(x)]_g$ con $\partial r(x) < 2$, dividiamo x^2 per $x^2 + 1$ e consideriamo il resto. Risulta $x^2 = (x^2 + 1) \cdot 1 + (-1)$ dunque il quoziente è $q(x) = 1$ e il resto è $r(x) = -1$. Allora

$$[x]_g \cdot [x]_g = [-1]_g.$$

Se invece moltiplichiamo due classi che hanno come rappresentante una costante otteniamo $[a_1]_g \cdot [a_2]_g = [a_1a_2]_g$ con $a_1, a_2 \in \mathbb{R}$, e il prodotto è già in forma standard. Non è difficile convincersi che il sottoinsieme di $\mathbb{R}[x]/(x^2 + 1)$ formato dalle classi della forma $[a]_g$ al variare di a in $\mathbb{R}$, cioè il sottoinsieme

$$\{[a]_g : a \in \mathbb{R}\}$$

si comporta, rispetto a somma e prodotto di classi, come l'insieme $\mathbb{R}$ rispetto alle usuali operazioni di somma e prodotto. questo giustifica che si identifichi la classe $[a]_g$ con il suo rapresentante a.

Posto $i = [x]_g$ abbiamo allora $i^2 = [x]_g \cdot [x]_g = [-1]_g = -1$ e pertanto

$$\mathbb{R}[x]/(x^2 + 1) = \{[bx + a]_g : a, b \in \mathbb{R}\} = \{[b]_g[x]_g + [a]_g : a, b \in \mathbb{R}\} = \{bi + a : a, b \in \mathbb{R}\}$$

con $i^2 = -1$. Si ha cioè che $\mathbb{R}[x]/(x^2 + 1)$ coincide con il campo $\mathbb{C}$ dei numeri complessi.

23 Radici di un polinomio

Definizione. *Siano K un campo, $f(x) \in K[x]$ e $\alpha \in K$. Se $f(\alpha) = 0$ si dice che α è una radice (o zero) di $f(x)$.*

Teorema (Ruffini)**.** *Siano K un campo, $f(x) \in K[x]$, e $\alpha \in K$. Si ha che α è radice di $f(x)$ se e solo se $x - \alpha$ divide $f(x)$.*

Dimostrazione. Se $x - \alpha \mid f(x)$ si ha $f(x) = (x - \alpha)q(x)$ per un $q(x) \in K[x]$. Segue che

$$f(\alpha) = (\alpha - \alpha)q(\alpha) = 0 \cdot q(\alpha) = 0$$

Viceversa se α è radice di $f(x)$, ovvero $f(\alpha) = 0$, la divisione con resto porge

$$f(x) = (x - \alpha)q(x) + r(x) \text{ con } \partial r(x) < 1$$

Poiché $\partial r(x) < 1$ abbiamo che $r(x)$ è il polinomio nullo oppure $r(x) = k$ con $k \in K^*$. Nel secondo caso avremmo

$$f(x) = (x - \alpha)q(x) + k$$

da cui

$$0 = f(\alpha) = (\alpha - \alpha)q(\alpha) + k$$

cioè $k = 0$, assurdo.
Rimane provato che $r(x)$ è il polinomio nullo e pertanto $f(x) = (x - \alpha)q(x)$. □ □

Osservazione. *Il teorema precedente permette di dare dei criteri di irriducibilità:*

1. *un polinomio $f(x) = ax + b \in K[x]$ di grado 1 (quindi $a \neq 0$) è irriducibile in $K[x]$ e ha l'unica radice $\alpha = -\dfrac{b}{a} = -ba^{-1}$ in K.*
2. *un polinomio $f(x) \in K[x]$ di grado maggiore di 1 che ammette la radice α in K è divisibile per $x - \alpha$ e quindi $f(x)$ è riducibile in $K[x]$. (Non è vero però il viceversa: un polinomio può essere riducibile in $K[x]$ e non ammettere radici in K. Per esempio $x^4 + 3x^2 + 2 \in \mathbb{R}[x]$ si fattorizza come $(x^2 + 1)(x^2 + 2)$ e quindi è riducibile in $\mathbb{R}[x]$, ma non ha radici in $\mathbb{R}$.)*
3. *un polinomio $f(x) \in K[x]$ di grado 2 oppure 3 è riducibile in $K[x]$ se e solo se ammette una radice in K.*

Definizione. *Siano K un campo, $f(x) \in K[x]$ e $\alpha \in K$. Si dice che α è una radice di $f(x)$ di molteplicità r (con $r \geq 1$) se $(x - \alpha)^r \mid f(x)$ ma $(x - \alpha)^{r+1} \nmid f(x)$. In particolare una radice di molteplicità 1 si dice una radice semplice.*

Esempi.

1. *$f(x) = x^2 - 2 \in \mathbb{Q}[x]$ non ha radici in $\mathbb{Q}$.*
   $f(x) = x^2 - 1 = (x-1)(x+1) \in \mathbb{Q}[x]$ ha in $\mathbb{Q}$ le radici semplici -1 e $+1$.
   $f(x) = x^4 - 2x^2 + 1 = (x-1)^2(x+1)^2 \in \mathbb{Q}[x]$ ha in $\mathbb{Q}$ le radici -1 e $+1$ entrambe di molteplicità 2.

2. *$f(x) = x^4 + 1 = (x+1)^4$ in $\mathbb{Z}_2[x]$ ha in $\mathbb{Z}_2$ la radice 1 con molteplicità 4.*

Teorema. *Siano K un campo e $f(x) \in K[x]$ un polinomio non nullo di grado n. La somma delle molteplicità delle radici di $f(x)$ è al più n.*

Dimostrazione. Se $n = 0$, $f(x)$ non ha radici in K.
Sia allora $n > 0$. Scriviamo $f(x)$ come prodotto di polinomi irriducibili in $K[x]$. Se nessuno di questi ha grado 1, $f(x)$ non ha radici in K. Altrimenti scriviamo

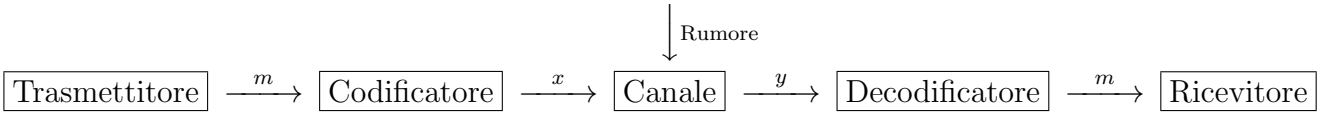
$$f(x) = k(x-\alpha_1)^{r_1}(x-\alpha_2)^{r_2}\dots(x-\alpha_t)^{r_t}g_1(x)\dots g_s(x)$$

dove $k \in K^*$, $\alpha_1, \dots, \alpha_t$ sono elementi distinti di K, $g_1(x), \dots, g_s(x)$ sono (eventuali) polinomi di grado maggiore di 1, irriducibili in $K[x]$.
Le radici di $f(x)$ in K sono pertanto $\alpha_1 \dots \alpha_t$ con molteplicità $r_1, \dots, r_t$ rispettivamente. Infatti è chiaro che α_i è radice con molteplicità r_i. D'altra parte $f(x)$ non ha altre radici perché se $\beta \in K$ con $\beta \neq \alpha_i$

$$f(\beta) = k(\beta-\alpha_1)^{r_1}\dots(\beta-\alpha_t)^{r_t}g_1(\beta)\dots g_s(\beta) \neq 0$$

Infine confrontando il grado di f e il grado di $(x-\alpha_1)^{r_1}\dots(x-\alpha_t)^{r_t}g_1(x)\dots g_s(x)$ si trova $r_1 + r_2 + \dots + r_t \leq n$
□ □

24 Teoria dei Codici: introduzione



Trasmettitore: emette il messaggio m

Codificatore: traduce il messaggio m nella *parola* x in modo che possa attraversare il canale.

Canale: mezzo attraverso il quale viaggiano le parole.

Decodificatore: trasforma la parola y in uscita dal canale nel messaggio m

Ricevitore: riceve il messaggio m

Rumore: disturbi di vario genere che potrebbero alterare le parole.

Teoria dei Codici: riconoscere se la parola ricevuta y contiene errori e, nel caso, correggerli.

Esempio (Esempio di Codifica)**.** *Trasmettiamo un messaggio nella lingua italiana. A ogni lettera dell'alfabeto associamo il suo numero d'ordine scritto in binario. Pertanto alla lettera a associamo* 1 *in binario, alla lettera b associamo* 2 *in binario etc. Otteniamo così la tabella*

$$\begin{array}{ccc} a & \to & 1 \\ b & \to & 10 \\ c & \to & 11 \\ \vdots & \vdots & \vdots \\ z & \to & 10101. \end{array}$$

Trasmettere la lettera a significa

$$a \to 1 \to \boxed{\textit{Canale}} \to 1 \to a$$

trasmettere la lettera z significa

$$z \to 10101 \to \boxed{\textit{Canale}} \to 10101 \to ?$$

Nel secondo caso, anche supponendo che non ci siano stati errori di trasmissione, il decodificatore non sa se sono state tramesse più lettere in successione o una sola lettera. Per esempio

$$\begin{array}{l} 10|10|1 \to bba \\ 10|101 \to be \\ 10101 \to z \end{array}$$

Per risolvere il problema si possono codificare le lettere dell'alfabeto con sequenze di stessa lunghezza. La lunghezza deve essere tale da permettere la codifica della sequenza più lunga.

Nell'esempio la sequenza più lunga corrisponde alla z quindi le lettere sono codificate con sequenze di (almeno) 5 *simboli, ottenuto inserendo un opportuno numero di zeri a sinistra delle sequenze più corte. Pertanto si avrà*

$$\begin{aligned} a &\to 00001 \\ b &\to 00010 \\ &\dots \\ z &\to 10101. \end{aligned}$$

Esempio. *In un laboratorio di un'università di un'altra città si effettua un esperimento. Tramite posta elettronica si riceve* 0 *se l'esperimento ha dato esito positivo,* 1 *se l'esperimento ha dato esito negativo. Nella trasmissione c'è una probabilità* $p = 0,01$ *di errore, cioè ogni* 100 *dati ricevuti uno è sbagliato. Se riceviamo* 0 *non siamo sicuri che l'esperimento abbia dato esito positivo. Per questo introduciamo ridondanza, cioè introduciamo ulteriori elementi che appesantiscono la trasmissione ma riducono la probabilità di errore. Per esempio chiediamo di trasmettere* 00 *se l'esperimento ha dato esito positivo e* 11 *se l'esperimento ha dato esito negativo. Supponiamo che l'esperimento abbia dato esito positivo. Elenchiamo le varie possibilità di messsaggio ricevuto e le rispettive probabilità:*

Messaggio ricevuto	*Probabilità*
11	$p^2 = 0,0001$
01	$(1-p)p = 0,0099$
10	$p(1-p) = 0,0099$
00	$(1-p)^2 = 0,9801.$

Osserviamo inoltre che se riceviamo 01 o 10 siamo certi che c'è stato un errore di trasmissione, dunque solo in un caso su 10000 commettiamo un errore.

Codici a blocchi

Definizione. *Sia* $A_q = \{x_1, x_2, \dots, x_q\}$ *un insieme finito di cardinalità* $|A_q| = q \geq 2$. *Si dice* codice a blocchi *un qualunque sottoinsieme non vuoto* C *di* A_q^n.

In particolare

- A_q si dice *alfabeto* di C;
- A_q^n è lo spazio delle parole di lunghezza n (nell'alfabeto A_q);
- una *parola* del codice C è una n-pla ordinata di simboli dell'alfabeto A_q e si denota con $x = (x_1, \dots, x_n)$ ovvero, per brevità, con $x = x_1, \dots, x_n$;
- n si dice la *lunghezza* del codice;
- la cardinalità di C si dice *grandezza* del codice.

Tipologie di errori

Supponiamo di aver mandato la parola $x = (x_1, \ldots, x_n)$ attraverso il canale e di aver avuto in uscita la parola $y = (y_1, \ldots, y_n)$, con $x \neq y$ dunque nel passaggio attraverso il canale sono occorsi degli errori. Elenchiamo alcune tipologie di errore

E1) un simbolo x_i di x viene alterato;

E2) uno o più simboli di x vanno persi;

E3) uno o più simboli extra compaiono in y.

La Teoria dei Codici, nella versione basica che affrontiamo qui, si occupa solo di errori di tipo $E1$). Inoltre se un simbolo x_i di x viene alterato contiamo un errore (così due simboli alterati sono due errori etc.). Assumiamo anche che gli errori siano indipendenti tra loro cioè alterare x_i non incide sugli x_j con $j \neq i$.

Distanza di Hamming

Definizione. *Siano $p = (x_1, \ldots, x_n)$ e $p' = (y_1, \ldots, y_n)$ due parole in A_q^n. Si dice* distanza di Hamming *tra p e p', e si scrive $d(p, p')$, il numero di componenti in cui p e p' differiscono, cioè*

$$d(p, p') = |\{i : x_i \neq y_i\}|.$$

Segue che la distanza di Hamming è una funzione

$$d : A_q^n \times A_q^n \to \mathbb{R}$$

tale che

1. $d(p, p') \geq 0$ e $d(p, p') = 0$ se e solo se $p = p'$,
2. $d(p, p') = d(p', p)$,
3. $d(p, p') \leq d(p, p'') + d(p'', p')$ (disuguaglianza triangolare),

per ogni $p, p', p'' \in A_q^n$.

Le proprietà 1. e 2. sono ovvie. La proprietà 3. si può argomentare come segue. Siano $p = (x_1, \ldots, x_n), p' = (y_1, \ldots, y_n)$ e $p'' = (z_1, \ldots, z_n)$ parole in A_q^n. Dobbiamo provare che

$$|\{i : x_i \neq y_i\}| \leq |\{i : x_i \neq z_i\}| + |\{i : y_i \neq z_i\}|.$$

Se per un indice i_0 si ha $x_{i_0} \neq y_{i_0}$ possono darsi i casi:

1. $z_{i_0} \neq x_{i_0}$ e $z_{i_0} \neq y_{i_0}$,
2. $z_{i_0} = x_{i_0}$ e $z_{i_0} \neq y_{i_0}$,
3. $z_{i_0} \neq x_{i_0}$ e $z_{i_0} = y_{i_0}$.

In tutti i casi sopra l'indice i_0 compare in almeno uno degli insiemi $\{i : x_i \neq z_i\}$ o $\{i : y_i \neq z_i\}$.

Definizione. *Dato un codice $C \subseteq A_q^n$ si dice distanza minima di C, e si indica con $d(C)$, il minimo delle distanze tra due parole distinte di C cioè*

$$d(C) = min\{d(p, p') : p, p' \in C, p \neq p'\}.$$

Esempio. *Sia $A_2 = \{0, 1\}$ e C il codice su A_2 di lunghezza 3 dato da*

$$C = \{001, 010, 100, 111\}.$$

Risulta $d(C) = 2$. Se invece consideriamo il codice $C' = C \cup \{000\}$ si ha $d(C') = 1$.

Codici rivelatori di errori e codici correttori di errore

Il principio con cui si correggono gli errori è quello della *massima verosimiglianza*. Supponiamo che sia stata ricevuta la parola $w \in A_q^n$. Il codice C corregge la parola w se e solo se esiste una e una sola parola in C a distanza minima da w, cioè se solo se esiste unica $x \in C$ con $d(x, w) = \min\{d(y, w) : y \in C\}$. In tal caso la parola w viene corretta con x.

Esempio. *Siano $A_3 = \{0, 1, 2\}$ e C il codice di lunghezza 6 su A_3 dato da*

$$C = \{000000, 111111, 222222\}.$$

Supponiamo che venga spedita la parola del codice 000000 *e venga ricevuta la parola* 001102. *Poichè*

$$d(000000, 001102) = 3, d(111111, 001102) = 4, d(222222, 001102) = 5$$

con la decodifica per massima verosimiglianza si decodifica 001102 *con* 000000. *Se invece si riceve la parola* 000111, *poichè* $d(000000, 000111) = 3 = d(111111, 000111)$ *la decodifica per massima verosimiglianza fallisce.*

Definizione. *Un codice $C \subseteq A_q^n$ si dice k-rivelatore se k è il numero massimo di errori che è in grado di rivelare.*

Definizione. *Un codice $C \subseteq A_q^n$ si dice h-correttore se h è il numero massimo di errori che è in grado di correggere.*

Teorema. *Un codice $C \subseteq A_q^n$ è k-rivelatore se e solo se $d = d(C) = k + 1$.*

Dimostrazione. Sia $d = k+1$. Se una parola $p \in C$ trasmessa subisce t errori, cioè se viene ricevuta la parola p' con $d(p, p') = t$ e $t \leq k$ allora $d(p, p') = t < d = \min\{d(w, w')|w, w' \in C, w \neq w'\}$, dunque $p' \notin C$. Pertanto i t errori sono rivelati. Se invece p subisce un numero di errori $s \geq d$, cioè la parola p'' ricevuta soddisfa $d(p'', p) = s \geq d$ può accadere che $p'' \in C$ e in tal caso gli s errori non sono rivelati.

Viceversa sia k il numero massimo di errori che il codice rivela. Se p è la parola trasmessa, ogni altra parola $p' \in C$ differisce da p in almeno $k+1$ componenti dunque $d = d(C) \geq k+1$. Inoltre, poichè C rivela k errori ma non $k+1$, esistono due parole $w, w' \in C$ con $d(w, w') = k+1$. Segue che $d = k+1$. □

Teorema. *Sia codice $C \subseteq A_q^n$ con distanza minima $d = d(C)$. Allora C è $\left\lfloor \frac{d-1}{2} \right\rfloor$-correttore.*

Dimostrazione. Sia $p \in C$ una parola trasmessa e supponiamo che nella tramissione p subisca t errori, con $t \leq \left\lfloor \frac{d-1}{2} \right\rfloor$. Questo vuol dire che viene ricevuta la n-pla p' (con $p' \notin C$) che differisce da p in t componenti ovvero $d(p, p') = t$. Vogliamo provare che p è l'unica parola in C che *più somiglia* a p' cioè che ogni altra parola di C dista da p' più di quanto p dista da p'. Detto in altro modo vogliamo provare che

$$\forall p'' \in C, p'' \neq p \quad \text{si ha} \quad d(p'', p') > d(p, p') = t.$$

Per farlo proviamo che

$$\forall p'' \in C, p'' \neq p \quad \text{si ha} \quad d(p'', p') \geq \left\lfloor \frac{d-1}{2} \right\rfloor + 1.$$

La dimostrazione dell'ultima affermazione è per assurdo, cioè supponiamo che sista $p''' \in C$, $p''' \neq p$ tale che $d(p''', p') \leq \left\lfloor \frac{d-1}{2} \right\rfloor$. Applicando la disuguaglianza triangolare si ha

$$d(p''', p) \leq d(p''', p') + d(p', p) \leq \left\lfloor \frac{d-1}{2} \right\rfloor + \left\lfloor \frac{d-1}{2} \right\rfloor = 2 \left\lfloor \frac{d-1}{2} \right\rfloor \leq d-1.$$

Dunque abbiamo trovato due parole distinte in C (p e p''') che hanno distanza minore di $d = d(C)$, assurdo. □

Corollario. *Sia codice $C \subseteq A_q^n$ con distanza minima $d = d(C)$.*

1. *Il codice C rivela t errori se e solo se $t < d$ ovvero se e solo se $d \geq t+1$.*
2. *Il codice C corregge t errori se e solo se $d \geq 2t+1$.*

Dimostrazione.

1. Il codice C rivela t errori se e solo se alterando una parola di C in $r \leq t$ componenti non si ottiene un'altra parola di C. Questo avviene se e solo se due parole di C distano almeno $t+1$.
2. Osserviamo che C corregge t errori se e solo se alterando una parola $p \in C$ in $r \leq t$ coordinate, la n-pla p' ottenuta soddisfa

   $$d(p'', p') > d(p, p') \quad \forall p'' \in C, p'' \neq p.$$

   Proviamo ora che C corregge t errori se e solo se $d \geq 2t+1$. Supponiamo $d \geq 2t+1$. Allora $\forall p, p'' \in C$, si ha $d(p, p'') \geq 2t+1$ e dunque

   $$2t+1 \leq d(p, p'') \leq d(p'', p') + d(p', p) = d(p'', p') + t,$$

da cui $d(p'', p') \geq t+1$. Viceversa supponiamo che C corregga t errori. Dobbiamo far vedere che $d \geq 2t+1$. Per assurdo supponiamo che $d \leq 2t$ e siano $p = (x_1, \cdots, x_n)$ e $p'' = (y_1, \cdots, y_n)$ due parole di C con $d(p, p'') = d$. Supponiamo per semplicità che d sia pari (il caso d dispari è simile). Le parole p e p'' differiscono in d componenti. Scegliamo $d/2$ componenti x_i con $x_i \neq y_i$ e supponiamo per semplicità che siano le prime $d/2$. Consideriamo la parola $p' \in A_q^n$ definita da $p' = (y_1, \cdots, y_{d/2}, x_{d/2}, \cdots, x_n)$. È chiaro che $d(p, p') = d/2 = d(p', p'')$ e $d/2 \leq t$ dunque p' si è ottenuta da p (o da p'') introducendo al più t errori, ma C non corregge p' perchè sia p che p'' sono a distanza minima da p'.

□

25 Codici Lineari

Indichiamo con $\mathbb{Z}_p^n$ lo spazio vettoriale delle n-ple di elementi di $\mathbb{Z}_p$, p primo.

Definizione. *Un codice lineare è un sottospazio vettoriale di $\mathbb{Z}_p^n$.*

Esempio. *Sia $p = 2$ e consideriamo il codice C in Z_2^5 definito come il sottospazio con base $B = \{b_1 = 10111, b_2 = 11110\}$. Allora $|C| = 2^2$ perchè ogni parola di C è un vettore della forma $\lambda_1 b_1 + \lambda_2 b_2$, con $\lambda_1, \lambda_2 \in \mathbb{Z}_2$. Esplicitamente*

$$C = \{00000, 10111, 11110, 01001\}.$$

Osservazioni.

1. *Un codice $C \subseteq \mathbb{Z}_p^n$ è lineare se e solo se*

   a) $w_1 + w_2 \in C$,

   b) $\lambda w_1 \in C$,

   per ogni $w_1, w_2 \in C$, $\lambda \in \mathbb{Z}_p$.

2. *Sia $C \subseteq \mathbb{Z}_p^n$ un codice lineare di dimensione k (come spazio vettoriale su $\mathbb{Z}_p$). Allora C ha p^k elementi. Infatti se $B = \{b_1, b_2, \ldots, b_k\}$ è una base di C, gli elementi di C si scrivono in modo unico come*

   $$\lambda_1 b_1 + \lambda_2 b_2 + \cdots + \lambda_k b_k$$

   con $\lambda_i \in Z_p$, $i = 1, \ldots, k$.

3. *Ogni codice lineare C contiene la parola $\underline{0} = 00\ldots0$, il vettore nullo di C.*

Definizione. *Per $x = x_1 \cdots x_n \in \mathbb{Z}_p^n$, il peso di Hamming di $w(x)$ di x è definito come*

$$w(x) = |\{i | x_i \neq 0\}|.$$

Teorema. *Sia C un codice lineare con distanza minima $d = d(C)$. Allora*

1. *$d(x, y) = w(x - y)$, per ogni $x, y \in C$.*
2. *d è pari al peso minimo delle parole non nulle di C.*

Dimostrazione. Basta osservare che il vettore nullo, ovvero la parola $\underline{0} = 00\cdots0$, appartiene a C quindi per ogni $y \in C$, $d(y, \underline{0}) = w(y)$. Poichè d è la distanza minima di C esistono $x, y \in C$ con $d = d(x, y) = w(x - y)$. Ora, se fosse

$$min\{w(z) : z \in C, z \neq 0\} < d$$

esisterebbe $z_0 \in C$ che realizza il peso minimo, cioè $w(z_0) = d(z_0, \underline{0}) < d$, assurdo. □

Matrici generatrici

Sia C in $\mathbb{Z}_p^n$ un codice lineare di dimensione k e siano $\mathcal{B}_C = \{b_1, b_2, \ldots, b_k\}$ una base di C e $\mathcal{B} = \{e_1, e_2 \ldots, e_n\}$ una base di $\mathbb{Z}_p^n$.

Ogni vettore b_i si scrive come combinazione lineare a coefficienti in $\mathbb{Z}_p$ dei vettori di $\mathcal{B}$:

$$\begin{aligned} b_1 &= \lambda_{11}e_1 + \lambda_{12}e_2 + \cdots + \lambda_{1n}e_n \\ b_2 &= \lambda_{21}e_1 + \lambda_{22}e_2 + \cdots + \lambda_{2n}e_n \\ &\vdots \\ b_k &= \lambda_{k1}e_1 + \lambda_{k2}e_2 + \cdots + \lambda_{kn}e_n. \end{aligned}$$

La matrice

$$G = \begin{pmatrix} \lambda_{11} & \lambda_{12} & \cdots & \lambda_{1n} \\ \lambda_{21} & \lambda_{22} & \cdots & \lambda_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ \lambda_{k1} & \lambda_{k2} & \cdots & \lambda_{kn} \end{pmatrix} \in \mathrm{Mat}(k \times n, \mathbb{Z}_p)$$

si dice *matrice generatrice* di C. La matrice G ha dunque come righe le componenti dei vettori di una base di C rispetto a una base di $\mathbb{Z}_p^n$.

Definizione. *Dato un vettore $m = m_1 m_2 \ldots m_k$ in $\mathbb{Z}_p^k$, la* codifica *di m è il vettore mG cioè*

$$(m_1, m_2, \ldots, m_k) \begin{pmatrix} \lambda_{11} & \lambda_{12} & \cdots & \lambda_{1n} \\ \lambda_{21} & \lambda_{22} & \cdots & \lambda_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ \lambda_{k1} & \lambda_{k2} & \cdots & \lambda_{kn} \end{pmatrix} \in C$$

Osservazione. *Codificare un vettore m in $\mathbb{Z}_p^k$ significa associargli una parola in C.*

Esempio. *Sia $C \subseteq \mathbb{Z}_2^5$ il codice lineare con base $\mathcal{B} = \{b_1 = 10001, b_2 = 11010, b_3 = 11101\}$. Consideriamo in $\mathbb{Z}_2^5$ la base canonica, allora*

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Se $m = 101 \in \mathbb{Z}_2^3$, la codifica di m è il vettore

$$mG = (1, 0, 1) \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \end{pmatrix} = 01100 \in C.$$

Definizione. *Siano C_1 e C_2 due codici lineari in $\mathbb{Z}_p^n$ di stessa dimensione. Si dice che C_1 e C_2 sono* equivalenti *se è possibile ottenere tutte le parole di uno a partire da quelle dell'altro applicando*

1. *una permutazione delle posizioni $1, 2, \dots n$ a tutte le parole,*
2. *la moltiplicazione dei simboli che compaiono in una data posizione per un elemento non nullo $\lambda \in \mathbb{Z}_p$ a tutte le parole*

Come conseguenza abbiamo che due matrici generatrici G_1 e G_2 in $\mathrm{Mat}(k \times n, \mathbb{Z}_p)$ danno luogo a due codici lineari equivalenti se una delle due può essere ottenuta dall'altra tramite un numero finito delle seguenti operazioni

1. *scambiare due righe,*
2. *moltiplicare gli elementi di una riga per un elemento non nullo di $\mathbb{Z}_p$,*
3. *sommare a una riga un'altra riga moltiplicata per un elemento non nullo di $\mathbb{Z}_p$,*
4. *permutare le colonne*
5. *moltiplicare gli elementi di una colonna per un elemento non nullo di $\mathbb{Z}_p$.*

Osserviamo che le operazioni $1-3$ corrispondono a cambiare base mentre le operazioni 4 e 5 corrispondono alle operazioni 1 e 2 nella definizione di codici equivalenti.

Sia $C \subseteq \mathbb{Z}_p^n$ un codice lineare di dimensione k. Tra tutte le matrici generatrici di C se ne può scegliere una della forma

$$S = \begin{pmatrix} 1 & 0 & \cdots & 0 & x_{1,k+1} & \cdots & x_{1,n} \\ 0 & 1 & \cdots & 0 & x_{2,k+1} & \cdots & x_{2,n} \\ \vdots & \vdots & \vdots & \vdots & & & \\ 0 & 0 & \cdots & 1 & x_{k,k+1} & \cdots & x_{k,n} \end{pmatrix}.$$

In modo compatto scriviamo $S = (I_k|A)$. Una matrice generatrice di questa forma si dice una matrice generatrice in *forma standard*.

Osservazioni. *1. Il vantaggio dell'uso di una matrice generatrice in forma standard è nella codifica di un messaggio perchè*

$$(m_1, \dots, m_k) \begin{pmatrix} 1 & 0 & \cdots & 0 & x_{1,k+1} & \cdots & x_{1,n} \\ 0 & 1 & \cdots & 0 & x_{2,k+1} & \cdots & x_{2,n} \\ \vdots & \vdots & \vdots & \vdots & & & \\ 0 & 0 & \cdots & 1 & x_{k,k+1} & \cdots & x_{k,n} \end{pmatrix} =$$

$$= (m_1, m_2, \dots, m_k, m_1 x_{1,k+1} + \cdots m_k x_{k,k+1}, \dots, m_1 x_{1,n} + \cdots m_k x_{k,n})$$

quindi le prima k componenti della codifica sono $m_1, \dots, m_k$ e la ridondanza è tutta nelle ultime componenti. Dunque se nella trasmissione non occorrono errori la parola ricevuta viene facilmente decodificata: basta considerare le prime k componenti per ottenere m.

2. *La forma standard di una matrice generatrice $S = (I_k|A)$ non è unica perchè si possono permutare le colonne di A, ovvero le ultime $n-k$ colonne di S, ottenendo ancora una matrice generatrice in forma standard.*

Codifica e decodifica

Sia $C \subseteq \mathbb{Z}_p^n$ un codice lineare di dimensione k con matrice generatrice

$$G = \begin{pmatrix} \lambda_{11} & \lambda_{12} & \cdots & \lambda_{1n} \\ \lambda_{21} & \lambda_{22} & \cdots & \lambda_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ \lambda_{k1} & \lambda_{k2} & \cdots & \lambda_{kn} \end{pmatrix} \in \mathrm{Mat}(k \times n, \mathbb{Z}_p).$$

La codifica di un messaggio l'abbiamo già vista e la ripetiamo brevemente. Per codificare il messaggio $m = (m_1, \ldots, m_k)$ in una parola $c \in C$ si moltiplica per G ovvero

$$m \cdot G = c$$

cioè

$$(m_1, \ldots, m_k) \begin{pmatrix} \lambda_{11} & \lambda_{12} & \cdots & \lambda_{1n} \\ \lambda_{21} & \lambda_{22} & \cdots & \lambda_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ \lambda_{k1} & \lambda_{k2} & \cdots & \lambda_{kn} \end{pmatrix} = (c_1, \ldots, c_n) = c.$$

La decodifica è più complessa e riportiamo senza dimostrazione un algoritmo di decodifica. Costruiamo una tabella $\Sigma = (\sigma_{i,j})$ come segue:

1. scriviamo nella prima riga di Σ le parole di C, con l'unica condizione che $\sigma_{1,1} = \underline{0}$;
2. scegliamo una parola $a_2 \in \mathbb{Z}_p^n$ di peso minimo tra le parole di $\mathbb{Z}_p^n \setminus C$ e poniamo $\sigma_{2,1} = a_2$;
3. scriviamo nella seconda riga di Σ le parole di

   $$a_2 + C = \{a_2 + c : c \in C\}$$

   in modo che $\sigma_{2,j} = a_2 + \sigma_{1,j}$;
4. scegliamo una parola $a_3 \in \mathbb{Z}_p^n$ di peso minimo tra le parole di $\mathbb{Z}_p^n \setminus (C \cup (a_2 + C))$ e poniamo $\sigma_{3,1} = a_3$;
5. scriviamo nella terza riga di Σ le parole di

   $$a_3 + C = \{a_3 + c : c \in C\}$$

   in modo che $\sigma_{3,j} = a_3 + \sigma_{1,j}$

procediamo in questo modo fino a esaurire le parole in $\mathbb{Z}_p^n$. La tabella Σ è costruita in modo tale che ogni parola di $\mathbb{Z}_p^n$ compaia una e una sola volta in una riga di Σ. Il decodificatore che riceve la n-pla $y \in \mathbb{Z}_p^n$ determina la riga di Σ in cui compare y, ovvero determina l'insieme $a_i + C$ che contiene y. Si corregge y con $y - a_i$, cioè con la parola di C che in Σ appartiene alla stessa colonna di y.

Esempio. *Sia C il codice lineare in $\mathbb{Z}_2^4$ dato da*

$$C = \{0000, 1011, 0101, 1110\}.$$

Tabella Σ:

0000	1011	0101	1110
1000	0011	1101	0110
0100	1111	0001	1010
0010	1001	0111	1100

abbiamo dunque scelto $a_2 = 1000$, $a_3 = 0100$ e $a_4 = 0010$.

Se il decodificatore riceve la parola $y = 1111$ corregge y con $y - a_3 = y - 0100 = 1011$ che è la parola di C che si trova nella prima riga di Σ e nella stessa colonna di y.

Codice duale e matrice di controllo

Definiamo un prodotto scalare in $\mathbb{Z}_p^n$ come segue: dati $x = (x_1, \ldots, x_n)$ e $y = (y_1, \ldots, y_n)$ in $\mathbb{Z}_p^n$ definiamo il prodotto scalare $x \cdot y$ tra x e y come

$$x \cdot y = (x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) = \sum_{i=1}^{n} x_i y_i.$$

Due vettori x e y si dicono ortogonali se $x \cdot y = 0$.

Il prodotto scalare in $\mathbb{Z}_p^n$ gode delle proprietà:

1. $x \cdot y = y \cdot x$;
2. $x \cdot (y + z) = x \cdot y + x \cdot z$;
3. $(\lambda x) \cdot y = \lambda(x \cdot y)$;

per ogni $x, y, z \in \mathbb{Z}_p^n$, $\lambda \in \mathbb{Z}_p$.

Definizione. *Sia C un codice in $\mathbb{Z}_p^n$ di dimensione k. Si dice codice duale $C^\perp$ di C l'insieme di tutti i vettori in $\mathbb{Z}_p^n$ che sono ortogonali a ogni vettore di C ovvero*

$$C^\perp = \{x \in \mathbb{Z}_p^n : x \cdot c = 0, \forall c \in C\}.$$

Se $C = C^\perp$ allora il codice C si dice autoduale.

Osservazioni. *1. $C^\perp$ è un sottospazio vettoriale di $\mathbb{Z}_p^n$. Infatti il vettore nullo è in $C^\perp$. Inoltre per $x, y \in C^\perp$ e $\lambda \in \mathbb{Z}_p$ si ha*

$$(x+y)\cdot c = x\cdot c + y\cdot c = 0$$
$$(\lambda x)\cdot c = \lambda(x\cdot c) = 0$$

per ogni $c \in C$, pertanto $x+y \in C^\perp$ e $\lambda x \in C^\perp$.

2. $C^\perp \cap C$ può non ridursi al solo vettore nullo. Per esempio se C è autoduale, $C \cap C^\perp = C \cap C = C$.

3. $(C^\perp)^\perp = C$.

Teorema. *Sia C in $\mathbb{Z}_p^n$ un codice lineare con dimensione k e matrice generatrice G. Un vettore $x \in \mathbb{Z}_p^n$ appartiene a $C^\perp$ se e solo se x è ortogonale a ogni vettore riga di G ovvero se e solo se $x \cdot G^t = \underline{0}$, dove G^t è la matrice trasposta di G.*

Dimostrazione. È chiaro che $x \in \mathbb{Z}_p^n$ appartiene a $C^\perp$ se e solo se x è ortogonale ai vettori di una base di C. Sia $\mathcal{B}_C = \{b_1, \cdots, b_k\}$ una base di C e $\mathcal{B} = \{e_1, \cdots, e_n\}$ una base di $\mathbb{Z}_p^n$. Scriviamo

$$b_i = \sum_{j=1}^{n} \lambda_{i,j} e_j \quad i = 1, \ldots, n$$

pertanto

$$G = \begin{pmatrix} \lambda_{11} & \lambda_{12} & \cdots & \lambda_{1n} \\ \lambda_{21} & \lambda_{22} & \cdots & \lambda_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ \lambda_{k1} & \lambda_{k2} & \cdots & \lambda_{kn} \end{pmatrix}.$$

Per $x = (x_1, \ldots, x_n) \in \mathbb{Z}_p^n$ si ha

$$xG^t = (x_1, \ldots, x_n) \begin{pmatrix} \lambda_{11} & \lambda_{21} & \cdots & \lambda_{k1} \\ \lambda_{12} & \lambda_{22} & \cdots & \lambda_{k2} \\ \vdots & \vdots & \vdots & \vdots \\ \lambda_{1n} & \lambda_{2n} & \cdots & \lambda_{kn} \end{pmatrix} =$$
$$= (x_1\lambda_{11} + \cdots + x_n\lambda_{1n}, \ldots, x_1\lambda_{k1} + \cdots + x_n\lambda_{kn})$$

e

$$x_1\lambda_{11} + \cdots + x_n\lambda_{1n} = (x_1, \ldots, x_n)\cdot(\lambda_{11}, \ldots, \lambda_{1n}) = x \cdot b_1$$
$$\vdots$$
$$x_1\lambda_{k1} + \cdots + x_n\lambda_{kn} = (x_1, \ldots, x_n)\cdot(\lambda_{k1}, \ldots, \lambda_{kn}) = x \cdot b_k.$$

Abbiamo allora che

$$x \cdot G^t = (x \cdot b_1, \ldots, x \cdot b_k).$$

□

Corollario. *Se C è un codice lineare in $\mathbb{Z}_p^n$ di dimensione k allora $C^\perp$ è un codice lineare in $\mathbb{Z}_p^n$ di dimensione $n-k$.*

Dimostrazione. Per il teorema precedente, abbiamo che $x = (x_1, \ldots, x_n) \in \mathbb{Z}_p^n$ appartiene a $C^\perp$ se e solo se $xG^t = 0$. Allora i vettori di $C^\perp$ sono tutti e soli le soluzioni del sistema omogeneo $xG^t = 0$ nelle incognite $x_1, \ldots, x_n$. Poichè la matrice dei coefficienti G^t ha rango k (come G) lo spazio delle soluzioni ha dimensione $n-k$. □

Definizione. *Sia C un codice lineare in $\mathbb{Z}_p^n$ di dimensione k. Si dice matrice di controllo per C una matrice generatrice H per $C^\perp$.*

Osservazione. $H \in \mathrm{Mat}((n-k) \times n, \mathbb{Z}_p)$.

Teorema. *Un vettore $x = (x_1, \ldots, x_n) \in \mathbb{Z}_p^n$ appartiene a C se e solo se $xH^t = 0$.*

Dimostrazione. Si ha che $x \in C$ se e solo se $x \in (C^\perp)^\perp$ ovvero se e solo se $xH^t = 0$. □

Osservazione. *Il teorema precedente ci garantisce che se conosciamo H possiamo controllare facilmente se un elemento $x \in \mathbb{Z}_p^n$ appartiene a C.*

Come si determina una matrice di controllo per un codice C? Se C ha come matrice generatrice la matrice in forma standard

$$S = (I_k|A)$$

allora la matrice

$$H = (-A^t|I_{n-k})$$

è una matrice di controllo per C. Si tratta infatti di verificare che $HS^t = 0$ e

$$\begin{aligned} HS^t &= (-A^t|I_{n-k})(I_k|A)^t = \\ &= (-A^t|I_{n-k}) \begin{pmatrix} I_k^t \\ A^t \end{pmatrix} = (-A^t|I_{n-k}) \begin{pmatrix} I_k \\ A^t \end{pmatrix} \\ &= -A^t + A^t = 0 \end{aligned}$$

Una matrice di controllo per C permette di calcolare la distanza minima di C. Infatti se H è una matrice di controllo per il codice C in $\mathbb{Z}_p^n$ di dimensione k, si può provare che la distanza minima di C è uguale al minimo ordine di un insieme linearmente dipendente di colonne della matrice H. In particolare se d è la distanza minima di C si ha che

1. $d-1$ colonne di H sono linearmente indipendenti,

2. H ha rango almeno $d-1$.

Esempio. *Sia H la matrice su $\mathbb{Z}_3$*

$$H = \begin{pmatrix} 2 & 0 & 0 & 1 & 1 \\ 0 & 2 & 0 & 0 & 2 \\ 0 & 0 & 1 & 2 & 0 \end{pmatrix}$$

con H matrice di controllo di un codice C. Determiniamo la dimensione di C. Poichè H è in $\mathrm{Mat}(3 \times 5, \mathbb{Z}_3)$ abbiamo $n = 5$ e $n - k = 3$ dunque $k = \dim C = 2$. Determiniamo ora la distanza minima di C. Le colonne di H sono a 2 a 2 linearmente indipendenti. Invece le colonne $1, 2$ e 5 sono dipendenti quindi $d = 3$.

Decodifica per sindrome

Sia C un codice lineare in $\mathbb{Z}_p^n$ di dimensione k, e sia H una matrice di controllo per C.

Definizione. *Dato un vettore $x \in \mathbb{Z}_p^n$, la sindrome di x è il vettore $s = xH^t \in \mathbb{Z}_p^{n-k}$.*

Osservazione. *$x \in C$ se e solo se $xH^t = \underline{0}$ cioè se e solo se la sua sindrome è il vettore nullo in $\mathbb{Z}_p^{n-k}$.*

Teorema. *Nelle ipotesi precedenti per C e H siano x e y in $\mathbb{Z}_p^n$. Allora*

$$y \in x + C = \{x + c : c \in C\}$$

se e solo se x e y hanno la stessa sindrome.

Dimostrazione. $y \in x + C \iff y = x + c, \quad \text{con } c \in C \iff y - x = c \iff (y - x)H^t = cH^t = \underline{0} \iff yH^t = xH^t.$ □

Possiamo allora semplificare leggermente lo schema di decodifica visto in precedenza. Precisamente supponiamo di conoscere la sindrome di ciascuna parola a_i della tabella Σ.

La decodifica si può fare come segue:

1. Si calcola la sindrome $s = yH^t$ del vettore y ricevuto.
2. se $s = \underline{0}$ allora $y \in C$ e y è il messaggio trasmesso (quindi non ci sono stati errori)
3. altrimenti si determina l'elemento a_i avente la stessa sindrome di y
4. si decodifica y con $y - a_i$.

Esempio. *Sia C in $\mathbb{Z}_2^4$ il codice con matrice di controllo*

$$H = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix}.$$

In $\mathbb{Z}_2^4$ abbiamo $a_2 = (1000)$, $a_3 = (0100)$, $a_4 = (0010)$ con sindromi: $s_2 = a_2H^t = (01)$, $s_3 = a_3H^t = (11)$, $s_4 = a_4H^t = (10)$. Riceviamo $y = (0101)$. Calcoliamo la sindrome di y: $s = yH^t t = (10)$. Poichè $s = s_4$ correggiamo y con $y - a_4 = (0101) - (0010) = (0111)$.

Caso particolare: codici 1-correttori

Sia C in $\mathbb{Z}_p^n$ un codice lineare con distanza minima $d = 3$, così C è un codice 1-correttore. Supponiamo che venga trasmessa la parola $x \in C$ e che sia ricevuto il vettore $y = x + e$ dove e è l'errore. Si ha $yH^t = (x+e)H^t = xH^t + eH^t = eH^t$ perchè $xH^t = \underline{0}$. Supponiamo che $e = (0, \ldots, e_i \ldots, 0)$. Sia

$$H = \begin{pmatrix} h_{11} & h_{12} & \cdots & h_{1n} \\ h_{21} & h_{22} & \cdots & h_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ h_{n-k,1} & h_{n-k,2} & \cdots & h_{n-k,n} \end{pmatrix}$$

così

$$\begin{aligned} eH^t &= (0, \ldots, e_i, 0 \ldots 0) \begin{pmatrix} h_{11} & h_{21} & \cdots & h_{n-k,1} \\ h_{12} & h_{22} & \cdots & h_{n-k,2} \\ \vdots & \vdots & \vdots & \vdots \\ h_{1,n} & h_{2,n} & \cdots & h_{n-k,n} \end{pmatrix} \\ &= (e_i h_{1,i}, e_i h_{2,i}, \cdots, e_i h_{n-k,i}) \\ &= e_i \underbrace{(h_{1,i}, h_{2,i}, \cdots, h_{n-k,i})}_{i\text{-ma colonna di } H} \end{aligned}$$

Dunque la sindrome di e è il prodotto tra un elemento di Z_p, e_i, che dà la "grandezza" dell'errore e la colonna di H corrispondente alla componente in cui è entrato l'errore. Il vettore y si corregge con

$$x = y - e = (y_1, \cdots, y_i, \cdots, y_n) - (0, \cdots, e_i, \cdots, 0) = (y_1, \cdots, y_i - e_i, \cdots y_n).$$

Riassumendo la decodifica avviene come segue:

1. si calcola la sindrome $yH^t = s$ del vettore y ricevuto;
2. se $s = \underline{0}$ allora y è la parola trasmessa;
3. se $s \neq \underline{0}$ si confronta s con ogni colonna di H;
4. se s è multiplo della i-ma colonna di H secondo lo scalare e_i allora l'errore è $e = (0, \cdots, e_i, \cdots 0)$ e y si decodifica con $x = y - e$.

Esempio. *Sia C il codice su $\mathbb{Z}_3$ con matrice di controllo*

$$H = \begin{pmatrix} 2 & 0 & 0 & 1 & 1 \\ 0 & 2 & 0 & 0 & 2 \\ 0 & 0 & 1 & 2 & 0 \end{pmatrix}$$

Supponiamo che venga trasmessa la parola $x = (10110)$ e che si riceva il vettore $y = (10010)$. Si ha

$$yH^t = (0, 0, 2) = 2(0, 0, 1).$$

Quindi l'errore è $e = (0, 0, 2, 0, 0)$ *e* y *viene corretto con*

$$y - e = (1, 0, 0, 1, 0) - (0, 0, 2, 0, 0) = (1, 0, 1, 1, 0).$$

26 Codici Ciclici

Per $x \in \mathbb{Z}_p^n$ scriviamo $x = (x_0, \ldots, x_{n-1})$.

Definizione. *Un codice lineare C in $\mathbb{Z}_p^n$ si dice ciclico se per ogni $c = (c_0, \ldots, c_{n-1}) \in C$, si ha $(c_{n-1}, c_0, \ldots, c_{n-2}) \in C$.*

Esempi. *1. Il codice $C \subseteq \mathbb{Z}_2^3$ dato da*

$$C = \{000, 011, 101, 110\}$$

è un codice ciclico.

2. Il codice $C \subseteq \mathbb{Z}_2^4$ dato da

$$C = \{0000, 0110, 1001, 1111\}$$

non è un codice ciclico, perchè $0110 \in C$ ma $1100 \notin C$.

3. Il codice $C \subseteq \mathbb{Z}_2^4$ che si ottiene scambiando la terza e la quarta entrata in ogni parola del codice dell'esempio precedente, cioè

$$C = \{0000, 0101, 1010, 1111\}$$

è un codice ciclico, equivalente al codice dell'esempio precedente.

Il motivo per cui abbiamo indicato gli elementi di $\mathbb{Z}_p^n$ con $(x_0, \ldots, x_{n-1})$ invece che con $(x_1, \ldots, x_n)$ è che possiamo guardare le componenti come i coefficienti di un polinomio. Cioè all'elemento $(a_0, \ldots, a_{n-1}) \in \mathbb{Z}_p^n$ associamo il polinomio

$$a(t) = a_0 + a_1 t + \cdots + a_{n-1} t^{n-1} \in \mathbb{Z}_p[t]$$

nell'anello dei polinomi a coefficienti in $\mathbb{Z}_p$ nella indeterminata t.

Poniamo

$$R_n = \mathbb{Z}_p[t]/(t^n - 1)$$

dunque R_n è un anello (e non un campo, per $n \geq 2$, perchè $t^n - 1$ ammette 1 come radice dunque è riducibile). Come sappiamo gli elementi di R_n sono le classi

$$[a(t)]_{t^n-1}$$

dove $a(t) \in \mathbb{Z}_p[t]$ e $\partial a(t) \leq n-1$. Per semplicità scriviamo $a(t)$ per $[a(t)]_{t^n-1}$. La congruenza modulo $t^n - 1$ è molto semplice da descrivere

$$t^n \equiv 1 \bmod t^n - 1, t^{n+1} = t^n t \equiv t \bmod t^n - 1, t^{n+2} = t^n t^2 \equiv t^2 \bmod t^n - 1$$

etc. In particolare se $a(t) = a_0 + a_1 t + \cdots + a_{n-1} t^{n-1}$ risulta

$$a(t)t = a_0 t + a_1 t^2 + \cdots + a_{n-1} t^n \equiv a_{n-1} + a_0 t + a_1 t^2 + \cdots + a_{n-2} t^{n-1} \bmod t^n - 1.$$

Adesso identifichiamo $\mathbb{Z}_p^n$ con R_n tramite

$$a_0 a_1 \ldots a_{n-1} \mapsto a_0 + a_1 t + \cdots + a_{n-1} t^{n-1}.$$

Proposizione. *Un sottoinsieme C di R_n è un codice ciclico se e solo se valgono le seguenti:*

1. *per ogni $a(t), b(t) \in C$, $a(t) + b(t) \in C$.*
2. *per ogni $a(t) \in C$, per ogni $r(t) \in R_n$, $a(t)r(t) \in C$.*

Dimostrazione. Sia C un codice ciclico. In particolare C è lineare quindi è un sottospazio di R_n. Segue che per ogni $a(t), b(t) \in C$, $a(t) + b(t) \in C$, dunque la prima condizione è verificata. Inoltre per ogni $\lambda \in \mathbb{Z}_p$ e per ogni $a(t) \in C$, si ha $\lambda a(t) \in C$. Dobbiamo ora provare che vale la seconda condizione. Siccome C è ciclico, per quello che abbiamo visto sopra, per ogni $a(t) \in C$ si ha $a(t)t \in C$. Ma allora $a(t)t^2 = (a(t)t)t \in C$, $a(t)t^3 \in C, \ldots, a(t)t^{n-1} \in C$. Se $r(t) = r_0 + r_1 t + \cdots + r_{n-1}t^{n-1} \in R_n$ risulta

$$a(t)r(t) = a(t)(r_0 + r_1 t + \cdots + r_{n-1}t^{n-1}) = a(t)r_0 + r_1 a(t)t + \cdots + r_{n-1}a(t)t^{n-1}.$$

Allora $a(t)r(t) \in C$ perchè $a(t)r(t)$ è una combinazione lineare (con coefficienti $r_0, \ldots, r_n$) di parole di C.

Viceversa sia C un sottoinsieme di R_n che soddisfa le condizioni 1 e 2. Allora C è un sottospazio di R_n perchè la condizione 1 assicura che C è chiuso rispetto alla somma e la condizione 2 con $r(t) = r_0 \in \mathbb{Z}_p$ assicura che C è chiuso rispetto al prodotto per scalare. Dobbiamo far vedere che C è ciclico. Per ogni $a(t) = a_0 + a_1 t + \cdots + a_{n-1}t^{n-1} \in C$, applicando la condizione 2 con $r(t) = t$ abbiamo $a(t)t = a_{n-1} + a_0 t + a_1 t^2 + \cdots + a_{n-2}t^{n-1} \in C$. Segue che C è un codice ciclico. □

Definizione. *Per $f(t) \in R_n$ definiamo*

$$(f(t)) = \{f(t)r(t) : r(t) \in R_n\}.$$

Proposizione. *L'insieme $(f(t))$ è un codice ciclico.*

Dimostrazione. Dobbiamo mostrare che l'insieme $(f(t))$ soddisfa le due condizioni della proposizione precedente. Per ogni $f(t)r(t)$ e $f(t)r_1(t)$ in $(f(t))$ si ha

$$f(t)r(t) + f(t)r_1(t) = f(t)(r(t) + r_1(t)) \in (f(t))$$

dunque la prima condizione è soddisfatta. Per la seconda, per ogni $f(t)r(t)$ in $(f(t))$ e per ogni $r_1(t) \in R_n$ si ha

$$f(t)r(t)r_1(t) \in (f(t)).$$

□

Esempio. *Siano $p = 2$ e $n = 3$. In $R_3 = \mathbb{Z}_2[t]/(t^3 - 1)$ condideriamo il codice ciclico $C = (1 + t^2)$. Le parole di C sono*

$$0, 1 + t^2, (1 + t^2)t = t + t^3 = t + 1, (1 + t^2)t^2 = (1 + t)t = t + t^2.$$

Nella notazione usuale con le n-ple le parole di C sono 000, 101, 110 *e* 011.

Teorema. *Sia $C \neq \{0\}$ un codice ciclico in R_n. Allora*

1. *esiste un unico polinomio monico $p(t)$ di grado minimo in C;*
2. *$C = (p(t))$;*
3. *il polinomio $p(t)$ divide $t^n - 1$.*

Dimostrazione. Siccome $C \neq \{0\}$ in C esistono polinomi non nulli. Sia $h(t) = h_0 + h_1 t + \cdots + h_k t^k$, con $k \leq n-1$, un polinomio non nullo in C, dunque $h_k \neq 0$. Allora per la linearità di C, il polinomio monico $h_k^{-1} h(t)$ appartiene a C. Segue che in C esistono polinomi monici. Sia $p(t)$ un polinomio monico di C di grado minimo tra i polinomi monici di C. Proviamo che $p(t)$ è unico. Se $q(t) \in C$ è un altro polinomio monico di C di grado minimo, deve essere $\partial p(t) = \partial q(t)$. Ma C è un sottospazio di R_n quindi anche $p(t) - q(t) \in C$ e $\partial(p(t) - q(t)) < \partial p(t)$. Per la minimalità di $\partial p(t)$, l'unica possibilità è che $p(t) = q(t)$.

Mostriamo che $(p(t)) \subseteq C$ e che $C \subseteq (p(t))$. La prima inclusione è immediata: se $p(t)s(t) \in (p(t))$ allora $p(t)s(t) \in C$ perchè $p(t) \in C$ e C è un codice ciclico. Viceversa se $f(t) \in C$ la divisione con resto fornisce $f(t) = p(t)q(t) + r(t)$ con $\partial r(t) < \partial p(t)$. Ma $p(t)q(t) \in C$ dunque $r(t) = f(t) - p(t)q(t) \in C$. Siccome $p(t)$ ha grado minimo tra i polinomi non nulli di C deve essere $r(t) = 0$.

Infine la divisione con resto in $\mathbb{Z}_p[t]$ fornisce

$$t^n - 1 = p(t)q(t) + r(t)$$

con $\partial r(t) < \partial p(t)$, pertanto $r(t) \equiv -p(t)q(t) \bmod t^n - 1$. Allora $r(t) \in (p(t)) = C$ e $\partial r(t) < \partial p(t)$. Per la minimalità di $\partial p(t)$, l'unica possibilità è $r(t) = 0$. □

Definizione. *Per un codice ciclico C, il polinomio $p(t)$ monico di grado minimo in C si dice il polinomio generatore di C.*

Osservazione. *Per un codice ciclico esistono più polinomi $h(t)$ tali che $C = (h(t))$ ma ne esiste uno solo monico di grado minimo in C.*

Esempio. *Siano $p = 2$ e $n = 3$. In $R_3 = \mathbb{Z}_2[t]/(t^3 - 1)$ condideriamo il codice ciclico $C = (1 + t^2)$. Le parole di C sono*

$$0, 1 + t^2, (1 + t^2)t = t + t^3 = t + 1, (1 + t^2)t^2 = (1 + t)t = t + t^2.$$

Risulta $C = (1 + t) = (1 + t^2) = (t + t^2)$. Il polinomio generatore di C è $p(t) = 1 + t$, che è anche l'unico che divide $t^3 - 1 = (t - 1)(t^2 + t + 1) = (t + 1)(t^2 + t + 1)$ in $\mathbb{Z}_2[t]$.

Il teorema precedente ci dice che i codici ciclici in R_n sono in corrispondenza biunivoca con i divisori monici di $t^n - 1$. Quindi trovare i codici ciclici di R_n consiste nel trovare i divisori monici di $t^n - 1$ in $\mathbb{Z}_p[t]$ ovvero consiste nel trovare la fattorizzazione in irriducubili di $t^n - 1$ in $\mathbb{Z}_p[t]$.

Esempio. *La fattorizzazione in irriducibili di* t^3-1 *in* $\mathbb{Z}_2[t]$ *è* $t^3-1=(t+1)(t^2+t+1)$. *I codici ciclici di* R_3 *sono allora*

polinomio generatore $p(t)$	*codice in* $R_3=\mathbb{Z}_2[t]/(t^3-1)$	*codice corrispondente in* $\mathbb{Z}_2^3$
1	R_3	$\mathbb{Z}_2^3$
$t+1$	$\{0,1+t,t+t^2,1+t^2\}$	$\{000,110,011,101\}$
t^2+t+1	$\{0,1+t+t^2\}$	$\{000,111\}$
$t^3-1\equiv 0$	$\{0\}$	$\{000\}$

A rigore l'ultimo non è un codice ciclico ma lo aggiungiamo per uniformità.

Dato un codice ciclico con polinomio generatore $p(t)$ è facile scrivere una matrice generatrice per C (non in forma standard).

Teorema. *Sia* C *un codice ciclico con polinomio generatore*

$$p(t)=p_0+p_1t+\cdots+p_{r-1}t^{r-1}+t^r$$

di grado r. *Allora* C *ha dimensione* $k=n-r$, *e una matrice generatrice per* C *è la matrice*

$$G=\begin{bmatrix} p_0 & p_1 & p_2 & \cdots & p_{r-1} & 1 & & 0 & \cdots & \cdots & 0 & 0 \\ 0 & p_0 & p_1 & p_2 & \cdots & p_{r-1} & 1 & 0 & \cdots & \cdots & 0 & \\ 0 & 0 & p_0 & p_1 & p_2 & \cdots & p_{r-1} & 1 & 0 & & 0 & \\ \vdots & & \ddots & & & & & & & \ddots & \vdots & \\ 0 & \cdots & \cdots & 0 & p_0 & p_1 & p_2 & \cdots & p_{r-1} & 1 & 0 & \\ 0 & 0 & \cdots & \cdots & 0 & p_0 & p_1 & p_2 & \cdots & p_{r-1} & 1 & \end{bmatrix}.$$

Esempio. *Il codice ciclico* C *in* $R_8=\mathbb{Z}_3[t]/(t^8-1)$ *con polinomio generatore* $p(t)=t^3+t-1$ *ha matrice generatrice*

$$G=\begin{bmatrix} -1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 1 \end{bmatrix}.$$