Teorema di Eulero

Gregorio D'Agostino

26 Marzo 2021

Teorema di Eulero

Elevando ogni numero a primo con n, alla funzione di Eulero di n ($\phi(n)$) si ottiene sempre un numero congruente all'unità:

$$a^{\phi(n)} \equiv 1 \ (mod \ n).$$

- In forma equivalente in $\mathbb{Z}$:

$$a^{\phi(n)} = 1 + k \cdot n.$$

Teorema di Eulero

Elevando ogni numero a primo con n, alla funzione di Eulero di n ($\phi(n)$) si ottiene sempre un numero congruente all'unità:

$$a^{\phi(n)} \equiv 1 \ (mod \ n).$$

- In forma equivalente in $\mathbb{Z}$:

$$a^{\phi(n)} = 1 + k \cdot n.$$

- Vedremo due dimostrazioni diverse: una algebrica ed una basata sulla teoria dei gruppi.

Teorema di Eulero

Elevando ogni numero a primo con n, alla funzione di Eulero di n ($\phi(n)$) si ottiene sempre un numero congruente all'unità:

$$a^{\phi(n)} \equiv 1 \ (mod \ n).$$

- In forma equivalente in $\mathbb{Z}$:

$$a^{\phi(n)} = 1 + k \cdot n.$$

- Vedremo due dimostrazioni diverse: una algebrica ed una basata sulla teoria dei gruppi.
- Rivediamo la funzione di Eulero:

$$\phi(n) \stackrel{def}{=} \phi(n_1) \cdot \phi(n_2) \cdots \phi(n_m);$$
$$\phi(n) = \phi((p_1)^{h_1}) \cdot \phi((p_2)^{h_2}) \cdots \phi((p_m)^{h_m});$$

$$\phi(n) = (p_1)^{h_1-1}(p_1-1) \cdot (p_2)^{h_2-1}(p_2-1) \cdots (p_m)^{h_m-1}(p_m-1).$$

Dimostrazione algebrica

$$a^{\phi(n)} \equiv 1 \ (mod \ n).$$

- Premesse: n si fattorizza in fattori primi in maniera unica:

$$n = (p_1)^{h_1} \cdot (p_2)^{h_2} \cdots (p_m)^{h_m}.$$

$$n = n_1 \cdot n_2 \cdots n_m.$$

Dimostrazione algebrica

$$a^{\phi(n)} \equiv 1 \ (mod \ n).$$

- Premesse: n si fattorizza in fattori primi in maniera unica:

$$n = (p_1)^{h_1} \cdot (p_2)^{h_2} \cdots (p_m)^{h_m}.$$

$$n = n_1 \cdot n_2 \cdots n_m.$$

- Dimostreremo prima il teorema nel caso di un solo fattore $n = (p)^h$

Dimostrazione algebrica

$$a^{\phi(n)} \equiv 1 \ (mod \ n).$$

- Premesse: n si fattorizza in fattori primi in maniera unica:

$$n = (p_1)^{h_1} \cdot (p_2)^{h_2} \cdots (p_m)^{h_m}.$$

$$n = n_1 \cdot n_2 \cdots n_m.$$

- Dimostreremo prima il teorema nel caso di un solo fattore $n = (p)^h$
- Dimostreremo che se il teorema è vero per due numeri primi tra loro è vero anche per il loro prodotto

Dimostrazione algebrica

$$a^{\phi(n)} \equiv 1 \ (mod \ n).$$

- Premesse: n si fattorizza in fattori primi in maniera unica:

$$n = (p_1)^{h_1} \cdot (p_2)^{h_2} \cdots (p_m)^{h_m}.$$

$$n = n_1 \cdot n_2 \cdots n_m.$$

- Dimostreremo prima il teorema nel caso di un solo fattore $n = (p)^h$
- Dimostreremo che se il teorema è vero per due numeri primi tra loro è vero anche per il loro prodotto
- Utilizzando la decomposizione unica otterremo il risultato generale.

Dimostrazione

- Lemma 1: Il teorema nel caso particolare in cui n è una potenza di p ($n = p^h$). Dimostreremo che per tutti gli a primi con p

$$a^{\phi(n)} = a^{(p)^{h-1}(p-1)} \equiv 1 \ (mod \ (p)^h).$$

Dimostrazione

- Lemma 1: Il teorema nel caso particolare in cui n è una potenza di p ($n = p^h$). Dimostreremo che per tutti gli a primi con p
$$a^{\phi(n)} = a^{(p)^{h-1}(p-1)} \equiv 1 \ (mod \ (p)^h).$$
- Lemma 2: Proprietà di composizione. Nel caso n sia il prodotto di numeri primi tra loro: $n = n_1 \cdot n_2 \cdots n_m$ con $n_1 \cdot n_2 \cdots n_m$ primi tra loro. Se la proprietà è vera per ogni n_i è vera per il loro prodotto.

Dimostrazione

- Lemma 1: Il teorema nel caso particolare in cui n è una potenza di p ($n = p^h$). Dimostreremo che per tutti gli a primi con p
$$a^{\phi(n)} = a^{(p)^{h-1}(p-1)} \equiv 1 \ (mod \ (p)^h).$$
- Lemma 2: Proprietà di composizione. Nel caso n sia il prodotto di numeri primi tra loro: $n = n_1 \cdot n_2 \cdots n_m$ con $n_1 \cdot n_2 \cdots n_m$ primi tra loro. Se la proprietà è vera per ogni n_i è vera per il loro prodotto.
- Utilizzando i due lemmi nel caso $n = (p_1)^{h_1} \cdot (p_2)^{h_2} \cdots (p_m)^{h_m}$ si ottiene la tesi.

Dimostrazione Lemma 1 ($n = p^h$)

- Si dimostra per induzione su h.

Dimostrazione Lemma 1 ($n = p^h$)

- Si dimostra per induzione su h.
- Il caso $h = 1$ è il piccolo teorema di Fermat.

Dimostrazione Lemma 1 ($n = p^h$)

- Si dimostra per induzione su h.
- Il caso $h = 1$ è il piccolo teorema di Fermat.
- Ricorsione su h. Se è vera per h, allora è vera per h+1

$$a^{\phi\left(p^{(h+1)}\right)} = a^{p\cdot\phi(p^h)} = (a^{\phi(p^h)})^p = \left(1 + k \cdot p^h\right)^p =$$

utilizzando la formula del binomio di Newton:

$$= 1 + \binom{p}{1} k \cdot p^h + \binom{p}{2} (k \cdot p^h)^2 + \cdots = 1 + k' p^{h+1} =$$

$$= 1 + k' p^{h+1} \equiv 1 \ (mod\ p^{h+1}).$$

Dimostrazione Lemma 2 ($n = n_1 \cdot n_2 \cdots n_m$)

- Poniamo:

$$x \stackrel{def}{=} a^{\phi(n)} = a^{\phi(n_1)\cdot\phi(n_2)\cdots}$$

e proiettiamola su tutti gli n_j:

$$\begin{cases} x = \left(a^{\frac{\phi(n)}{\phi(n_1)}}\right)^{\phi(n_1)} \equiv x_1 \pmod{n_1}; \\ x = \left(a^{\frac{\phi(n)}{\phi(n_2)}}\right)^{\phi(n_2)} \equiv x_2 \pmod{n_2}; \\ \cdots \\ x = \left(a^{\frac{\phi(n)}{\phi(n_j)}}\right)^{\phi(n_j)} \equiv x_j \pmod{n_j}; \\ \cdots \\ x = \left(a^{\frac{\phi(n)}{\phi(n_m)}}\right)^{\phi(n_m)} \equiv x_m \pmod{n_m}. \end{cases}$$

Dimostrazione Lemma 2 cont $(n = n_1 \cdot n_2 \cdots n_m)$

- Per ipotesi, per ogni b primo con n $((b, n) = 1)$: $b^{\phi(n_j)} \equiv 1 \ (mod \ n_j)$;

  in particolare anche per $b = a^{\frac{\phi(n)}{\phi(n_j)}}$. Quindi $\forall j \ x_j = 1$

Dimostrazione Lemma 2 cont $(n = n_1 \cdot n_2 \cdots n_m)$

- Per ipotesi, per ogni b primo con n $((b, n) = 1)$: $b^{\phi(n_j)} \equiv 1 \ (mod \ n_j)$;

  in particolare anche per $b = a^{\frac{\phi(n)}{\phi(n_j)}}$. Quindi $\forall j \ x_j = 1$
- Il sistema diviene

$$\begin{cases} x & \equiv & 1 & (mod \ n_1); \\ x & \equiv & 1 & (mod \ n_2); \\ \dots & \dots & \dots & \\ x & \equiv & 1 & (mod \ n_j); \\ \dots & \dots & \dots & \\ x & \equiv & 1 & (mod \ n_m). \end{cases}$$

Dimostrazione Lemma 2 cont $(n = n_1 \cdot n_2 \cdots n_m)$

- Per ipotesi, per ogni b primo con n $((b, n) = 1)$: $b^{\phi(n_j)} \equiv 1 \ (mod \ n_j)$;

  in particolare anche per $b = a^{\frac{\phi(n)}{\phi(n_j)}}$. Quindi $\forall j \ x_j = 1$
- Il sistema diviene

$$\begin{cases} x & \equiv & 1 & (mod \ n_1); \\ x & \equiv & 1 & (mod \ n_2); \\ \dots & \dots & \dots & \\ x & \equiv & 1 & (mod \ n_j); \\ \dots & \dots & \dots & \\ x & \equiv & 1 & (mod \ n_m). \end{cases}$$

- che, per il teorema cinese dei resti equivale a $x \equiv 1 \ (mod \ n = n_1 \cdot n_2 \cdots n_m)$ CVD.

Dimostrazione basata sulla teoria dei gruppi

- $\mathbb{Z}_n = \{0, 1, \cdots, n-1\}$ indica l'anello dei primi n numeri reali dotato di somma $(+)$ e prodotto. Questo equivale alla classe dei resti di ordine n, cioè allo spazio quoziente di $\mathbb{Z}$ rispetto alla congruenza modulo n.

Dimostrazione basata sulla teoria dei gruppi

- $\mathbb{Z}_n = \{0, 1, \cdots, n-1\}$ indica l'anello dei primi n numeri reali dotato di somma $(+)$ e prodotto. Questo equivale alla classe dei resti di ordine n, cioè allo spazio quoziente di $\mathbb{Z}$ rispetto alla congruenza modulo n.
- Si definisce $\mathbb{Z}^*_n$ l'insieme dei numeri (classi) minori di n e primi con n (quindi anche diversi da zero).
  In questo insieme tutti gli elementi sono dotati di inverso rispetto al prodotto, si dice quindi un "dominio di integrità".
  Si noti che non è un anello perché sommando due suoi elementi si possono ottenere numeri non primi con n, cioè non è chiuso rispetto alla somma. Esempio in $\mathbb{Z}^*_8 = \{1, 3, 5, 7\}$, $5 + 1 = 6 \notin \mathbb{Z}^*_8$

Dimostrazione basata sulla teoria dei gruppi

- $\mathbb{Z}_n = \{0, 1, \cdots, n-1\}$ indica l'anello dei primi n numeri reali dotato di somma $(+)$ e prodotto. Questo equivale alla classe dei resti di ordine n, cioè allo spazio quoziente di $\mathbb{Z}$ rispetto alla congruenza modulo n.
- Si definisce $\mathbb{Z}^*{}_n$ l'insieme dei numeri (classi) minori di n e primi con n (quindi anche diversi da zero).
  In questo insieme tutti gli elementi sono dotati di inverso rispetto al prodotto, si dice quindi un "dominio di integrità".
  Si noti che non è un anello perché sommando due suoi elementi si possono ottenere numeri non primi con n, cioè non è chiuso rispetto alla somma. Esempio in $\mathbb{Z}^*{}_8 = \{1, 3, 5, 7\}$, $5 + 1 = 6 \notin \mathbb{Z}^*{}_8$
- Abbiamo visto che la funzione di Eulero $\phi(n)$ è la cardinalità di $\mathbb{Z}^*{}_n$, conta infatti i numeri coprimi con n:

$$\phi(n) = |\mathbb{Z}^*{}_n| .$$

Automorfismi di anelli

- Definiamo l'operatore T_a che opera moltiplicando per il numero a in $\mathbb{Z}_n$:

$$T_a : \mathbb{Z}_n \to \mathbb{Z}_n$$

$$t_a(b) \stackrel{def}{=} ab \ (mod \ n).$$

Automorfismi di anelli

- Definiamo l'operatore T_a che opera moltiplicando per il numero a in $\mathbb{Z}_n$:

$$T_a : \mathbb{Z}_n \to \mathbb{Z}_n$$

$$t_a(b) \stackrel{def}{=} ab \ (mod \ n).$$

- Se $a \in \mathbb{Z}_n^*$ anche i trasformati appartengono a $\mathbb{Z}_n^*$ (se due numeri sono primi con n lo è anche il loro prodotto) . Inoltre la trasformazione è iniettiva. Ripetiamo l'argomento:

$$t_a(b) - t_a(c) = ab - ac = a(b - c) \neq 0 \ (mod \ n).$$

Qundi trasformando tutti gli elementi di $\mathbb{Z}_n^*$ si otterrà lo stesso insieme permutato.

Automorfismi di anelli: prodotto invariante

- Il prodotto di tutti gli elementi di $\mathbb{Z}_n^*$ è un "invariante" L rispetto alle trasformazioni T_a:

$$L \stackrel{def}{=} \prod_{b \in \mathbb{Z}_n^*} b \ (mod \ n);$$

Se indichiamo con b' il trasformato di b $(b' = t_a(b))$:

$$L \equiv \prod_{b' \in \mathbb{Z}_n^*} b' \equiv \prod_{b \in \mathbb{Z}_n^*} b \ (mod \ n).$$

Automorfismi di anelli: prodotto invariante

- Il prodotto di tutti gli elementi di $\mathbb{Z}_n^*$ è un "invariante" L rispetto alle trasformazioni T_a:

$$L \stackrel{def}{=} \prod_{b \in \mathbb{Z}_n^*} b \ (mod\ n);$$

Se indichiamo con b' il trasformato di b ($b' = t_a(b)$):

$$L \equiv \prod_{b' \in \mathbb{Z}_n^*} b' \equiv \prod_{b \in \mathbb{Z}_n^*} b \ (mod\ n).$$

- Ma $b' = ab$ quindi:

$$L = \prod_{b' \in \mathbb{Z}_n^*} b' \equiv \prod_{b \in \mathbb{Z}_n^*} ab = a^{\phi(n)} \prod_{b \in \mathbb{Z}_n^*} b = a^{\phi(n)} L \ (mod\ n).$$

Siccome L possiede un inverso (il prodotto degli inversi di tutti gli elementi):

$$L \equiv a^{\phi(n)} L \Leftrightarrow a^{\phi(n)} \equiv 1 \ (mod\ n).$$

Il caso più semplice: gli anelli primali

- Nel caso degli anelli primali il modulo n è un numero primo che indicheremo con la lettera p:

Il caso più semplice: gli anelli primali

- Nel caso degli anelli primali il modulo n è un numero primo che indicheremo con la lettera p:
- La funzione di Eulero si semplifica

$$d = \phi(p) = p - 1.$$

Il caso più semplice: gli anelli primali

- Nel caso degli anelli primali il modulo n è un numero primo che indicheremo con la lettera p:
- La funzione di Eulero si semplifica

$$d = \phi(p) = p - 1.$$

- Per ogni a primo con n, il teorema di Eulero diviene il teorema di Fermat:

$$a^{\phi(p)} = a^{(p-1)} \equiv 1 \ (mod \ p).$$

Il caso più semplice: gli anelli primali

- Nel caso degli anelli primali il modulo n è un numero primo che indicheremo con la lettera p:
- La funzione di Eulero si semplifica

$$d = \phi(p) = p - 1.$$

- Per ogni a primo con n, il teorema di Eulero diviene il teorema di Fermat:

$$a^{\phi(p)} = a^{(p-1)} \equiv 1 \ (mod \ p).$$

- Si definisce $\mathbb{Z}^*{}_p$ l'insieme dei numeri (classi) 1,2,..., p-1 (diversi da zero). Questo insieme è un campo: è un gruppo rispetto alla somma, ogni elemento non nullo ammette un inverso rispetto al prodotto e vale la proprietà distribuitiva.

Proprietà anelli primali $\mathbb{Z}_p$

- Ogni $a \in \mathbb{Z}^*{}_p$ definisce un automorfismo (isomorfismo di $\mathbb{Z}^*{}_p$ in se) tramite la trasformazione:

$$\forall b \in \mathbb{Z}_p : T_a(b) \stackrel{def}{=} a \cdot b \, (mod \ p).$$

Proprietà anelli primali $\mathbb{Z}_p$

- Ogni $a \in \mathbb{Z}^*{}_p$ definisce un automorfismo (isomorfismo di $\mathbb{Z}^*{}_p$ in se) tramite la trasformazione:

$$\forall b \in \mathbb{Z}_p : T_a(b) \stackrel{def}{=} a \cdot b \ (mod\ p).$$

- T_a rispetta la somma:

$$\forall b, c : T_a(b+c) \equiv a(b+c) \equiv ab+ac \ (mod\ p) = T_a(b)+T_a(c).$$

Proprietà anelli primali $\mathbb{Z}_p$

- Ogni $a \in \mathbb{Z}^*{}_p$ definisce un automorfismo (isomorfismo di $\mathbb{Z}^*{}_p$ in se) tramite la trasformazione:

$$\forall b \in \mathbb{Z}_p : T_a(b) \stackrel{def}{=} a \cdot b \ (mod\ p).$$

- T_a rispetta la somma:

$$\forall b, c : T_a(b+c) \equiv a(b+c) \equiv ab+ac \ (mod\ p) = T_a(b)+T_a(c).$$

- Il prodotto nel nuovo insieme non coincide col prodotto canonico. Sia α l'inverso di a rispetto al prodotto canonico.

$$a\alpha \stackrel{def}{=} 1 \ (mod\ p).$$

Il nuovo prodotto bxc indotto dall'isomorfismo è definito come segue:

$$bxc \stackrel{def}{=} bc\alpha \ (mod\ p).$$

Proprietà anelli primali $\mathbb{Z}_p$

- Ogni $a \in \mathbb{Z}^*{}_p$ definisce un automorfismo (isomorfismo di $\mathbb{Z}^*{}_p$ in se) tramite la trasformazione:

$$\forall b \in \mathbb{Z}_p : T_a(b) \stackrel{def}{=} a \cdot b \ (mod\ p).$$

- T_a rispetta la somma:

$$\forall b, c : T_a(b+c) \equiv a(b+c) \equiv ab+ac \ (mod\ p) = T_a(b)+T_a(c).$$

- Il prodotto nel nuovo insieme non coincide col prodotto canonico. Sia α l'inverso di a rispetto al prodotto canonico.

$$a\alpha \stackrel{def}{=} 1 \ (mod\ p).$$

Il nuovo prodotto bxc indotto dall'isomorfismo è definito come segue:

$$bxc \stackrel{def}{=} bc\alpha \ (mod\ p).$$

- Esercizio: dimostrare che $T_a(bc) = T_a(b)xT_a(c)$ e che $\mathbb{Z}^*{}_p$ forma un gruppo rispetto al nuovo prodotto.

Pseudoprimi

- Abbiamo visto alcune condizioni necessarie affinché un numero sia primo. Ad esempio deve soddisfare l'dentità di Fermat oppure essere indivisibile per un sottoinsieme di numeri.
  I numeri pseudoprimi soddisfano queste identità ma non sono necessariamente primi.

Pseudoprimi

- Abbiamo visto alcune condizioni necessarie affinché un numero sia primo. Ad esempio deve soddisfare l'dentità di Fermat oppure essere indivisibile per un sottoinsieme di numeri.
  I numeri pseudoprimi soddisfano queste identità ma non sono necessariamente primi.
- Primalità "cinese". I "primi cinesi", meglio detti "pseudoprimi cinesi" soddisfano l'equazione:

$$2^{(p-1)} \equiv 1 \ (mod \ p).$$

  Si tratta di una condizione necessaria ma non sufficiente.
  Ironizzando si potrebbe dire che i primi cinesi sono come certi prodotti cinesi di scarso valore in commercio

Un caso importante: Il modulo n è il prodotto di due primi.

$$n \stackrel{def}{=} p_1 \cdot p_2.$$

i numeri p_1 e p_2 sono "divisori dello zero". Significa che moltiplicati per un altro numero possono dare zero.

- La funzione di Eulero si semplifica
  $\phi(n) = \phi(p_1) \cdot \phi(p_2) = (p_1 - 1) \cdot (p_2 - 1)$

Un caso importante: Il modulo n è il prodotto di due primi.

$$n \stackrel{def}{=} p_1 \cdot p_2.$$

i numeri p_1 e p_2 sono "divisori dello zero". Significa che moltiplicati per un altro numero possono dare zero.

- La funzione di Eulero si semplifica
  $\phi(n) = \phi(p_1) \cdot \phi(p_2) = (p_1 - 1) \cdot (p_2 - 1)$
- Lo spazio $\mathbb{Z}^*{}_n$ si definisce come l'insieme dei numeri minori di n, primi con n cioè primi con p_1 e p_2:

$$\mathbb{Z}^*{}_n \stackrel{def}{=} \{a < n : (a, n) = 1\}.$$

la cardinalità di $\mathbb{Z}^*{}_n$ è per definizione la funzione di Eulero.

Un caso importante: Il modulo n è il prodotto di due primi.

$$n \stackrel{def}{=} p_1 \cdot p_2.$$

i numeri p_1 e p_2 sono "divisori dello zero". Significa che moltiplicati per un altro numero possono dare zero.

- La funzione di Eulero si semplifica
  $\phi(n) = \phi(p_1) \cdot \phi(p_2) = (p_1 - 1) \cdot (p_2 - 1)$
- Lo spazio $\mathbb{Z}^*{}_n$ si definisce come l'insieme dei numeri minori di n, primi con n cioè primi con p_1 e p_2:

  $$\mathbb{Z}^*{}_n \stackrel{def}{=} \{a < n : (a, n) = 1\}.$$

  la cardinalità di $\mathbb{Z}^*{}_n$ è per definizione la funzione di Eulero.
- Per ogni a primo con n (cioè $a \in \mathbb{Z}^*{}_n$), il teorema di Eulero diviene:

  $$a^{\phi(n)} = a^{(p_1-1)\cdot(p_2-1)} \equiv 1 \ (mod\ n).$$

Il modulo n è il prodotto di due primi (cont).

- I numeri non coprimi con n sono "divisori dello zero" o loro multipli. Sono i multipli di p e di q minori di n.

Il modulo n è il prodotto di due primi (cont).

- I numeri non coprimi con n sono "divisori dello zero" o loro multipli. Sono i multipli di p e di q minori di n.
- I numeri primi con n formano un gruppo rispetto al prodotto.

Il modulo n è il prodotto di due primi (cont).

- I numeri non coprimi con n sono "divisori dello zero" o loro multipli. Sono i multipli di p e di q minori di n.
- I numeri primi con n formano un gruppo rispetto al prodotto.
- Il prodotto di un numero primo con n per un divisore dello zero è un divisore dello zero.

Il modulo n è il prodotto di due primi (cont).

- I numeri non coprimi con n sono "divisori dello zero" o loro multipli. Sono i multipli di p e di q minori di n.
- I numeri primi con n formano un gruppo rispetto al prodotto.
- Il prodotto di un numero primo con n per un divisore dello zero è un divisore dello zero.
- I divisori dello zero formano un ideale rispetto al prodotto. Il concetto di ideale sarà sviluppato in seguito.

Il modulo n è il prodotto di due primi (cont).

- I numeri non coprimi con n sono "divisori dello zero" o loro multipli. Sono i multipli di p e di q minori di n.
- I numeri primi con n formano un gruppo rispetto al prodotto.
- Il prodotto di un numero primo con n per un divisore dello zero è un divisore dello zero.
- I divisori dello zero formano un ideale rispetto al prodotto. Il concetto di ideale sarà sviluppato in seguito.
- Esercizio: dimostrare i primi tre punti.

Verifica proprietà ed esercizi alla lavagna.

- Esercizi Tabelle pitagoriche e potenze in $\mathbb{Z}_n^*$; calcolo delle ciclicità.

Verifica proprietà ed esercizi alla lavagna.

- Esercizi Tabelle pitagoriche e potenze in $\mathbb{Z}_n^*$; calcolo delle ciclicità.
- Esempi Isomorfismi interni.

Verifica proprietà ed esercizi alla lavagna.

- Esercizi Tabelle pitagoriche e potenze in $\mathbb{Z}_n^*$; calcolo delle ciclicità.
- Esempi Isomorfismi interni.
- Calcolo rapido dei periodi (prossima lezione).

Verifica proprietà ed esercizi alla lavagna.

- Esercizi Tabelle pitagoriche e potenze in $\mathbb{Z}_n^*$; calcolo delle ciclicità.
- Esempi Isomorfismi interni.
- Calcolo rapido dei periodi (prossima lezione).
- Calcolo delle potenze con Octave (prossima lezione).

Messaggio

- Abbiamo visto le prime trasformazioni algebriche di anelli (numeri minori di un valore assegnato) in se. Un modo per dare una (particolare) permutazione è fornire un numero per cui moltiplicare (modulo n), ma come vedremo in seguito, non è una crifratura molto solida.

Messaggio

- Abbiamo visto le prime trasformazioni algebriche di anelli (numeri minori di un valore assegnato) in se. Un modo per dare una (particolare) permutazione è fornire un numero per cui moltiplicare (modulo n), ma come vedremo in seguito, non è una crifratura molto solida.
- Abbiamo introdotto dei criteri approssimati (necessari ma non sufficienti) di primalità: pseudo-primalità.

Messaggio

- Abbiamo visto le prime trasformazioni algebriche di anelli (numeri minori di un valore assegnato) in se. Un modo per dare una (particolare) permutazione è fornire un numero per cui moltiplicare (modulo n), ma come vedremo in seguito, non è una crifratura molto solida.
- Abbiamo introdotto dei criteri approssimati (necessari ma non sufficienti) di primalità: pseudo-primalità.
- Abbiamo calcolato alcune potenze dei numeri negli anelli.

Messaggio

- Abbiamo visto le prime trasformazioni algebriche di anelli (numeri minori di un valore assegnato) in se. Un modo per dare una (particolare) permutazione è fornire un numero per cui moltiplicare (modulo n), ma come vedremo in seguito, non è una crifratura molto solida.
- Abbiamo introdotto dei criteri approssimati (necessari ma non sufficienti) di primalità: pseudo-primalità.
- Abbiamo calcolato alcune potenze dei numeri negli anelli.
- Abbiamo visto che elevando un numero alla funzione di Eulero si ottiene (quasi sempre) l'unità.