Algebra I

Paolo Bettelini

Contents

1 Richiami di teoria degli insiemi

Data una famiglia finita o infinite di insiemi $\{A_i\}_{i\in I}$, la loro intersection

$$\bigcap_{i\in I} A_i$$

è l'insieme degli elementi che stanno in tutti gli insiemi A_i, mentre la loro unione

$$\bigcup_{i\in I} A_i$$

è l'insieme degli elementi che stanno in almeno uno degli insiemi A_i.

2 Classi di equivalenza

Esempio insieme quoziente $\sim$ su $\mathbb{Z}$ dove $a \sim b \iff |a| = |b|$ è dato da

$$\{\{0\}, \{1, -1\}, \{2, -2\}, \cdots\}$$

L'unica relazione di equivalenza che è un ordine è l'uguaglianza.

3 Esempi di maggiorante etc.

In $\mathbb{R}$ consideriamo l'usuale ordinamento. Consideriamo i sottoinsiemi

$$A = \{x \in \mathbb{R} \,|\, x > 0\}$$

$$B = \{x \in \mathbb{R} \,|\, x \geq 0\}$$

e

$$C = \{x \in \mathbb{R} \,|\, 0 < x \leq 2\}$$

Il sottoinsieme A non ha maggioranti. Ogni numero non-positivo è minorante di A. A non ha nè massimo nè minimo.

Il sottoinsieme B non ha maggioranti. Ogni numero non-positivo è minorante di B. B ha 0 come minimo.

Il sottoinsieme C ha minoranti e maggioranti ma non minimo e ho 2 come massimo.

Consideriamo ora la relazione di divisibilità in $\mathbb{N}$. L'unico maggiorante è 0 in quanto tutti dividono zero, ed è un massimo. Il numero 1 è minorante, ed è un minimo.

Se ora prendiamo l'insieme $\{2, 3, 4, 5\}$, i maggioranti sono mulitpli del minimo comune multiplo (60), i minoranti sono i divisori comuni. Non ci sono massimo e minimo.

Proposition Il massimo è unico

Il massimo, se esiste, è unico.

Proof Il massimo è unico

Diciamo che a, b sono due massimi di A, cioè maggioranti di A che appartiene ad A. Abbiamo allora $a \geq b$ (in quanto a è un maggiorante) e $b \geq a$ (in quando b è un maggiorante). Abbiamo quindi che $a = b$.

Definizione Massimale

Un elemento $a \in A$ con A insieme partzialmente ordinato è detto massimale in A se non esiste alcun $b \in A$ tale che $a \leq b$ dove $a \neq b$.

Definizione Minimale

Un elemento $a \in A$ con A insieme partzialmente ordinato è detto minimale in A se non esiste alcun $b \in A$ tale che $a \geq b$ dove $a \neq b$.

Ogni massimo è massimale, ogni minimo è minimale.

Esempio in cui i massimali non sono massimi: in $\mathbb{N}$, rispetto alla divisibilità, consideriamo l'insieme $A = \{2, 3, 4, 5, 6\}$.

- Il numero 2 è minimale ma non massimale.
- Il numero 3 è minimale ma non massimale.
- Il numero 4 è massimale perché non divide nient'altro, ma non minimale.
- Il numero 5 è sia massimale che minimale.
- Il numero 6 è massimale ma non minimale.

In una relazione d'ordine totale un eventuale elemento massimale è massimo. Infatti, se a è massimale per A, preso un qualsiasi elemento $b \in A$, sappiamo che vale almeno una tra $a \leq b$ e $b \leq a$. Se vale la prima, per la definizione di massimalità di a, non può essere $a \neq b$. Nel secondo caso, $b \leq a$ e quindi a è un massimo. Analogamente per i minimali.

3.1 Relazioni irriflessiva

Data una relazione d'ordine $\leq$, possiamo ottenere la relazione d'ordine stretta $<$ dicendo che $a < b$ se $a \leq b$ e $a \neq b$.

Si può definire l'ordine stretto rimpiazzando la proprietà riflessiva con quella irriflessiva.

4 Funzioni

Una funzione $\phi\colon A \to B$ dove A è il dominio mentre B è il codominio, preso un elemento $a \in A$, la sua immagine viene denotata $\phi(a)$ oppure af.

Se $C \subseteq A$, la sua immagine tramite ϕ è indicata come $C\phi$ che è un sottoinsieme di B.

$$C\phi = \{c\phi \mid c \in C\}$$

Se D è un sottoinsieme di B, la sua immagine inversa tramite ϕ è il sottoinsieme $D\phi^{-1}$ di A degli elementi la cui immagine appartiene a D.

$$D\phi^{-1} = \{a \in A \mid a\phi \in D\}$$

Esempio Funzione

Sia $\phi\colon \mathbb{R} \to \mathbb{R}$ definita ponendo $\phi x \triangleq x^2$.

Consideriamo ora $A = \{-1, 0, 1, 2\}$. Abbiamo allora $A\phi = \{1, 0, 4\}$. Consideriamo poi $B = \{-1, 0, 2, 9\}$. Abbiamo allora $B\phi^{-1} = \{0, \sqrt{2}, 3, -3\}$.

L'immagine di una funzione è chiaramente l'immagine per il suo dominio come insieme considerato.

4.1 Proprietà

Proposition

Se $C \subseteq D \subseteq A$, abbiamo $C\phi \subseteq D\phi$.

Proof

Abbiamo che

$$C\phi = \{c\phi \mid c \in C\}$$

Dunque $x \in C\phi$ se e solo se esiste $c \in C$ tale che $x = c\phi$. Ma $C \subseteq D$, dunque $c \in D$. Quindi, $x = c\phi \in D\phi$.

Non è detto che se $C \subset D$ allora $C\phi \subset D\phi$. Mostriamo un esempio in cui $C \subset D$ ma $C\phi = D\phi$. Prendiamo $C = \{1\} \subset D = \{1, -1\}$. Se prendiamo la funzione del quadrato, in ambo caso trovo la stessa immagine per via di ambo gli insiemi.

Ciò non avviene nel caso in cui la funzione fosse iniettiva.

Proposition

Se $E \subseteq F \subseteq B$, abbiamo che $E\phi^{-1} \subseteq F\phi^{-1}$.

TODO: esercizio proof.

Anche qui la medesima proposizione ma con l'inclusione stretta non è assicurata.

Proposition

Se $C \subseteq A$, allora $C\phi\phi^{-1} \supseteq C$.

Proof

Sia $x \in C$. Bisogna mostrare $x \in C\phi\phi^{-1}$. Ricordiamo che $D\phi^{-1} = \{y \in A \,|\, y\phi \in D\}$. Dunque $Cy\phi = \{y \in A \,|\, y\phi \in C\phi\}$. Ma ora $x\phi \in C\phi$, perché $x \in C$. Dunque $x \in C\phi\phi^{-1}$.

Nel solito esempio

$$\{1, -1\}\phi\phi^{-1} = \{1, -1\}$$

e

$$\{1\}\phi\phi^{-1} = \{1, -1\}$$

Proposition

Se $D \subseteq B$ allora $D\phi^{-1}\phi \subseteq D$. L'inclusione può essere stretta.

Proof

Sia $x \in D\phi^{-1}\phi$. Ciò significa che $x = z\phi$ per qualche $z \in D\phi^{-1}$. Ma $D\phi^{-1} = \{y \,|\, y\phi \in D\}$. Dunque, $z \in D\phi^{-1}$, allora $z\phi \in D$, cioè $x \in D$.

Con il solito esempio

$$\{1, 2\}\phi^{-1}\phi = \{1\}$$
$$\{-1\}\phi^{-1}\phi = \emptyset$$

Proposition

Siano $\phi\colon A \to B$, $\psi\colon B \to C$ e $\theta\colon C \to D$ funzioni. allora

$$(\phi\psi)\theta = \phi(\psi\theta)$$

Proof

Notiamo che $\phi\psi\colon A \to C$ e $\theta\colon C \to D$. Dunque $\phi\psi\colon A \to D$. Analogamente $\phi\colon A \to B$, $\psi\theta\colon B \to D$ e quindi $\phi(\psi\theta)\colon A \to D$. Per mostrare l'uguaglianua devo mostrare che per ogni $x \in A$ risulta

$$a((\phi\psi)\theta) = a(\phi(\psi\theta))$$

Abbiamo infatti $a((\phi\psi)\theta) = (a(\phi\psi\theta)) = ((a\phi)\psi)\theta$ e $a(\phi(\psi\theta)) = (a\phi)(\psi\theta) = ((a\phi)\psi)\theta$.

Dunque possiamo scrivere semplicemente $\phi\psi\theta$ senza ambiguità.

Siano $\phi\colon A \to B$, $\psi\colon B \to C$ funzioni. Ci chiediamo ora che $\psi\phi = \phi\psi$. Chiaramente, non è detto che $\phi\psi$ esista. Possiamo confrontarle solo che $A = B$.

Allora guardiamo $\phi\colon A \to A$ e $\psi\colon A \to A$. Non è comunque detto che $\psi\phi = \phi\psi$ siano uguali.

Definizione Funzione identità

Dato un insieme A, la *funzione identica* di A è la funzione $\mathrm{Id}_A\colon A \to A$ definita come $a\mathrm{Id}_A \triangleq a$.

Proposition

Sia $\phi\colon A \to B$, allora $\phi\mathrm{Id}_B = \phi$ e $\mathrm{Id}_A\phi = \phi$. TODO: dimostrazione.

4.2 Iniettività suriettività

La definizione di iniettività è equivalente a dire che $b\phi^{-1}$ contiene solo un elemento.
La definizione di suriettività è equivalente a dire che $b\phi^{-1}$ contiene almeno un elemento.
La definizione di suriettività è equivalente a dire che $b\phi^{-1}$ e $b\phi$ contengono solo un elemento.

4.3 Composizione

Date f e g cosa possiamo dire di f e g sapendo che $g(f)$ è suriettiva o iniettiva?

Supponiamo che $g(f)$ sia suriettiva. Dunque, per ogni $c \in C$ esiste a tale che $c = g(f(a))$. In particolare, posto $b = f(a) \in B$, abbiamo che $g(b) = c$ cioè g è suriettiva.

Supponiamo che $g(f)$ sia iniettiva. Dunque, per ogni $a_1, a_2 \in A$ dove $a_1 \neq a_2$, risulta che $g(f(a_1)) \neq g(f(a_2))$. Sicuramente la prima funzione non può fare convergere i due elementi, in quando non potrebbero uscire separati dopo la seconda funzione. In particolare, $f(a_1) \neq f(a_2)$. Quindi, f è iniettiva.

Esempio

Siano $A = \{a\}$ e $B = \{b, b'\}$ con $b \neq b'$, $C = \{c\}$e $f\colon A \to B$ data $f(a) = b$ e $g\colon B \to C$ data $g(b) = c$ e $g(b') = c$. Allora $g(f)$ è biettiva. f è iniettiva e g non è iniettiva. f non è suriettiva e g è suriettiva.

4.4 Definizione di invertibilità

Data $f\colon A \to B$, allora f è invertibile se esiste $g\colon B \to A$ tale che $g(f)$ è la funzione identità su A e $f(g)$ è la funzione identità su B.

Proposition

Se f è invertibile, allora g è unica.

Proof

Prendiamo $h\colon B \to A$ tale che $h(f(a)) = a$ e $f(h(b)) = b$. Allora $g = g\mathrm{Id}_A = g(fh) = (gf)h = \mathrm{Id}_B h = h$ e quindi è la funzione identità.

Proposition

Ogni inverso è anch'esso invertibile ${f^{-1}}^{-1}$.

Proposition

Se $f\colon A \to B$ e $g\colon B \to C$ sono invertibili, allora $g(f)$ è invertibile e $(g(f))^{-1} = f^{-1}(g^{-1})$.

Proof

Sappiamo che esistono f^{-1} e g^{-1}. Dunque esiste $f^{-1}(g^{-1})$. Mostriamo che componendo le due in maniera simmetrica si trovano le identità di A e di B.

Proof Invertibilità è equivalente a biettività

($\Longrightarrow$) Sia f invertibile. Allora sappiamo che $f(f^{-1})$ è la funzione identità di A e $f^{-1}(f)$ è la funzione identità di B. Ora, l'identità di A è iniettiva (anche biettiva), dunque f è iniettiva e l'identità di B è suriettiva (dalle due proposizioni di prima), dunque f è suriettiva.

($\Longleftarrow$) Sia f biettiva. Dobbiamo costruire $g\colon B \to A$ tale che $f(g)$ è l'identità di A e $f(g)$ è l'identità di B. Sappiamo che per ogni $b \in B$ esiste un unico $a \in A$ tale che $f(a) = b$. Poniamo allora $g(b) = a$. Se $b \in B$, allora $f(g(b)) = f(a) = b$. Se $a \in A$, abbiamo che $g(f(a))$ è per definizione di g l'unico elemento $a' \in A$ tale che $f(a') = f(a)$. Siccome f è iniettiva, $a' = a$, e quindi $g(f(a)) = a$ e quindi $g = f^{-1}$.

5 Matrici

Data una matrice A indichiamo con $A_{i,j}$ l'emenento di posto (i,j).

La trasporta di una triangolare inferiore è triangolare superiore, e viceversa. La trasporta di una matrice diagonale rimane uguale.

Una matrice uguale alla sua trasporta è detta simmetrica.

Definizione

Dato un anello commutativo R diciamo $M_{m,n}(R)$ l'insieme delle matricii $m \times n$ a coefficienti in R.

L'addizione è associativa e commutativa (come nell'anello commutativo). Esiste l'elemento neutro (matrice nulla $0_{m,n}$). Esiste l'elemento inverso $-A = -1 \cdot A$. Si dovrebbe dimostrare l'unicità dell'elemento inverso e del neutro.

Proposition

Date matrici A e B della stessa dimensione, si ha

$$(A+B)^t = A^t + B^t$$

Teorema Moltiplicazione associativa

Se $A \in M_{m,n}(R)$ e $B \in M_{n,p}(R)$ e $C \in M_{p,r}(R)$, allora

$$(AB)C = A(BC)$$

Proof Moltiplicazione associativa

AB è di tipo $m \times p$. L'elemento di posto (i,j) è

$$\sum_{k=1}^{n} A_{i,j} B_{k,j} = D_{i,j}$$

La matrice $(AB)C$ ha dimensione $m \times r$. L'elemento di posto (i,l) è

$$\begin{aligned} \sum_{j=1}^{p} D_{i,j} C_{j,l} &= \sum_{j=1}^{n} \left(\sum_{k=1}^{n} A_{i,k} B_{k,j} \right) C_{j,l} \\ &= \sum_{j=1}^{p} \sum_{k=1}^{n} A_{i,k} B_{k,j} C_{j,l} \end{aligned}$$

BC è ha dimensione $n \times r$. L'elemento di post (k,l) è

$$\sum_{j=1}^{p} B_{k,j} C_{j,e} = E_{k,e}$$

$A(BC)$ ha dimensione $m \times r$. L'elemento di posto (i,l) è

$$\begin{aligned} \sum_{k=1}^{n} A_{i,k} E_{k,l} &= \sum_{k=1}^{n} A_{i,k} \left(\sum_{j=1}^{p} B_{k,j} C_{j,e} \right) \\ &= \sum_{k=1}^{n} \sum_{j=1}^{p} A_{i,k} B_{k,j} C_{j,e} \end{aligned}$$

Proposition Distributività destra

Con $A, B \in M_{m,n}(R)$ e $C \in M_{n,p}(R)$

$$(A+B)C = AC + BC$$

Proposition Distributività sinistra

Con $A, B \in M_{m,n}(R)$ e $C \in M_{n,p}(R)$

$$A(B+C) = AB + AC$$

In generale non vale $AB = BA$. Ambo le operazioni sono definite solo se ambo le matrici sono quadrate con dimensione $n \times n$. In tal caso, non è comunque detto che la proprietà valga. Nel caso in cui $n = 1$ la proprietà commutativa vale necessariamente.

Il principio di annullamento del prodotto non vale.

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

In questo caso il risultato è la matrice nulla ma nessuno dei due era nulla.

Proposition

Se A e B sono invertibili e dello stesso ordine, allora AB è invertibile e $(AB)^{-1=B^{-1}A^{-1}}$.

Esempio Matrice non invertibile

$$\begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix} \begin{bmatrix} x & y \\ z & w \end{bmatrix} = \begin{bmatrix} x+2z & y+2w \\ 2x+4z & 2y+4w \end{bmatrix}$$

Notiamo che i punti dove dovrebbe esserci uno 0 sono il doppio di quelli con 1, quindi non vi è soluzione e non è invertibile.

Se A e B sono due matrici quadrate della stessa dimensione tali che $AB = I_n$ allora anche $BA = I_n$ (La dimostrazione non è banale).

Proposition

Se $A \in M_{m,n}(R)$ e $B \in B_{n,p}(R)$ allora $B^t A^t \in M_{p,m}(R)$. Abbiamo quindi che

$$B^t A^t = (AB)^t$$

Proposition

Se A è invertibile, allora

$$(A^t)^{-1} = (A^{-1})^t$$

6 Numeri naturali

Definizione Assiomi di Peano

I numeri naturali sono un insieme $\mathbb{N}$ dotati di una funzione successore $S\colon \mathbb{N} \to \mathbb{N}$ e di un elemento fissato 0 tali che:

- la funzione S è iniettiva;
- $0 \notin \mathrm{Im}_S$;
- se $A \subseteq \mathbb{N}$ tale che $0 \in A$ e $As \subseteq A$, allora $A = \mathbb{N}$;

L'esistenza di un tale insieme è garantita dalla teoria assiomatica. Tuttavia, dobbiamo garantire che i modelli degli assiomi di Peano siano isomorfi, quindi trovare una funzione biettiva fra tutti i modelli. Quindi, dati due modelli $(\mathbb{N}, S, 0)$ e $(\mathbb{N}', S', 0')$ bisogna trovare una funzione biettiva $f\colon \mathbb{N} \to \mathbb{N}'$ tale che $f(0) = 0'$ e $nfs' = nsf$

$$\begin{array}{ccc} n & \xrightarrow{f} & n' \\ {\scriptstyle s}\downarrow & & \downarrow{\scriptstyle s'} \\ ns & \xrightarrow[f]{} & n's' \end{array}$$

Questo può essere fatto con un procedimento cosidetto per ricorrenza, dipende fortemente dall'assioma 3. In generale gli assiomi di Peano mi permettono di definire successioni di oggetti per ricorrenza, cioè assegnando un oggetto associato a 0 e il modo di costruire l'oggetto associato (come per esempio il fattoriale o l'addizione nei naturali).

La somma è definita nel seguente modo ricorrente: $m + n = 0$ e $m + S(n) = S(m + n)$.

Usango gli assiomi posso dimsotrare varie proprietà dell'addizione, detta moltiplicazione (da definire anch'esso per ricorrenza) e dell'ordine (anch'esso da definire per ricorrenza).

L'ordine è definito solamente da $n \leq S(n)$.

Le proprietà per $m, n, p \in \mathbb{N}$ sono:

1. **somma associativa:** $(m + n) + p = m + (n + p)$;
2. **somma distributiva:** $m + n = n + m$;
3. **somma nulla:** $m + 0 = m$;
4. **prodotto associativo:** $(mn)p = m(np)$;
5. **prodotto distributivo:** $mn = nm$;
6. **prodotto nullo:** $mS(0) = m$;
7. **distributiva:** $(m + n)p = mp + np$;
8. **cancellazione somma:** $m + n = m + p \implies n = p$;
9. **cancellazione prodotto:** $mn = mp \land m \neq 0 \implies n = p$;
10. **compatibilità tra somma e ordine:** $m \leq n \implies m + p \leq n + p$;
11. **compatibilità tra prodotto e ordine:** $m \leq n \implies mp \leq np$;

Detto 1 il numero $S(0)$ risulterà che $S(n) = n + 1$.

Assioma 3:

Proposition

Un altro modo per dire l'assioma 3 è che ogni sottoinsieme non vuoto di $\mathbb{N}$ ammette un minimo.

Proof

Per dimostrarlo sia $A \subseteq B$ l'insieme di tutti i minoranti. L'insieme A contiene sicuramente 0. Infatti, $0 \leq n$ per ogni $n \in \mathbb{N}$. L'insieme A è diverso da $\mathbb{N}$. Infatti, preso un $n \in B$, sappiamo che $B \neq \emptyset$, abbiamo che $n+1$ non è minore o uguale di n, quindi non è un minorante di B. Pertanto $n+1 \notin A$. Sappiamo per gli assiomi di Peano che un sottoinsieme di $\mathbb{N}$ che contiene 0 e contiene il successore di ogni elemento, coincide con $\mathbb{N}$. Poiché $0 \in A$ e $A \neq \mathbb{N}$, possiamo concludere che esiste $k \in A$ tale che $k+1 \notin A$, cioè k è minorante di B ma $k+1$ no. Ma allora esiste $i \in A$ tale che $k+1 \not\leq i$. Poiché l'ordine è totale, ciò significa che $i < k+1$. D'altra parte k è minorante di B. In particolare, $k \leq i$, che è minore di $k+1$. Per la proprietà dell'ordine dei naturali, si ha che $k = 1$, cioè $k \in B$. Dunque, k è minorante di B che appartiene a B come volevamo (è il nostro minimo).

Non è necessario l'assioma della scelta per prendere $n \in B$ in quando B è ben definito e sappiamo come sceglierlo.

7 Numeri interi

Fatto l'anello commutativo degli interi si possono dimostrare delle proprietà come ad esempio $n \cdot 0 = 0$ per ogni n.

Per dimostrare invece il principio di annullamento del prodotto, cioè che $mn = 0$ se e solo se almeno uno tra m e n è 0. In alcuni anelli commutativi il principio di annullamento del prodotto non vale.

Si dimostra poi che dato $n \in \mathbb{Z}$, si ha che $n \in \mathbb{Z}$ oppure $0 - nn \in \mathbb{Z}$ per ogni n intero. Si pone allora

$$|n| = \begin{cases} n & \text{è un naturale} \\ -n & \text{altrimenti} \end{cases}$$

Una volta introdotto l'ordine negli interi (compatibile con quello dei naturali), si dimostrano queste proprietà:

1. $a \leq b \implies a + c \leq b + c$;
2. $a \leq b \land c \geq 0 \implies ac \leq bc$;
3. $|a + b| \leq |a| + |b|$;
4. $|a \cdot b| \leq |a| \cdot |b|$.

7.1 Divisione con resto

Estendiamo l'mcd a valori tutti nulli. Dati due interi il loro mcd è il numero naturali d che divide entrambi ed è multiplo di tutti i divisori comuni. Se almeno uno tra questi è nullo, questo coincide con la definizione precedente. Se tutti sono zero, definiamo l'mcd come zero, in quanto zero è un multiplo di zero.

7.2 Massimo comun divisore

Dimostrare l'esistenza di un massimo comune divisore su più interi per induzione: il caso base è quello in cui il numero di interi è 2. Usare l'esistenza del membro a destra e verificare che soddisfa la definizione.

8 Classi di resto

Consideriamo i non-multipli di 3. La differenza fra un non-multiplo di 3 e quello dopo è o 1 o 2. Dividiamo allora i non-multipli di 3 saltando 2 a 2, ossia

$$-5, -2, +1, +4, +7, +10$$

e

$$-4, -1, +2, +5, +8, +11$$

La somma di due numeri corrispondenti è sempre un numero di 3. In generale, se considero le tre liste

$$-6, -3, +0, +3, +6, +9 - 5, -2, +1, +4, +7, +10$$
$$-4, -1, +2, +5, +8, +11$$

Se facciamo la somma di due termini, la lista in cui è il risutato è dato solamente dalle liste dei due addenti.

8.1 Funzione di Eulero

Sia $[a]_n$ invertibile. Classi inveritbili di $\mathbb{Z}/n$ siano

$$[b_1]_n, [b_2]_n, \cdots, [b_{\varphi(n)}]_n$$

Ora

$$[a]_n[b_1]_n, [a]_n[b_2]_n, \cdots, [a]_n[b_{\varphi(n)}]_n$$

1. Siccome il prodoto di due invertibili è invertibile, queste due sono tutte invertibili
2. Poiché $[a]_n$ è invertibile, per la legge di cancellazione, le classi della seconda lista sono tutte diverse.
3. (1+2) implicano che la prima e la seconda lista coincidano a mano dell'ordinamento.

Dunque,

$$\dots$$

Abbiamo quindi dimostrato il teorema di Eulero

Teorema

Se a è un intero coprimo con n, allora

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

Corollario Piccolo teorema di Fermat

Sia p un primo e a un intero. Allora

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

Proof

Se a è coprimo con p, per il teorema di Eulero abbiamo che $a^{\varphi(p)} \equiv 1 \pmod{p}$. Ma $\varphi(p) = p - 1$ poiché p è primo e, dunque, $a^{p-1} \equiv 1 \pmod{p}$ da cui, moltiplicando per a, si ottiene $a^p \equiv a \pmod{p}$.
Se a non è coprimo con p, allora $p \mid a$, cioè $a \equiv 0 \pmod{p}$ e, quindi, ogni potenza con esponente positivo di a è congruo a $0 \pmod{p}$. In particolare, $a^p \equiv 0 \pmod{p}$.