Matematica Discreta, a.a. 2018-19

CDL in informatica

Alessandro Berarducci

Dipartimento di Matematica
stanza 216, primo piano

Slides in costruzione e da sistemare.
In continuo aggiornamento

- Home page docente: http://people.dm.unipi.it/berardu/
- Home page del corso: https://elearning.di.unipi.it/
- Selezionare: Corso di Laurea in Informatica L-31, e poi "Matematica Discreta e Algebra Lineare 2018-19" (non 2017-18!).
- password: mdal2019

Matematica Discreta e Algebra Lineare

Ricevimento: ore 18, Stanza 216 del Dipartimento di Matematica, o per appuntamento.

Lunedì	11-13	MD
Martedì	14-16	AL
Mercoledì	9-11	MD
Giovedì	14-16	AL

Esame scritto e orale; il superamento dei compitini esonera dallo scritto.

Sezioni

Numeri

- $\mathbb{N} = \{0, 1, 2, \ldots\}$ numeri naturali.
- $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ numeri interi.
- $\mathbb{Q} =$ insieme dei numeri razionali (frazioni $\frac{m}{n}$ di interi, con $n \neq 0$);
- $\mathbb{R} =$ numeri reali. Include oltre ai razionali anche $\sqrt{2} = 1,4142\ldots$, $\pi = 3,1415\ldots$, ecc.
- $\mathbb{C} =$ numeri complessi. Include l'unità immaginaria $i = \sqrt{-1}$ e tutto ciò che si ottiene dai reali ed i con somme e prodotti, come $3 + 4i$.
- $\mathbb{Z}/(12) =$ interi modulo 12. Sono come gli interi salvo che quando si arriva a 12 si ricomincia da zero, come nell'orologio. Ad esempio $7 + 8 = 15 = 12 + 3 = 0 + 3 = 3$.
- $\mathbb{Z}/(n) =$ interi modulo n. Come prima, salvo che c'è n invece di 12. Ad esempio per i giorni della settimana $n = 7$.

Quando diciamo interi positivi intendiamo $\{1, 2, 3, \ldots\}$, senza lo zero. Gli interi non negativi sono invece i numeri naturali, con anche lo zero.

Tavole di verità

Date due proposizioni A, B

$$
\begin{array}{cccl}
\neg A & \text{significa} & \text{non } A & \text{(negazione)}, \\
A \wedge B & \text{significa} & A \text{ e } B & \text{(congiunzione)}, \\
A \vee B & \text{significa} & A \text{ o } B & \text{(disgiunzione)}, \\
A \implies B & \text{significa} & \text{se } A \text{, allora } B & \text{(implicazione)}, \\
A \iff B & \text{significa} & A \text{ se e solo se } B & \text{(doppia implicazione)}.
\end{array}
$$

Ponendo 0 = Falso, 1 = Vero, i connettivi propagano questi valori nel modo seguente.

A	B	$A \wedge B$	$A \vee B$	$A \implies B$	$A \iff B$
0	0	0	0	1	1
0	1	0	1	1	0
1	0	0	1	0	0
1	1	1	1	1	1

Relazioni d'ordine

Definizione

Un ordine totale è un insieme su cui è definita una relazione binaria $\leq$ che verifica le seguenti proprietà

- $x \leq y \wedge y \leq z \implies x \leq z$ *(transitiva)*
- $x \leq x$ *(riflessiva)*
- $x \leq y \wedge y \leq x \implies x = y$ *(antisimmetrica)*
- $x \leq y \vee y \leq x$ *(totalità)*

Se omettiamo la totalità si ottiene la nozione di ordine parziale

- L'usuale ordinamento su $\mathbb{N}, \mathbb{Q}$ o $\mathbb{R}$ è un ordine totale.
- Un esempio di ordine parziale è dato dalla relazione "x divide y" tra numeri naturali.
- Un altro esempio di ordine parziale è dato dalla relazione "X è un sottoinsieme di Y" tra insiemi.

Minore stretto

Definizione

Data una relazione d'ordine $\leq$ definiamo il corrispondente ordine stretto: $x < y :\iff x \leq y \wedge x \neq y$.

Valgono le seguenti proprietà:

- $x < y \wedge y < z \implies x < z$ (transitiva)
- $x \not< x$ (antiriflessiva)
- $x < y$ o $y < x$ o $x = y$, se l'ordine $\leq$ è totale.

Definizione

Viceversa, dato un ordine stretto $<$ definiamo $x \leq y :\iff x < y \vee x = y$.

Approfondimento

Esercizio

Dalle proprietà del $<$ si ottengono quelle del $\leq$ e viceversa.

Suggerimento: usare le definizioni, le tavole di verità, e le proprietà dell'uguaglianza:

- $x = x$;
- se $x = y$ posso sostituire x con y in qualsiasi formula.

Buoni ordini

Definizione

Un insieme totalmente ordinato è un buon ordine, o è bene ordinato, se non ammette successioni infinite decrescenti $a_0 > a_1 > a_2 > \dots$.

1. $\mathbb{N}$ è un buon ordine. In altre parole ogni successione $a_0 > a_1 > a_2 > \dots$ di numeri naturali termina dopo un numero finito di passi.
2. Di contro, i razionali non sono un buon ordine, anche considerando solo quelli non negativi: $1 > \frac{1}{2} > \frac{1}{3} > \frac{1}{4} > \dots$.

Il buon ordinamento di $\mathbb{N}$ è alla base delle "definizioni ricorsive" e delle "dimostrazioni per induzione".

Principio del minimo

Definizione

Dato un sottoinsieme A di un insieme ordinato X, scriviamo $m = \min(A)$ ("m è il minimo di A") se valgono le condizioni seguenti:

1. *$m \in A$,*
2. *per ogni $a \in A$ si ha $m \leq a$.*

Il fatto che $\mathbb{N}$ sia un buon ordine equivale al

Principio del minimo

Ogni sottoinsieme non vuoto A di numeri naturali ha un minimo elemento.

Approfondimento: Si dimostra che X è un buon ordine se e solo se tutti i sottoinsiemi non vuoti $A \subseteq X$ abbiamo un minimo.
Attenzione: Se prendo come X l'insieme dei reali maggiori o uguali a zero, ho che X ha un minimo (lo zero) ma non è un buon ordine (perché esistono sottoinsiemi non vuoti di X senza minimo).

Definizioni ricorsive

1. Una funzione f sui numeri naturali (cioè che prende in input numeri naturali) si dice definita ricorsivamente se è dato un valore iniziale per $f(0)$ e una legge per ottenere $f(n+1)$ a partire da $f(n)$.
2. Consideriamo ad esempio la funzione fattoriale
$$n! = \text{ il prodotto dei primi } n \text{ interi positivi.}$$
3. La possiamo definire per ricorsione:
$$\begin{cases} 0! = 1 \\ (n+1)! = (n+1) \cdot n! \end{cases}$$
4. Applico la definizione ricorsiva:
$$3! = 3 \cdot 2! = 3 \cdot 2 \cdot 1! = 3 \cdot 2 \cdot 1 \cdot 0! = 3 \cdot 2 \cdot 1 \cdot 1 = 6$$
(spero si capisca perché ho definito $0! = 1$ anziché $0! = 0$).
5. La regola ricorsiva spiega come calcolare $(n+1)!$ supponendo di sapere calcolare $n!$. Ciò richiede a sua volta di calcolare $(n-1)!$, poi $(n-2)!$, ecc. Siccome $\mathbb{N}$ è bene ordinato, prima o poi si arriva a $0!$ e si evita un regresso all'infinito.

Sommatorie

1. Una somma di più addendi può essere indicata con il simbolo di sommatoria $\sum$ applicato ad un'espressione dotata di un indice di cui sia stato specificato il valore iniziale e finale.
2. Ad esempio
$$\sum_{i=2}^{5} x_i \ = \ x_2 + x_3 + x_4 + x_5$$
(somma per i che va da 2 a 5 di x_i).
3. La stessa somma può essere indicata in modi diversi cambiando l'indice di scorrimento:
$$\sum_{j=1}^{4} x_{j+1} = x_2 + x_3 + x_4 + x_5$$
(se j va da 1 a 4, $i = j + 1$ va da 2 a 5).

Definizione ricorsiva della sommatoria

Possiamo definire la sommatoria $\sum_{i=0}^{n} x_i$ per ricorsione su n:

- $$\sum_{i=0}^{0} x_i = x_0$$
- $$\sum_{i=0}^{n+1} x_i = \sum_{i=0}^{n} x_i + x_{n+1}$$

  (prima sommo i primi n addendi e poi aggiungo l'ultimo).

Esempi

- Somma dei primi cinque quadrati:

$$\sum_{i=1}^{5} i^2 \ = \ 1^2 + 2^2 + 3^2 + 4^2 + 5^2$$

- Somma dei primi n quadrati:

$$\sum_{i=1}^{n} i^2 = 1^2 + 2^2 + \ldots + n^2$$

La notazione con $\sum$ è più precisa di quella con i puntini di sospensione.

1. I puntini $\ldots$ sono incomprensibili per un calcolatore, che invece riesce a capire la definizione ricorsiva di $\sum$.
2. Nella formula con i puntini sembra che 2^2 ci sia sempre, mentre se $n = 1$ la sommatoria si ferma a 1^2.

Linearità della sommatoria

Applicando la proprietà distributive si verifica che un fattore comune c si può portare fuori dalla sommatoria:

$$\sum_{i=a}^{a+n} c \cdot x_i \;=\; c \cdot \sum_{i=a}^{a+n} x_i$$

Ad esempio

$$\begin{aligned}\sum_{i=1}^{3} 7 \cdot i^2 &= 7 \cdot 1^2 + 7 \cdot 2^2 + 7 \cdot 3^2 \\ &= 7 \cdot (1^2 + 2^2 + 3^2) \\ &= 7 \cdot \sum_{i=0}^{3} i^2\end{aligned}$$

Analogamente

$$\sum_{i=a}^{a+n} (x_i + y_i) = \sum_{i=a}^{a+n} x_i + \sum_{i=a}^{a+n} y_i .$$

Produttoria

Il simbolo di produttoria $\prod$ è definito analogamente a $\sum$ salvo che invece delle somme si fanno i prodotti.

$$\prod_{i=0}^{0} x_i = x_0$$

e

$$\prod_{i=0}^{n+1} x_i = (\prod_{i=0}^{n} x_i) \cdot x_{n+1}$$

Nella notazione con i puntini

$$\prod_{i=0}^{n} x_i = x_0 \cdot \ldots \cdot x_n$$

Se tutti i fattori x_i sono uguali ad x si ottiene x^{n+1}.
Ricorsivamente: $x^0 = 1,\ x^{n+1} = x^n \cdot x$.

Ricorsione su più valori precedenti

Possiamo definire una funzione sui numeri naturali dando una legge per ottenere $f(n)$ a partire da $f(i)$ per vari $i < n$. Un esempio è dato dalla successione di Fibonacci.

Successione di Fibonacci

Consideriamo la successione di numeri F_n ($n \in \mathbb{N}$) così definita:

- $F_0 = 0$
- $F_1 = 1$
- per ogni $n \in \mathbb{N}$, $F_{n+2} = F_{n+1} + F_n$.

Si noti che sono necessari due valori iniziali per "costruire" i numeri della successione:

$$
\begin{aligned}
F_0 &= 0 \\
F_1 &= 1 \\
F_2 &= F_0 + F_1 = 0 + 1 = 1 \\
F_3 &= F_2 + F_1 = 1 + 1 = 2 \\
F_4 &= F_3 + F_2 = 2 + 1 = 3 \\
F_5 &= F_4 + F_3 = 3 + 2 = 5 \\
F_6 &= F_5 + F_4 = 5 + 3 = 8
\end{aligned}
$$

I numeri F_n si dicono **numeri di Fibonacci** (con riferimento a Leonardo da Pisa, che pubblicò sotto il nome di Fibonacci il *Liber abaci*, nel 1202). return

Dimostrazioni per induzione

Il principio che sta alla base delle dimostrazioni per induzione è simile a quello che sta alla base delle definizioni ricorsive: ci si riconduce ai casi precedenti.

- Le definizioni ricorsive servono a definire delle funzioni (su numeri naturali).
- Le dimostrazioni per induzione servono invece a dimostrare degli enunciati (sui numeri naturali).

L'idea alla base dell'induzione

Per illustrare il principio supponiamo che, in base ad una certa regola, qualcuno abbia colorato i numeri naturali:

$$0, 1, 2, 3, 4, 5, 6, \ldots .$$

Sia $\mathrm{Red}(n)$ l'enunciato "n è rosso". Supponiamo che qualcuno ci assicuri che:

1. 7 è rosso (cioè vale $\mathrm{Red}(7)$);
2. il successore di un numero rosso è rosso (cioè, per ogni k, vale l'implicazione $\mathrm{Red}(k) \implies \mathrm{Red}(k+1)$).

In base al principio di induzione ne deduciamo $\forall n \geq 7\ \mathrm{Red}(n)$, ovvero tutti gli interi maggiori o uguali a 7 sono rossi.

Dimostrazioni per induzione

Principio di induzione

Consideriamo una proposizione $P(n)$ che dipende da un parametro $n \in \mathbb{N}$, come ad esempio $3^n \leq n!$, oppure $n^3 \leq 2^n$. Sia $k \in \mathbb{N}$ un certo valore iniziale e supponiamo di riuscire a dimostrare le seguenti due cose:

- **Base dell'induzione:** $P(k)$ è vera.
- **Passo induttivo:** per qualsiasi $n \geq k$, se vale $P(n)$, allora vale anche $P(n+1)$ (ovvero vale l'implicazione $P(n) \implies P(n+1)$).

In questo caso possiamo concludere, in base al "principio di induzione", che $P(n)$ è vera per ogni $n \geq k$.

ma

Esercizio

Per ogni intero positivo n vale $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

Soluzione

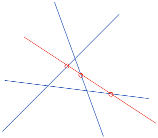
- *Nel caso in cui* $n = 1$ *(caso di base) la prova è diretta:* $\sum_{i=1}^{1} i = 1 = \frac{1(1+1)}{2}$.
- *Suppongo che* $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$ *per un certo* k *(ipotesi induttiva).*
- *Verifico il caso* $k + 1$*:*

$$\begin{aligned}
\sum_{i=1}^{k+1} i &= \sum_{i=1}^{k} i + (k+1) \quad \textit{(per definizione di } \textstyle\sum\textit{)} \\
&= \frac{k(k+1)}{2} + (k+1) \quad \textit{(sfruttando l'ipotesi induttiva)} \\
&= \frac{(k+1)(k+2)}{2}
\end{aligned}$$

Esercizio

Se si tracciano n rette nel piano, quante regioni si possono ottenere?

1. con una retta, 2 regioni.
2. con due rette, 4 regioni.
3. con tre rette, 7 regioni.



Soluzione ricorsiva

1. se vi sono già n rette e ne aggiungo un'altra, questa può al massimo intersecare ciascuna delle n rette in un punto, venendo spezzata in $n+1$ segmenti e creando $n+1$ regioni in più.
2. Se $f(n)$ è il numero delle regioni con n rette, $f(n+1) = f(n) + n + 1$.
3.

n	=	1	2	3	4	5	6	...
f(n)	=	2	4	7	11	16	23	...

Soluzione esplicita

n rette dividono il piano al massimo in $\frac{n(n+1)}{2} + 1$ regioni $(\dagger_n)$

Dimostrazione

1. Dimostro $\dagger_n$ per induzione su n.
2. Caso base: per $n = 1$ ho due regioni e $\frac{1(1+1)}{2} + 1 = \frac{2}{2} + 1 = 2$, quindi vale $\dagger_1$.
3. Suppongo per ipotesi induttiva che valga $\dagger_n$ per un certo n e cerco di dimostrare $\dagger_{n+1}$.
4. Se $f(n)$ è il numero delle regioni con n rette, per quanto visto prima
$$\begin{aligned} f(n+1) &= f(n) + n + 1 \\ &= \frac{n(n+1)}{2} + 1 + n + 1 \\ &= \frac{(n+1)(n+2)}{2} + 1 \end{aligned}$$
dove ho usato l'ipotesi induttiva $f(n) = \frac{n(n+1)}{2} + 1$.
5. L'uguaglianza così ottenuta è proprio la $\dagger_{n+1}$.
6. Per il principio di induzione la formula vale per tutti gli n.

Induzione forte

Induzione forte

Per dimostrare $\forall n \in \mathbb{N}\ P(n)$ è sufficiente riuscire a dimostrare $P(0)$ (caso base) e, per ogni $n > 0$, l'implicazione $P(0) \wedge \ldots \wedge P(n-1) \implies P(n)$ (passo induttivo).

- Come nel caso dell'induzione semplice esistono delle varianti: invece di partire da 0 si può partire da un altro valore iniziale.
- Conviene usare l'induzione debole o la forte? Se siete in dubbio usate la forte. Se funziona la debole funziona anche la forte.

Numeri primi

Definizione

Un intero $p > 1$ è primo se è divisibile solo per 1 e per p, ovvero non si può scomporre come prodotto $p = ab$ con entrambi i fattori a, b minori di n.

Esistenza della scomposizione in primi

Un tipico esempio in cui si usa l'induzione forte è nella dimostrazione che ogni intero > 1 si scompone in fattori primi.

Teorema

Ogni numero intero > 1 si scrive come prodotto di fattori primi.

Dimostrazione

Per induzione su n. Assumiamo per ipotesi induttiva che sia vero per tutti gli interi più piccoli di n (e maggiori di 1) e dimostriamolo per n.

- Dato $n > 1$ distinguiamo due casi.
- Se n è primo abbiamo finito.
- Se n non è primo si scrive come prodotto $n = ab$ di due fattori $< n$.
- Non è detto che a, b siano primi, ma essendo più piccoli di n per ipotesi induttiva sia a sia b si scrivono come prodotti di fattori primi.
- Mettendo insieme le scomposizioni in primi di a e di b se ne ottiene una per n.

Principio del minimo e induzione forte

Il principio del minimo si può usare in alternativa all'induzione forte. Ad esempio possiamo ridimostrare l'esistenza della scomposizione in primi con il principio del minimo.

Seconda dimostrazione

- Supponiamo per assurdo che esista un intero > 1 che non si scompone in fattori primi.
- Per il principio del minimo esiste il minimo $n > 1$ che non si scompone in fattori primi.
- Ovviamente n non può essere primo (altrimenti sarebbe già scomposto).
- Quindi $n = ab$ con $a < n, b < n$.
- Siccome n era il minimo che non si scomponeva, a e b si scompongono in primi.
- Ma allora dall'uguaglianza $n = ab$ deduciamo che si scompone anche n, e abbiamo un assurdo.

Divisione euclidea

- Dati due interi positivi a e b, possiamo considerare il quoziente q e il resto r della divisione di a per b.
- Ad esempio dati $a = 20, b = 7$, abbiamo $q = 2$, e $r = 6$.

Il quoziente e il resto di $a : b$ sono caratterizzati dalle seguenti proprietà:

- $a = bq + r$
- $0 \leq r < b$.

- Possiamo definire quoziente e resto anche se a è negativo, l'importante è che si mantengano le due proprietà.
- Ad esempio per $a = -20$ e $b = 7$ il quoziente è -3 e il resto è 1, in quanto $-20 = 7 \cdot (-3) + 1$. Il resto deve sempre essere positivo e minore di b.
- In generale se so trovare il quoziente e il resto della divisione $a : b$ con $a > 0$ lo so trovare anche di $-a : b$. Infatti se $a = bq + r$, allora $-a = b(-q) + (-r) = b(-q + 1) + (b - r)$, quindi $-a : b$ ha resto $-q + 1$ e resto $b - r$.

Sezioni

Divisione euclidea: esistenza del quoziente e resto

Proposizione

Dati due interi positivi a e b, esistono q (quoziente) e r (resto) tali che $a = bq + r$ e $0 \leq r < b$.

Dimostrazione

- Ragiono per induzione su a.
- Se $a < b$, prendo $q = 0, r = a$. Ad esempio $3 : 7$ ha quoziente 0 e resto 3.
- Se $a \geq b$, sia $a' = a - b$. Siccome a' è più piccolo di a, per ipotesi induttiva esistono q', r' tali che $a' = bq' + r'$ e $0 \leq r' < b$.
- Ma allora $a = a' + b = b(q' + 1) + r'$, quindi posso prendere $q = q' + 1$ e $r = r'$.

Unicità del quoziente e resto

Proposizione

Dati $a, b \in \mathbb{Z}$ *con* $b \neq 0$*, se ho*

$$\begin{cases} a = bq + r, & 0 \leq r < b \\ a = bq' + r', & 0 \leq r' < b \end{cases}$$

allora $q = q'$ *e* $r = r'$*.*

Dimostrazione

- Sottraendo le due equazioni ho $0 = b(q - q') + (r - r')$, quindi $r - r'$ è un multiplo di b.
- Tuttavia $r - r'$ è strettamente minore di b, essendo differenza di due interi positivi minori di b.
- L'unico numero strettamente minore di b che sia multiplo di b è zero (che è multiplo di ogni intero), quindi $r = r'$.
- A questo punto ho $0 = b(q - q')$, quindi $q - q' = 0$ (essendo $b \neq 0$), e concludo che $q = q'$.

Divisibilità

Definizione

Dati $n, k \in \mathbb{Z}$, diciamo che n divide m (notazione $n|m$) se esiste $k \in \mathbb{Z}$ tale che $nk = m$. In altre parole m è un multiplo di n.

Se n divide m, la divisione $m : n$ ha resto 0. Esempi:

- $3|6$
- $3|-6$
- $3|0$.

Sezioni

Massimo comun divisore

Definizione

Dati due numeri interi a, b non entrambi nulli, il loro massimo comun divisore $mcd(a, b)$ è il più grande numero intero positivo che divide sia a sia b.

- Esempio: $24 = 2 \cdot 2 \cdot 2 \cdot \cdot 3$ e $60 = 2 \cdot 2 \cdot 3 \cdot 5$, quindi $\mathrm{mcd}(24, 60) = 2 \cdot 2 \cdot 3 = 12$. Si prende il massimo numero di fattori che compaiono in entrambe le scomposizioni in primi.
- Con i numeri negativi non cambia sostanzialmente nulla: $\mathrm{mcd}(24, 60) = \mathrm{mcd}(-24, 60) = \mathrm{mcd}(24, -60) = \mathrm{mcd}(-24, -60) = 4$.
- Se i numeri sono grandi ci sono metodi più veloci basati sulla proprietà $\mathrm{mcd}(a, b) = \mathrm{mcd}(a - b, b)$.
- Ad esempio $\mathrm{mcd}(1001276, 1001275) = \mathrm{mcd}(1001276 - 1001275, 1001275) = \mathrm{mcd}(1, 1001275) = 1$.

Algoritmo di Euclide

Lemma

Dati due numeri interi a, b non entrambi nulli,
$mcd(a, b) = mcd(a - b, b)$*.*

Dimostrazione

- Se un intero divide due numeri divide anche la loro somma e la loro differenza.
- Quindi se x divide a e b, allora divide anche $a - b$ e b.
- Viceversa, se x divide $a - b$ e b, allora divide anche a e b (essendo a la somma di $a - b$ e b).
- L'insieme dei numeri che dividono sia a sia b coincide quindi con l'insieme dei numeri che dividono sia $a - b$ sia b.
- Se due insiemi coincidono hanno lo stesso massimo, quindi il massimo comun divisore di a e b coincide con il massimo comun divisore di $a - b$ e b.

Applicando k volte il lemma si ottiene $\mathrm{mcd}(a, b) = \mathrm{mcd}(a - kb, b)$ (funziona anche per k negativo).

Corollario

Se $a \equiv a' \bmod b$*, allora* $mcd(a, b) = mcd(a', b)$.

Dimostrazione

Se $a \equiv a' \bmod b$ esiste $k \in \mathbb{Z}$ tale che $a = a' + kb$, quindi posso applicare il risultato precedente.

Algoritmo di Euclide per il mcd

L'algorimo di Euclide per calcolare $\text{mcd}(a, b)$ consiste nell'applicare ripetutamente la regola $\text{mcd}(b, a) = \text{mcd}(a, b) = \text{mcd}(a - kb, b)$ per ricondurmi a numeri sempre più piccoli finché uno dei due è 0 e l'mcd è l'altro numero.

Esempio

$$\begin{aligned} mcd(1020,\ 351) &= mcd(318,\ 351) \\ &= mcd(318,\ 33) \\ &= mcd(21,\ 33) \\ &= mcd(21,\ 12) \\ &= mcd(9,\ 12) \\ &= mcd(9,\ 3) \\ &= mcd(0,\ 3) = 3 \end{aligned}$$

Esempio

$$\begin{aligned} mcd(744241,\ 743437) &= mcd(744241 - 743437,\ 743437) \\ &= mcd(804,\ 743437) \\ &= mcd(804,\ 743437 - 924 \cdot 804) \\ &= mcd(804,\ 541) \\ &= mcd(263,\ 541) \\ &= mcd(263,\ 15) \\ &= mcd(263 - 17 \cdot 15,\ 15) = mcd(8,\ 15) \\ &= mcd(8,\ 7) \\ &= mcd(1,\ 7) \\ &= mcd(1,\ 0) = 1 \end{aligned}$$

Con la scomposizione in primi sarebbe stato difficile. Non è facile scomporre numeri così grandi; io ho imbrogliato: sono partito dai fattori primi (cercati in una tabella di primi grandi) e li ho moltiplicati tra loro.

$$744241 = 751 \cdot 991, \qquad 743437 = 601 \cdot 1237$$

Sezioni

Teorema di Bezout

Teorema

Se a, b sono numeri interi non entrambi nulli e d è il loro massimo comun divisore, esistono $x, y \in \mathbb{Z}$ tali che $ax + by = d$.

Dimostrazione

- Se vale per i positivi, vale per i negativi: $\mathrm{mcd}(a, b) = ax + by \implies \mathrm{mcd}(-a, b) = \mathrm{mcd}(a, b) = -a \cdot (-x) + by$.
- Considero il caso $a, b \geq 0$.
- Sia n il massimo tra a e b e procediamo per induzione su n.
- Il teorema è vero quando $n = 1$ (caso base). Ad esempio $\mathrm{mcd}(1, 0) = 1 = 1 \cdot 1 + 0 \cdot 0$.
- Se $n > 1$ ci riduciamo ad un valore di n più piccolo sottraendo al più grande tra a e b l'altro numero. Se ad es. $a \geq b$, per ipotesi induttiva esistono x', y' tali che $(a - b)x' + by' = d$, dove $d = \mathrm{mcd}(a - b, b) = \mathrm{mcd}(a, b)$.
- Lo riscrivo come $ax' + b(-x' + y') = d$. Prendendo $x = x'$ e $y = -x' + y'$, ottengo $ax + by = d$.

Procedura per Bezout (return)

Trovare x, y interi tali che $\mathrm{mcd}(252, 198) = 252x + 198y$.

Per prima cosa calcoliamo $\mathrm{mcd}(252, 198)$. Rimpiazzo 252 con il resto della divisione 252 : 198 che è 54, e itero.

$$\begin{aligned} 252 &= 198 \cdot 1 + 54 \\ 198 &= 54 \cdot 3 + 36 \\ 54 &= 36 \cdot 1 + 18 \\ 36 &= 18 \cdot 2 + 0 \end{aligned}$$

Dunque $\mathrm{mcd}(252, 198) = \mathrm{mcd}(54, 198) = \mathrm{mcd}(54, 36) = \mathrm{mcd}(18, 36) = \mathrm{mcd}(18, 0) = 18$. Scriviamo ora:

$$\begin{array}{ccccccc} & & 252 & = & 252 \cdot \boxed{1} & + & 198 \cdot \boxed{0} \\ & & 198 & = & 252 \cdot \boxed{0} & + & 198 \cdot \boxed{1} \\ 252 - 198 & = & 54 & = & 252 \cdot \boxed{1} & + & 198 \cdot \boxed{(-1)} \\ 198 - 54 \cdot 3 & = & 36 & = & 252 \cdot \boxed{(-3)} & + & 198 \cdot \boxed{4} \\ 54 - 36 & = & 18 & = & 252 \cdot \boxed{4} & + & 198 \cdot \boxed{(-5)} \end{array}$$

Equazioni diofantee lineari

Equazione diofantea significa che si cercano le soluzioni in $\mathbb{Z}$.

Teorema

◂ diofantee *Dati $a, b \in \mathbb{Z}$, l'equazione diofantea $ax + by = c$ è risolubile se e solo se c è multiplo di $mcd(a, b)$.*

- Se c è uguale a $\mathrm{mcd}(a, b)$ lo sappiamo per Bezout.
- Se $c = k\mathrm{mcd}(a, b)$ e u, v sono soluzioni di $au + bv = \mathrm{mcd}(a, b)$, allora $x = uk$ e $y = vk$ sono soluzioni di $ax + by = c$.
- Se c non è multiplo di $\mathrm{mcd}(a, b)$ l'equazione è impossibile perché se $\mathrm{mcd}(a, b)$ divide $ax + by$ per qualsiasi scelta di x, y, quindi se fosse $ax + by = c$, $\mathrm{mcd}(a, b)$ deve dividere c.

Esempio I

Esempio

Ho 83 centesimi in monete da 1, 5 e 10 centesimi. In tutto ho 13 monete. Quante ne ho di ciascun tipo?

- Chiamo x, y, z il numero di monete da 1, 5 e 10 centesimi rispettivamente.
- $\begin{cases} 83 = x + 5y + 10z \\ 13 = x + y + z \end{cases}$
- Cerco x, y, z interi non negativi.
- Equazione 1 - Equazione 2: $\implies 70 = 4y + 9z$.
- $\mathrm{mcd}(4, 9) = 1$. Per Bezout esistono $u, v \in \mathbb{Z}$ tali che $1 = 4u + 9v$.
- $$\begin{array}{rcrcrcr} & & 9 & = & 9 \cdot \boxed{1} & + & 4 \cdot \boxed{0} \\ & & 4 & = & 9 \cdot \boxed{0} & + & 4 \cdot \boxed{1} \\ 9 - 2 \cdot 4 & = & 1 & = & 9 \cdot \boxed{1} & + & 4 \cdot \boxed{(-2)} \end{array}$$

Esempio II

- Moltiplico per 70 l'ultima equazione: $70 = 9 \cdot 70 + 4 \cdot (-140)$.
- Soluzione particolare

$$70 = 9z_0 + 4y_0 = \\ 9 \cdot 70 + 4 \cdot (-140)$$

- L'omogenea associata $0 = 9z' + 4y'$ ha soluzioni $y' = 9k$ e $z' = -4k$.
- Le soluzioni di $70 = 9z + 4y$ si ottengono aggiungendo ad una soluzione particolare le soluzioni dell'omogenea associata: $70 = 9(70 - k4) + 4(-140 + k9) = 9z + 4y$.
- Scelgo k in modo che i numeri vengano positivi. Con $k = 16$ ho $y = -140 + k9 = 4$ e ricavo $z = 6$.
- Poi da $13 = x + y + z$ ricavo $x = 3$.
- Faccio la riprova: $83 = 3 + 4 \cdot 5 + 6 \cdot 10$.

MCD proprietà

Proposizione

Il massimo comun divisore $\text{mcd}(a, b)$ di a e b, è un multiplo di ciascun divisore comune di a e b.

Dimostrazione

- Supponiamo che c divida sia a sia b.
- Dobbiamo dimostrare che c divide $\text{mcd}(a, b)$.
- Per Bezout esitono $x, y \in \mathbb{Z}$ tali che $\text{mcd}(a, b) = ax + by$.
- c divide sia ax (perché divide a) sia by (perché divide b), quindi divide la loro somma $ax + by$, che è proprio $\text{mcd}(a, b)$.

Esempio: se sappiamo che $\text{mcd}(a, b) = 40$ e c divide sia a sia b, quali valore può assumere c?

Se un intero divide un prodotto ...

1. Supponiamo che c divida un prodotto ab. Possiamo dire che c divide a o c divide b?
2. In generale no, ad esempio 6 divide $3 \cdot 4$ ma non divide né 3 né 4.

Lemma

Supponiamo che c divida un prodotto ab e che $mcd(c, a) = 1$. Allora c divide b.

Dimostrazione

- Per Bezout esistono $x, y \in \mathbb{Z}$ tali che $cx + ay = 1$.
- Moltiplicando per b ottengo $cbx + aby = b$.
- c divide sia cbx sia aby (in quanto divide ab), quindi divide la loro somma, che è b.

Sezioni

Se un primo divide un prodotto ...

Teorema

Se un primo p divide un prodotto ab di due numeri interi, allora p divide uno dei due.

Dimostrazione

1. $\mathrm{mcd}(p, a)$ può essere 1 o p in quanto non vi sono altri divisori di p.
2. Se $\mathrm{mcd}(p, a) = p$, vuol dire che p divide a.
3. Se $\mathrm{mcd}(p, a) = 1$, per il lemma precedente p divide b.

Applicando il teorema più volte si ottiene:

Corollario

Se un primo p divide un prodotto di un numero finito di fattori, allora divide uno di essi.

Ad esempio se p divide abc, scrivendo abc come $a(bc)$ otteniamo che p divide a oppure p divide bc. Nel primo caso abbiamo finito. Nel secondo p divide b o p divide c.

Esercizio

Sapendo che 601 *è primo, stabilire se esiste un numero intero* n *tale che* $601^5 \cdot n = 7^4 \cdot 11^3 \cdot 13^4 \cdot 17^9 \cdot 19^{15} \cdot 601^2 \cdot 751^{101} \cdot 991^{444}$.

Soluzione

- *Mostro che non è possibile.*
- *Supponendo che valga l'uguaglianza, dividendo per* 601^2 *ottengo* $601^3 \cdot n = 7^4 \cdot 11^3 \cdot 13^4 \cdot 17^9 \cdot 19^{15} \cdot 751^{101} \cdot 991^{444}$.
- *Se un primo divide un prodotto deve dividere uno dei fattori, quindi* 601 *deve divere uno dei numeri* $7, 11, 13, 17, 19, 751, 991$, *cosa manifestamente impossibile.*

Unicità della scomposizione in primi

Ragionando come nell'esercizio si dimostra:

Proposizione

Se p è primo e $a, b \in \mathbb{N}$ sono tali che $p^a m = p^b k$ dove m, k sono prodotti di numeri primi diversi da p, allora $a = b$ ed $m = k$.

Da questo si deduce:

Teorema

La scomposizione in primi è unica a parte l'ordine dei fattori, ovvero se un primo p compare con esponente a in una fattorizzazione in primi di un intero n, allora compare in tutte le fattorizzazioni e con lo stesso esponente.

Sezioni

Congruenze

Definizione

Sia m un intero positivo. Scriviamo

$$a \equiv b \bmod m$$

se $a - b$ è un multiplo di m, ovvero uno dei due numeri si ottiene dall'altro sommandogli un multiplo di m.

La scrittura $a \equiv b \bmod m$ si legge "a e b sono congrui modulo m".

Osservazione

$a \equiv 0 \bmod m$ *se e solo se a è multiplo di m.*

Conguenze e resti

Proposizione

$a \equiv a'$ mod m *se e solo se* a *e* a' *danno lo stesso resto divisi per* m.

Dimostrazione

- Scriviamo le equazioni per i quozienti e i resti:

$$a = mq + r, \quad 0 \leq r < m$$
$$a' = mq' + r', \quad 0 \leq r < m$$

- $a - a' = m(q - q') + (r - r') \quad (*)$.
- Quindi $r = r' \implies a \equiv a'$ mod m.
- Viceversa se $a \equiv a'$ mod m, da (*) ottengo che $r - r'$ è multiplo di m, ma visto che $0 \leq r, r' < m$ questo avviene solo se $r = r'$.

Le congruenze rispettano somme e prodotti

Teorema

classi *Se* $a \equiv a' \bmod m$ *e* $b \equiv b' \bmod m$*, allora* $a + b \equiv a' + b' \bmod m$ *e* $ab \equiv a'b' \bmod m$*.*

Dimostrazione

- Supponiamo che $a' = a + km$ e $b' = b + k'm$.
- Allora $a' + b' = a + b + (k + k')m$, e quindi $a + b \equiv a' + b' \bmod m$.
- Inoltre $a'b' = (a + km)(b + k'm) = ab + kmb + k'ma + kk'm^2$, e siccome $kmb + k'ma + kk'm^2$ è un multiplo di m possiamo concludere $a'b' \equiv ab \bmod m$.

return

Esempio

Trovare il resto della divisione euclidea di $1253423 \cdot 134432$ *per* 5.

Soluzione

- *Visto che* $1253423 \equiv 3 \bmod 5$ *e che* $134432 \equiv 2 \bmod 5$, *possiamo sostituire e scrivere:* $1253423 \cdot 134432 \equiv 3 \cdot 2 \equiv 6 \equiv 1 \bmod (5)$.
- *Quindi il resto è* 1.

Esempio

Trovare il resto della divisione euclidea di 2^{99} *per* 7.

Soluzione

- $2^{99} = 2^{3\cdot 33} = 8^{33}$.
- *Ora, 8 è congruo a 1 modulo 7 dunque possiamo continuare sostituendo:* $8^{33} \equiv 1^{33} \equiv 1 \bmod 7$.
- *Quindi il resto è* 1.

Attenzione Gli esponenti non possono essere sostituiti dal loro resto: Ad esempio $99 \equiv 1 \bmod 7$, ma $2^{99} \not\equiv 2^1 \bmod 7$.

Esempio

Trovare il resto della divisione di 3^{11} *per* 5.

Soluzione

- *Modulo* 5 *abbiamo le seguenti congruenze:* $3^{11} \equiv 3^2 3^2 3^2 3^2 3^2 3 \equiv 4 \cdot 4 \cdot 4 \cdot 4 \cdot 4 \cdot 3 \equiv (-1) \cdot (-1) \cdot (-1) \cdot (-1) \cdot (-1) \cdot 3 \equiv -3 \equiv 2 \bmod (5)$.
- *Quindi il resto è* 2.

- Quando scriviamo un numero, ad esempio 1234567, implicitamente sottintendiamo che esso è scritto in base 10, ovvero:

  $$1234567 = 1 \cdot 10^6 + 2 \cdot 10^5 + 3 \cdot 10^4 + 4 \cdot 10^3 + 5 \cdot 10^2 + 6 \cdot 10 + 7$$

- Utilizzando il linguaggio delle congruenze possiamo trovare dei modi rapidi di calcolare il resto della divisione euclidea. I prossimi esempi illustrano il caso in cui il divisore è $3, 9, 11, 4, 7$ (e in particolare ci fanno riottenere i famosi criteri di divisibilità per $3, 4, 7, 11$).

Esempio

Trovare il resto della divisione di 1234564 *per* 3*.*

Soluzione

- $1234567 = 1 \cdot 10^6 + 2 \cdot 10^5 + 3 \cdot 10^4 + 4 \cdot 10^3 + 5 \cdot 10^2 + 6 \cdot 10 + 7$
- *Siccome* $10 \equiv 1 \bmod 3$*, nel fare le congruenze modulo* 3 *possiamo sostituire* 10 *con* 1 *nell'espansione decimale ottenendo:* $1234564 \equiv 1 + 2 + 3 + 4 + 5 + 6 + 4 \equiv 1 \bmod 3$*.*
- *Quindi il resto è* 1*.*
- *Se avessimo cercato il resto della divisione di* 1234564 *per* 9*, avremmo anche in questo caso sostituito il 10 con 1 ottenendo* $1234564 \equiv 1 + 2 + 3 + 4 + 5 + 6 + 4 \equiv 7 \bmod 9$*.*

Esempio

Trovare il resto della divisione di 1234567 *per* 11.

Soluzione

- $1234567 = 1 \cdot 10^6 + 2 \cdot 10^5 + 3 \cdot 10^4 + 4 \cdot 10^3 + 5 \cdot 10^2 + 6 \cdot 10 + 7$
- *Siccome* $10 \equiv -1 \bmod (11)$, *nel fare le congruenze modulo* 11 *possiamo sostituire* 10 *con* -1 *nell'espansione decimale.*
- $1234567 \equiv 1 - 2 + 3 - 4 + 5 - 6 + 7 \equiv 4$. *Quindi il resto è* 4.

Esempio

Trovare il resto della divisione di 1234567 *per* 4.

Soluzione

- *osserviamo che* $100 = 25 \cdot 4 \equiv 0 \bmod (4)$.
- *Quindi* $1234567 = 12345 \cdot 100 + 67 \equiv 67 \equiv 3 \bmod (4)$.

Esempio

Trovare il resto della divisione di 1234567 *per* 7.

Soluzione

- *Osserviamo che* $1000 = 7 \cdot 143 - 1 \equiv -1 \bmod (7)$.
- *Quindi* $1234567 = 1 \cdot 1000^2 + 234 \cdot 1000 + 567 \equiv 1 - 234 + 567 \equiv 334 \equiv 5 \bmod 7$.

Esempio

Si dimostri che $\sqrt{1234567}$ *non è un intero.*

Soluzione

- *per assurdo supponiamo che vi sia un intero* x *tale che* $x^2 = 1234567$.
- *Per un esercizio precedente* $1234567 \equiv 3 \bmod 4$.
- *Quindi basta mostrare che* x^2 *non può essere congruente a* 3 *modulo* 4.
- *Siccome* x *è congruo a* $0, 1, 2$ *o* 3 *modulo* 4*, ci sono solo quattro verifiche da fare*

$$\begin{aligned} 0^2 &\equiv 0 \bmod 4 \\ 1^2 &\equiv 1 \bmod 4 \\ 2^2 &\equiv 0 \bmod 4 \\ 3^2 &\equiv 1 \bmod 4 \end{aligned}$$

perché poi si ripete ciclicamente $4^2 \equiv 0^2, 5^2 \equiv 1^2, 6^2 \equiv 2^2$ *ecc.*

Sezioni

Coprimi

Due interi a, b sono coprimi se $\text{mcd}(a, b) = 1$.

Teorema

Se $mcd(a, b) = d$, dividendo a, b per d si ottengono due numeri coprimi.

Dimostrazione

- Siano $a' = \frac{a}{d}$ e $b' = \frac{b}{d}$ e osserviamo che a', b' sono interi.
- Sia $k = \text{mcd}(a', b')$ e mostriamo che $k = 1$.
- Siccome k divide a', b', posso scrivere $ku = a', kv = b'$ con $u, v \in \mathbb{Z}$.
- Ne segue che $kud = a$ e $kvd = b$, quindi kd divide sia a sia b.
- Siccome d era il massimo dei divisori comuni, k deve essere 1, altrimenti kd sarebbe un divisore comune più grande.

Equazioni diofantee lineari omogenee

Teorema

Siano $a, b \in \mathbb{Z}$ coprimi. Le soluzioni intere di $ax + by = 0$ sono tutte e sole le coppie (x, y) della forma $x = -bk$ e $y = ak$ con $k \in \mathbb{Z}$.

Dimostrazione

- Siano $x, y \in \mathbb{Z}$ tali che $ax + by = 0$.
- Lo posso scrivere come $ax = -by$.
- $a|ax \implies a| - by$.
- Siccome $\text{mcd}(a, -b) = \text{mcd}(a, b) = 1$, ottengo $a|y$.
- Questo significa che $y = ak$ per un certo $k \in \mathbb{Z}$.
- Sostituendo ottengo $x = -bk$.

Esempio

Esempio

Le soluzioni di $3x + 5y = 0$ *sono le coppie* (x, y) *della forma* $(5k, -3k)$, *e non vi sono altre soluzioni perché* $mcd(3, 5) = 1$.

Se i coefficienti non sono coprimi non funziona:

- L'equazione $12x + 20y = 0$, oltre alle soluzioni $x = -20k, y = 12k$, ha anche le soluzioni $x = 5k, y = -3k$ (sono di più perché ora vi è una x ogni 5 numeri consecutivi anziché ogni 20).
- Per trovare tutte le soluzioni di $12x + 20y = 0$ conviene prima dividere per 4 in modo da ricondursi all'equazione equivalente $3x + 5y = 0$ in cui i coefficienti sono coprimi.

Diofantee lineari non omogenee

Teorema

L'equazione diofantea $ax + by = c$ è risolubile se e solo se $mcd(a, b)|c$ vedi*. Le soluzioni si ottengono aggiungendo ad una soluzione particolare (x_0, y_0) le soluzioni dell'equazione omogenea associata $ax + by = 0$.*

Dimostrazione

Basta osservare che se (x_0, y_0) è una soluzione, e (x, y) è un'altra soluzione, facendo la differenza ottengo una soluzione dell'omogenea associata:

$$\begin{array}{cl} ax + by & = c \\ ax_0 + by_0 & = c \\ \hline a(x - x_0) + b(y - y_0) & = 0 \end{array}$$

La generica soluzione (x, y) è quindi ottenuta sommando a (x_0, y_0) una soluzione dell'omogenea associata.

Esempio

Trovare tutte le soluzioni dell'equazione diofantea $435x + 102y = 15$.

- Prima calcolo l'mcd dei coefficienti

$$435 = 102 \cdot 4 + 27$$

$$102 = 27 \cdot 3 + 21$$

$$27 = 21 \cdot 1 + 6$$

$$21 = 6 \cdot 3 + 3$$

$$6 = 3 \cdot 2 + 0$$

  $\implies \text{mcd}(435, 102) = \text{mcd}(27, 102) = \text{mcd}(27, 21) = \text{mcd}(6, 21) = \text{mcd}(6, 3) = \text{mcd}(0, 3) = 3$.
- Siccome $3 | 15$, l'equazione ha soluzione.
- Per l'identità di Bezout esistono x', y' tali che $3 = 435x' + 102y'$.
- Una volta trovati li moltiplico per 5 e trovo una soluzione particolare di $15 = 435x + 102y$.

Continuo l'esempio ...

Cerco una soluzione di $3 = 435x' + 102y'$. Posso farlo come in procedura oppure come segue

$$
\begin{aligned}
435 &= 102 \cdot 4 + 27 \\
102 &= 27 \cdot 3 + 21 \\
27 &= 21 \cdot 1 + 6 \\
21 &= 6 \cdot 3 + 3 \\
6 &= 3 \cdot 2 + 0
\end{aligned}
\qquad \longrightarrow \qquad
\begin{aligned}
27 &= 435 - 102 \cdot 4 \\
21 &= 102 - 27 \cdot 3 \\
6 &= 27 - 21 \cdot 1 \\
3 &= 21 - 6 \cdot 3
\end{aligned}
$$

$$
\begin{aligned}
\mathrm{mcd}(435, 102) = 3 &= 21 - 6 \cdot 3 \\
&= 21 - (27 - 21)3 \\
&= 21 \cdot 4 - 27 \cdot 3 \\
&= (102 - 27 \cdot 3)4 - 27 \cdot 3 = 102 \cdot 4 - 27 \cdot 15 \\
&= 102 \cdot 4 - (435 - 102 \cdot 4) \cdot 15 \\
&= 102 \cdot 64 - 435 \cdot 15 = 102 \cdot \boxed{64} + 435 \cdot \boxed{\text{-15}}
\end{aligned}
$$

Quindi $y' = 64, x' = -15$.

Continuo ...

- Ho trovato che $(x', y') = (-15, 64)$ è una soluzione di

$$3 = 435x' + 102y'$$

- L'equazione che ci interessava però era

$$15 = 435x + 102y.$$

- Quindi devo moltiplicare per 5 e ottengo la soluzione particolare

$$(x, y) = (-75, 320).$$

Osservazione

Poteva essere più conveniente dividere $15 = 435x + 102y$ *per* 3 *ottenendo l'equazione equivalente (ovvero con le stesse soluzioni)* $5 = 145x + 34y$.

Continuo...

- $(x, y) = (-75, 320)$ è una soluzione particolare dell'eq. diofantea
$$435x + 102y = 15.$$
- Considero l'omogenea associata
$$435x + 102y = 0$$
- Dividendo per $3 = \text{mcd}(435, 102)$ trovo che equivale a
$$145x + 34y = 0$$
- Le soluzioni sono $(x, y) = (k34, -k145)$ (con $k \in \mathbb{Z}$). Non ce ne sono altre perché 145 e 34 sono coprimi.
- Le sommo alla soluzione particolare della non omogenea e ottengo $\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} -75 \\ 320 \end{bmatrix} + k \begin{bmatrix} 34 \\ -145 \end{bmatrix} = \begin{bmatrix} -75 + k34 \\ 320 - k145 \end{bmatrix}$. Queste sono tutte le soluzioni della non omogenea.

Congruenze ed equazioni diofantee

- Risolvere le congruenze del tipo

$$ax \equiv b \bmod m$$

equivale sostanzialmente a risolvere equazioni diofantee del tipo

$$ax + my = b.$$

- Infatti se (x, y) risolve $ax + my = b$, allora x risolve $ax \equiv b \bmod m$.
- Viceversa se x risolve $ax \equiv b \bmod m$, allora esiste $k \in \mathbb{Z}$ tale che

$$ax + b = mk.$$

- La posso scrivere come $ax + my = b$ con $y = -k$, quindi (x, y) risolve

$$ax + my = b.$$

- Dalla discussione appena fatta segue che se sapete risolvere la diofantee
$$ax + by = m$$
sapete anche risolvere la congruenza
$$ax \equiv b \bmod m.$$
Basta prendere la soluzione (x, y), tenersi la x e buttare via la y.
- In pratica è però spesso più comodo risolvere direttamente la congruenza perché sono possibili varie semplificazioni.

Esempio

Risolvere la congruenza $435x \equiv 15 \bmod 102$.

- Avevamo già risolto l'equazione diofantea

$$435x + 102y = 15$$

  con $x = -75, y = 320$.

- Questo vuol dire che $x = -75$ risolve la congruenza

$$435x \equiv 15 \bmod 102.$$

- Però potevamo rimpiazzare 435 con $27 \equiv 435 \bmod 102$ e considerare direttamente la congruenza più semplice

$$27x \equiv 15 \bmod 102$$

Sezioni

Inversi modulo n

- Quando scriviamo $\frac{1}{5}$ intendiamo quel numero che moltiplicato per 5 fa 1.
- Negli interi modulo n (con n fissato), dato un intero x, vorrei definire x^{-1} come un intero (se esiste) che moltiplicato per x è congruo ad 1 modulo n.
- Ad esempio $5 \cdot 6 = 30 \equiv 1 \bmod 29$, quindi $6 = 5^{-1}$ modulo 29 (analogamente $5 = 6^{-1} \bmod 29$).
- 5 non ha un inverso modulo 30, in quanto se avessimo $5y \equiv 1 \bmod 30$, moltiplicando per 6 otterremo $6 \cdot 5 \cdot y \equiv 6 \bmod 30$, che è assurdo in quando $5 \cdot 6 \equiv 0 \bmod 30$ (e non possiamo avere $0 \equiv 6 \bmod 30$).
- Vedremo che un intero x è invertibile modulo n (ovvero x^{-1} esiste), se e solo se x è coprimo con n.

Definizione

Diciamo che un intero x è invertibile modulo n se esiste un $y \in \mathbb{Z}$ tale che $xy \equiv 1 \bmod n$. Diremo in questo caso che x ed y sono l'uno l'inverso dell'altro modulo n e scriveremo $y \equiv x^{-1} \bmod n$.

- Talvolta, se è noto di quale n si stia parlando, scriveremo $y = x^{-1}$ invece di $y \equiv x^{-1} \bmod n$.
- Notiamo che se $xy \equiv 1 \bmod n$ e $y \equiv y' \bmod n$, allora anche $xy' \equiv 1 \bmod n$, quindi se c'è un inverso ce ne sono tanti, ma in genere x^{-1} indica quello tra i tanti compreso tra 0 ed $n-1$.
- Ad esempio 6 è un inverso di 5 modulo 29, ma anche $35 = 6 + 29$ è un inverso di 5 modulo 29, tuttavia $6 = 5^{-1}$ è l'unico inverso tra 0 e 28.

Trovare gli inversi

Esercizio

Trovare, se esiste, un inverso di 9 *modulo* 34. return

- Un inverso è un $x \in \mathbb{Z}$ tale che $9x \equiv 1 \mod 34$.
- Devo quindi trovare x, y tali che $9x + 34y = 1$ e poi prendere la x.
- $$\begin{array}{rcccccc} & & 34 & = & 34 \cdot \boxed{1} & + & 9 \cdot \boxed{0} \\ & & 9 & = & 34 \cdot \boxed{0} & + & 9 \cdot \boxed{1} \\ 34 - 3 \cdot 9 & = & 7 & = & 34 \cdot \boxed{1} & + & 9 \cdot \boxed{(\text{-}3)} \\ 9 - 7 & = & 2 & = & 34 \cdot \boxed{(\text{-}1)} & + & 9 \cdot \boxed{4} \\ 7 - 2 \cdot 3 & = & 1 & = & 34 \cdot \boxed{4} & + & 9 \cdot \boxed{(\text{-}15)} \end{array}$$
- Quindi un inverso è -15.
- Siccome -15 è congruo a 19 modulo 34 anche 19 è un inverso: $9 \cdot 19 \equiv 1 \mod 34$.
- Ho quindi $9^{-1} \equiv 19$ modulo 34.

Teorema

◂ inversi *Dato $a \in \mathbb{Z}$, abbiamo che a è invertibile modulo n (ovvero esiste un inverso) se e solo se a è coprimo con n, ovvero $mcd(a, n) = 1$.*

Dimostrazione

- Se $\text{mcd}(a, n) = 1$, per l'identità di Bezout esistono $x, y \in \mathbb{Z}$ tali che $ax + ny = 1$.
- Una tale x verifica $ax \equiv 1 \bmod n$, e quindi $x \bmod a^{-1} \bmod n$.
- Viceversa, supponiamo che esista un inverso x di a.
- Questo significa che $ax \equiv 1 \bmod n$.
- Per definizione di congruenza, esiste $y \in \mathbb{Z}$ tale che $ax + ny = 1$, e ne deduciamo che $\text{mcd}(a, n) = 1$ (altrimenti la diofantea non sarebbe risolubile).

Sezioni

Tecniche per le congruenze

Abbiamo già visto che le congruenze rispettano somme e prodotti. Inoltre

- Se $A \equiv B + C \bmod n$, allora $A - B \equiv C \bmod n$.
- Se $A \equiv B \bmod n$, allora $AC \equiv BC \bmod n$.
- Se A, B, n sono divisibili per d,

$$A \equiv B \bmod n \implies \frac{A}{d} \equiv \frac{B}{d} \bmod \frac{n}{d}$$

- Se A, B sono divisibili per d e d è invertibile modulo n, allora

$$A \equiv B \bmod n \implies \frac{A}{d} \equiv \frac{B}{d} \bmod n$$

Si possono fare gli stessi passaggi che si usano per le equazioni (spostare un termine da un lato all'altro cambiando segno, moltiplicare entrambi i lati per un numero dato, ecc., ma occorre stare attenti a dividere: se divido anche il modulo si può fare, se divido solo i due lati della congruenza si può fare solo se il numero d per il quale divido è invertibile.

Perché funziona?

Per dimostrare le proprietà delle congruenze ci si riconduce a quelle delle equazioni.

- Ad esempio supponiamo

$$A \equiv B \bmod n.$$

  Questo significa che esiste $y \in \mathbb{Z}$ che verifica l'equazione $A = B + ny$

- Moltiplicando l'equazione per C ottengo $AC = BC + n(yC)$ e quindi

$$AC \equiv BC \bmod n.$$

- Se A, B, n sono divisibili per d, dividendo l'equazione per d ottengo $\frac{A}{d} = \frac{B}{d} + \frac{n}{d}y$ e quindi

$$\frac{A}{d} \equiv \frac{B}{d} \bmod \frac{n}{d}.$$

Continua ...

- Supponiamo che
$$A \equiv B \bmod n$$
e A, B siano divisibili per d, ovvero $A' = \frac{A}{d}$ e $B' = \frac{B}{d}$ sono interi.
- Supponiamo che d abbia un inverso d^{-1} modulo n. Moltiplicando per d^{-1}:
$$d^{-1}A \equiv d^{-1}B \bmod n.$$
- Lo posso riscrivere come
$$d^{-1}d\frac{A}{d} \equiv dd^{-1}\frac{B}{d} \bmod n.$$
- Ma $dd^{-1} \equiv 1 \bmod n$, quindi lo posso cancellare e ho
$$\frac{A}{d} \equiv \frac{B}{d} \bmod n.$$

In sintesi, il motivo per cui posso dividere per d, è che è come moltiplicare per d^{-1}.

Esercizio

Risolvere la congruenza $435x \equiv 15 \bmod 102$.

- L'avevamo già risolta, ma lo facciamo in un altro modo. Osservo che $435 \equiv 27 \bmod 102$, quindi $435x \equiv 27x \bmod 102$ e la congruenza diventa

$$27x \equiv 15 \bmod 102.$$

- Divido tutto per 3 incluso il modulo:

$$9x \equiv 5 \bmod 34$$

- Siccome $\mathrm{mcd}(9, 34) = 1$, esiste l'inverso 9^{-1} di 9 modulo 34. Lo avevamo già calcolato ed era 19 vedi.
- Moltiplicando per $9^{-1} \bmod 34$ ottengo

$$x \equiv 9^{-1}5 \equiv 19 \cdot 5 \bmod 34.$$

- Siccome $19 \cdot 5$ ha resto 27 mod 34, $x = 27$ è una soluzione, e le altre sono $x = 27 + k34$.

Precedentemente avevamo trovato $x = -75 + k34$, ma è la stessa cosa perché 27 e -75 differiscono per un multiplo di 34.

Esercizio

Trovare tutte le soluzioni di $26x \equiv 13 \bmod 75$.

- Siccome $\text{mcd}(13, 75) = 1$, posso dividere per 13 (senza bisogno di calcolare l'inverso di 13, che comunque è 52):

$$2x \equiv 1 \bmod 75.$$

- Ora osservo che $2 \cdot 38 = 76 \equiv 1 \bmod 75$, quindi $2^{-1} = 38 \bmod 75$ e moltiplicando entrambi i membri della congruenza per 2^{-1} ottengo

$$x \equiv 2^{-1} \equiv 38 \bmod 75.$$

Le soluzioni sono $x = 38 + k75$.

Condizione necessaria per la risolubilità di $ax \equiv b \bmod m$

Lemma

Siano $a, b, m \in \mathbb{Z}$ con $m > 0$. Se la congruenza $ax \equiv b \bmod m$ è risolubile, allora $mcd(a, m)$ divide b.

Dimostrazione

- Supponiamo che la congruenza sia risolubile, ovvero esiste una $x \in \mathbb{Z}$ tale che $ax \equiv b \bmod m$.
- Per definizione di congruenza ciò significa che esiste $k \in \mathbb{Z}$ tale che $ax = b + km$.
- L'mcd tra a ed m divide sia ax sia km, quindi deve dividere la loro differenza $ax - km$, che è proprio b.

Esempio

$10x \equiv 5 \bmod 14$ *non è risolubile in quanto* $mcd(10, 14) = 2$ *e* 2 *non divide* 5.

Condizione sufficiente per la risolubilità di $ax \equiv b \bmod m$

Lemma

Siano $a, b, m \in \mathbb{Z}$ con $m > 0$. Se $mcd(a, m) = 1$, la congruenza $ax \equiv b \bmod m$ è risolubile.

Dimostrazione

1. Poiché $\mathrm{mcd}(a, m) = 1$, sappiamo che a è invertibile mod m
   invertibile
2. Infatti considero l'identità di Bezout $au + mv = 1$ e prendo $a^{-1} = u$.
3. L'equivalenza diventa $x \equiv a^{-1}b \bmod m$.
4. Le soluzioni sono $x = a^{-1}b + km$.

Criterio per la risolubilità di $ax \equiv b \bmod m$

Teorema

return *Siano $a, b, m \in \mathbb{Z}$ con $m > 0$. La congruenza*

$$ax \equiv b \bmod m$$

è risolubile se e solo se mcd(a, m) divide b. Se x_0 è una soluzione, le altre si ottengono aggiungendo ad x_0 un multiplo di m.

Dimostrazione

- Sia $d = \text{mcd}(a, m)$ e supponiamo che $d | b$.
- Dividendo a, m, b per d otteniamo tre numeri interi $a_1 = \frac{a}{d}$, $m_1 = \frac{m}{d}$, $b_1 = \frac{b}{d}$ e una congruenza equivalente

$$a_1 x \equiv b_1 \bmod m_1.$$

- Siccome $\text{mcd}(a_1, m_1) = 1$ esiste l'inverso a_1^{-1} di a_1.
- Una soluzione è $x_0 = a_1^{-1} b_1$, le altre sono della forma $x = a_1^{-1} b_1 + k m_1$, ovvero $x \equiv a_1^{-1} b_1 \bmod m_1$.

Sezioni

Sistemi di congruenze

Esercizio

Trovare le soluzioni del sistema $\begin{cases} x \equiv 1 \bmod 5 \\ x \equiv 2 \bmod 7 \end{cases}$

- Se x risolve la prima, $x = 1 + 5y$ per qualche $y \in \mathbb{Z}$.
- Sostituisco questo valore nella seconda: $1 + 5y \equiv 2 \bmod 7$
- Sottraggo 1 da entrambi i lati:

$$5y \equiv 1 \bmod 7.$$

- Cerco l'inverso di 5. Posso farlo utilizzando la procedura o per tentativi (ci sono al massimo 7 tentativi). Scopro che $3 \cdot 5 = 15 \equiv 1 \bmod 7$ quindi $5^{-1} \equiv 3 \bmod 7$.
- Moltiplico per 5^{-1} e ottengo:

$$y \equiv 3 \bmod 7$$

  ovvero $y = 3 + 7k$.
- Sostituisco questo valore in $x = 1 + 5y$ e ottengo $x = 1 + 5(3 + 7k) = 16 + 35k$.
- In altre parole le soluzioni sono gli x tali che $x \equiv 16 \bmod 35$.

Esercizio

Ho x matite. Se le distribuisco tra 9 persone me ne avanzano 3, se le distribuisco tra 8 persone me ne avanzano 5, e se le distribuisco tra 7 persone me ne avanzano 2. Quante matite ho?

Il problema equivale a risolvere un sistema di congruenze (slide successiva). Non c'è un'unica soluzione!

Esercizio

Risolvere il sistema $\begin{cases} x \equiv 3 \bmod 9 \\ x \equiv 5 \bmod 8 \\ x \equiv 2 \bmod 7 \end{cases}$

- Dalla prima ricavo $x = 3 + 9y$ per qualche $y \in \mathbb{Z}$.
- Sostituisco nella seconda e ottengo $3 + 9y \equiv 2 \bmod 8$, ovvero $9y \equiv 2 \bmod 8$.
- Siccome 9 è congruo a 1 modulo 8, lo posso scrivere come $y \equiv 2 \bmod 8$, ovvero $y = 2 + 8z$.
- Sostituendo nell'espressione $x = 3 + 9y$ ottengo $x = 3 + 9(2 + 8z)$, cioè $x = 21 + 72z$.
- Le prime due congruenze equivalgono quindi alla singola congruenza $x \equiv 21 \bmod 72$.
- Sostituendo l'espressione per x nella terza ottengo $21 + 72z \equiv 2 \bmod 7$, ovvero $0 + 2z \equiv 2 \bmod 7$.
- Siccome $\mathrm{mcd}(2, 7) = 1$, posso dividere per 2 e ottengo $z \equiv 1 \bmod 7$, cioè $z = 1 + 7k$.
- $\implies x = 21 + 72(1 + 7k) = 93 + 504k$, cioè $x \equiv 93 \bmod 504$.

Sezioni

Minimo comune multiplo

Definizione

$mcm(a,b)$ è il più piccolo intero positivo che è multiplo sia di a sia di b.

Esempio

$mcm(6,14) = 42$.

MCD ed MCM

Teorema

Sia p un numero primo. Supponiamo che

- *p compare nella scomposizione in primi di x con esponente* e_x*;*
- *p compare nella scomposizione in primi di y con esponente* e_y*.*

Allora:

- *p compare nella scomposizione di* $mcm(x, y)$ *con esponente* $\max\{e_x, e_y\}$*.*
- *p compare nella scomposizione di* $mcd(x, y)$ *con esponente* $\min\{e_x, e_y\}$*.*
- *p compare nella scomposizione di* xy *con esponente* $e_x + e_y$*.*

Si intende che se un primo non compare è come se comparisse con esponente 0*.*

Esempio

Se $x = 3^5 7^4 13^9$ *e* $y = 2^4 3^7 13^5$, *allora*

- $mcm(x, y) = 3^5 \cdot 13^5$
- $mcm(x, y) = 2^4 3^7 7^4 13^9$
- $xy = 2^4 3^{11} 7^4 13^{14} = mcm(x, y) \cdot mcd(x, y)$

Il prodotto xy è uguale a $\mathrm{mcm}(x, y) \cdot \mathrm{mcd}(x, y)$ perché, dato un primo p che compare in x con esponente e_x e in y con esponente e_y, abbiamo che p compare in xy con esponente $e_x + e_y$ e in $\mathrm{mcm}(x, y) \cdot \mathrm{mcd}(x, y)$ con esponente $\max\{e_x, e_y\} + \min\{e_x, e_y\}$, che è uguale ad $e_x + e_y$.

Osservazione

Se due interi positivi x *ed* y *sono coprimi,* $mcm(x, y) = xy$ *(se considero anche gli interi negativi e* xy *è negativo, allora* $mcm(x, y) = -xy$*).*

Esercizio

Quanti sono i divisori positivi di $3^5 7^4 13^9$*?*

- I divisori devono essere della forma $3^a 7^b 13^c$ con $a \leq 5, b \leq 4, c \leq 9$, senza escludere il caso in cui a, b o c siano zero.
- Ci sono 6 scelte per a; 5 per b; 10 per c.
- In tutto ho $6 \cdot 5 \cdot 10 = 300$ possibili divisori.

Ad esempio uno dei divisori è $42 = 3^2 \cdot 7^1 \cdot 13^0$.

Teorema

$a|c \wedge b|c \iff mcm(a, b)|c.$

- Se $\mathrm{mcm}(a, b)|c$ chiaramente $a|c \wedge b|c$.
- Se $a|c \wedge b|c$, scriviamo $c = \mathrm{mcm}(a, b)q + r$ con $0 \leq r < \mathrm{mcm}(a, b)$.
- La differenza di due multipli di un numero è multiplo di quel numero.
- Quindi r è multiplo sia di a sia di b.
- Essendo $r < \mathrm{mcm}(a, b)$ (che è il più piccolo multiplo comune positivo), r deve essere zero.
- Quindi $c = \mathrm{mcm}(a, b)q$ e $\mathrm{mcm}(a, b)|c$.

Corollario

$$\begin{cases} x \equiv b \bmod m_1 \\ x \equiv b \bmod m_2 \end{cases} \iff x \equiv b \bmod mcm(m_1, m_2)$$

Dimostrazione

$x - b$ è multiplo sia si m_1 sia di m_2 se e solo se è multiplo di $\mathrm{mcm}(m_1, m_2)$.

Sezioni

Lemma

Il sistema

$$\begin{cases} x \equiv a_1 \bmod m_1 \\ x \equiv a_2 \bmod m_2 \end{cases}$$

è risolubile se e solo se $a_1 \equiv a_2 \bmod mcd(m_1, m_2)$ *(ovvero* $mcd(m_1, m_2)$ *divide* $a_1 - a_2$*).*

- Dalla prima ricavo $x = a_1 + m_1 y$.
- Sostituisco nella seconda: $a_1 + m_1 y \equiv a_2 \bmod m_2$.
- Lo riscrivo come

$$m_1 y = a_2 - a_1 \bmod m_2.$$

- Questa è una singola congruenza nell'incognita y e sappiamo già che è risolubile se e solo se $\text{mcd}(m_1, m_2) | a_1 - a_2$. Questo è spiegato in vedi dove si dice anche come trovare la soluzioni.
- Siccome la x si ricava dalla y, questa è anche la condizione perché sia risolubile il sistema.

Corollario

Se m_1 ed m_2 sono coprimi, allora un sistema della forma

$$\begin{cases} x \equiv a_1 \bmod m_1 \\ x \equiv a_2 \bmod m_2 \end{cases}$$

ha sempre soluzione.

Dimostrazione

Se $1 = \mathrm{mcd}(m_1, m_2)$, allora ovviamente $\mathrm{mcd}(m_1, m_2)$ divide $a_1 - a_2$.

Esempio

Determinare per quali valori del parametro b Il sistema

$$\begin{cases} x \equiv 8 \bmod 221 \\ x \equiv b \bmod 247 \end{cases}$$

è risolubile.

- $\text{mcd}(221, 247) = 13$ (essendo $221 = 13 \cdot 17$ e $247 = 13 \cdot 19$).
- Il sistema è risolubile $\iff$ $b \equiv 8 \bmod 13$.
- Ad esempio per $b = \ldots, 34, 21, 8, -5, -18, -31 \ldots$ il sistema è risolubile, mentre per $b = 3$ non lo è.
- Un altro modo di vedere che il sistema non ha soluzione se $b \not\equiv 8 \bmod 13$ è il seguente: se due numeri sono congrui modulo un certo numero, sono anche congrui modulo i suoi divisori. Quindi una x che risolva il sistema deve essere congrua sia a 8 sia a b modulo 13, e questo può accadere solo se 8 è congruo a b modulo 13.

Esempio

Trovare una soluzione del sistema

$$\begin{cases} x \equiv 8 \text{ mod } 221 \\ x \equiv -31 \text{ mod } 247 \end{cases}$$

- Dalla prima ricavo $x \equiv 8 + 221y$.
- Sostituisco nella seconda: $8 + 221y \equiv -31$ mod 247, ovvero $221y \equiv -39$ mod 247.
- Divido tutto per $13 = \text{mcd}(221, 247)$ e ottengo $17y \equiv -3$ mod 19.
- Cerco l'inverso di 17 modulo 19:

$$\begin{array}{ccccccc} & & 19 & = & 19 \cdot \boxed{1} & + & 17 \cdot \boxed{0} \\ & & 17 & = & 19 \cdot \boxed{0} & + & 17 \cdot \boxed{1} \\ 19 - 17 & = & 2 & = & 19 \cdot \boxed{1} & + & 17 \cdot \boxed{(-1)} \\ 17 - 2 \cdot 8 & = & 1 & = & 19 \cdot \boxed{(-8)} & + & 17 \cdot \boxed{9} \end{array}$$

$\implies 9 = 17^{-1}$ mod 19.

- Deduco $y = -3 \cdot 9$ mod 19, ad es. $y = 11$ va bene.
- Siccome $x = 8 + 221y$, una soluzione è $x = 8 + 221 \cdot 11 = 2439$.

Lemma

Se x_0 è una soluzione del sistema

$$\begin{cases} x \equiv a_1 \bmod m_1 \\ x \equiv a_2 \bmod m_2 \end{cases}$$

allora anche $x_0 + k\,mcm(m_1, m_2)$ è una soluzione, e al variare di $k \in \mathbb{Z}$ queste sono tutte le soluzioni.

Dimostrazione

Basta dimostrare che date due soluzioni x_0 ed x esse differiscono per un multiplo di $\mathrm{mcm}(m_0, m_1)$.

$$\begin{cases} x \equiv a_1 \bmod m_1 \\ x \equiv a_2 \bmod m_2 \end{cases} \quad \begin{cases} x \equiv a_1 \bmod m_1 \\ x \equiv a_2 \bmod m_2 \end{cases} \longrightarrow \begin{cases} x - x_0 \equiv 0 \bmod m_1 \\ x - x_0 \equiv 0 \bmod m_2 \end{cases}$$

$$\longrightarrow x \equiv x_0 \bmod \mathrm{mcm}(m_1, m_2)$$

Esempio

Trovare tutte le soluzioni del sistema

$$\begin{cases} x \equiv 8 \bmod 221 \\ x \equiv -31 \bmod 247 \end{cases}$$

- $$\begin{aligned} \mathrm{mcm}(221, 247) &= \mathrm{mcm}(13 \cdot 17,\ 13 \cdot 19) \\ &= 13 \cdot 17 \cdot 19 \\ &= 4199 \end{aligned}$$
- Avevamo già trovato la soluzione $x_0 = 2439$.
- Le altre sono $x = 2439 + k4199$.
- Il sistema equivale alla singola congruenza $x \equiv 2439 \bmod 4199$.

Ricapitolando

Teorema

- *Il sistema*
$$\begin{cases} x \equiv a_1 \bmod m_1 \\ x \equiv a_2 \bmod m_2 \end{cases}$$
è risolubile se e solo se $a_1 \equiv a_2 \bmod mcd(m_1, m_2)$ *(ovvero* $mcd(m_1, m_2)$ *divide* $a_1 - a_2$*).*
- *Se* $x = x_0$ *è una soluzione, le altre si ottengono sommando ad* x_0 *un multiplo di* $mcm(m_1, m_2)$ *e quindi in questo caso il sistema equivale a*
$$x \equiv x_0 \bmod mcm(m_1, m_2)$$
- *Se* m_1, m_2 *sono coprimi, il sistema ha sempre soluzione.*

Nel teorema sono coinvolti sia il massimo comun divisore (mcd) sia il minimo comune multiplo (mcm).

Corollario

Se m_1 ed m_2 sono coprimi, allora la congruenza

$$x \equiv b \bmod m_1 m_2$$

equivale al sistema

$$\begin{cases} x \equiv b \bmod m_1 \\ x \equiv b \bmod m_2 \end{cases}$$

Dimostrazione

Il risultato precedente mi darebbe $\mathrm{mcm}(m_1, m_2)$ invece di $m_1 m_2$, ma visto che i moduli sono coprimi le due cose coincidono.

Teorema cinese del resto

Teorema

Un sistema della forma

$$\begin{cases} x \equiv a_1 \bmod m_1 \\ x \equiv a_2 \bmod m_2 \\ \dots \\ x \equiv a_k \bmod m_k \end{cases}$$

dove i moduli m_i sono a due a due coprimi, ha sempre soluzione. Se x_0 è una soluzione la altre sono $x = x_0 + Mk$ dove $M = m_1 \cdot m_2 \cdot \ldots m_k$ è il prodotto dei moduli.

Dimostrazione

- Se $x = b$ risolve le prime due, il sistema formato dalle prime due equivale alla singola congruenza $x \equiv b \bmod m$ dove $m = m_1 \cdot m_2$.
- Mi sono ridotto ad un sistema con una congruenza in meno, e procedendo in questo modo mi riduco ad una sola congruenza della forma $x \equiv c \bmod M$ dove M è il prodotto dei moduli.

Sezioni

Relazioni di equivalenza

Definizione

Data una relazione binaria R su un insieme X, diciamo che R è una relazione di equivalenza se verifica:

- $xRy \wedge yRz \implies xRz$ *(transitiva);*
- $xRy \implies yRx$ *(simmetrica).*
- xRx *(riflessiva).*

Esempio

- *Se definisco xRy come "x ed y frequentano la stessa classe, ho che R è una relazione di equivalenza sull'insieme X degli studenti.*
- *Sia n un intero positivo e definiamo xRy come "x è congruo ad y modulo n". Allora R è una relazione di equivalenza sull'insieme $\mathbb{Z}$.*

Classi di equivalenza

Definizione

Sia R una relazione di equivalenza sull'insieme X e sia $a \in X$. La classe di equivalenza di a, indicata talvolta con $[a]$, è l'insieme di tutti gli elementi b di X che sono equivalenti ad a.

Teorema

Le classi di equivalenza dividono X in insiemi a due a due disgiunti.

Example

- Sia R la relazione di equivalenza definita da $xRy \iff x \equiv y \bmod 2$. Vi sono due classi di equivalenza: l'insieme dei numeri pari, e l'insieme dei numeri dispari.
- Sia R la relazione di equivalenza definita da $xRy \iff x \equiv y \bmod 3$. Vi sono tre classi di equivalenza: l'insieme dei multipli di 3, l'insieme dei numeri che diviso 3 hanno resto 1, e l'insieme dei numeri che diviso 3 hanno resto 2.
- Analogamente l'equivalenza modulo n divide $\mathbb{Z}$ in n classi a seconda che il resto sia $0, 1, \ldots, n-1$.

Insieme quoziente

Definizione

Data una relazione di equivalenza su un insieme X, posso creare un nuovo insieme i cui elementi sono le classi di equivalenza rispetto alla relazione R. Tale insieme viene detto insieme quoziente di X modulo R e viene talvolta indicato con X/R.

L'anello degli interi modulo n

Definizione

Sia R la relazione di equivalenza su $\mathbb{Z}$ definita da
$xRy \iff x \equiv y \bmod n$*.*

- *L'insieme quoziente viene indicato con $\mathbb{Z}/(n)$. I suoi elementi sono le classi di equivalenza modulo n.*
- *Dato $x \in \mathbb{Z}$, indichiamo con $[x]_n$ la classe di equivalenza di x modulo n.*
- *Definiamo una somma e un prodotto di classi ponendo $[x]_n + [y]_n = [x + y]_n$ e $[x]_n \cdot [y]_n = [x \cdot y]_n$.*
- *Con queste operazioni $\mathbb{Z}/(n)$ è un anello, con $0 = [0]_n$ e $1 = [1]_n$.*

Esempi e osservazioni

- $[1]_5 = \{1, 6, 11, \dots, -4, -9, \dots\}$ è l'insieme dei numeri congrui ad 1 modulo 5 (i numeri che diviso 5 hanno resto 1). Gli interi $1, 6, 11, \dots, -4, -9, \dots$ sono diversi rappresentanti della classe $[1]_5$.
- Dire $x \equiv y \bmod 5$ equivale a dire $[x]_5 = [y]_5$.
- $\mathbb{Z}/(5)$ consiste di 5 classi: $[0]_5, [1]_5, [2]_5, [3]_5, [4]_5$. Notiamo che $[5]_5 = [0]_5$, $[1]_5 = [6]_5$, ecc.
- Affinché la definizione di somma e prodotto di classi abbia senso occorre verificare che $[x]_n = [x']_n \wedge [y]_n = [y']_n \implies [x+y]_n = [x'+y']_n$ (stesso input deve dare stesso output) e similmente per il prodotto. Questo ci è assicurato dal fatto che le classi di $x+y$ e di $x \cdot y$ dipendono solo dalle classi di x e di y e non dalla scelta dei rappresentanti rispettano,
- Se invece tentassimo di definire $[x]_n^{[y]_n} = [x^y]_n$ la cosa non funzionerebbe: $[1]_5 = [6]_5$, ma $[2]_5^{[1]_5} \neq [2]_5^{[6]_5}$ (il primo termine è la classe di 2, il secondo quella di 4).

Per semplicità scrivo gli elementi di $\mathbb{Z}/(n)$ come $0, 1, 2, \ldots, n-1$ invece che come $[0]_n, [1]_n, [2]_n, \ldots, [n-1]_n$. Diamo la tabellina del prodotto di $\mathbb{Z}/(5)$.

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Sezioni

Progressioni geometriche

Definizione

Una successione $a_0, a_1, a_2, \ldots$ si dice una progressione geometrica se i rapporti tra due termini consecutivi sono costanti, ovvero $a_{n+1} = ra_n$ dove r è un numero fisso che non dipende da n detto "ragione" della successione.

Esempio

Consideriamo una progressione geometrica a_n di ragione 3 tale che $a_0 = 5$. Trovare una formula per a_n.

- Per definizione $a_0 = 5$ e $a_{n+1} = 3a_n$. Calcolo i primi termini $a_0 = 5, a_1 = 3 \cdot 5, a_2 = 3^2 5, a_3 = 3^3 5, \ldots$.
- Sembra che la formula sia $a_n = 3^n 5$.
- Lo dimostro per induzione. Il caso $n = 0$ funziona perché $a_0 = 5 = 3^0 5$.
- Mostro che se funziona per $n = k$, funziona per $n = k + 1$.
- Supponiamo per ipotesi induttiva che $a_k = 3^k 5$. Se moltiplico entrambi i lati per 3 ottengo $3a_k = 3^{k+1} 5$. Ma $3a_k$ è proprio a_{k+1}, quindi la formula vale per $n = k + 1$.

Esercizio

Data una progressione geometrica $a_0, a_1, a_2, \ldots$ *con* $a_n = 5, a_{n+1} = 3a_n$*, calcolate* $\sum_{i=0}^n a_i$*.*

- Abbiamo $a_n = 3^n 5$, quindi occorre calcolare $\sum\limits_{i=0}^{n} 3^i 5$.
- Per le proprietà delle sommatorie, $\sum\limits_{i=0}^{n} 3^i 5 = 5\big(\sum\limits_{i=0}^{n} 3^i\big)$.
- Applico la formula $1 + x + \ldots + x^n = \frac{x^{n+1}-1}{x-1}$ con $x = 3$ e ottengo $\sum\limits_{i=0}^{n} 3^i = \frac{3^{n+1}-1}{3-1} = \frac{3^{n+1}-1}{2}$.
- Quindi $\sum_{i=0}^n a_i = \frac{5}{2}(3^{n+1} - 1)$.

Esercizio

Avete 500 euro investiti in banca ad un tasso di interesse del 3%. Quanto avete dopo 10 anni?

- All'inizio ho $a_0 = 1000$ euro.
- Se dopo n anni ho a_n euro, popo $n+1$ anni ho $a_{n+1} = a_n + \frac{2}{100} a_n$ euro, ovvero $a_{n+1} = (1 + \frac{2}{100}) a_n$.
- Per induzione $a_n = 500(1 + \frac{3}{100})^n$.
- Dopo 10 anni ho $a_{10} = 500(1 + \frac{3}{100})^{10}$ euro.

Può essere utile ricordare la disuguaglianza di Bernoulli $(1+x)^n \geq 1 + nx$, quindi $a_{10} \geq 500(1 + \frac{30}{100})$.

Disuguaglianza di Bernoulli

Teorema

$(1+x)^n \geq 1+nx$.

- Induzione su n.
- Caso base. $(1+x)^0 = 1$ e $1+0x = 1$, quindi nel caso $n=0$ la disuguaglianza è vera (e vale anche l'uguaglianza).
- Supponiamo che la disuguaglianza sia vera per $n=k$ e dimostriamola per $n=k+1$.
- Per il caso $n=k$ ho $(1+x)^k \geq 1+kx$.
- Quindi

$$\begin{aligned}(1+x)^{k+1} &= (1+x)^k(1+x)\\ &\geq (1+kx)(1+x)\\ &= 1+x+kx+x^2\\ &\geq 1+(k+1)x\end{aligned}$$

e ho la disuguaglianza nel caso $n=k+1$.

Forse ricordate dalle scuole come trasformare un numero periodico decimale in frazione. Ad esempio $0,\overline{75} = \frac{75}{99}$.

- Posso vedere $0,\overline{75} = 0,757575\ldots$ come $\frac{75}{100} + \frac{75}{100^2} + \frac{75}{100^3} + \ldots = \sum_{k=1}^{\infty} \frac{75}{100^k} = 75 \sum_{k=1}^{\infty} \frac{1}{100^k}$.
- Usando la formula $1 + x + x^2 + \ldots + x^n = \frac{1-x^{n+1}}{1-x}$ e portando 1 dall'altro lato ho

$$\sum_{k=1}^{n} \frac{1}{100^k} = \frac{1}{100} + \frac{1}{100^2} + \ldots + \frac{1}{100^n}$$
$$= \frac{1 - \frac{1}{100}^{n}}{1 - \frac{1}{100}} - 1 \approx \frac{1}{1 - \frac{1}{100}} - 1 = \frac{1}{99}$$

- L'approssimazione è tanto migliore quanto più grande è n, quindi $\sum_{k=1}^{\infty} \frac{1}{100^k} = \frac{1}{99}$.
- Sostituendo ottengo $0,\overline{75} = \frac{75}{99}$.

Esercizio

Trovate due progressioni geometriche che sommate tra loro diano la successione di Fibonacci F_n $(n = 0, 1, 2, \ldots)$ vedi.

Nelle prossime slide spiego come risolverlo.

Successioni definite per ricorrenza lineare

Una successione $a_0, a_1, a_2, \ldots$ verifica una relazione di ricorrenza lineare omogenea di grado 2, se per ogni n vale

$$a_{n+2} = Ra_{n+1} + Sa_n,$$

con R, S numeri fissi (per la successione di Fibonacci $R = S = 1$).

- Associo alla relazione di ricorrenza l'equazione caratteristica

$$x^2 = Rx + S$$

- Le soluzioni dell'equazione caratteristica sono le radici di $x^2 - Rx - S$ (polinomio caratteristico), ovvero

$$x = \frac{R \pm \sqrt{R^2 + 4S}}{2}$$

(se $R^2 + 4S > 0$ vi sono due soluzioni reali).
- Se $x = \alpha$ è una delle radici, ho $\alpha^2 = R\alpha + S$, e moltiplicando per α^n ottengo

$$\alpha^{n+2} = R\alpha^{n+1} + S\alpha^n,$$

quindi la progressione geometrica $a_n = \alpha^n$ verifica la relazione di ricorrenza $a_{n+2} = Ra_{n+1} + Sa_n$.

- Abbiamo visto che se α è una soluzione dell'equazione caratteristica
$$x^2 = Rx + S,$$
la progressione geometrica
$a_0 = 1, a_1 = \alpha, a_2 = \alpha^2, \dots, a_n = \alpha^n, \dots$ verifica la relazione di ricorrenza
$$a_{n+2} = Ra_{n+1} + Sa_n.$$
Ora vediamo come trovarne altre con diverse condizioni iniziali.
- Se a_n verifica la ricorrenza, anche Aa_n la verifica $(n = 0, 1, \dots)$.
- Sommando due successioni a_n e b_n che verificano la ricorrenza se ne ottiene un'altra $c_n = a_n + b_n$ che verifica la ricorrenza
$$\begin{aligned} c_{n+2} &= a_{n+2} + b_{n+2} \\ &= (Ra_{n+1} + Sa_n) + (Rb_{n+1} + Sb_n) \\ &= R(a_{n+1} + b_{n+1}) + S(a_n + b_n) \\ &= Rc_{n+1} + Sc_n \end{aligned}$$
- Quindi una combinazione lineare $Aa_n + Bb_n$ di due successioni a_n e b_n che verificano la ricorrenza, continua a verificarla.

Formula di Binet per i numeri di Fibonacci

Trovate due progressioni geometriche che sommate tra loro diano la successione di Fibonacci F_n $(n = 0, 1, 2, \ldots)$ vedi.

- La relazione di ricorrenza è $F_{n+2} = F_{n+1} + F_n$.
- L'equazione caratteristica è $x^2 = x + 1$.
- Le radici sono $\alpha = \frac{1+\sqrt{5}}{2}$ e $\beta = \frac{1-\sqrt{5}}{2}$.
- Le progressioni geometriche α^n e β^n verificano la relazione, ed anche una loro combinazione lineare $c_n = A\alpha^n + B\beta^n$.
- Impongo le condizioni iniziali $c_0 = F_0 = 0, c_1 = F_1 = 1$.
- $\implies A\alpha^0 + B\beta^0 = 0$ e $A\alpha^1 + B\beta^1 = 1$.
- $\implies \begin{cases} A\alpha + B\beta = 1 \\ A + B = 0 \end{cases} \implies \begin{cases} B = -A \\ A(\alpha - \beta) = 1 \end{cases}$
- $\alpha - \beta = \sqrt{5}$, quindi $A = \frac{1}{\sqrt{5}}$ e $B = -\frac{1}{\sqrt{5}}$.
- $\implies c_n = F_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$.

- Verifico per induzione su n che

$$F_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$$

- Ricordo che $\alpha = \frac{1+\sqrt{5}}{2}$ e $\beta = \frac{1-\sqrt{5}}{2}$ sono le soluzioni di $x^2 = x + 1$.
- Caso $n = 0$: $\frac{1}{\sqrt{5}}\alpha^0 - \frac{1}{\sqrt{5}}\beta^0 = \frac{1}{\sqrt{5}} - \frac{1}{\sqrt{5}} = 0 = F_0$.
- Caso $n = 1$: $\frac{1}{\sqrt{5}}\alpha - \frac{1}{\sqrt{5}}\beta = 1 = F_1$.
- Supponendo che la formula valga per $n = k$ e $n = k + 1$ verifichiamola per $n = k + 2$.

$$\begin{aligned} F_{k+2} &= F_{k+1} + F_k \\ &\frac{1}{\sqrt{5}}\alpha^{k+1} - \frac{1}{\sqrt{5}}\beta^{k+1} + \frac{1}{\sqrt{5}}\alpha^k - \frac{1}{\sqrt{5}}\beta^k \\ &= \frac{1}{\sqrt{5}}\alpha^k(\alpha+1) + \frac{1}{\sqrt{5}}\beta^k(\beta+1) \\ &= \frac{1}{\sqrt{5}}\alpha^k\alpha^2 + \frac{1}{\sqrt{5}}\beta^k\beta^2 \\ &\frac{1}{\sqrt{5}}\alpha^{k+2} + \frac{1}{\sqrt{5}}\beta^{k+2} \end{aligned}$$

Sezioni

Coefficienti binomiali

Definizione

Per $0 \leq i \leq n$, *definiamo* $\binom{n}{i} = \frac{n!}{(n-i)!i!}$

- Ad esempio $\binom{5}{3} = \frac{5!}{2!3!} = \frac{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{(2 \cdot 1)(3 \cdot 2 \cdot 1)} = \frac{5 \cdot 4 \cdot 3}{3 \cdot 2 \cdot 1} = 10$.
- Notiamo che se scambio i con $n - i$ il risultato non cambia. Ad esempio $\binom{5}{2} = \binom{5}{3} = 10$.

Proposizione

- $\binom{n}{0} = \binom{n}{n} = 1$.
- $\binom{n}{i} = \binom{n}{n-i}$.
- $\binom{n}{i} + \binom{n}{i-1} = \binom{n+1}{i}$.

Divisibilità e coefficienti binomiali

Proposizione

Se p è primo, i coefficienti binomiali $\binom{p}{i}$ con $i \neq 0$ e $i \neq p$ sono divisibili per p, mentre $\binom{p}{0} = \binom{p}{p} = 1$.

Dimostrazione

- Per definizione $\binom{p}{i} = \frac{p!}{(p-i)!i!}$.
- Ne segue che $p! = \binom{p}{i}(p-i)!i!$
- Chiaramente p divide $p!$, quindi p deve dividere $\binom{p}{i}(p-i)!i!$
- Un primo divide un prodotto se e solo se divide uno dei fattori.
- Se $i \neq 0$ e $i \neq p$, il primo p non può dividere $(p-i)!$ o $i!$ in quanto entrambe queste quantità sono prodotti di numeri minori di p.
- L'unica possibilità rimasta è che p divida $\binom{p}{i}$.

Triangolo di Tartaglia

$$
\begin{array}{ccccccccccc l}
 & & & & & 1 & & & & & & (x+y)^0 = 1 \\
 & & & & 1 & & 1 & & & & & (x+1)^1 = x+y \\
 & & & 1 & & 2 & & 1 & & & & (x+y)^2 = x^2+2xy+y^2 \\
 & & 1 & & 3 & & 3 & & 1 & & & (x+y)^3 = x^3+3x^2y+3xy^2+y^3 \\
 & 1 & & 4 & & 6 & & 4 & & 1 & & (x+y)^4 = x^4+4x^3y+6x^2y^2+4xy^3+y^4 \\
1 & & 5 & & 10 & & 10 & & 5 & & 1 & (x+y)^5 = x^5+5x^4y+10x^3y^2+10x^2y^3+5xy^4+y^5
\end{array}
$$

- Sui bordi del triangolo ci sono degli 1. Ogni numero interno si ottiene sommando i due numeri che gli stanno immediatamente sopra.
- Nello sviluppo di $(x+y)^n$ il coefficiente di $x^{n-i}y^i$ coincide con l'i-esimo numero della riga n (a partire da $i=0$).
- Tale coefficiente si indica con $\binom{n}{i}$; ad esempio $\binom{5}{2} = \binom{5}{3} = 10$.

Teorema del binomio di Newton

Teorema (Binomio di Newton)

Per ogni $n \in \mathbb{N}$ *si ha* $(x+y)^n = \sum_{i=1}^{n} \binom{n}{i} x^{n-i} y^i$

Dimostrazione

Per induzione su n.

- Per $n = 0$, $\quad \sum_{i=0}^{0} \binom{n}{i} x^i y^{n-i} = \binom{0}{0} x^0 y^{0-0} = 1 = (x+y)^0$.
- Dimostriamo il caso $n+1$ assumendo per ipotesi induttiva il caso n.
- Il caso $n+1$ è $(x+y)^{n+1} = \sum_{i=1}^{n+1} \binom{n+1}{i} x^{n+1-i} y^i$.
- Per passare dal caso n al caso $n+1$ faremo uso della formula $\binom{n}{j} + \binom{n}{j-1} = \binom{n+1}{j}$ (valida per $0 < j \leq n$).
- I calcoli sono nella pagina seguente. Il passaggio evidenziato in rosso è un cambio di indici che ha il fine di avere il monomio $x^{n+1-j} y^j$ in entrambe le sommatorie in modo da poterle riunire in un'unica sommatoria sommando i rispettivi coefficienti.

$$
\begin{aligned}
(x+y)^{n+1} &= x(x+y)^n + y(x+y)^n \\
&= x\sum_{i=0}^{n}\binom{n}{i}x^{n-i}y^i + y\sum_{i=0}^{n}\binom{n}{i}x^{n-i}y^i \\
&= \sum_{i=0}^{n}\binom{n}{i}x^{n+1-i}y^i + \sum_{i=0}^{n}x^{n-i}y^{i+1} \\
&= x^{n+1} + \sum_{i=1}^{n}\binom{n}{i}x^{n+1-i}y^i + \sum_{i=0}^{n-1}\binom{n}{i}x^{n-i}y^{i+1} + y^{n+1} \\
&= x^{n+1} + \sum_{j=1}^{n}\binom{n}{j}x^{n+1-j}y^j + \sum_{j=1}^{n}\binom{n}{j-1}x^{n+1-j}y^j + y^{n+1} \\
&= x^{n+1} + \sum_{j=1}^{n}\binom{n+1}{j}x^{n+1-j}y^j + y^{n+1} \\
&= \sum_{j=0}^{n+1}\binom{n+1}{j}x^{n+1-j}y^j \quad \square
\end{aligned}
$$

Esercizi

Esercizio

- *Se si sommano i numeri della riga n (a partire da* 0*) del triangolo di Tartaglia si ottiene* 2^n*. Ad esempio la riga* 6 *contiene i numeri* $1, 6, 15, 20, 15, 6, 1$ *e la loro somma è* 2^6*.*
- *Se si sommano i numeri di una riga con segni alterni si ottiene zero:* $1 - 6 + 15 - 20 + 15 - 6 + 1 = 0$*.*

Sezioni

Binomio di Newton mod p

Lemma

Se p è primo, $(x+y)^p \equiv x^p + y^p \bmod p$.

Dimostrazione

- Per il binomio di Newton $(x+y)^p = \sum_{i=1}^{p} \binom{p}{i} x^{p-i} y^i$.
- Poiché p è primo, per una proposizione precedente tutti i coefficienti binomiali $\binom{p}{i}$ tranne quello con $i = 0$ o $i = p$ sono multipli di p.
- Quindi nella sommatoria tutti i termini si cancellano mod p tranne il primo e l'ultimo: $(x+y)^p \equiv \binom{p}{0} x^p + \binom{p}{p} y^p \bmod p$.
- Siccome $1 = \binom{p}{0} = \binom{p}{p}$, ottengo $(x+y)^p \equiv x^p + y^p \bmod p$.

Piccolo teorema di Fermat

Teorema

Se p è primo, per ogni intero x si ha $x^p \equiv x \mod p$.

Dimostrazione

- Dimostriamo prima il caso $x \geq 0$. Lo facciamo per induzione su x.
- Il caso base (con $x = 0$) è facile: $0^p \equiv 0 \mod p$.
- Supponiamo per ipotesi induttiva di avere $x^p \equiv x \mod p$ per un certo x e dimostriamo $(x+1)^p \equiv (x+1) \mod p$.
- Per un lemma precedente $(x+1)^p \equiv x^p + 1^p \mod p$.
- Visto che $1^p = 1$, e per l'ipotesi induttiva $x^p \equiv x \mod p$, ottengo $(x+1)^p \equiv (x+1) \mod p$.
- Ho così dimostrato il teorema per gli $x \geq 0$.
- La dimostrazione per i negativi è nella pagina seguente.

Dimostrazione di $x^p \equiv x \bmod p$ per $x < 0$.

- Se x è negativo, scrivo $x = -n$ con n positivo.
- Faccio prima il caso in cui il primo p sia diverso da 2, quindi dispari. In questo caso $(-1)^p = -1$ e quindi $(-n)^p = -n^p$.
- Siccome n è positivo, $n^p \equiv n \bmod p$ per quanto già dimostrato.
- Cambiando i segni di entrambi i lati della congruenza ottengo $x^p \equiv x \bmod p$.
- Resta il caso in cui $p = 2$.
- In questo caso la congruenza diventa $x^2 \equiv x \bmod 2$.
- Ovviamente funziona per $x = 0$ e $x = 1$, e visto che ogni intero è congruo a 0 o 1 vale in tutti i casi.

Sezioni

Teorema di Eulero

Teorema (Teorema di Eulero)

Se $x \in \mathbb{Z}$ è invertibile modulo n, allora $x^{\phi(n)} \equiv 1 \bmod n$.

Dimostrazione

- Siano $a_1, \ldots, a_k$ gli interi positivi minori di n invertibili modulo n. Per definizione della ϕ ve ne sono $\phi(n)$, quindi $k = \phi(n)$.
- Fisso x invertibile mod n. Mostro che $x^k \equiv 1 \bmod n$.
- Considero i k numeri $xa_1, \ldots, xa_k$. Il prodotto di invertibili è invertibile, quindi $xa_1, \ldots, xa_n$ sono invertibili. I loro resti mod n sono tutti diversi tra loro in quanto se $xa_i \equiv xa_j \bmod n$, moltiplicando per l'inverso di x avrei $a_i \equiv a_j \bmod n$, cosa impossibile se $i \neq j$.
- Salvo l'ordine, i resti mod n dei numeri $xa_1, \ldots, xa_k$ devono dunque coincidere con gli elementi dell'insieme $\{a_1, \ldots, a_k\}$.
- Ne seque che i prodotti dei due rispettivi insiemi coincidono mod n, ovvero

$$xa_1 \cdot \ldots \cdot xa_k \equiv a_1 \cdot \ldots \cdot a_k \bmod n.$$