

Metodi Algebrici per l'Informatica

- Quack

Metodi Algebrici per l'Informatica

~Quack



Per la parte di **teoria**, vedrai la pagina a sinistra



Per la parte di **esercitazione**, vedrai la pagina a destra

Indice:

Capitolo 1: Principio di Induzione e Algoritmo della Divisione	3
Capitolo 2: Massimo Comun Divisore	5
Capitolo 3: Numeri in base in b	8
Capitolo 4: I numeri primi e il teorema fondamentale dell'aritmetica	10
Capitolo 5: Equazioni Difantee	11
Capitolo 6: Relazioni su un Insieme	14
Capitolo 7: Congruenza modulo n	16
Capitolo 8: Conguenze lineari e Teorema Cinese del Resto	19
Capitolo 9: Strutture Algebriche, Somma e Prodotto in \mathbb{Z}_n	20
Capitolo 10: Invertibili in \mathbb{Z}_n , Funzione di Euler	23
Capitolo 11: Piccolo Teorema di Fermat e Teorema di Euler	26
Capitolo 12: Permutazioni	28
Capitolo 13: Potenze Modulo n	32
Capitolo 14: Crittografia	34



CheatSheet Metodi

~Quack

Capitolo 3: Principio di Induzione e Algoritmo della divisione

Principio di induzione

• 1^a forma: Siano $n_0 \in \mathbb{Z}$ e $P(n)$ un enunciato che ha senso per ogni $n \geq n_0$. Se

1) $P(n_0)$ è vero

base induzione

2) $\forall n > n_0$, $P(n-1)$ vero implica $P(n)$ vero.

passo induttivo

Allora $P(n)$ è vero per ogni $n \geq n_0$.

• 2^a forma: Siano $n_0 \in \mathbb{Z}$ e $P(n)$ un enunciato che ha senso per ogni $n \geq n_0$. Se

1) $P(n_0)$ è vero

base induzione

2) $\forall n > n_0$, $P(m)$ vero per ogni $n_0 \leq m \leq n$, implica $P(n)$ vero. passo induttivo

Allora $P(n)$ è vero per ogni $n \geq n_0$.

n.b.: Il principio del buon ordinamento in \mathbb{Z} è equivalente al Principio di induzione.

Algoritmo della divisione: $n > m > 0$, permette di trovare due interi q ed r (quoziente e resto)

tali che mq è il multiplo di m che meglio approssima per difetto n .

Siano n e m interi con $m \neq 0$. Esistono e sono univocamente determinati due interi

q ed r tali che

$$1) \quad n = mq + r$$

$$2) \quad 0 \leq r < |m| \leftarrow \text{modulo}$$

} $q = \text{quoziente}, r = \text{resto}$

CheatSheet Metodi



~Quack

Ese su Cap 3 : Principio di Induzione e Algoritmo della divisione

Principio di induzione

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

Caso base: $P(1) = \sum_{k=1}^1 k^2 = \frac{1}{6} \cdot 1 \cdot 2 \cdot 3$
 $1 = 1 \quad \checkmark$

Passo Induttivo: Sia $n > 1$, assumiamo vero $P(n-1)$ ed dimostro $P(n)$

$P(n-1): \sum_{k=1}^{n-1} k^2 = \frac{1}{6}(n-1)n(2n-1) \quad \checkmark$ per ipotesi.

$$\begin{aligned} P(n): \quad & \sum_{k=1}^n k^2 = \sum_{k=1}^{n-1} k^2 + n^2 = \frac{1}{6}(n-1)n(2n-1) + n^2 \\ & \left| \frac{n(n-1)(2n-1) + 6n^2}{6} \right. \\ & = \frac{n(n-1)(2n-1) + 6n^2}{6} \\ & = \frac{n(2n^2 + 3n + 1)}{6} \\ & = \frac{n(n+1)(2n+1)}{6} \\ & = \frac{1}{6}n(n+1)(2n+1) \end{aligned}$$

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

Caso base: $n_0 = 1$, $P(1) = \sum_{k=1}^1 k^3 = \left(\frac{1}{2} \cdot 1 \cdot 2\right)^2$
 $1 = \left(\frac{1}{2} \cdot 2\right)^2 = 1^2 = 1 \quad \checkmark$

Passo Induttivo: Sia $n > 1$, assumiamo vero $P(n-1)$ ed dimostro $P(n)$

$P(n-1): \sum_{k=1}^{n-1} k^3 = \left(\frac{1}{2}(n-1)n\right)^2 \quad \checkmark$ per ipotesi.

$$\begin{aligned} P(n): \quad & \sum_{k=1}^n k^3 = \sum_{k=1}^{n-1} k^3 + n^3 = \left(\frac{1}{2}(n-1)n\right)^2 + n^3 \\ & \left| \frac{\frac{1}{4}n^2(n-1)^2 + n^3}{4} \right. \\ & = \frac{n^2(n-1)^2 + 4n^3}{4} \\ & = \frac{n^2(n^2 - 2n + 4n)}{4} \\ & = \frac{n^2(n^2 + 2n + 1)}{4} \\ & = \frac{n^2(n+1)^2}{4} = \left(\frac{1}{2}n(n+1)\right)^2 \quad \checkmark \end{aligned}$$



CheatSheet Metodi

~Quack

Capitolo 2: Massimo Comun Divisore

Def: Siano $a, b \in \mathbb{Z}$. Dico che b divide a se $\exists c \in \mathbb{Z}$ tc: $a = bc$.

Dico che b è un divisore/fattore di a , ovvero che a è multiplo di b . In simboli: $b | a$.

Per $a \in \mathbb{Z}$, ± 1 e $\pm a$ sono fattori di a . Se $b | a$ con $b \neq \pm 1$ e $b \neq \pm a$, dico che b è fattore proprio di a .

Se $c = \pm 1 \rightarrow a = \pm b$

Def: Se $c | a, c | b$ allora $c | a \pm b$

Siccome $c | a \exists z_1 \in \mathbb{Z}$ tc $a = cz_1$, Siccome $c | b \exists z_2 \in \mathbb{Z}$ tc $b = cz_2$. Quindi $a \pm b = cz_1 \pm cz_2$

Dunque $a \pm b = c(z_1 \pm z_2) \rightarrow c | a \pm b$ ✓

Def: Se $c | a, c | b$ allora $c | ax + by$ con $x, y \in \mathbb{Z}$

Siccome $c | a \exists z_1 \in \mathbb{Z}$ tc $a = cz_1$, Siccome $c | b \exists z_2 \in \mathbb{Z}$ tc $b = cz_2$.

Quindi $ax + by = cz_1x + cz_2y = c(z_1x + z_2y) \in \mathbb{Z} \rightarrow c | ax + by$ ✓

MCD: Siano $a, b \in \mathbb{Z}$ con $a \neq 0, b \neq 0$, si dice che un M.C.D tra a e b è un qualunque intero d tc:

- $d | a, d | b$

- $\forall c \in \mathbb{Z}$ tc $c | a$ e $c | b$, allora $c | d$.

Identità di Bezout: Siano $a, b \in \mathbb{Z}$ con $a, b > 0$, esiste un mcd tra a e b ; inoltre esistono s, t $\in \mathbb{Z}$ tc: $as + bt = d$

Def: Siano $a, b \in \mathbb{Z}$ con $a, b \neq 0$. Se d è un mcd, l'unico altro mcd è $-d$. Risulta: $(a, b) = (-a, b) = (a, -b) = (-a, -b)$

Def: Due interi $a, b \in \mathbb{Z}$ si dicono coprimi o relativamente primi tra loro se $(a, b) = 1$

Def: Siano $a, b, c \in \mathbb{Z}$. Sia $a | bc$. Non è vero che $a | b$ o $a | c$. (è vero con numeri primi)

Def: Siano $a, b, c \in \mathbb{Z}$. Sia $a | bc$ e $(a, b) = 1$. Allora $a | c$.

Def: Siano $a, b \in \mathbb{Z}$, $d = (a, b)$, $a = da$, $b = db$, $(\bar{a}, \bar{b}) = 1$.

Metodi Algebrici per l'Informatica



~Quack

Ese su Cap 2: Massimo Comun Divisore

Massimo comun divisore

- ① Calcolare $(1492, 3776)$ usando Euclide e scrivere l'identità di Bezot.

Euclide

$$1776 = 1492 \cdot 1 + 284$$

$$1492 = 284 \cdot 5 + 72$$

$$284 = 72 \cdot 3 + 68$$

$$72 = 68 \cdot 1 + 4 \quad \text{r.c.o}$$

$$68 = 4 \cdot 17 + 0 \quad \text{trvo o}$$

Bezot

$$a = 1776, b = 1492$$

$$284 = 1776 - 1492 = a - b$$

$$72 = b \cdot 3 \cdot 284 = b - 3(a - b)$$

$$\begin{aligned} &= 6b - 5a \\ &= 6b - 5a \end{aligned}$$

$$68 = 284 - 72 \cdot 3 = a - b - 3(6b - 5a)$$

$$\begin{aligned} &= 16a - 19b \\ &= 16a - 19b \end{aligned}$$

$$4 = 72 - 68$$

$$\begin{aligned} &= 6b - 5a - 16a + 19b \\ &= -21a + 25b \end{aligned}$$

$$(a, b) = 4 = -21 \cdot 1776 + 25 \cdot 1492$$

- ② Calcolare $(3819, 3587)$ usando Euclide e scrivere l'identità di Bezot.

Euclide

$$3587 = 3819 \cdot 1 + 1768$$

Bezot

$$a = 3587, b = 3819$$

$$3819 = 1768 \cdot 1 + 51$$

$$1768 = a - b$$

$$1768 = 51 \cdot 34 + 34$$

$$51 = 3819 - 1768 = b - a - b = 2b - a$$

$$51 = 34 \cdot 1 + 17 \quad \text{r.c.o}$$

$$34 = a - b - (2b - a) \cdot 34 = a - b - 68b - 34a = 35a - 69b$$

$$34 = 37 \cdot 2 + 0$$

$$7 = 51 - 34 = +2b - a - 38a + 69b = 73b - 36a$$

$$3587(-36) + 3819(73)$$

Metodi Algebrici per l'Informatica

~Quack



Esercitazione 2: Massimo Comun Divisore

Divisibilità

① Provare che per ogni n , $3 \mid n^3 - n$.

$n^3 - n = n(n-1)(n+1)$. Dividendo con resto risultav: $n = 3q + r$ con $r=0, 1, 2$:

$$\cdot r=0, \quad 3 \mid n \rightarrow 3 \mid n^3 - n$$

$$\cdot r=1, \quad n=3q+1 \text{ quindi } 3 \mid n-1 \rightarrow 3 \mid n^3 - n$$

$$\cdot r=2, \quad n=3q+2 \text{ quindi } 3 \mid n+1 \rightarrow 3 \mid n^3 - n$$

Criteri di divisibilità

Inserisca questi parentesi su cd perché possono essere comodi agli esami.

2	Se la cifra delle unità è pari.	30812, 7612, 42983612
3	Se la somma delle sue cifre è multiplo di 3	32313, 30813, 38313
5	Se la cifra delle unità è 0 o 5.	4515 30015 930705
7	Se il numero senza unità - 2 cifre unità è multiplo di 7. Se il numero escluso decine e unità - 2 + decine è unità è multiplo di 7.	$\begin{array}{c} 9-2 \\ 93 \quad 7 \end{array}$ $\begin{array}{c} 16-2 \\ 363 \quad 7 \end{array}$ $\begin{array}{c} 10+39 \\ 539 \quad 7 \end{array}$ $\begin{array}{c} 1062+58 \\ 53358 \quad 7 \end{array}$
11	Se la diff. tra somma cifre par e pari è multiplo di 11.	24926137 323133



Metodi Algebrici per l'Informatica

~Quack

Capitolo 3: I numeri in base b.

Tes: Sia $b \in \mathbb{Z}$, $b \geq 2$. Ogni intero $n \geq 0$ può essere scritto in un e un solo modo, nella forma:

$$n = d_k b^k + d_{k-1} b^{k-1} + \dots + d_1 b + d_0, \text{ dove } 0 \leq d_i < b \text{ per } i=0, \dots, k \text{ e } d_k \neq 0 \text{ se } k > 0$$

Gli interi d_0, d_1, \dots, d_k si dicono le cifre della scrittura di n in base b e n si indica con la sequenza delle sue cifre in base b.

Ese: $n = (63405)_7 = 6 \cdot 7^4 + 3 \cdot 7^3 + 4 \cdot 7^2 + 0 \cdot 7 + 5 = 14950$

Conversione da base b a base 10

Sia n un intero rappresentato dalla sequenza $n = (d_k d_{k-1} \dots d_0)_b$.

Il modo più efficace è il seguente: $n = ((d_k b + d_{k-1})b + d_{k-2})b + \dots + d_1)b + d_0$.

In questo modo eseguo k moltiplicazioni e k addizioni.

Conversione da base 10 a base b

Osserviamo che le cifre d_0, d_1, \dots, d_k di n in base b sono i resti delle divisioni:

$$n = bq + d_0 \quad 0 \leq d_0 < b$$

$$q = bq_1 + d_1 \quad 0 \leq d_1 < b$$

$$q_1 = bq_2 + d_2 \quad 0 \leq d_2 < b$$

fino a quoziente nullo.

Metodi Algebrici per l'Informatica

~Quack



Ese su Cap 3: I numeri in base b.

① Convertire dai base b indicate alla base 10 i seguenti numeri:

$$a. (235)_8 \rightarrow (\quad)_{10}$$

$$b. (54350)_6 \rightarrow (\quad)_{10}$$

$$c. (\underline{1} C_4)_{16} \rightarrow (\quad)_{30}$$

$$\begin{aligned}
 0.235 &= (2 \cdot 8 + 3) \cdot 8 + 5 \\
 &= 19 \cdot 8 + 5 \\
 &= 152 + 5 \\
 &= 157
 \end{aligned}$$

$$\begin{aligned}
 &= 6 \cdot (5 \cdot 6 + 4) \cdot 6 + 3 \\
 &= (34 \cdot 6 + 3) \cdot 6 + 6 \\
 &= (207 \cdot 6 + 3) \cdot 6 \\
 &= 1247 \cdot 6
 \end{aligned}$$

$$C(G_1 G_2)_{36} = (G \cdot 36 + 32) \cdot 16 + 4$$

|

$$= 28 \cdot 16 + 4$$

|

$$452$$

② Conversione da λ a b

$$(1987)_{10} \rightarrow (3110)_3$$

$$(4215)_{50} \rightarrow (1110111)_2$$

$$(267)_{30} \rightarrow (308)_{16}$$

$$\begin{array}{r|l} \text{a. } 1987 & 0 \\ 155 & 1 \\ 22 & 1 \\ 3 & 3 \\ 0 & \end{array}$$

$$\begin{array}{r|l}
 b. & 4215 \\
 & 2107 \\
 & 2093 \\
 & 526 \\
 & 263 \\
 & 131 \\
 & 65 \\
 & 32 \\
 & 16 \\
 & 8 \\
 & 4 \\
 & 2 \\
 & 0
 \end{array}$$

$$\begin{array}{r|l} 267 & 11 \\ \hline 16 & 0 \\ 1 & 1 \\ 0 & \end{array}$$

③ Addizioni

$$a) (32345)_7 + (3498)_7$$

	1	2	3	4	5	6	7	8
a)	1	2	3	4	5	3	A	9
	3	4	5	3			C	F
	1	6	3	7	6		S	8

$$b) (AqFg)_f + (ccsq)_f$$



Metodi Algebrici per l'Informatica

~Quack

Capitolo 4 : Numeri Primi e Teorema Fondamentale dell' Aritmetica

Def: Un intero $p \in \mathbb{Z}$ con $p > 0$ e $p \neq 1$ si dice **primo** se $\forall a, b \in \mathbb{Z}$ $p \mid ab$ implica $p \mid a$ o $p \mid b$.

Def: Un intero $p \in \mathbb{Z}$ con $p > 0$ e $p \neq 1$ si dice **irriducibile** se $\forall a \in \mathbb{Z}$ $a \mid p$ implica $a = \pm 1$ o $a = \pm p$.

Teo: In \mathbb{Z} p è primo se e solo se irriducibile.

Lemma: Sia p primo. Se $p \mid a_1, a_2, \dots, a_n$ allora p divide almeno un fattore $p \mid a_i$ per qualche $1 \leq i \leq n$.

TFA: Ogni intero $n \geq 2$ si può scrivere come prodotto di $s \geq 1$ numeri primi.

Teorema Euclide: Esistono infiniti numeri primi.



Metodi Algebrici per l'Informatica

~Quack

Capitolo 5: Equazioni Diofantee

Def. È un'equazione della forma: $ax+by=c$ con $a, b, c \in \mathbb{Z}$, $a, b \neq 0$ e x, y incognite.

Una soluzione è sempre $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ con $ax_0 + by_0 = c$.

Prop: Data l'equazione Diofantea $ax+by=c$. Cond. necessaria e sufficiente affinché abbia soluzione è che $(a, b) | c$.

Prop: Data $ax+by=c$, poniamo $d=(a, b)$ e supponiamo $d | c$.

Allora tutte e sole le soluzioni di $ax+by=c$ sono le coppie $(x_k, y_k) \in \mathbb{Z} \times \mathbb{Z}$ dove

$$\left. \begin{array}{l} x_k = x_0 + \frac{b}{d}k \\ y_k = y_0 - \frac{a}{d}k \end{array} \right\} \text{al variare di } k \text{ in } \mathbb{Z}$$

Metodi Algebrici per l'Informatica

~Quack



Ese su Cap 5: Equazioni Diofantee

Determinare tutte le soluzioni delle equazioni diofantee

a. $2173x + 2493y = 230$ b. $258x + 147y = 369$ c. $109x + 25y = 32$

a. Trovo prima di tutto il mcd.

$$2493 = 2173 \cdot 1 + 318$$

$$2173 = 318 \cdot 6 + 265$$

$$318 = 265 + 53$$

$$265 = 53 \cdot 5$$

Poiché $53 \nmid 230$, non ha soluzioni.

b. Trovo prima di tutto il mcd.

$$258 = 147 + 111$$

$$147 = 111 + 36$$

$$111 = 36 \cdot 3 + 3$$

$$36 = 3 \cdot 12 + 0$$

Poiché $3 \mid 369$, ha soluzione. Esigo Bézout

$$a = 258, b = 147$$

$$m = a - b$$

$$36 = 2b - a$$

$$3 = 4a - 7b$$

$$3 = 3 \cdot 258 - 7 \cdot 147$$

Pongo $c = 13$ in quanto $c \cdot \text{mod} = c$, cioè $123 \cdot 3 = 369$, e ottengo

$$369 = 258 \cdot 492 + 147 \cdot (-863)$$

Quindi una sol. dell'eq. diofantea è $x_0 = 492, y_0 = -863$

Tutte le sol. sono le coppie (x_k, y_k) dove $x_k = x_0 + \frac{b}{d}k$ e $y_k = y_0 - \frac{a}{d}k$

$$\begin{aligned} x_k &= 492 + \frac{147}{3}k \\ &= 492 + 49k \end{aligned}$$

$$\begin{aligned} y_k &= -863 - \frac{258}{3}k \\ &= -863 - 86k \end{aligned}$$

con $k \in \mathbb{Z}$

Metodi Algebrici per l'Informatica

~Quack



Ese su Cap 5: Equazioni Diofantee

c. Trovo prima di tutto il nco.

$$109 = 25 \cdot 4 + 9$$

$$25 = 9 \cdot 2 + 7$$

$$9 = 7 \cdot 1 + 2$$

$$7 = 2 \cdot 3 + 1$$

109 e 25 sono primi tra loro, dunque abbiamo ad. Esegua bezout

Pongo $\bar{c} = -12$ in quanto $\bar{c} \cdot \text{mod} = c$, cioè $32 \cdot 1 = 32$ e ottengo:

$$-32 = 109 \cdot (-132) + 25(576)$$

Una sol è (x_0, y_0) con $x_0 = -132$ e $y_0 = 576$

Tutte le sol sono (x_k, y_k) dove $x_k = x_0 + \frac{b}{d}k$ e $y_k = y_0 - \frac{a}{d}k$

Determinare n° naturale più grande di 70 per cui ammette sol l'equazione diofantea:

$$8x + 16y = K$$

$(8, 16) = 8$ ammette sol e dovendo essere multiplo di 8 e > 70 troiamo 64

$8x + 16y = 64$ avendo $x + 2y = 8$ e quindi sceglio $x_0 = 4$ e $y_0 = 2$ e tutte le coppie (x_k, y_k) con $x_k = 4 + \frac{2}{8}k = 4 + \frac{1}{4}k$ e $y_k = 2 - \frac{1}{8}k = 2 - \frac{1}{8}x$ al variare di $k \in \mathbb{Z}$



Metodi Algebrici per l'Informatica

~Quack

Capitolo 6: Relazione su un insieme

Sia A insieme non vuoto. Una relazione R su A è un sottoinsieme di $A \times A$. Se R relazione su A e $(a, b) \in R$ si scrive anche aRb .

Proprietà relazioni:

· riflessiva $\forall a \in A, (a, a) \in R$

· simmetrica $\forall a, b \in A, \text{ se } (a, b) \in R \text{ allora } (b, a) \in R$

· antisimmetrica $\forall a, b \in A, \text{ se } (a, b) \in R \text{ e } (b, a) \in R \text{ allora } a = b$

· transitiva $\forall a, b, c \in A, \text{ se } (a, b), (b, c) \in R \text{ allora } (a, c) \in R$

Ese. $A = \{a, b, c\}$ $R = \{(a, a), (b, b), (c, c), (a, b), (b, a), (a, c), (c, a), (b, c), (c, b)\}$ è rifl., trans, sim.

A qualsiasi $R_{\text{rel. equivalenza tra elementi}}$ cioè $(a, b) \Leftrightarrow a \sim b \rightarrow$ rifl, trans, simm e antisimm.

X qualsiasi, $P(X)$ parti di X . R relazione di inclusione tra i sottinsiemi cioè $R = \{(Y, Z) | Y, Z \in P(X) \text{ e } Y \subseteq Z\}$ allora è riflessiva, antisimm, trans.

relazione d'equivalenza: rifl, simm, trans

relazione d'ordine: rifl, antisimm, trans

Classi di equivalenza: Sia A / \sim e R rel. equivalenza su A . Per $a \in A$ si definisce classe di equivalenza di a l'insieme:

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

n.b.: $[a]_R$ sottoinsieme di A

$[a]_R \neq \emptyset$ perché R riflessiva, dunque $(a, a) \in R \rightarrow a \in [a]_R$

Ese. $A = \{a, b, c, d\} R = \{(a, a), (b, b), (c, c), (d, d), (a, d), (d, a), (a, c), (c, a), (d, c), (c, d)\}$

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

$$[b]_R = \{b\}$$

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



Metodi Algebrici per l'Informatica

~Quack

Capitolo 6: Relazione su un Insieme

Insieme quoziente. L'insieme quoziente $A/R = \{[a]_R \mid a \in A\}$ insieme delle c.d.e.

n.b.: le relazioni di equivalenza si indicano anche con \sim

Prop.: Due c.d.e. o coincidono o sono disgiunte $[a]_R = [b]_R$ opp. $[a]_R \cap [b]_R = \emptyset$

Partizioni: A non vuota. Partizione \mathcal{F} di A è una famiglia di sottinsiemi t.c.:

- ogni $x \in A$ / $\in \mathcal{F}$
- $\bigcup_{x \in A} X = A$
- $\forall X, Y \in \mathcal{F}$ se $X \neq Y$ allora $X \cap Y = \emptyset$

Dunque ogni r.d.e. R su A è partizione di A , con elementi: le c.d.e.



Metodi Algebrici per l'Informatica

~Quack

Capitolo 7: Congruenza Modulo n

Def. Sia $n \in \mathbb{Z}$ con $n \geq 1$, si è congruo a b modulo n ($a \equiv b \pmod{n}$) se $n | a - b$, quindi se $\exists k \in \mathbb{Z}$ t.c. $a - b = nk$.

Estendiamo anche ai casi:

$n=0$ $a \equiv b \pmod{0}$ sse $a - b = 0 \cdot k$, quindi sse $a = b$. mod 0 = rel. ugualanza

$n < 0$ $n | a - b$ sse $-n | a - b$ per concludere che $a \equiv b \pmod{n}$ sse $a \equiv b \pmod{-n}$.

Teo. Per ogni $n \geq 1$ la rel. cong. mod. n è una rel. di equivalenza, ovvero:

$$[a]_n, [s]_n, \dots, [n-s]_n$$

Def. L'insieme quoziente di \mathbb{Z} rispetto alla r.c.m.n ($n \geq 1$) si dice insieme delle classi di resti e si denota con \mathbb{Z}_n .

$$\begin{aligned} \text{Es. 1) } n=2, \mathbb{Z}_2 &= \{[0]_2, [1]_2\} \text{ dove } [0]_2 = \{b \in \mathbb{Z} \mid 2 \mid b - 0\} = [1]_2 = \{b \in \mathbb{Z} \mid 2 \mid b - 1\} \\ &= \{b \in \mathbb{Z} \mid 2 \mid b\} = \{b \in \mathbb{Z} \mid b - 1 = 2k\} \\ &= \{k \in \mathbb{Z}\} \\ &= \{\dots, -4, -2, 0, 2, 4, 6, \dots\} = \{1 + 2k \mid k \in \mathbb{Z}\} \\ &= \{\dots, -5, -3, -1, 1, 3, 5, \dots\} \end{aligned}$$

$$2) n=3, \mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\} \text{ dove } [0]_3 = \{\dots, -6, -3, 0, 3, 6, 9, \dots\} = [1]_3 = \{\dots, -8, -3, 2, 1, 4, 7, \dots\} = [2]_3 = \{\dots, -7, -4, -1, 2, 5, 8, 11, \dots\}$$

In generale si ha $[a]_n = \{nk\}, [s]_n = \{1+nk\}, \dots, [n-s]_n = \{n-s+nk\}$ con $k \in \mathbb{Z}$

Oss: La c.m.n è r.d.e. su \mathbb{Z} anche per $n=0$, in quanto r.d.e = r.d.o. per $n=0$

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

$$1. a \equiv b \pmod{n} \quad 5. a \in [b]_n$$

$$2. n | a - b \quad 6. b \in [a]_n$$

$$3. a - b = nk \text{ con } k \in \mathbb{Z} \quad 7. [a]_n = [b]_n$$

$$4. a = b + nk \text{ con } k \in \mathbb{Z} \quad 8. a \text{ e } b \text{ divisi per } n \text{ danno lo stesso resto.}$$



Metodi Algebrici per l'Informatica

~Quack

Capitolo 8: Congruenze Lineari e Teorema Cinese del Resto

Def. Si dice congruenza lineare (modulo n) ogni espressione $ax \equiv b \pmod{n}$ con $a, b \in \mathbb{Z}$.

Si dice soluzione ogni intero c t.c. $ac \equiv b \pmod{n}$

Ese: La congruenza $2x \equiv 3 \pmod{7}$ ha $c=5$ perché $2 \cdot 5 = 10 \equiv 3 \pmod{7}$. In generale, $c=5+7k$ con $k \in \mathbb{Z}$

n.b.: alcune congruenze non hanno sol. es: $2x \equiv 3 \pmod{4}$

Def: Teorema Cinese del Resto

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

$$\begin{cases} x_1 \equiv b_1 \pmod{n_1} \\ x_2 \equiv b_2 \pmod{n_2} \\ \vdots \\ x_r \equiv b_r \pmod{n_r} \end{cases}$$

è risolvibile. Se c e c' sono due sol., allora $c \equiv c' \pmod{N}$, dove $N = n_1 \cdot n_2 \cdots n_r = \prod_{i=1}^r n_i$

Metodi Algebrici per l'Informatica

~Quack



Ese su Cap 3: Congruenza Lineare

Risolvere determinando tutte le soluzioni in \mathbb{Z}

a) $23x \equiv 41 \pmod{39}$

1. Posso riscrivere come $4x \equiv 3 \pmod{39}$. Equazione Diofantea associata:

2. $4x + 39y = 3$. Calcolo rrcd.

3. $(4, 39) = 1$ in quanto primi tra loro, dunque ammette sol. Esegui Bezout

4. $a=39, b=4 \quad 3=a-4b \quad 3=b-(a-4b)=sb-a \quad 3=4 \cdot 5 + 39 \cdot (-1)$

5. Trovo che $\bar{c}=3$, quindi $3=15 \cdot 4 + 39 \cdot (-3)$

6. Una soluzione è dunque $x_0=35$. Tutte le soluzioni sono gli interi nella forma $35 + 39k$, al variare di k in \mathbb{Z} .

b) $54x \equiv 14 \pmod{130}$

1. Equazione diofantea associata: $54x + 130y = 14$. Esegui rrcd

2. $130 = 54 \cdot 2 + 22 \quad 54 = 22 \cdot 2 + 10 \quad 22 = 10 \cdot 2 + 0 \quad 10 = 2 \cdot 5 + 0 \quad 2 \mid 14$. Ho soluzione. Calcolo Bezout

3. $a=130, b=54 \quad 22=a-2b \quad 10=b-2(a-2b)=5b-2a \quad 2=a-2b-2(5b-2a)=-12b+5a \quad 2=54 \cdot (-12)+130 \cdot 5$

4. Trovo che $\bar{c}=7$ dunque ho $14=54 \cdot (-84) + 130 \cdot 35$

5. Una soluzione è dunque $x_0=84$. Tutte le soluzioni sono gli interi nella forma $-84 + \frac{130}{2}k = -84 + 65k$, al variare di k in \mathbb{Z} .

c) $77x \equiv 22 \pmod{385}$

1. Equazione diofantea associata: $77x + 385y = 22$. Calcolo rrcd

2. $385 = 77 \cdot 5 + 0$, dunque $(77, 385) = 77$. $77 \nmid 22$ quindi l'eq. diofantea associata non ha soluzione pertanto la congruenza non ha soluzioni.

Metodi Algebrici per l'Informatica

~Quack



Ese su Cap 8: Teorema Cinese del Resto

Dato il sistema di congruenze

$$\begin{cases} x \equiv 3 \pmod{33} \\ x \equiv 4 \pmod{32} \\ x \equiv 2 \pmod{33} \end{cases}$$

Determina sol. particolare e tutte le sol. in \mathbb{Z} e la minima sol. positiva.

1. $(33, 32) = (32, 33) = (33, 33) = 1$. L'ipotesi del Teorema Cinese del resto è confermata. Risulta dunque

2. $N = 33 \cdot 32 \cdot 33 = 3736 \quad N_1 = 32 \cdot 33 = 356 \quad N_2 = 33 \cdot 33 = 363 \quad N_3 = 33 \cdot 32 = 332$. Risolvo congruenze lineari.

3. $N_1 y \equiv 1 \pmod{33} \rightarrow 356y \equiv 1 \pmod{33} \rightarrow 2y \equiv 1 \pmod{33} \rightarrow y_1 \equiv 6$

$N_2 y \equiv 1 \pmod{32} \rightarrow 363y \equiv 1 \pmod{32} \rightarrow -y \equiv 1 \pmod{32} \rightarrow y_2 \equiv -1$

$N_3 y \equiv 1 \pmod{33} \rightarrow 332y \equiv 1 \pmod{33} \rightarrow 2y \equiv 1 \pmod{33} \rightarrow y_3 \equiv 7$

4. Una soluzione particolare del sistema è $c_0 \sum_{i=1}^3 N_i y_i b_i = 356 \cdot 6 \cdot 3 + 363 \cdot (-1) \cdot 4 + 332 \cdot 7 \cdot 2 = 1086$.

5. Tutte le soluzioni del sistema sono $1086 + 3736k$ al variare di k in \mathbb{Z} .

6. La minima soluzione positiva è $652 = 1086 - 3736/2$.



Metodi Algebrici per l'Informatica

~Quack

Capitolo 9 : Strutture Algebriche e Somma e Prodotto in \mathbb{Z}_n

Def. Dato un insieme non vuoto A , un'operazione binaria su A è una funzione:

$$*: A \times A \rightarrow A$$

$$(a, b) \rightarrow a * b$$

ovvero è una regola per associare a ogni coppia ordinata (a, b) un elemento di A .

Def. Una struttura algebrica è un insieme non vuoto di A con una o più operazioni binarie. Una operazione si dice:

• **associativa:** $\forall a, b, c \in A, (a * b) * c = a * (b * c)$

• **commutativa:** $\forall a, b \in A, a * b = b * a$

• **dotta di elemento neutro:** $\exists e \in A \text{ tc } \forall a \in A, a * e = a$

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

• **somma:** $[a]_n, [b]_n \in \mathbb{Z}_n, [a_n] + [b_n] = [a+b]_n$

• **prodotto:** $[a]_n, [b]_n \in \mathbb{Z}_n, [a_n] \cdot [b_n] = [ab]_n$

Ese. In $n=5$, $\mathbb{Z}_5 = \{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\}$

$$[1]_5 + [3]_5 = [4]_5, \quad [2]_5 \cdot [3]_5 = [6]_5 = [1]_5$$

$\xrightarrow{5}$

$$\text{Dunque } [1]_5 = [6]_5, \quad [3]_5 = [8]_5. \text{ infatti } [6]_5 + [8]_5 = [14]_5 = [4]_5$$

Prop. 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

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

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

• **commutativa:** $\forall [a]_n, [b]_n, [c]_n \in \mathbb{Z}_n, ([a]_n + [b]_n) + [c]_n = [a]_n + ([b]_n + [c]_n)$

• **associativa:** $\forall [a]_n, [b]_n \in \mathbb{Z}_n, [a]_n + [b]_n = [b]_n + [a]_n$

• **dotta di elemento neutro:** $\exists [0]_n \in \mathbb{Z}_n \text{ tc } \forall [a]_n \in \mathbb{Z}_n, [a]_n + [0]_n = [a]_n$

• **ogni elemento ha inverso:** $\forall [a]_n \in \mathbb{Z}_n \exists [n-a]_n \in \mathbb{Z}_n \text{ tc } [a]_n + [n-a]_n = [0]_n$

Il prodotto gode di commutatività, associatività, elem. neutro ($[1]_n$)



Metodi Algebrici per l'Informatico

~Quack

Capitolo 9 : Strutture Algebriche e Somma e Prodotto in \mathbb{Z}_n

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

- 1) L'operazione $*$ è associativa.
- 2) \exists elemento neutro.
- 3) \exists elemento inverso.

Se l'operazione è anche commutativa si dice che il gruppo è abeliano.

Ese. $(\mathbb{Z}, +)$ è un gruppo abeliano con el. neutro 0 e inverso di a è $-a$.

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

Inverso: $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = (ad - bc)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

Metodi Algebrici per l'Informatica

~Quack



Ese su Cap 9: Relazione su insieme

Gruppi

① Indichiamo con a l'elemento $[a]$ in \mathbb{Z}_{37} . Sia G l'insieme:

$$G = \left\{ \begin{pmatrix} a & 0 \\ b & 1 \end{pmatrix} : a, b \in \mathbb{Z}_{37}, a \neq 0 \right\}$$

i) Mostrare che G è un gruppo rispetto al prodotto tra matrici.

ii) Determinare n° elementi di G

iii) Determinare l'inverso degli elementi. $x = \begin{pmatrix} 3 & 0 \\ 4 & 1 \end{pmatrix}$ $y = \begin{pmatrix} 8 & 0 \\ 5 & 1 \end{pmatrix}$

i) Per dimostrare che G sia gruppo rispetto prod. matr. deve soddisfare:

a) Chiusura. $\forall \begin{pmatrix} a & 0 \\ b & 1 \end{pmatrix}, \begin{pmatrix} c & 0 \\ d & 1 \end{pmatrix} \in G, \begin{pmatrix} ac & 0 \\ bc+d & 1 \end{pmatrix} \in G$, vero perché $ac, bc+d \in \mathbb{Z}_{37}$ e $ac \neq 0$ per $a \neq 0$ e $c \neq 0$ ✓

b) Elem neutro. $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in G$ per $a=1$ e $b=0$ ✓

c) Inversi. $\forall \begin{pmatrix} a & 0 \\ b & 1 \end{pmatrix} \in G, \begin{pmatrix} a & 0 \\ b & 1 \end{pmatrix}^{-1} = \begin{pmatrix} a^{-1} & 0 \\ -b & 1 \end{pmatrix} = a^{-1} \begin{pmatrix} 1 & 0 \\ -b & 1 \end{pmatrix} = a^{-1} \begin{pmatrix} 1 & 0 \\ -ba^{-1} & 1 \end{pmatrix} \in G$ ✓

Ha dimostrato che G è gruppo rispetto al prod. matr.

ii) $|G| = 36 \cdot 37$ perché abbiamo 36 scelte per a e 37 per b

iii) Risulta $x^{-1} = \begin{pmatrix} 3 & 0 \\ 4 & 1 \end{pmatrix}^{-1} = 3^{-1} \begin{pmatrix} 1 & 0 \\ -4 & 1 \end{pmatrix}$, inverso di 3 in base 37 è $[3]_{37}$ $[x] = [3]_{37} [x] = [1]_{37}$ quindi $x = 6 \rightarrow 38 \equiv 1 \pmod{37}$

aggiungo +37 a -4 e ottengo $6 \begin{pmatrix} 1 & 0 \\ -33 & 1 \end{pmatrix} = \begin{pmatrix} 6 & 0 \\ -30 & 1 \end{pmatrix}$

$$y^{-1} = 8^{-1} \begin{pmatrix} 1 & 0 \\ -5 & 1 \end{pmatrix} = 35 \begin{pmatrix} 1 & 0 \\ 32 & 1 \end{pmatrix} = \begin{pmatrix} 35 & 0 \\ 20 & 1 \end{pmatrix}$$



Metodi Algebrici per l'Informatica

~Quack~

Capitolo 30: Invertibili in Z_n , Funzione di Euler.

Def. Vogliamo trovare dato $[a]_n$ un $[b]_n$ tc $[a][b]_n = [1]_n$

Se $[a]_n = [0]_n$ allora $\forall [b]_n$ risulta $[a]_n$. Dunque se esiste $[b]_n$ con $[a][b]_n = [1]_n$ deve essere $[a]_n = [1]_n$ ovvero $a \equiv 0 \pmod{n}$.

L'unica possibilità è con $n=1$, altrimenti non esiste.

Prop. Siano $n > 1$ e $a \in \mathbb{Z}$. La classe di resto $[a]_n$ è invertibile in Z_n sse $(a, n) = 1$

Oss. Se esiste inverso di $[a]_n$ si indica con $[a]_n^{-1}$.

Ese. In Z_{53} , $[33]_{53}$ è invertibile perché $(33, 53) = 1$

Def. La funzione di Euler $\varphi: \mathbb{N} \rightarrow \mathbb{N}^*$ è definita da:

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

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

Proprietà:

- 1) Se p primo, $\varphi(p) = p-1$
- 2) Se p primo e $m \geq 1$ un n° naturale, $\varphi(p^m) = p^m - p^{m-1} = p^{m-1}(p-1)$
- 3) La funz. di Euler è multiplicativa, cioè $\forall a, b \in \mathbb{N}^*$ con $(a, b) = 1$ si ha $\varphi(ab) = \varphi(a) \cdot \varphi(b)$

Ese. Per $n = 32 = 2^5 \cdot 3$ si ha $\varphi(32) = 2^5 \cdot 3 \cdot (2-1)(3-1) = 4$

Oss. 1) $\varphi(n)$ è uguale al n° di elementi invertibili in Z_n .

2) Se p primo dispari con $p \nmid n$ allora $p-1 \mid \varphi(n)$.

Metodi Algebrici per l'Informatica

~Quack



Ese su Cap 30: Funzione di Euler

Funzione di Euler

① Calcolare $\varphi(4332)$.

Risultato $4332 = 2 \cdot 2166$

$$\begin{aligned} &= 2^2 \cdot 1078 \\ &= 2^3 \cdot 539 \\ &= 2^3 \cdot 7 \cdot 77 \\ &= 2^3 \cdot 7^2 \cdot 11 \end{aligned}$$

$$\text{Dunque } \varphi(4332) = \varphi(2^3 \cdot 7^2 \cdot 11) = 2^2(2-1) \cdot 7^1(7-1) \cdot 11^0(11-1)$$

$$= 2^2 \cdot 3 \cdot 7 \cdot 6 \cdot 10 = 1680$$

③ Determinare tutti gli interi $n \geq 1$ tali che: $\varphi(n) = 6$

a) Trovo divisori: I divisori di 6 sono 1, 2, 3, 6, sommo 3 e tengo i primi, dunque $p=2, p=3, p=7$

b) Scrivo la formula $n = 2^a \cdot 3^b \cdot 7^c$ con $a, b, c \geq 0$. Risultato $\varphi(n) = 2^{a-1}(3) \cdot 3^{b-1}(2) \cdot 7^{c-1}(6) = 6$

c) Parto dal primo + grande e trovo così c deve essere ≤ 1 poiché 7 non può essere fattore, dunque $0 \leq c \leq 1$.

$$\cdot c=1 \rightarrow 2^{a-1}(3) \cdot 3^{b-1}(2) \cdot 6 = 6 \text{ da cui } b=0 \text{ così tolgo il } 2 \text{ e } a=0 \text{ o } a=1$$

$$\cdot b=0, a=0 \rightarrow n = 2^0 \cdot 3^0 \cdot 7^1 = 7$$

$$\cdot b=0, a=1 \rightarrow n = 2^1 \cdot 3^0 \cdot 7^1 = 14$$

$$\cdot c=0 \rightarrow n = 2^a \cdot 3^b \text{ quindi } \varphi(n) = 2^{a-1}(3) \cdot 3^{b-1}(2) = 6 \quad b \text{ deve essere } \leq 1 \text{ perché m'interessa il } 2, \text{ mentre } a \leq 1.$$

$$\cdot a=1 \quad b=1 \rightarrow n = 2^1 \cdot 3^1 = 6$$

$$\cdot a=0 \quad b=1 \rightarrow n = 2^0 \cdot 3^1 = 3$$

Metodi Algebrici per l'Informatica

~Quack



Ese su Cap 10. Funzione di Eulero

Funzione di Eulero

② Determinare tutti $n \geq 1$ t.c. $\varphi(n) = 26$

- a) Divisori 26: 1, 2, 13, 26. Somma + e tango primi: 2, 3.
- b) Funzione $n = 2^a 3^b$ con $a, b \geq 0$. $\varphi(n) = 2^{a-1}(1) \cdot 3^{b-1}(2) = 26$
- c) Non trovo nessuna combinazione che mi permette di trovare 26. $\nexists n \geq 1$ t.c. $\varphi(n) = 26$

③ Determinare tutti $n \geq 1$ t.c. $\varphi(n) = 36$

- a) Divisori 36: 1, 2, 3, 4, 6, 8, 12, 18, 36. Somma + e tango primi: 2, 3, 5, 17.
- b) Funzione $n = 2^a 3^b 5^c 7^d$ con $a, b, c, d \geq 0$. $\varphi(n) = 2^{a-1}(1) \cdot 3^{b-1}(2) \cdot 5^{c-1}(4) \cdot 7^{d-1}(36) = 36$.
- c) Caso max: $d \leq 1$:
 - $d=1$ $\varphi(n) = 2^{a-1}(1) \cdot 3^{b-1}(2) \cdot 5^{c-1}(4) \cdot 36 = 36$, quindi $b=0, c=0, a=0 \Rightarrow a=3$
 - $a=0, b=0, c=0$: $2^0 \cdot 3^0 \cdot 5^0 \cdot 7^1 = 7$ $\cancel{36 = 36}$
 - $a=1, b=0, c=0$: $2^1 \cdot 3^0 \cdot 5^0 \cdot 7^1 = 14$ $\cancel{36 = 36}$
 - $d=0$ $\varphi(n) = 2^{a-1}(1) \cdot 3^{b-1}(2) \cdot 5^{c-1}(4) = 16$, quindi $c \leq 1$.
 - $c=1$ $\varphi(n) = 2^{a-1}(1) \cdot 3^{b-1}(2) \cdot 4 = 16$, quindi $b=1$ e $a=2$ oppure $b=0$ e $a=3$
 - $b=1$ $a=2$: $2^2 \cdot 3^1 \cdot 5^1 \cdot 7^0 = 4 \cdot 3 \cdot 5 = 60$ $\cancel{2 \cdot 2 \cdot 4 = 16}$
 - $b=0$ $a=3$: $2^3 \cdot 3^0 \cdot 5^1 \cdot 7^0 = 8 \cdot 5 = 40$ $\cancel{4 \cdot 4 = 16}$
 - $c=0$ $\varphi(n) = 2^{a-1}(1) \cdot 3^{b-1}(2) = 36$ quindi $b \leq 1$
 - $b=1$ $\varphi(n) = 2^{a-1}(1) \cdot 2 = 16$ quindi $a=4$
 - $a=4$: $2^4 \cdot 3^1 \cdot 5^0 \cdot 7^0 = 16 \cdot 3 = 48$ $\cancel{2 \cdot 2 \cdot 2 \cdot 2 = 16}$
 - $b=0$ $\varphi(n) = 2^{a-1}(1) = 16$ quindi $a=5$
 - $a=5$: $2^5 \cdot 3^0 \cdot 5^0 \cdot 7^0 = 32$ $\cancel{2 \cdot 2 \cdot 2 \cdot 2 = 16}$

Le soluzioni sono 37, 34, 60, 40, 48, 32.



Metodi Algebrici per l'Informatica

~Quack~

Capitolo 11: Piccolo Teorema di Fermat e Teorema di Euler

Teo. Piccolo teorema di Fermat: Sia p primo. Ogni intero a soddisfa la congruenza:

$$a^p \equiv a \pmod{p}$$

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

$$a^{p-1} \equiv 1 \pmod{p}$$

Teo. Teorema di Euler: Sia $n \geq 1$ intero e $a \in \mathbb{Z}$ con $(a, n) = 1$. Allora:

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

Metodi Algebrici per l'Informatica



~Quack

Ese su Cap 11: Teorema di Fermat e Eulero

① Calcolare $81^{81^{81}} \pmod{39}$

a. Risolviamo sentito esponente: $81 \equiv 5 \pmod{39}$.

b. Calcolo $\varphi(39) = 38$

c. Per il teorema di Fermat: $81^{38} \equiv 5^{38} \equiv 1 \pmod{39}$

d. Divido l'esponente per $\varphi(n)$ e trovo $81^{81^{81}} \pmod{39} \equiv 5^{81^{81}} \pmod{39}$

$$\begin{array}{r} 98 \\ 81 \\ 98 \\ 81 \\ 98 \\ \hline 9 \end{array} \rightarrow \text{resto}$$

e. Dunque $81^{81^{81}} \equiv 5^{81^{81}} \equiv (5^{38})^{45454} \cdot 5^9 \equiv 5^9 \pmod{39}$

f. Risolviamo $5^9 = 5^8 \cdot 5$, per trovare 5^8 prima trovo $5^2 \cdot 5^4$:

$$5^2 = 25 \equiv 6 \pmod{39},$$

$$5^4 = 625 \equiv 36 \equiv -2 \pmod{39}$$

$$5^8 = 6 \cdot -2 \equiv 4 \pmod{39}$$

$$5^9 = 5^8 \cdot 5 \equiv 20 \equiv 1 \pmod{39}$$

g. In conclusione $81^{81^{81}} \equiv 1 \pmod{39}$

$78^{89989} \pmod{39}$

$$78 \equiv 2 \pmod{39}, \quad \varphi(39) = 38$$

$$78^{38} \equiv 2^{38} \pmod{39}, \quad 89989 \mid 18 = 4999 + 7$$

$$78^{89989} \equiv (2^{38})^{4999} \cdot (2)^7 \equiv (2)^7 \pmod{39}$$

$$2^6 \equiv 64 \equiv 5 \pmod{39}$$

$$2^7 \equiv 2 \pmod{39}$$

$$2^7 \equiv 5 \cdot 2 \pmod{39} = 10 \pmod{39}$$



Metodi Algebrici per l'Informatica

~Quack~

Capitolo 12: Permutazioni

Def. Sia X non vuoto. Una biiezione $f: X \rightarrow X$ è permutazione di X . Indichiamo con S_X l'insieme delle permutazioni su X .

Operazione: composizione tra applicazioni.

Se $|X|=n$, S_X si indica con S_n e ha ordine $n!$. Una permutazione $f \in S$ si può scrivere nella forma:

$$f = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix} \text{ dove } b_i = f(a_i). \quad (\text{L'ordinamento delle righe è arbitrario.})$$

Ese. $n=5$, $f \in S_5$ data da $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix}$ cioè $f(1)=2$, $f(2)=5$.

$$\begin{pmatrix} c_1 & c_2 & \dots & c_{r-1} & c_r & \dots & c_n \\ c_2 & c_3 & \dots & c_r & c_{r+1} & \dots & c_n \end{pmatrix}$$

Def. Una permutazione debba formar $\begin{pmatrix} c_1 & c_2 & \dots & c_{r-1} & c_r & \dots & c_n \\ c_2 & c_3 & \dots & c_r & c_{r+1} & \dots & c_n \end{pmatrix}$ si dice ciclo di lunghezza r ($2 \leq r \leq n$) e si indica con (c_1, c_2, \dots, c_r) .

Ese. $n=3$

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

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

Def. Una permutazione $f \in S_n$ muove un elemento α se $f(\alpha) \neq \alpha$, altrimenti si dice che f fissa l'elemento α .

Def. Due permutazioni $f, g \in S_n$ sono disgiunte se gli elementi mossi da f sono fissati su g e viceversa. Se disgiunte, $f \circ g = g \circ f$.

Teo. Ogni permutazione f identità, è un ciclo oppure prodotto di cicli disgiunti.

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

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 9 & 32 & 33 & 6 & 7 & 11 & 2 & 3 & 4 & 10 & 1 & 5 & 8 \end{pmatrix}$$

Risulta $f = (1, 9, 4, 6, 11)(2, 32, 5, 7)(3, 33, 8)$. 10 è fisso da f .



Metodi Algebrici per l'Informatica

~Quack

Capitolo 32: Permutazioni

Def: Sia G gruppo e $g \in G$. Il minimo intero positivo n tc $g^n = 1_G$ si dice **ordine** o **periodo** di g . Se non esiste, g ha ordine infinito.

Nb. Se l'operazione è la somma, $g \in G$ ha ordine n se n è il min. int. pos. tc:

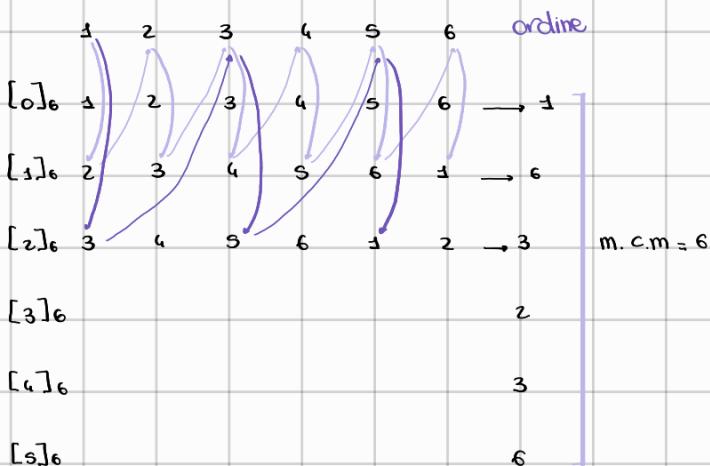
$$ng = \underbrace{g + \dots + g}_{n \text{ volte}} = 0$$

Def: Una permutazione f di S_n che sia prodotto di t cicli disgiunti di lunghezze r_1, r_2, \dots, r_t ha ordine m.c.m di r_1, r_2, \dots, r_t .

Ese: S_{12} ciclo $(7, 10, 8)$ ha ordine 3. La permutazione

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

Ese: con classi di resto \mathbb{Z}_6 voglio ordine permutazione.



Metodi Algebrici per l'Informatica

~Quack



Ese su Cap 12: Permutazioni.

① Si sia $\sigma \in S_{13}$ la permutazione

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

a) Scrivere σ come prodotto di cicli disgiunti e determinare l'ordine.

b) Nota $\tau = (9, 13, 7)(1, 12, 5, 8, 3)(11, 4, 10)(2, 6)$ in S_{13} si calcolino i prodotti $\sigma \cdot \tau$ e $\tau \cdot \sigma$

a) Si tratta di guardare la permutazione e collegare. Ese $f(1)=9 \rightarrow f(9)=4 \dots f(13)=1$

$$\sigma = (1, 9, 4, 6, 11)(2, 12, 5, 7)(3, 13, 8).$$

Per l'ordine si fa m.c.m dell'ordine dei cicli (n° elementi)

$$\delta(\sigma) = \text{m.c.m } (5, 4, 3) = 60$$

b) Per prodotto tra cicli disgiunti bisogna ricreare la tabella del secondo termine $f(x)=y$, ora si prende l'altro prodotto e si esegue $f(y)=z$

$$\sigma \cdot \tau = (1, 9, 4, 6, 11)(2, 12, 5, 7)(3, 13, 8) \cdot (9, 13, 7)(1, 12, 5, 8, 3)(11, 4, 10)(2, 6)$$

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

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

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

$$\sigma \cdot \tau = (8, 13, 2, 11, 6, 12, 7, 4, 10, 3, 5, 1, 9)$$

$$\tau \cdot \sigma = (9, 13, 7)(1, 12, 5, 8, 3)(11, 4, 10)(2, 6) \cdot (1, 9, 4, 6, 11)(2, 12, 5, 7)(3, 13, 8)$$

$$= (13, 2, 9, 5, 7, 3, 13, 9, 6, 10, 1, 11, 12, 8, 1)$$

Metodi Algebrici per l'Informatica

~Quack



Ese su Cap 12: Permutazioni.

① Sia $\sigma \in S_{13}$ la permutazione

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

c) Determinare tutti gli interi k t.c. $\sigma^k = (2, 5)(7, 12)$

c) $\sigma^k = (1, 9, 4, 6, 11)^k \cdot (2, 12, 5, 7)^k \cdot (3, 13, 8)^k$

1. Devo annullare il primo e l'ultimo, dunque $5|k$ e $3|k$ (5 e 3 sono gli ordini) dunque k deve essere multiplo di entrambi.

2. Per soddisfare l'ugualanza trovo che $k \equiv 2 \pmod{4}$.

\downarrow \downarrow
3° esponente che ordine ciclo
soddisfa

3. Una possibilità dunque è $k=30$, che soddisfa entrambe le richieste e $k=30$, tutte le altre sol. saranno $30 + 3 \cdot 5 \cdot 4 \cdot \mathbb{Z}$, ovvero $30 + 60z$ con $z \in \mathbb{Z}$

② Sia $\theta \in S_{15}$ la permutazione

$$\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 4 & 9 & 2 & 7 & 5 & 10 & 11 & 14 & 13 & 12 & 3 & 6 & 8 & 1 & 15 \end{pmatrix}$$

a) Scrivere θ come prodotto di cicli disgiunti e determinare l'ordine.

b) Si scrivano in prodotto di cicli disgiunti le permutazioni θ^{-1} .

a) $\theta = (1, 4, 7, 11, 5, 15)(2, 9, 13, 3)(6, 10, 12)(8, 14)$ e $\delta(\theta) = \text{m.c.m}(6, 4, 3, 2) = 32$

b). Posso riscrivere θ^{-1} come $\theta^{32} \cdot \theta^{-1}$ in quanto θ^{32} essendo 32 è come moltiplicare per 1.

$$\theta^{-1} = \theta^{32} = (1, 4, 7, 11, 5, 15)^{32} \cdot (2, 9, 13, 3)^{32} \cdot (6, 10, 12)^{32} \cdot (8, 14)^{32}$$

• Adesso canto l'ordine di ciascuno e con modulo vedo a quanto elevare. Es: 6 elementi elevato 32, $32 \equiv 5 \pmod{6}$

$$\theta^{32} = (1, 4, 7, 11, 5, 15)^5 \cdot (2, 9, 13, 3)^3 \cdot (6, 10, 12)^2 \cdot (8, 14)$$

• Ora mi sposto di tante posizioni quanto il grado. Es: $(1, 4, 7, 11, 5, 15)^5 = (1, 4, 7, 11, 5, 15) = (1, 15, 6, 11, 7, 4)$

$$(1, 15, 6, 11, 7, 4)(2, 3, 13, 9)(6, 2, 10)(8, 14)$$

N.b. Se n elementi = grado, si ottiene 1, es. $(2, 4)^2 = 1$



Metodi Algebrici per l'Informatica

~Quack~

Capitolo 13. Potenze modulo m.

Def: Quadrati ripetuti: Un modo semplice per calcolare $a^n \bmod m$ è il seguente:

- Scrivo esponente in base 2 ottenendo $n = (d_{k-1}, \dots, d_1, d_0)$

- costruiamo tabella

$$\begin{array}{c|l} (n)_2 & c_0 = 1 \\ \hline d_{k-1} & c_1 \equiv c_0^2 \cdot a^{d_{k-1}} \bmod m \\ d_{k-2} & c_2 \equiv c_1^2 \cdot a^{d_{k-2}} \bmod m \\ \vdots & \end{array}$$

- Risulta $a^n = c_k \bmod m$.

Metodi Algebrici per l'Informatica



~Quack

Ese su Cap 33: Potenze modulo n.

① Calcolare $5^{43} \bmod 55$:

$$(43)_{10} = 101011_2$$

43	$c_0 = 1$
1	$c_1 \equiv 1^2 \cdot 5^1 \equiv 5 \bmod 55$
0	$c_2 \equiv 5^2 \cdot 5^0 \equiv 25 \bmod 55$
1	$c_3 \equiv 25^2 \cdot 5^1 \equiv 45 \equiv -10 \bmod 55$
0	$c_4 \equiv (-10)^2 \cdot 5^0 \equiv -10 \bmod 55$
1	$c_5 \equiv (-10)^1 \cdot 5^4 \equiv 5 \bmod 55$
1	$c_6 \equiv 5^2 \cdot 5^1 \equiv 15 \bmod 55$

Quindi $5^{43} \equiv 15 \bmod 55$

② Calcolare $3^{90} \bmod 91$. $(90)_{10} \rightarrow (100100)_2$, dunque

$(90)_2$	$c_0 = 1$
1	$c_1 \equiv 1^2 \cdot 3^1 \equiv 3 \bmod 91$
0	$c_2 \equiv 3^2 \cdot 3^0 \equiv 9 \bmod 91$
1	$c_3 \equiv 9^2 \cdot 3^1 \equiv 81 \cdot 3 \equiv (-10) \cdot 3 \equiv -30 \bmod 91$
1	$c_4 \equiv (-30)^2 \cdot 3^1 \equiv -30 \bmod 91$
0	$c_5 \equiv (-30)^1 \cdot 3^0 \equiv -30 \bmod 91$
1	$c_6 \equiv (-10)^2 \cdot 3^1 \equiv 20 \bmod 91$
0	$c_7 \equiv (20)^2 \cdot 3^0 \equiv 1 \bmod 91$

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



Metodi Algebrici per l'Informatica

~Quack~

Capitolo 14: Crittografia

Def. Un sistema crittografico si può rappresentare come $P \xrightarrow{f} C \xrightarrow{f^{-1}} P$ dove:

- P è l'insieme dei possibili messaggi elementari in chiaro.
- C è l'insieme dei messaggi crittati.
- f è una funzione che critta i messaggi.
- f^{-1} è una funzione che decrittua i messaggi.

Ese. Per semplicità scrivo p, c, a, b intendendo $[p]_N, [c]_N, [a]_N, [b]_N$.

$P = Z_N = C$ e $f: P \rightarrow C$ la funzione dove $f(p) = p + b$, con $b \in Z_N$. $f^{-1}: C \rightarrow P$ definita da $f^{-1}(c) = c - b$.

Esempio pratico: Cifrario di Cesare, dove $b=3$, dunque $A \rightarrow D, D \rightarrow G$ ecc..

Def. La scienza che studia il modo di decifrare messaggi è la crittoanalisi. Si assume di conoscere la forma generale del sistema e che debba scoprire la chiave.



Metodi Algebrici per l'Informatica

~Quack~

Capitolo 14: Crittografia

E₀: Funzionamento algoritmo RSA.

- Supponiamo che ad ogni lettera dell'alfabeto sia associato un numero:

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z
2	3	4	5	6	7	8	9	29	31	32	33	34	37	36	37	38	39	43	23	23

- Persona X sceglie i primi p=5 e q=11, calcola N=pq=55, $\varphi(55)=4 \cdot 10 \cdot 10$. X poi sceglie r tc $(r, \varphi(55)) = (r, 40) = 1$,

ad esempio r=37. Tramite Euclide calcola s et tc $s = 40t + 37 \Rightarrow$ ottenendo t=-12 e s=23.

Infine X pubblica $(N, r) = (55, 37)$. Questa coppia è la chiave pubblica

- Persona Y legge le informazioni e spedisce

26	7	23	9	52	7	52	41	23	28	24	7	18	49	7
----	---	----	---	----	---	----	----	----	----	----	---	----	----	---

- X inizia col primo numero 26 e calcola $26^3 \bmod N$ cioè $26^{33} \bmod 55$ ed ottiene 33. Per farlo si può usare la tecnica dei quadrati ripetuti.

Decifrando 26 ottengo 33 ovvero L. È vicino seguito.

Def: firma digitale con chiavi pubbliche e private. Supponiamo:

X	Y
(N_A, r_A)	pubblica
sA	privata

X sceglie la sua firma in chiaro un intero F tc $F < N_A$ e $F < N_B$. Distinguiamo due casi:

- $N_A < N_B$, X calcola prima $F_A = F^{r_A} \bmod N_A$ e poi $F_{A,B} = F_A^{r_B} \bmod N_B$. Spedisce $F_{A,B}$ a Y che calcola $F_{A,B}^{r_A} \bmod N_B = F_A$ e poi $F_A^{r_A} \bmod N_A = F$

- $N_B < N_A$, X calcola prima $F_B = F^{r_B} \bmod N_B$ e poi $F_{B,A} = F_B^{r_A} \bmod N_A$. Spedisce $F_{B,A}$ a Y che calcola $F_{B,A}^{r_B} \bmod N_A = F_B$ e poi $F_B^{r_B} \bmod N_B = F$



Metodi Algebrici per l'Informatica

~Quack~



Capitolo 14: Crittografia

Pagina sia teorica che pratica in quanto è il funzionamento dell'algoritmo RSA ed'è una domanda FISSA all'esame.

- ① Spiegare dettagliatamente l'algoritmo RSA per una chiave generica (N, r)

Alice

1. Sceglie due numeri primi p e q grandi dispari e distinti. Calcola $N = p \cdot q$ e $\varphi(N) = (p-1)(q-1)$.
2. Sceglie un numero intero r coprimo con $\varphi(N)$, ovvero $(\varphi(N), r) = 1$.
3. Calcola con l'algoritmo di Euclide due interi s e t in modo che $rs + \varphi(N)t = 1$.
4. Pubblica la coppia (N, r) mentre tiene ben segreto $p, q, \varphi(N)$ e s .

Bob

1. Vuole mandare ad Alice il messaggio b , dove b è un numero intero con $0 < b < N$.
2. Legge la coppia (N, r) che Alice ha pubblicato e calcola $a = b^r \pmod{N}$ e invia il numero ad Alice.

3. Riceve il messaggio a da Bob e deve ricostruire il messaggio originale, cioè b . Calcola $a^s \pmod{N}$ e ritrova b .

Metodi Algebrici per l'Informatica

~Quack



Ese su Cap 14: Criptografia

- ① Supponiamo che la chiave pubblica sia $(N, r) = (143, 67)$ dunque $p=11$ e $q=13$. Riceviamo il messaggio 43. Decifrare.
- Ricerca N come prodotto di due numeri primi e tolgo uno ad entrambi. (I due numeri primi p e q sono dati in consegna!)

$$143 = 11 \cdot 13 \rightarrow \varphi(N) = 10 \cdot 12 = 120$$

- Applico Euclide e Bezout a $\varphi(N)$ e ad r . In questo caso 120 e 67. Così facendo trovo s.

$$\begin{array}{l} 120 = 67 \cdot 1 + 53 \\ 67 = 53 \cdot 1 + 14 \\ 53 = 14 \cdot 3 + 11 \\ 14 = 11 \cdot 1 + 3 \\ 11 = 3 \cdot 3 + 2 \\ 3 = 2 \cdot 1 + 1 \\ 2 = 1 \cdot 2 + 0 \end{array} \quad \begin{array}{l} a_0 = 120 \quad b = 67 \\ 53 = a_0 - b \\ 14 = b - (a_0 - b) = b - a_0 + b = 2b - a_0 \\ 11 = a_0 - b - 3(2b - a_0) = a_0 - b - 6b + 3a_0 = 4a_0 - 7b \\ 3 = 2b - a_0 - (4a_0 - 7b) = 2b + 7b - 4a_0 - 4a_0 = 9b - 8a_0 \\ 2 = (4a_0 - 7b) - 3(9b - 8a_0) = 4a_0 - 7b - 27b + 16a_0 = 19a_0 - 34b \\ 1 = 9b - 8a_0 - 19a_0 + 34b = 43b - 24a_0 \end{array}$$

$$1 = 67 - 24 \cdot 120 \quad s = 43$$

- Calcolo $mex^3 \bmod N$. In questo caso $13^{13} \bmod 143$. Per farlo uso quadrati ripetuti. Ottengo mex decifrato

$$\begin{array}{r} 43 = 301031 \\ \text{---} \\ 1 \quad 43 \\ 0 \quad 1 \\ 1 \quad 0 \\ 0 \quad 1 \\ 1 \quad 0 \\ 0 \quad 1 \end{array} \quad \begin{array}{l} c_0 = 1 \\ c_1 = 1^2 \cdot 13^3 \equiv 13 \bmod 143 \\ c_2 = 13^2 \cdot 13^3 \equiv 26 \bmod 143 \\ c_3 = 26^2 \cdot 13^3 \equiv 65 \bmod 143 \\ c_4 = 65^2 \cdot 13^3 \equiv -65 \bmod 143 \\ c_5 = -65^2 \cdot 13^3 \equiv 33 \bmod 143 \\ c_6 \equiv 13^2 \cdot 13^3 \equiv 52 \bmod 143 \end{array}$$

Il messaggio decifrato è 52.

Metodi Algebrici per l'Informatica

~Quack



Ese su Cap 14: Crittografia

- ② Alice vuole trasmettere la propria firma $F=2$ a Bob. Sapendo che la chiave pubblica di Alice è $(ss, 3)$ e quella di Bob è $(23, s)$, determinare il messaggio trasmesso da Alice.

Abbiamo $(N_a, r_a) = (ss, 3)$ e $(N_b, r_b) = (23, s)$. Determiniamo s_a .

- 1) Ricavo N_a come prodotto di due numeri primi e tolgo uno ad entrambi.

$$ss = 33 \quad s = 30 \quad \phi(n) = 30 \cdot 4 = 40$$

- 2) Applico Euclide e Bezout a $\phi(N_a)$ e ad r_a . In questo caso 40 e 3 . Così facendo trovo s_a .

$$\begin{aligned} 40 &= 3 \cdot 13 + 1 \quad a = 40 \quad b = 3, \quad z = a - 13b \rightarrow z = -13 \cdot 3 + 1 \cdot 40 \quad \text{c'è} \quad s_a \text{ positivo} \\ &\quad | \\ &\quad = 3(-13 + 40) + 40(1 - 3) \\ &\quad | \\ &\quad = 3 \cdot 27 + 40 \cdot (-2) \end{aligned}$$

s_a è dunque 27 .

- 3) Confronto N_a e N_b e determino cosa devo calcolare primo. In questo caso $N_a > N_b$.

$$F_b = F^{r_b} \mod N_b = 2^s \mod 23 = 11$$

$$F_{b,a} = F_b^{s_a} \mod N_a = 11^{27} \mod ss.$$

Quod rip: $27 = (1+0+1+1)_2$

$$\begin{array}{l} 27 \\ \hline 1 \quad c_0 = 1 \\ 1 \quad c_1 = 11 \mod ss \\ 1 \quad c_2 = 11^3 = 1331 \equiv 11 \mod ss \\ 0 \quad c_3 = 11^7 \equiv 11 \mod ss \\ 1 \quad c_4 = 11^9 \equiv 11 \mod ss \\ 1 \quad c_5 = 11^{11} \equiv 11 \mod ss. \end{array}$$

Dunque il messaggio che spedisce Alice è $F_{b,a} = 11$

Crediti

- Professoressa Avitabile, con i suoi appunti ed esercitazioni, ordinariamente esaurienti ed ordinati.
- Chiara "Blue3341", con il suo gentile supporto nelle sezioni meno chiare.
- Ruben "Shurbo", per il supporto e chiarimenti in qualche occasione.

