Potenze, gruppi ciclici e spazi quoziente

Gregorio D'Agostino

3 Aprile 2020

Calcolo delle potenze

Gruppi Quoziente

Calcolo delle potenze

- In molte occasioni è necessario calcolare le potenze di un elemento A di un gruppo G ad una potenza n. Il gruppo può non essere numerico e nemmeno abeliano. Vedremo il prodotto a sinistra, ma il ragionamento è analogo per il prodotto a destra.

Calcolo delle potenze

- In molte occasioni è necessario calcolare le potenze di un elemento A di un gruppo G ad una potenza n. Il gruppo può non essere numerico e nemmeno abeliano. Vedremo il prodotto a sinistra, ma il ragionamento è analogo per il prodotto a destra.
- L'algoritmo più semplice consiste nello iterare il prodotto (a sinistra) per A:

$$A^{k+1} = A \cdot A^k.$$

Calcolo delle potenze

- In molte occasioni è necessario calcolare le potenze di un elemento A di un gruppo G ad una potenza n. Il gruppo può non essere numerico e nemmeno abeliano. Vedremo il prodotto a sinistra, ma il ragionamento è analogo per il prodotto a destra.
- L'algoritmo più semplice consiste nello iterare il prodotto (a sinistra) per A:
$$A^{k+1} = A \cdot A^k.$$
- Questo algoritmo richiede $n-1$ prodotti e una allocazione di memoria pari a 3 volte quella dell'elemento A. Se A è un numero intere servono 3 interi. Se A è una matrice di interi 5x5 serviranno 3 x(5x5)=75 interi.

Potenze di Operatori

- Ad ogni elemento A è associato un operatore lineare T_A:

$$T_A(B) \stackrel{def}{=} A \cdot B.$$

Potenze di Operatori

- Ad ogni elemento A è associato un operatore lineare T_A:

$$T_A(B) \stackrel{def}{=} A \cdot B.$$

- Per il calcolo dell'azione dell'operatore iterato n volte occorrono n passi:

$$T_A^{(n)}(B) \stackrel{def}{=} \overbrace{T_A(\ldots T_A(B)\ldots)}^{n \text{ volte}} = T_A(T_A^{(n-1)}(B)) = A \cdot T_A^{(n-1)}(B).$$

Calcolo Rapido delle potenze.

- Dobbiamo calcolare $B = A^k$:

Calcolo Rapido delle potenze.

- Dobbiamo calcolare $B = A^k$:
- Scriviamo k in formato binario (naturale sui computer). Poniamo $m = [\log_2(k)]$ (nextpow già studiato).

$$k = \sum_{i=0,m} b_i 2^i :$$

Calcolo Rapido delle potenze.

- Dobbiamo calcolare $B = A^k$:
- Scriviamo k in formato binario (naturale sui computer). Poniamo $m = [\log_2(k)]$ (nextpow già studiato).

$$k = \sum_{i=0,m} b_i 2^i :$$

- Si può riscrivere:

$$k = b_0 + 2(b_1 + 2(b_2 + \cdots 2b_m)))));$$

- Esponenziando

$$A^k = A^{b_0+2(b_1+2(b_2+\cdots 2b_m)))};$$

Calcolo Rapido delle potenze.

- Dobbiamo calcolare $B = A^k$:
- Scriviamo k in formato binario (naturale sui computer). Poniamo $m = [\log_2(k)]$ (nextpow già studiato).

$$k = \sum_{i=0,m} b_i 2^i :$$

- Si può riscrivere:

$$k = b_0 + 2(b_1 + 2(b_2 + \cdots 2b_m)))));$$

- Esponenziando

$$A^k = A^{b_0+2(b_1+2(b_2+\cdots 2b_m)))};$$

- Che equivale a:

$$A^k = A^{b_0} * (A^2)^{(b_1)} * (A^4)^{(b_2)} \cdots (A^{2^m})^{b_m}.$$

Calcolo Rapido delle potenze: algoritmo

- Vediamo uno schema per l'algoritmo per il calcolo di $B = T_A^{(k)} A_0 = A^k A_0$ (ad esempio $B = A^k$)

Calcolo Rapido delle potenze: algoritmo

- Vediamo uno schema per l'algoritmo per il calcolo di $B = T_A^{(k)} A_0 = A^k A_0$ (ad esempio $B = A^k$)
- Inizializzazione: B=I (in generale $B = A_0$);

Calcolo Rapido delle potenze: algoritmo

- Vediamo uno schema per l'algoritmo per il calcolo di $B = T_A^{(k)} A_0 = A^k A_0$ (ad esempio $B = A^k$)
- Inizializzazione: B=I (in generale $B = A_0$);
- Ciclo: y=mod(k,2) (legge primo bit a dx di k)

Calcolo Rapido delle potenze: algoritmo

- Vediamo uno schema per l'algoritmo per il calcolo di $B = T_A^{(k)} A_0 = A^k A_0$ (ad esempio $B = A^k$)
- Inizializzazione: B=I (in generale $B = A_0$);
- Ciclo: y=mod(k,2) (legge primo bit a dx di k)
- if (y != 0) B=A*B (in generale $B = T_A(B)$);

Calcolo Rapido delle potenze: algoritmo

- Vediamo uno schema per l'algoritmo per il calcolo di $B = T_A^{(k)} A_0 = A^k A_0$ (ad esempio $B = A^k$)
- Inizializzazione: B=I (in generale $B = A_0$);
- Ciclo: y=mod(k,2) (legge primo bit a dx di k)
- if (y != 0) B=A*B (in generale $B = T_A(B)$);
- A=A*A

Calcolo Rapido delle potenze: algoritmo

- Vediamo uno schema per l'algoritmo per il calcolo di $B = T_A^{(k)} A_0 = A^k A_0$ (ad esempio $B = A^k$)
- Inizializzazione: B=I (in generale $B = A_0$);
- Ciclo: y=mod(k,2) (legge primo bit a dx di k)
- if (y != 0) B=A*B (in generale $B = T_A(B)$);
- A=A*A
- k=(k-y)/2; (shift a dx di 1 passo).

Calcolo Rapido delle potenze: algoritmo

- Vediamo uno schema per l'algoritmo per il calcolo di $B = T_A^{(k)} A_0 = A^k A_0$ (ad esempio $B = A^k$)
- Inizializzazione: B=I (in generale $B = A_0$);
- Ciclo: y=mod(k,2) (legge primo bit a dx di k)
- if (y != 0) B=A*B (in generale $B = T_A(B)$);
- A=A*A
- k=(k-y)/2; (shift a dx di 1 passo).
- Continua il ciclo e si arresta per k=0.

Calcolo Rapido delle potenze: algoritmo

- Vediamo uno schema per l'algoritmo per il calcolo di $B = T_A^{(k)} A_0 = A^k A_0$ (ad esempio $B = A^k$)
- Inizializzazione: B=I (in generale $B = A_0$);
- Ciclo: y=mod(k,2) (legge primo bit a dx di k)
- if (y != 0) B=A*B (in generale $B = T_A(B)$);
- A=A*A
- k=(k-y)/2; (shift a dx di 1 passo).
- Continua il ciclo e si arresta per k=0.
- Bastano m passi, cioè $\log_2 k$ iterazioni e allocazione di 4 interi (o due interi e due oggetti di tipo A).

Calcolo Rapido delle potenze: algoritmo

- Vediamo uno schema per l'algoritmo per il calcolo di $B = T_A^{(k)} A_0 = A^k A_0$ (ad esempio $B = A^k$)
- Inizializzazione: B=I (in generale $B = A_0$);
- Ciclo: y=mod(k,2) (legge primo bit a dx di k)
- if (y != 0) B=A*B (in generale $B = T_A(B)$);
- A=A*A
- k=(k-y)/2; (shift a dx di 1 passo).
- Continua il ciclo e si arresta per k=0.
- Bastano m passi, cioè $\log_2 k$ iterazioni e allocazione di 4 interi (o due interi e due oggetti di tipo A).
- Esercizio: Scrivere codice Octave per il "quickpower".

Definizioni

- Dato un gruppo G (non necessariamente abeliano). La potenza k-esima (con $k \in \mathbb{N}$) di un suo elemento $a \in G$ è definita dalle proprietà seguenti:

$$\begin{cases} a^0 & \stackrel{def}{=} & I, \\ a^{k+1} & \stackrel{def}{=} & a^k \cdot a; \end{cases}$$

in cui I è l'elemento neutro del gruppo.

Definizioni

- Dato un gruppo G (non necessariamente abeliano). La potenza k-esima (con $k \in \mathbb{N}$) di un suo elemento $a \in G$ è definita dalle proprietà seguenti:

$$\begin{cases} a^0 & \stackrel{def}{=} & I, \\ a^{k+1} & \stackrel{def}{=} & a^k \cdot a; \end{cases}$$

  in cui I è l'elemento neutro del gruppo.

- Quando esiste, si definisce "periodo" τ di un elemento a, il numero più piccolo non nullo per il quale vale l'eguaglianza:

$$a^\tau = I.$$

Definizioni

- Dato un gruppo G (non necessariamente abeliano). La potenza k-esima (con $k \in \mathbb{N}$) di un suo elemento $a \in G$ è definita dalle proprietà seguenti:

$$\begin{cases} a^0 & \stackrel{def}{=} & I, \\ a^{k+1} & \stackrel{def}{=} & a^k \cdot a; \end{cases}$$

  in cui I è l'elemento neutro del gruppo.

- Quando esiste, si definisce "periodo" τ di un elemento a, il numero più piccolo non nullo per il quale vale l'eguaglianza:

$$a^\tau = I.$$

- Esplicitando: $\tau(a) = \tau$ equivale alle eguaglianze seguenti:

$$\begin{cases} a^k & \neq & I & \text{for } k < \tau, \\ a^\tau & = & I & , \\ a^k & = & I & \Rightarrow k = m\tau. \end{cases}$$

Esempi di periodi nei gruppi abeliani

- $G = (\mathbb{Z}_p, \cdot)$ cioè il gruppo moltiplicativo dei numeri tra 1 e $p-1$ modulo p. I periodi di tutti gli elementi devono essere sottomultipli della funzione di Eulero, cioè divisori di $p-1$ nel caso in cui p è primo.

$$a^{\phi(p)+1} \equiv a \ (mod \ p) \Rightarrow \phi(p) = p - 1 = m\tau;$$

cioè:

$$\tau | p - 1.$$

Esempi di periodi nei gruppi abeliani

- $G = (\mathbb{Z}_p, \cdot)$ cioè il gruppo moltiplicativo dei numeri tra 1 e $p-1$ modulo p. I periodi di tutti gli elementi devono essere sottomultipli della funzione di Eulero, cioè divisori di $p-1$ nel caso in cui p è primo.

$$a^{\phi(p)+1} \equiv a \ (mod \ p) \Rightarrow \phi(p) = p - 1 = m\tau;$$

cioè:

$$\tau | p - 1.$$

- Alcuni elementi hanno un periodo strettamente minore di $p-1$. Ad esempio il numero $p-1$ ha sempre periodo 2:

$$(p-1)^2 = p^2 - 2p + 1 = p(p-2) + 1 \equiv 1 \ (mod \ p).$$

$$(p-1)^3 \equiv p - 1 \ (mod \ p).$$

Esempi di periodi nei gruppi abeliani

- $G = (\mathbb{Z}_p, \cdot)$ cioè il gruppo moltiplicativo dei numeri tra 1 e $p-1$ modulo p. I periodi di tutti gli elementi devono essere sottomultipli della funzione di Eulero, cioè divisori di $p-1$ nel caso in cui p è primo.

$$a^{\phi(p)+1} \equiv a \ (mod \ p) \Rightarrow \phi(p) = p - 1 = m\tau;$$

cioè:

$$\tau | p - 1.$$

- Alcuni elementi hanno un periodo strettamente minore di $p-1$. Ad esempio il numero $p-1$ ha sempre periodo 2:

$$(p-1)^2 = p^2 - 2p + 1 = p(p-2) + 1 \equiv 1 \ (mod \ p).$$

$$(p-1)^3 \equiv p - 1 \ (mod \ p).$$

- Vedremo che se p è primo esistono elementi aventi per periodo tutti i sottomultipli di $p-1$.

Sottogruppo

- Un sottogruppo di un gruppo G è un sottoinsieme S del gruppo che forma anch'esso un gruppo (cioè è chiuso rispetto all'operazione e possiede elemento neutro ed inversi).

Sottogruppo

- Un sottogruppo di un gruppo G è un sottoinsieme S del gruppo che forma anch'esso un gruppo (cioè è chiuso rispetto all'operazione e possiede elemento neutro ed inversi).
- Tutti i sottogruppi devono quindi contenere l'unità I.

Sottogruppo

- Un sottogruppo di un gruppo G è un sottoinsieme S del gruppo che forma anch'esso un gruppo (cioè è chiuso rispetto all'operazione e possiede elemento neutro ed inversi).
- Tutti i sottogruppi devono quindi contenere l'unità I.
- I sottogruppi si dicono propri o non banali se non coincidono con il solo elemento neutro o con tutto il gruppo G. $S \neq G$, $S \neq \{I\}$.

Sottogruppo

- Un sottogruppo di un gruppo G è un sottoinsieme S del gruppo che forma anch'esso un gruppo (cioè è chiuso rispetto all'operazione e possiede elemento neutro ed inversi).
- Tutti i sottogruppi devono quindi contenere l'unità I.
- I sottogruppi si dicono propri o non banali se non coincidono con il solo elemento neutro o con tutto il gruppo G. $S \neq G$, $S \neq \{I\}$.
- Il teorema di Lagrange (che dimostreremo) ci assicura che la cardinalità di un sottogruppo è un sottomultiplo della cardinalità del gruppo in cui è immerso.

Ogni sottogruppo induce un'equivalenza

- Dato un gruppo G è un suo sottogruppo proprio S. Si definisce una equivalenza tra gli elementi di G mediante la relazione:

$$A \sim B \Leftrightarrow \exists C \in S : A = B \cdot C.$$

Ogni sottogruppo induce un'equivalenza

- Dato un gruppo G è un suo sottogruppo proprio S. Si definisce una equivalenza tra gli elementi di G mediante la relazione:

$$A \sim B \Leftrightarrow \exists C \in S : A = B \cdot C.$$

- Verifichiamo che si tratta di una equivalenza: la proprietà riflessiva è ovvia:

$$A \sim A \Leftrightarrow \exists C = I \in S : A = A \cdot I.$$

Ogni sottogruppo induce un'equivalenza

- Dato un gruppo G è un suo sottogruppo proprio S. Si definisce una equivalenza tra gli elementi di G mediante la relazione:

$$A \sim B \Leftrightarrow \exists C \in S : A = B \cdot C.$$

- Verifichiamo che si tratta di una equivalenza: la proprietà riflessiva è ovvia:

$$A \sim A \Leftrightarrow \exists C = I \in S : A = A \cdot I.$$

- La proprietà simmetrica:

$$A \sim B \Leftrightarrow \exists C \in S : A = B \cdot C \Rightarrow B = A \cdot inv(C) \Leftrightarrow B \sim A.$$

Ogni sottogruppo induce un'equivalenza

- Dato un gruppo G è un suo sottogruppo proprio S. Si definisce una equivalenza tra gli elementi di G mediante la relazione:

$$A \sim B \Leftrightarrow \exists C \in S : A = B \cdot C.$$

- Verifichiamo che si tratta di una equivalenza: la proprietà riflessiva è ovvia:

$$A \sim A \Leftrightarrow \exists C = I \in S : A = A \cdot I.$$

- La proprietà simmetrica:

$$A \sim B \Leftrightarrow \exists C \in S : A = B \cdot C \Rightarrow B = A \cdot inv(C) \Leftrightarrow B \sim A.$$

- La proprietà transitiva:

$$(A \sim B) \wedge (B \sim C) \Rightarrow A \sim C. \Leftrightarrow$$

$$(A = B \cdot D) \wedge (B = C \cdot E) \Rightarrow A = C \cdot (ED).$$

Classi laterali

- Le classi definite dalla nozione di equivalenza con l'azione a destra degli elementi del sottogruppo si chiamano classi destre. Analogamente si definiscono le classi sinistre.

Classi laterali

- Le classi definite dalla nozione di equivalenza con l'azione a destra degli elementi del sottogruppo si chiamano classi destre. Analogamente si definiscono le classi sinistre.
- L'orbita destra dell'elemento A di un gruppo G rispetto ad un sottogruppo S è l'insieme degli elementi che si ottengono con l'azione degli elementi del sottogruppo a destra:

$$O_A(S) \stackrel{def}{=} \{B \in G : B \sim A\} = \{B \in G : \exists C \in S : B = A \cdot C\}.$$

Classi laterali

- Le classi definite dalla nozione di equivalenza con l'azione a destra degli elementi del sottogruppo si chiamano classi destre. Analogamente si definiscono le classi sinistre.
- L'orbita destra dell'elemento A di un gruppo G rispetto ad un sottogruppo S è l'insieme degli elementi che si ottengono con l'azione degli elementi del sottogruppo a destra:

$$O_A(S) \stackrel{def}{=} \{B \in G : B \sim A\} = \{B \in G : \exists C \in S : B = A \cdot C\}.$$

- L'orbita di un elemento coincide con la classe laterale a cui esso appartiene. L'elemento si dice rappresentante della classe.

Classi laterali

- Le classi definite dalla nozione di equivalenza con l'azione a destra degli elementi del sottogruppo si chiamano classi destre. Analogamente si definiscono le classi sinistre.
- L'orbita destra dell'elemento A di un gruppo G rispetto ad un sottogruppo S è l'insieme degli elementi che si ottengono con l'azione degli elementi del sottogruppo a destra:

$$O_A(S) \stackrel{def}{=} \{B \in G : B \sim A\} = \{B \in G : \exists C \in S : B = A \cdot C\}.$$

- L'orbita di un elemento coincide con la classe laterale a cui esso appartiene. L'elemento si dice rappresentante della classe.
- Vedremo che le orbite posseggono tutte la stessa cardinalità.

Orbite

- Per definizione due elementi non equivalenti appartengono ad orbite diverse.

Orbite

- Per definizione due elementi non equivalenti appartengono ad orbite diverse.
- Gli elementi di un orbita sono pari alla cardinalità del sottogruppo che la genera. Dati $B_1, B_2 \dots B_{m=|S|} \in S$, possiamo costruire

$$A_i \stackrel{def}{=} A \cdot B_i;$$

Orbite

- Per definizione due elementi non equivalenti appartengono ad orbite diverse.
- Gli elementi di un orbita sono pari alla cardinalità del sottogruppo che la genera. Dati $B_1, B_2 \dots B_{m=|S|} \in S$, possiamo costruire

$$A_i \stackrel{def}{=} A \cdot B_i;$$

- Gli elementi dell'orbita sono tutti diversi

$$A_i \neq A_j \Leftrightarrow A \cdot B_i \neq A \cdot B_j \leftrightarrow inv(A)AB_i \neq inv(A)AB_j \leftrightarrow B_i \neq B_j.$$

Orbite

- Per definizione due elementi non equivalenti appartengono ad orbite diverse.
- Gli elementi di un orbita sono pari alla cardinalità del sottogruppo che la genera. Dati $B_1, B_2 \dots B_{m=|S|} \in S$, possiamo costruire

$$A_i \stackrel{def}{=} A \cdot B_i;$$

- Gli elementi dell'orbita sono tutti diversi

$$A_i \neq A_j \Leftrightarrow A \cdot B_i \neq A \cdot B_j \leftrightarrow inv(A)AB_i \neq inv(A)AB_j \leftrightarrow B_i \neq B_j.$$

- Quindi tutte le classi laterali posseggono la stessa cardinalità.

Teorema di Lagrange

- Siccome elementi non equivalenti generano orbite distinte vale il Teorema di Lagrange "La cardinalità di un sottogruppo è sempre un divisore della cardinalità del gruppo". Se chiamiamo L il numero delle classi laterali:

$$|G| = mL = |S|L.$$

Teorema di Lagrange

- Siccome elementi non equivalenti generano orbite distinte vale il Teorema di Lagrange "La cardinalità di un sottogruppo è sempre un divisore della cardinalità del gruppo". Se chiamiamo L il numero delle classi laterali:

$$|G| = mL = |S|L.$$

- La dimostrazione avviene per costruzione. Si considerano gli elementi del gruppo e se ne calcola l'orbita (la classe laterale dell'elemento scelto). Poi si continua scegliendo un elemento che non appartiene a nessuna delle classi laterali precedenti. Quando la procedura si arresta non può essere rimasto alcun elemento di G e dunque la sua cardinalità è multipla di quella di S.

Gruppo Quoziente

- Data una equivalenza è sempre possibile costruire lo spazio quoziente (lo spazio delle classi indotte). Si pone il problema di stabilire quando tale spazio costituisca ancora un gruppo.

Gruppo Quoziente

- Data una equivalenza è sempre possibile costruire lo spazio quoziente (lo spazio delle classi indotte). Si pone il problema di stabilire quando tale spazio costituisca ancora un gruppo.
- Un sottogruppo proprio S è normale se verifica:

$$GS \equiv SG;$$

ovvero

$$\forall a \in G, b \in S : \exists b' \in S : ab = b'a.$$

Gruppo Quoziente

- Data una equivalenza è sempre possibile costruire lo spazio quoziente (lo spazio delle classi indotte). Si pone il problema di stabilire quando tale spazio costituisca ancora un gruppo.
- Un sottogruppo proprio S è normale se verifica:

$$GS \equiv SG;$$

ovvero

$$\forall a \in G, b \in S : \exists b' \in S : ab = b'a.$$

- Se il sottogruppo S è normale lo spazio quoziente è anch'esso un gruppo.

Gruppo Quoziente

- Data una equivalenza è sempre possibile costruire lo spazio quoziente (lo spazio delle classi indotte). Si pone il problema di stabilire quando tale spazio costituisca ancora un gruppo.
- Un sottogruppo proprio S è normale se verifica:

$$GS \equiv SG;$$

ovvero

$$\forall a \in G, b \in S : \exists b' \in S : ab = b'a.$$

- Se il sottogruppo S è normale lo spazio quoziente è anch'esso un gruppo.
- I gruppi abeliani (commutativi) ammettono solo sottogruppi normali. Basta scegliere b'=b.

Gruppi quoziente rispetto ad un sottogruppo normale

- L'unico punto da verificare è che il prodotto tra le classi sia indipendente dalla scelta del rappresentante.

Gruppi quoziente rispetto ad un sottogruppo normale

- L'unico punto da verificare è che il prodotto tra le classi sia indipendente dalla scelta del rappresentante.
- In formula:

$$a \cdot s_1 \in C_a \wedge b \cdot s_2 \in C_b \Rightarrow (a \cdot s_1) \cdot (b \cdot s_2) = a \cdot ((s_1 \cdot b) \cdot s_2) =$$

Gruppi quoziente rispetto ad un sottogruppo normale

- L'unico punto da verificare è che il prodotto tra le classi sia indipendente dalla scelta del rappresentante.
- In formula:

$$a \cdot s_1 \in C_a \wedge b \cdot s_2 \in C_b \Rightarrow (a \cdot s_1) \cdot (b \cdot s_2) = a \cdot ((s_1 \cdot b) \cdot s_2) =$$

- per l'ipotesi di normalità $\exists s_3 \in S : s_1 \cdot b = b \cdot s_3$, quindi

$$(a \cdot s_1) \cdot (b \cdot s_2) = a \cdot ((s_1 \cdot b) \cdot s_2) = a \cdot ((b \cdot s_3) \cdot s_2) = (a \cdot b) \cdot (s_3 \cdot s_2);$$

Gruppi quoziente rispetto ad un sottogruppo normale

- L'unico punto da verificare è che il prodotto tra le classi sia indipendente dalla scelta del rappresentante.
- In formula:

  $a \cdot s_1 \in C_a \wedge b \cdot s_2 \in C_b \Rightarrow (a \cdot s_1) \cdot (b \cdot s_2) = a \cdot ((s_1 \cdot b) \cdot s_2) =$

- per l'ipotesi di normalità $\exists s_3 \in S : s_1 \cdot b = b \cdot s_3$, quindi

  $(a \cdot s_1) \cdot (b \cdot s_2) = a \cdot ((s_1 \cdot b) \cdot s_2) = a \cdot ((b \cdot s_3) \cdot s_2) = (a \cdot b) \cdot (s_3 \cdot s_2)$;

- Siccome anche $s_3 \cdot s_2 \in S$ il prodotto di due qualsiasi rappresentanti di una classe è un rappresentante della classe del prodotto dei rappresentati.

Gruppi quoziente rispetto ad un sottogruppo normale

- L'unico punto da verificare è che il prodotto tra le classi sia indipendente dalla scelta del rappresentante.
- In formula:

  $a \cdot s_1 \in C_a \wedge b \cdot s_2 \in C_b \Rightarrow (a \cdot s_1) \cdot (b \cdot s_2) = a \cdot ((s_1 \cdot b) \cdot s_2) =$

- per l'ipotesi di normalità $\exists s_3 \in S : s_1 \cdot b = b \cdot s_3$, quindi

  $(a \cdot s_1) \cdot (b \cdot s_2) = a \cdot ((s_1 \cdot b) \cdot s_2) = a \cdot ((b \cdot s_3) \cdot s_2) = (a \cdot b) \cdot (s_3 \cdot s_2)$;

- Siccome anche $s_3 \cdot s_2 \in S$ il prodotto di due qualsiasi rappresentanti di una classe è un rappresentante della classe del prodotto dei rappresentati.
- Quindi anche l'inverso di una classe esiste ed è indipendente dal rappresentante:

  $$a \cdot x = I;$$

  ammente una soluzione perché G è un gruppo (ed esiste quindi inverso di a in G) e l'orbita di questa soluzione rappresenta la classe inversa di a.

Alcune conseguenze utili

- Se un gruppo possiede cardinalità prima allora non può avere sottogruppi propri.

Alcune conseguenze utili

- Se un gruppo possiede cardinalità prima allora non può avere sottogruppi propri.
- Tutti gli spazi quoziente di un gruppo commutativo sono ancora dei gruppi commutativi.

Alcune conseguenze utili

- Se un gruppo possiede cardinalità prima allora non può avere sottogruppi propri.
- Tutti gli spazi quoziente di un gruppo commutativo sono ancora dei gruppi commutativi.
- Lo spazio quoziente G/S è un gruppo perché i sottogruppi di un gruppo abeliano sono abeliani e dunque normali.

Alcune conseguenze utili

- Se un gruppo possiede cardinalità prima allora non può avere sottogruppi propri.
- Tutti gli spazi quoziente di un gruppo commutativo sono ancora dei gruppi commutativi.
- Lo spazio quoziente G/S è un gruppo perché i sottogruppi di un gruppo abeliano sono abeliani e dunque normali.
- Il prodotto di due classi di un gruppo abeliano è commutativo:

$$(a \cdot s_1) \cdot (b \cdot s_2) = a \cdot (b \cdot s_3) \cdot s_2 = (a \cdot b) \cdot (s_3 \cdot s_2) = (b \cdot a) \cdot (s_3 \cdot s_2).$$

Alcune conseguenze utili

- Se un gruppo possiede cardinalità prima allora non può avere sottogruppi propri.
- Tutti gli spazi quoziente di un gruppo commutativo sono ancora dei gruppi commutativi.
- Lo spazio quoziente G/S è un gruppo perché i sottogruppi di un gruppo abeliano sono abeliani e dunque normali.
- Il prodotto di due classi di un gruppo abeliano è commutativo:

$$(a \cdot s_1) \cdot (b \cdot s_2) = a \cdot (b \cdot s_3) \cdot s_2 = (a \cdot b) \cdot (s_3 \cdot s_2) = (b \cdot a) \cdot (s_3 \cdot s_2).$$

- quindi G/S è un gruppo commutativo.

Esercizi svolti alla lavagna

- Calcolare i periodi di $\mathbb{Z}_n^*$ e $\mathbb{Z}_n$ (con n=7,14,15,9). Calcolare le cardinalità di D_n (elementi minori di n e non primi con n) e $\mathbb{Z}_n^*$ e verificare la funzione di Eulero.

Esercizi svolti alla lavagna

- Calcolare i periodi di $\mathbb{Z}_n^*$ e $\mathbb{Z}_n$ (con n=7,14,15,9). Calcolare le cardinalità di D_n (elementi minori di n e non primi con n) e $\mathbb{Z}_n^*$ e verificare la funzione di Eulero.
- Abbiamo verificato che $\mathbb{Z}_9^*$, $\mathbb{Z}_{14}^*$ e $\mathbb{Z}_7^*$ hanno 2 generatori.

Esercizi svolti alla lavagna

- Calcolare i periodi di $\mathbb{Z}_n^*$ e $\mathbb{Z}_n$ (con n=7,14,15,9). Calcolare le cardinalità di D_n (elementi minori di n e non primi con n) e $\mathbb{Z}_n^*$ e verificare la funzione di Eulero.
- Abbiamo verificato che $\mathbb{Z}_9^*$, $\mathbb{Z}_{14}^*$ e $\mathbb{Z}_7^*$ hanno 2 generatori.
- Abbiamo verificato che $\mathbb{Z}_{15}^*$ non ha generatori e il suo massimo periodo è 4.

Esercizi svolti alla lavagna

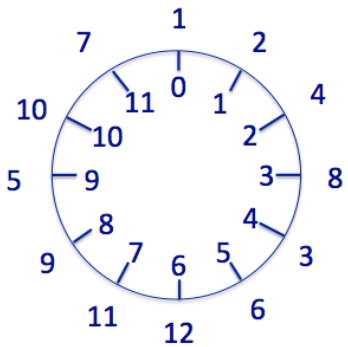
- Calcolare i periodi di $\mathbb{Z}_n^*$ e $\mathbb{Z}_n$ (con n=7,14,15,9). Calcolare le cardinalità di D_n (elementi minori di n e non primi con n) e $\mathbb{Z}_n^*$ e verificare la funzione di Eulero.
- Abbiamo verificato che $\mathbb{Z}_9^*$, $\mathbb{Z}_{14}^*$ e $\mathbb{Z}_7^*$ hanno 2 generatori.
- Abbiamo verificato che $\mathbb{Z}_{15}^*$ non ha generatori e il suo massimo periodo è 4.
- Verifica della "regola dell'orologio" per il periodo delle potenze di un elemento.

Esercizi svolti alla lavagna

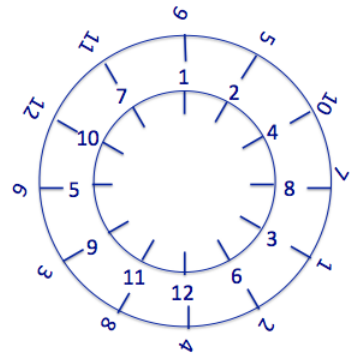
- Calcolare i periodi di $\mathbb{Z}_n^*$ e $\mathbb{Z}_n$ (con n=7,14,15,9). Calcolare le cardinalità di D_n (elementi minori di n e non primi con n) e $\mathbb{Z}_n^*$ e verificare la funzione di Eulero.
- Abbiamo verificato che $\mathbb{Z}_9^*$, $\mathbb{Z}_{14}^*$ e $\mathbb{Z}_7^*$ hanno 2 generatori.
- Abbiamo verificato che $\mathbb{Z}_{15}^*$ non ha generatori e il suo massimo periodo è 4.
- Verifica della "regola dell'orologio" per il periodo delle potenze di un elemento.
- Quick Power con Octave.

Il regolo ciclico

- $\mathbb{Z}_{13}^*$ è ciclico. 2 è un generatore. La serie da esso generata è: $\{1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7\}$. Possiamo rappresentare la serie su una circonferenza.



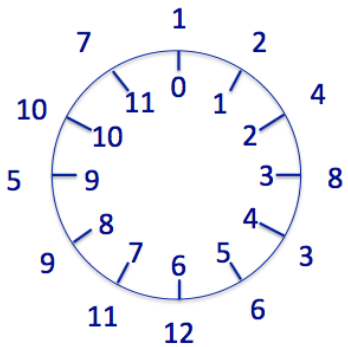
Rappresentazione ciclica di $\mathbb{Z}_{13}^*$ in base 2.



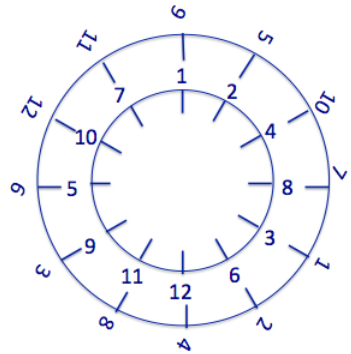
Regolo ciclico di $\mathbb{Z}_{13}^*$ in base 2. Tabellina del 3

Il regolo ciclico

- $\mathbb{Z}_{13}^*$ è ciclico. 2 è un generatore. La serie da esso generata è: $\{1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7\}$. Possiamo rappresentare la serie su una circonferenza.



Rappresentazione ciclica di $\mathbb{Z}_{13}^*$ in base 2.



Regolo ciclico di $\mathbb{Z}_{13}^*$ in base 2. Tabellina del 3

- Essendo 2 un generatore, ad ogni k si associa un esponente j_k compreso tra 0 e 11:

$$\forall k \ \exists j_k : 2^{j_k} = k;$$

gli esponenti (che possiamo chiamare logoritmi) definiscono una trasformazione biunivoca:

$$k \to t(k) = j_k \stackrel{def}{=} log_2(k).$$

Additività

- Il prodotto di due numeri in $\mathbb{Z}_{13}^* = G(\{1, 2, \ldots, 12\}, \cdot)$ (gruppo rispetto al prodotto modulo 13) corrisponde alla somma dei loro trasformati in $G(\{0, 1, 2, \ldots, 11\}, +)$ (gruppo rispetto alla somma):

$$k_1 \cdot k_2 = 2^{l_1} \cdot 2^{l_2} = 2^{l_1 + l_2};$$

in cui $k_1 = 2^{l_1}$ e $k_2 = 2^{l_2}$.

Additività

- Il prodotto di due numeri in $\mathbb{Z}_{13}^* = G(\{1, 2, \ldots, 12\}, \cdot)$ (gruppo rispetto al prodotto modulo 13) corrisponde alla somma dei loro trasformati in $G(\{0, 1, 2, \ldots, 11\}, +)$ (gruppo rispetto alla somma):

$$k_1 \cdot k_2 = 2^{l_1} \cdot 2^{l_2} = 2^{l_1 + l_2};$$

  in cui $k_1 = 2^{l_1}$ e $k_2 = 2^{l_2}$.
- Quindi la trasformazione $t() = log_2()$ definisce un isomorfismo tra $G(\{1, 2, \ldots, 12\}, \cdot)$ e $G(\{0, 1, \ldots, 11\}, +)$. Trasforma il prodotto in una somma.

Messaggio

- Le potenze generano Orbite chiuse nei sistemi finiti

Messaggio

- Le potenze generano Orbite chiuse nei sistemi finiti
- Le potenze possono essere calcolate con algoritmi che scalano con il logaritmo dell'esponente

Messaggio

- Le potenze generano Orbite chiuse nei sistemi finiti
- Le potenze possono essere calcolate con algoritmi che scalano con il logaritmo dell'esponente
- In qualsiasi gruppo l'insieme delle orbite generate da un elemento forma un sottogruppo (ciclico)

Messaggio

- Le potenze generano Orbite chiuse nei sistemi finiti
- Le potenze possono essere calcolate con algoritmi che scalano con il logaritmo dell'esponente
- In qualsiasi gruppo l'insieme delle orbite generate da un elemento forma un sottogruppo (ciclico)
- La cardinalià dei sottogruppi e quindi l'ordine di ogni elemento deve essere sottomultiplo della cardinalità del gruppo.