Anelli ciclici

Gregorio D'Agostino

13 Aprile 2021

Comunicazioni

Ciclicità

Ciclicity

Gauss

Carmichael

Comunicazioni Esami e lezioni

- Le lezioni dovrebbero durare fino a Giugno, ma continueremo solo martedì e venerdì.

Comunicazioni Esami e lezioni

- Le lezioni dovrebbero durare fino a Giugno, ma continueremo solo martedì e venerdì.
- Martedì in presenza ma solo se avete altre lezioni.

Comunicazioni Esami e lezioni

- Le lezioni dovrebbero durare fino a Giugno, ma continueremo solo martedì e venerdì.
- Martedì in presenza ma solo se avete altre lezioni.
- Devo fissare le date per l'appello: ne sono previsti due ma siete solo tre. Non è chiaro in che forma si faranno. Chiedete anche per gli altri corsi quando sono previsti.

Comunicazioni Esami e lezioni

- Le lezioni dovrebbero durare fino a Giugno, ma continueremo solo martedì e venerdì.
- Martedì in presenza ma solo se avete altre lezioni.
- Devo fissare le date per l'appello: ne sono previsti due ma siete solo tre. Non è chiaro in che forma si faranno. Chiedete anche per gli altri corsi quando sono previsti.
- Ci sarà un scritto di 1-2 ore (se online 1 ora) e l'orale subito dopo.

Quando un gruppo moltiplicativo $(\mathbb{Z}_n^*, x)$ è ciclico? cioè quando ammette un generatore?

- Il problema fondamentale dei gruppi moltiplicativi $(\mathbb{Z}_n^*, x)$ è capire se esiste un generatore. Questo consente di trovare notevoli proprietà per lo spazio ed in particolare per i periodi dei suoi elementi.

Quando un gruppo moltiplicativo $(\mathbb{Z}_n^*, x)$ è ciclico? cioè quando ammette un generatore?

- Il problema fondamentale dei gruppi moltiplicativi $(\mathbb{Z}_n^*, x)$ è capire se esiste un generatore. Questo consente di trovare notevoli proprietà per lo spazio ed in particolare per i periodi dei suoi elementi.
- Dimostreremo che tutti e soli gli spazi che ammettono un generatore sono $(\mathbb{Z}_p^*, x)$ (con p primo), $(\mathbb{Z}_{p^k}^*, x)$ (con p primo dispari), $(\mathbb{Z}_{2p^k}^*, x)$, $\mathbb{Z}_2^*$ e $\mathbb{Z}_4^*$

Quando un gruppo moltiplicativo $(\mathbb{Z}_n^*, x)$ è ciclico? cioè quando ammette un generatore?

- Il problema fondamentale dei gruppi moltiplicativi $(\mathbb{Z}_n^*, x)$ è capire se esiste un generatore. Questo consente di trovare notevoli proprietà per lo spazio ed in particolare per i periodi dei suoi elementi.
- Dimostreremo che tutti e soli gli spazi che ammettono un generatore sono $(\mathbb{Z}_p^*, x)$ (con p primo), $(\mathbb{Z}_{p^k}^*, x)$ (con p primo dispari), $(\mathbb{Z}_{2p^k}^*, x)$, $\mathbb{Z}_2^*$ e $\mathbb{Z}_4^*$
- In altri termini, $(\mathbb{Z}_n^*, x)$ è un gruppo ciclico se e solo se n è della forma su dette:

$$n = 2^{\alpha} p^{h};$$

con $\alpha = \{0, 1\}$ e p primo dispari oppure $p = 2$ e $h = 1$.

Periodi degli elementi dei Gruppi Ciclici

- Dato un gruppo ciclico G di cardinalità $N = |G|$, generato da un generatore g:

$$G \stackrel{def}{=} \left\{1, g, g^2, \ldots, g^{N-1}\right\} \stackrel{def}{=} \{g_0, g_1, g_2, \ldots, g_{N-1}\}.$$

  Valgono diverse proprietà utili:

Periodi degli elementi dei Gruppi Ciclici

- Dato un gruppo ciclico G di cardinalità $N = |G|$, generato da un generatore g:

$$G \stackrel{def}{=} \left\{1, g, g^2, \ldots, g^{N-1}\right\} \stackrel{def}{=} \{g_0, g_1, g_2, \ldots, g_{N-1}\}.$$

Valgono diverse proprietà utili:

- Ogni generatore ha periodo $\tau = N$. Infatti tutti gli elementi devono essere diversi tra loro:

$$g^k \neq g^m;$$

altrimenti se $\tau < N$, per $m = k + \tau$: $g^m = g^{k+\tau}$.

Periodi degli elementi dei Gruppi Ciclici

- Dato un gruppo ciclico G di cardinalità $N = |G|$, generato da un generatore g:

$$G \stackrel{def}{=} \left\{1, g, g^2, \ldots, g^{N-1}\right\} \stackrel{def}{=} \{g_0, g_1, g_2, \ldots, g_{N-1}\}.$$

Valgono diverse proprietà utili:

- Ogni generatore ha periodo $\tau = N$. Infatti tutti gli elementi devono essere diversi tra loro:

$$g^k \neq g^m;$$

altrimenti se $\tau < N$, per $m = k + \tau$: $g^m = g^{k+\tau}$.

- Quindi $g^k = 1$ implica $k = l \cdot N$ [k multiplo di N].

Periodi degli elementi dei Gruppi Ciclici

- Dato un gruppo ciclico G di cardinalità $N = |G|$, generato da un generatore g:

$$G \stackrel{def}{=} \left\{1, g, g^2, \ldots, g^{N-1}\right\} \stackrel{def}{=} \{g_0, g_1, g_2, \ldots, g_{N-1}\}.$$

Valgono diverse proprietà utili:

- Ogni generatore ha periodo $\tau = N$. Infatti tutti gli elementi devono essere diversi tra loro:

$$g^k \neq g^m;$$

altrimenti se $\tau < N$, per $m = k + \tau$: $g^m = g^{k+\tau}$.

- Quindi $g^k = 1$ implica $k = l \cdot N$ [k multiplo di N].
- Il periodo di ogni elemento è un divisore di N:

$$a^\tau = (g^k)^\tau = g^{k\tau} \Rightarrow k\tau = l \cdot N.$$

ne dedurremo che il periodo di g_k è il rapporto tra N ed MCD tra N e k.

Il periodo di un elemento di ordine k

- In un gruppo ciclico di ordine N; se $a = g_k = g^k$ il suo periodo è pari a N diviso per (k,N).
  Dim: Abbiamo visto che

$$k\tau = l \cdot N.$$

Il periodo di un elemento di ordine k

- In un gruppo ciclico di ordine N; se $a = g_k = g^k$ il suo periodo è pari a N diviso per (k,N).
  Dim: Abbiamo visto che

$$k\tau = l \cdot N.$$

- Sia M=(k,N) il MCD tra N e k. Possiamo porre:

$$\begin{cases} k' & \stackrel{def}{=} & k/M \\ N' & \stackrel{def}{=} & N/M \end{cases}$$

Il periodo di un elemento di ordine k

- In un gruppo ciclico di ordine N; se $a = g_k = g^k$ il suo periodo è pari a N diviso per (k,N).
  Dim: Abbiamo visto che

$$k\tau = l \cdot N.$$

- Sia M=(k,N) il MCD tra N e k. Possiamo porre:

$$\begin{cases} k' & \stackrel{def}{=} & k/M \\ N' & \stackrel{def}{=} & N/M \end{cases}$$

- Quindi

$$k'\tau = l \cdot N'.$$

  il più piccolo dei τ si ottiene per $l = k'$ e $\tau = N'$. Infatti k' e N' sono primi tra loro e quindi per l'unicità della decomposizione in fattori τ è un multiplo di $N' = N/M$.

Generatori di $\mathbb{Z}_p^*$

- Dimostreremo che $(\mathbb{Z}_p^*, x)$ (con p primo) ammette sempre un generatore e dunque ne ammette $\phi(N) = \phi(\phi(p))$. Useremo i seguenti lemmi:

Generatori di $\mathbb{Z}_p^*$

- Dimostreremo che $(\mathbb{Z}_p^*, x)$ (con p primo) ammette sempre un generatore e dunque ne ammette $\phi(N) = \phi(\phi(p))$. Useremo i seguenti lemmi:
- Lemma 1: "Commensurabilità": Se un elemento ha due ciclicità prime tra loro allora è l'elemento neutro.

Generatori di $\mathbb{Z}_p^*$

- Dimostreremo che $(\mathbb{Z}_p^*, x)$ (con p primo) ammette sempre un generatore e dunque ne ammette $\phi(N) = \phi(\phi(p))$. Useremo i seguenti lemmi:
- Lemma 1: "Commensurabilità": Se un elemento ha due ciclicità prime tra loro allora è l'elemento neutro.
- Lemma 2: "Prodotto": Se due elementi hanno periodi primi tra loro, il loro prodotto ha per periodo il prodotto dei periodi.

Generatori di $\mathbb{Z}_p^*$

- Dimostreremo che $(\mathbb{Z}_p^*, x)$ (con p primo) ammette sempre un generatore e dunque ne ammette $\phi(N) = \phi(\phi(p))$. Useremo i seguenti lemmi:
- Lemma 1: "Commensurabilità": Se un elemento ha due ciclicità prime tra loro allora è l'elemento neutro.
- Lemma 2: "Prodotto": Se due elementi hanno periodi primi tra loro, il loro prodotto ha per periodo il prodotto dei periodi.
- Lemma 3: Unicità delle radici di ogni grado in un campo.

Generatori di $\mathbb{Z}_p^*$

- Dimostreremo che $(\mathbb{Z}_p^*, x)$ (con p primo) ammette sempre un generatore e dunque ne ammette $\phi(N) = \phi(\phi(p))$. Useremo i seguenti lemmi:
- Lemma 1: "Commensurabilità": Se un elemento ha due ciclicità prime tra loro allora è l'elemento neutro.
- Lemma 2: "Prodotto": Se due elementi hanno periodi primi tra loro, il loro prodotto ha per periodo il prodotto dei periodi.
- Lemma 3: Unicità delle radici di ogni grado in un campo.
- Mettendo insieme i lemmi si deduce che il massimo periodo di $\mathbb{Z}_p^*$ è $p-1$ e dunque ammette un generatore ed è ciclico.

Solo l'elemento neutro possiede ciclicità prime tra loro

Dimostrazione usando l'algoritmo di iterativo di Euclide.

- Una ciclicità di un elemento è una potenza elevata alla quale si ottiene l'unità. L'elemento a è ciclico di ordine k significa:

$$a^k = 1.$$

Solo l'elemento neutro possiede ciclicità prime tra loro

Dimostrazione usando l'algoritmo di iterativo di Euclide.

- Una ciclicità di un elemento è una potenza elevata alla quale si ottiene l'unità. L'elemento a è ciclico di ordine k significa:

$$a^k = 1.$$

- Per ogni coppia m e k primi tra loro (con $m > k$), si può utilizzare l'algoritmo di Euclide per ottenere un sistema di equazioni con esponenti minori.

$$\begin{cases} a^k = 1, \\ a^m = 1; \end{cases} \Rightarrow \begin{cases} a^k = 1, \\ a^{k\cdot q+r} = 1; \end{cases} \Rightarrow \begin{cases} a^k = 1, \\ a^r = 1; \end{cases}$$

in cui r è il resto della divisione di m per k: $m = k \cdot q + r$ e quindi $r < k < m$.

Solo l'elemento neutro possiede ciclicità prime tra loro

Dimostrazione usando l'algoritmo di iterativo di Euclide.

- Una ciclicità di un elemento è una potenza elevata alla quale si ottiene l'unità. L'elemento a è ciclico di ordine k significa:

$$a^k = 1.$$

- Per ogni coppia m e k primi tra loro (con $m > k$), si può utilizzare l'algoritmo di Euclide per ottenere un sistema di equazioni con esponenti minori.

$$\begin{cases} a^k = 1, \\ a^m = 1; \end{cases} \Rightarrow \begin{cases} a^k = 1, \\ a^{k\cdot q+r} = 1; \end{cases} \Rightarrow \begin{cases} a^k = 1, \\ a^r = 1; \end{cases}$$

  in cui r è il resto della divisione di m per k: $m = k \cdot q + r$ e quindi $r < k < m$.

- L'algoritmo di Euclide ci assicura che iterando il procedimento si ottiene il MCD che in questo caso è un esponente unitario, essendo $MCD = (k, m) = 1$. Quindi solo $a = 1$ possiede entrambe le ciclicità.

Ogni elemento di Z_n^* possiede un inverso di stesso periodo

- Ogni elemento a primo con n (quindi $a \in Z_n^*$), deve possedere un periodo τ_a (divisore di $\phi(n)$): $a^k = 1 \Rightarrow k = l\tau_a$.

Ogni elemento di Z_n^* possiede un inverso di stesso periodo

- Ogni elemento a primo con n (quindi $a \in Z_n^*$), deve possedere un periodo τ_a (divisore di $\phi(n)$): $a^k = 1 \Rightarrow k = l\tau_a$.
- Come abbiamo già visto, esiste sempre $b = a^{\tau_a - 1}$ che è l'inverso di a:

$$inv(a) \cdot a = a^{\tau_a - 1} \cdot a = a^{\tau_a} = 1.$$

Siccome $\tau_a - 1$ e τ_a sono sempre primi tra loro, a e b hanno lo stesso periodo.

Ogni elemento di Z_n^* possiede un inverso di stesso periodo

- Ogni elemento a primo con n (quindi $a \in Z_n^*$), deve possedere un periodo τ_a (divisore di $\phi(n)$): $a^k = 1 \Rightarrow k = l\tau_a$.
- Come abbiamo già visto, esiste sempre $b = a^{\tau_a - 1}$ che è l'inverso di a:

$$inv(a) \cdot a = a^{\tau_a - 1} \cdot a = a^{\tau_a} = 1.$$

  Siccome $\tau_a - 1$ e τ_a sono sempre primi tra loro, a e b hanno lo stesso periodo.
- Calcoliamo le potenze dell'inverso:

$$(inv(a))^k = \left(a^{\tau_a - 1}\right)^k = a^{(\tau_a - 1) \cdot k}.$$

Ogni elemento di Z_n^* possiede un inverso di stesso periodo

- Ogni elemento a primo con n (quindi $a \in Z_n^*$), deve possedere un periodo τ_a (divisore di $\phi(n)$): $a^k = 1 \Rightarrow k = l\tau_a$.
- Come abbiamo già visto, esiste sempre $b = a^{\tau_a - 1}$ che è l'inverso di a:

$$inv(a) \cdot a = a^{\tau_a - 1} \cdot a = a^{\tau_a} = 1.$$

  Siccome $\tau_a - 1$ e τ_a sono sempre primi tra loro, a e b hanno lo stesso periodo.
- Calcoliamo le potenze dell'inverso:

$$(inv(a))^k = \left(a^{\tau_a - 1}\right)^k = a^{(\tau_a - 1)\cdot k}.$$

- Verifichiamo che potenze k-esime di $inv(a)$ sono diverse da 1 per $k < \tau_a$. Se $inv(a)^k = 1$

$$(inv(a))^k = \left(a^{\tau_a - 1}\right)^k = a^{(\tau_a - 1)\cdot k} = a^{\tau_a (k-1)} a^{\tau_a - k} = a^{\tau_a - k}.$$

  Ma, per definizione di periodo, $a^{\tau_a - k} = 1$ solo per $\tau_a - k = l \cdot \tau_a$, cioè $k = \tau_a$ e $l = 0$ (essendo $k < \tau_a$).

Se due elementi hanno periodi primi tra loro, allora il periodo del loro prodotto è il prodotto dei loro periodi:

- Siano τ_a il periodo di a e τ_b il periodo di b:

$$\begin{cases} a^k = 1, \\ b^j = 1; \end{cases} \Rightarrow \begin{cases} k = l \cdot \tau_a, \\ j = l' \cdot \tau_b; \end{cases}$$

Se due elementi hanno periodi primi tra loro, allora il periodo del loro prodotto è il prodotto dei loro periodi:

- Siano τ_a il periodo di a e τ_b il periodo di b:

$$\begin{cases} a^k = 1, \\ b^j = 1; \end{cases} \Rightarrow \begin{cases} k = l \cdot \tau_a, \\ j = l' \cdot \tau_b; \end{cases}$$

- Effettivamente $m = \tau_a \cdot \tau_b$ è una ciclicità di ab:

$$(ab)^m = (ab)^{\tau_a \tau_b} = a^{\tau_a \tau_b} \cdot b^{\tau_a \tau_b} = (a^{\tau_a})^{\tau_b} \cdot (b^{\tau_b})^{\tau_a} = 1^{\tau_b} \cdot 1^{\tau_a} = 1.$$

Se due elementi hanno periodi primi tra loro, allora il periodo del loro prodotto è il prodotto dei loro periodi:

- Siano τ_a il periodo di a e τ_b il periodo di b:

$$\begin{cases} a^k = 1, \\ b^j = 1; \end{cases} \Rightarrow \begin{cases} k = l \cdot \tau_a, \\ j = l' \cdot \tau_b; \end{cases}$$

- Effettivamente $m = \tau_a \cdot \tau_b$ è una ciclicità di ab:

$$(ab)^m = (ab)^{\tau_a \tau_b} = a^{\tau_a \tau_b} \cdot b^{\tau_a \tau_b} = \left(a^{\tau_a}\right)^{\tau_b} \cdot \left(b^{\tau_b}\right)^{\tau_a} = 1^{\tau_b} \cdot 1^{\tau_a} = 1.$$

- Verifichiamo che non esistono ciclicità k minori di $m = \tau_a \cdot \tau_b$:

$$(ab)^m = 1;$$

Elevando entrambi i membri dell'equazione a τ_a ed a τ_b si ottiene:

$$\begin{cases} \left((ab)^k\right)^{\tau_a} = a^{k\tau_a} \cdot b^{k\tau_a} = b^{k\tau_a} = 1, \\ \left((ab)^k\right)^{\tau_b} = a^{k\tau_b} \cdot b^{k\tau_b} = a^{k\tau_b} = 1; \end{cases}$$

quindi k deve essere un multiplo di τ_b per la prima equazione ed un multiplo di τ_a per la seconda: cioè k è multiplo di m.

Periodi e radici dell'unità

- Dire che un elemento x ha ciclicità q in $\mathbb{Z}_p^*$ significa che soddisfa l'equazione diofantea:

$$x^q \equiv 1 \ (mod \ p).$$

Periodi e radici dell'unità

- Dire che un elemento x ha ciclicità q in $\mathbb{Z}_p^*$ significa che soddisfa l'equazione diofantea:

$$x^q \equiv 1 \ (mod \ p).$$

- Quando si trova un elemento x che soddisfa l'equazione si dice che si è trovata una radice q-esima dell'unità.

Periodi e radici dell'unità

- Dire che un elemento x ha ciclicità q in $\mathbb{Z}_p^*$ significa che soddisfa l'equazione diofantea:

$$x^q \equiv 1 \ (mod \ p).$$

- Quando si trova un elemento x che soddisfa l'equazione si dice che si è trovata una radice q-esima dell'unità.
- Per il piccolo teorema di Fermat, una condizione necessaria affinché esistano radici q-esime dell'unità è che q sia un divisore di $\phi(p) = p - 1$.

Periodi e radici dell'unità

- Dire che un elemento x ha ciclicità q in $\mathbb{Z}_p^*$ significa che soddisfa l'equazione diofantea:

$$x^q \equiv 1 \ (mod \ p).$$

- Quando si trova un elemento x che soddisfa l'equazione si dice che si è trovata una radice q-esima dell'unità.
- Per il piccolo teorema di Fermat, una condizione necessaria affinché esistano radici q-esime dell'unità è che q sia un divisore di $\phi(p) = p - 1$.
- vedremo che le radici q-esime dell'unità sono tutte e sole le potenze di un elemento di periodo q.

Unicità delle radici dell'unità

- Th: "Dato un elemento a di periodo q in un anello primale $\mathbb{Z}_p$, l'equazione diofantea ammette per soluzioni solo le potenze di a":

$$x^q \equiv 1 \ (mod \ p).$$

Unicità delle radici dell'unità

- Th: "Dato un elemento a di periodo q in un anello primale $\mathbb{Z}_p$, l'equazione diofantea ammette per soluzioni solo le potenze di a":

$$x^q \equiv 1 \ (mod \ p).$$

- Utilizzeremo una notevole identità (in x):

$$x^q - 1 \equiv (x-1)\cdot(x-a)\cdots(x-a_{q-1}) \equiv \prod_{i=0}^{q-1} (x - a_i) \equiv 1 \ (mod \ p).$$

in cui $a_i \stackrel{def}{=} (a)^i$.

Unicità delle radici dell'unità

- Th: "Dato un elemento a di periodo q in un anello primale $\mathbb{Z}_p$, l'equazione diofantea ammette per soluzioni solo le potenze di a":

$$x^q \equiv 1 \ (mod \ p).$$

- Utilizzeremo una notevole identità (in x):

$$x^q - 1 \equiv (x-1)\cdot(x-a)\cdots(x-a_{q-1}) \equiv \prod_{i=0}^{q-1} (x - a_i) \equiv 1 \ (mod \ p).$$

  in cui $a_i \stackrel{def}{=} (a)^i$.
- Per dimostrare l'identità sviluppiamo il prodotto. Il termine di ordine più elevato è x^q.

Unicità delle radici dell'unità

- Th: "Dato un elemento a di periodo q in un anello primale $\mathbb{Z}_p$, l'equazione diofantea ammette per soluzioni solo le potenze di a":

$$x^q \equiv 1 \ (mod \ p).$$

- Utilizzeremo una notevole identità (in x):

$$x^q - 1 \equiv (x-1)\cdot(x-a)\cdots(x-a_{q-1}) \equiv \prod_{i=0}^{q-1} (x - a_i) \equiv 1 \ (mod \ p).$$

  in cui $a_i \stackrel{def}{=} (a)^i$.
- Per dimostrare l'identità sviluppiamo il prodotto. Il termine di ordine più elevato è x^q.
- Il secondo termine è:

$$-x^{q-1} \left(\sum_{i=0}^{q-1} a_i \right);$$

  perché in ogni fattore del prodotto dove non si prende x, si sceglie un a_i diverso.

Unicità delle radici dell'unità - cont

- Il coefficiente del secondo termine è nullo:

$$\sum_{i=0,q-1} a_i = \sum_{i=0}^{q-1} a^i = \frac{1-a^q}{1-a} = \frac{1-1}{1-a} = 0.$$

Unicità delle radici dell'unità - cont

- Il coefficiente del secondo termine è nullo:

$$\sum_{i=0,q-1} a_i = \sum_{i=0}^{q-1} a^i = \frac{1-a^q}{1-a} = \frac{1-1}{1-a} = 0.$$

- Il terzo termine è:

$$x^{q-2} \left(\sum_{i=0}^{q-1} \sum_{j=0}^{q-1} {}^{(j \neq i)} a_i a_j \right);$$

perché in ogni fattore del prodotto dove non si prende x si sceglie a_i o a_j al posto di x, ma i non può essere uguale a j.

Unicità delle radici dell'unità - cont

- Il coefficiente del secondo termine è nullo:

$$\sum_{i=0,q-1} a_i = \sum_{i=0}^{q-1} a^i = \frac{1-a^q}{1-a} = \frac{1-1}{1-a} = 0.$$

- Il terzo termine è:

$$x^{q-2}\left(\sum_{i=0}^{q-1}\sum_{j=0}^{q-1}{}^{(j\neq i)} a_i a_j\right);$$

perché in ogni fattore del prodotto dove non si prende x si sceglie a_i o a_j al posto di x, ma i non può essere uguale a j.

- Anche questo coefficiente è nullo:

$$\sum_{i=0}^{q-1}\sum_{j=0}^{q-1}{}^{(j\neq i)} a_i a_j = \sum_{i=0}^{q-1} a_i \left[\left(\sum_{j=0}^{q-1} a_j\right) - a_i\right] =$$

$$= \left(\sum_{i=0}^{q-1} a_i\right)^2 + \sum_{i=0}^{q-1} a_i^2 = (0)^2 + \sum_{i=0}^{q-1} a^{2i} = \frac{1-(a^2)^q}{1-a^2} = 0.$$

Unicità delle radici dell'unità - cont

- Il coefficiente del quarto termine è:

$$C_4 = -\sum_{i=0}^{q-1} \left(\sum_{j=0}^{q-1} {}^{(j \neq i)} \left(\sum_{k=0}^{q-1} {}^{(k \neq i,j)} \left(a_i a_j a_k \right) \right) \right) .$$

Unicità delle radici dell'unità - cont

- Il coefficiente del quarto termine è:

$$C_4 = -\sum_{i=0}^{q-1}\left(\sum_{j=0}^{q-1}{}^{(j\neq i)}\left(\sum_{k=0}^{q-1}{}^{(k\neq i,j)}\left(a_i a_j a_k\right)\right)\right).$$

- Anche questo può essere elaborato:

$$C_4 = -\sum_i a_i\left(\sum_{j\neq i} a_j\left(\sum_k a_k - a_i - a_j\right)\right);$$

$$C_4 = -\left(\sum_i a_i \sum_{j\neq i}\left(a_j\left(\sum_k a_k - a_j\right) - \sum_i (a_i)^2 \sum_{j\neq i} a_j\right)\right);$$

$$C_4 = -\sum_i a_i \sum_j a_j \sum_k a_k + \sum_i a_i \sum_j a_j^2 + \sum_i a_i^2 \sum_j a_j - \sum_i a_i^3 = 0;$$

Unicità delle radici dell'unità - cont

- In generale il procedimento può essere reiterato. Tutti i coefficienti vengono in forma di prodotti del tipo:

$$\sum_{i=0}^{q-1}(a_i)^r = 0;$$

che sono tutti nulli fatta eccezione per $r = q$:

$$\sum_{i=0}^{q-1}(a_i)^q = \sum_{i=0}^{q-1} a^{iq} = \sum_{i=0}^{q-1}(a^q)^i = \sum_{i=0}^{q-1} 1 = q + 1 = 1;$$

Unicità delle radici dell'unità - cont

- In generale il procedimento può essere reiterato. Tutti i coefficienti vengono in forma di prodotti del tipo:

$$\sum_{i=0}^{q-1}(a_i)^r = 0;$$

che sono tutti nulli fatta eccezione per $r = q$:

$$\sum_{i=0}^{q-1}(a_i)^q = \sum_{i=0}^{q-1} a^{iq} = \sum_{i=0}^{q-1}(a^q)^i = \sum_{i=0}^{q-1} 1 = q + 1 = 1;$$

- L'ultimo coefficiente è quindi -1. Si può anche verificare direttamente essendo il prodotto di tutti i termini non contenenti la x:

$$\prod_{i=0}^{q-1}(-a_i) = (-1)^q \prod_{i=0}^{q-1} a^i = -\left(a^{\sum_{i=0}^{q-1} i}\right) = -a^{q(q-1)/2} = -1.$$

Unicità delle radici dell'unità: induzione

- Per dimostrare formalmente la nullità di tutti i coefficienti, bisogna (come sempre) utilizzare l'induzione. In questo caso la proposizione da dimostrare è la seguente:
"Qualunque somma simmetrica di prodotti di potenze di una radice primaria a è nulla se la somma degli esponenti è minore di q"

$$\sum_{\substack{k_1,\ldots,k_m \\ k_i \in [0,q-1]}} \prod_{i=0}^{m} (a^{h_i})^{k_i} = 0 \quad \forall h_1, \ldots, h_m : \sum_{i=1,m} h_i < q;$$

in cui il simbolo $[k_1, \ldots, k_m]$ indica tutte le possibili m-ple di interi diversi tra loro.

Unicità delle radici dell'unità: induzione

- Per dimostrare formalmente la nullità di tutti i coefficienti, bisogna (come sempre) utilizzare l'induzione. In questo caso la proposizione da dimostrare è la seguente:
  "Qualunque somma simmetrica di prodotti di potenze di una radice primaria a è nulla se la somma degli esponenti è minore di q"

$$\sum_{\substack{k_1,\ldots,k_m \\ k_i \in [0,q-1]}} \prod_{i=0}^{m} (a^{h_i})^{k_i} = 0 \quad \forall h_1, \ldots, h_m : \sum_{i=1,m} h_i < q;$$

  in cui il simbolo $[k_1, \ldots, k_m]$ indica tutte le possibili m-ple di interi diversi tra loro.
- Lo dimostriamo per induzione su m.

Unicità delle radici dell'unità: induzione

- Caso $m = 1$

$$\sum_{k_1 \in [0, q-1]} (a^{h_1})^{k_1} = 0 \quad \forall h_1 < q.$$

utilizzando la formula chiusa delle serie geometriche:

$$\sum_{k_1 \in [0, q-1]} (a^{h_1})^{k_1} = \frac{(a^{h_1})^q - 1}{a^{h_1} - 1};$$

che proiettata in Z_n^* si annulla per $a^{h_1} - 1$ prima con n. Nel caso degli anelli primali equivale ad $a \neq 1$.

Unicità delle radici dell'unità: induzione

- Caso $m = 1$

$$\sum_{k_1 \in [0, q-1]} (a^{h_1})^{k_1} = 0 \quad \forall h_1 < q.$$

utilizzando la formula chiusa delle serie geometriche:

$$\sum_{k_1 \in [0, q-1]} (a^{h_1})^{k_1} = \frac{(a^{h_1})^q - 1}{a^{h_1} - 1};$$

che proiettata in Z_n^* si annulla per $a^{h_1} - 1$ prima con n. Nel caso degli anelli primali equivale ad $a \neq 1$.

- Vediamo la formula di ricorrenza:

Unicità delle radici dell'unità: induzione

- Caso $m+1$

$$\sum_{\substack{k_1,\ldots,k_{m+1}\\ k_i\in[0,q-1]}} \prod_{i=0}^{m+1}(a^{h_i})^{k_i} = \sum_{\substack{k_1,\ldots,k_{m+1}\\ k_i\in[0,q-1]}} \prod_{i=0}^{m}(a^{h_i})^{k_i}(a^{h_{m+1}})^{k_{m+1}} =$$

$$= \sum_{\substack{k_1,\ldots,k_m\\ k_i\in[0,q-1]}} \sum_{k_{m+1}=0,q-1} \left[\prod_{i=0}^{m}(a^{h_i})^{k_i}\right] \left[(a^{h_{m+1}})^{k_{m+1}} - \sum_{j=1,m}(a^{h_{m+1}})^{k}_{j}\right] =$$

$$= \left[\sum_{k_{m+1}=0,q-1}(a^{h_{m+1}})^{k_{m+1}}\right] \left[\sum_{\substack{k_1,\ldots,k_m\\ k_i\in[0,q-1]}} \prod_{i=0}^{m}(a^{h_i})^{k_i}\right] -$$

$$\sum_{\substack{k_1,\ldots,k_m\\ k_i\in[0,q-1]}} \prod_{i=0}^{m}(a^{h_i})^{k_i} \left[\sum_{j=1,m}(a^{h_{m+1}})^{k_j}\right] =$$

Unicità delle radici dell'unità: induzione cont.

- Il termine

$$\left[\sum_{k_{m+1}=0,q-1}(a^{h_{m+1}})^{k_{m+1}}\right]\left[\sum_{\substack{k_1,\ldots,k_m \\ k_i\in[0,q-1]}}\prod_{i=0}^{m}(a^{h_i})^{k_i}\right]-$$

si annulla essendo il primo fattore pari a $[(a^{h_{m+1}})^q-1]/[a^{h_{m+1}}-1]$ quando $a^{h_{m+1}}-1$ è diverso da zero.

Unicità delle radici dell'unità: induzione cont.

- Il termine

$$\left[\sum_{k_{m+1}=0,q-1}(a^{h_{m+1}})^{k_{m+1}}\right]\left[\sum_{\substack{k_1,\ldots,k_m\\ k_i\in[0,q-1]}}\prod_{i=0}^{m}(a^{h_i})^{k_i}\right]-$$

si annulla essendo il primo fattore pari a $[(a^{h_{m+1}})^q-1]/[a^{h_{m+1}}-1]$ quando $a^{h_{m+1}}-1$ è diverso da zero.

- Tutti gli altri termini sono della forma:

$$\sum_{\substack{k_1,\ldots,k_m\\ k_i\in[0,q-1]}}\prod_{i=0}^{m}(a^{h_i})^{k_i}[(a^{h_{m+1}})^{k_j}]=\sum_{\substack{k_1,\ldots,k_m\\ k_i\in[0,q-1]}}\prod_{i=0}^{j-1}(a^{h_i})^{k_i}(a^{h_j+h_{m+1}})^{k_j}\prod_{i=0}^{m}(a^{h_i})^{k_i};$$

e si annullano per ipotesi di ricorrenza ponendo $h'_j \stackrel{def}{=} h_j+h_{m+1}$ e $h'_i=h_i$ per $i\neq j$.

Unicità delle radici dell'unità: induzione cont.

- Il termine

$$\left[\sum_{k_{m+1}=0,q-1}(a^{h_{m+1}})^{k_{m+1}}\right]\left[\sum_{\substack{k_1,\ldots,k_m\\ k_i\in[0,q-1]}}\prod_{i=0}^{m}(a^{h_i})^{k_i}\right]-$$

  si annulla essendo il primo fattore pari a $[(a^{h_{m+1}})^q-1]/[a^{h_{m+1}}-1]$ quando $a^{h_{m+1}}-1$ è diverso da zero.

- Tutti gli altri termini sono della forma:

$$\sum_{\substack{k_1,\ldots,k_m\\ k_i\in[0,q-1]}}\prod_{i=0}^{m}(a^{h_i})^{k_i}[(a^{h_{m+1}})^{k_j}]=\sum_{\substack{k_1,\ldots,k_m\\ k_i\in[0,q-1]}}\prod_{i=0}^{j-1}(a^{h_i})^{k_i}(a^{h_j+h_{m+1}})^{k_j}\prod_{i=0}^{m}(a^{h_i})^{k_i};$$

  e si annullano per ipotesi di ricorrenza ponendo $h'_j \stackrel{def}{=} h_j+h_{m+1}$ e $h'_i=h_i$ per $i\neq j$.

- La condizione $\sum_{i=1,m}h'_i<q$ è rispettata perché $\sum_{i=1,m}h'_i=\sum_{i=1,m+1}h_i<q$

Unicità delle radici dell'unità - cont

- L'equazione diofantea

$$x^q - 1 = \ (mod\ p);$$

non può ammettere soluzioni diverse dalle potenze di a:

$$x^q - 1 = (x-1)\cdot(x-a)\cdot(x-a^2)\cdots(x-a^{q-1}) = 0\ (mod\ p);$$

Unicità delle radici dell'unità - cont

- L'equazione diofantea

$$x^q - 1 = \ (mod\ p);$$

non può ammettere soluzioni diverse dalle potenze di a:

$$x^q - 1 = (x-1)\cdot(x-a)\cdot(x-a^2)\cdots(x-a^{q-1}) = 0\ (mod\ p);$$

- ovvero in $\mathbb{Z}$:

$$x^q - 1 = (x-1)\cdot(x-a)\cdot(x-a^2)\cdots(x-a^{q-1}) = p\cdot N.$$

Unicità delle radici dell'unità - cont

- L'equazione diofantea

$$x^q - 1 = \ (mod\ p);$$

non può ammettere soluzioni diverse dalle potenze di a:

$$x^q - 1 = (x-1)\cdot(x-a)\cdot(x-a^2)\cdots(x-a^{q-1}) = 0\ (mod\ p);$$

- ovvero in $\mathbb{Z}$:

$$x^q - 1 = (x-1)\cdot(x-a)\cdot(x-a^2)\cdots(x-a^{q-1}) = p\cdot N.$$

- Infatti p è primo e tutti i fattori $(x - a_k)$ sono (in valore assoluto) minori di p (e dunque primi con p).
In realtà avevamo già visto che $\mathbb{Z}_p^*$ è un campo e quindi se il prodotto di due elementi è nullo deve esserlo almeno uno di loro.

Unicità delle radici dell'unità - cont

- L'equazione diofantea

$$x^q - 1 = \ (mod\ p);$$

non può ammettere soluzioni diverse dalle potenze di a:

$$x^q - 1 = (x-1)\cdot(x-a)\cdot(x-a^2)\cdots(x-a^{q-1}) = 0\ (mod\ p);$$

- ovvero in $\mathbb{Z}$:

$$x^q - 1 = (x-1)\cdot(x-a)\cdot(x-a^2)\cdots(x-a^{q-1}) = p\cdot N.$$

- Infatti p è primo e tutti i fattori $(x - a_k)$ sono (in valore assoluto) minori di p (e dunque primi con p).
  In realtà avevamo già visto che $\mathbb{Z}_p^*$ è un campo e quindi se il prodotto di due elementi è nullo deve esserlo almeno uno di loro.
- In generale in ogni campo, la decomposizione di un polinomio (non solo di $x^q - 1$) è unica e quindi ci sono solo q radici. Ma non ci serve dimostrarlo.

Unicità delle radici dell'unità - cont

- L'equazione diofantea

$$x^q - 1 = \ (mod\ p);$$

non può ammettere soluzioni diverse dalle potenze di a:

$$x^q - 1 = (x-1)\cdot(x-a)\cdot(x-a^2)\cdots(x-a^{q-1}) = 0\ (mod\ p);$$

Unicità delle radici dell'unità - cont

- L'equazione diofantea

$$x^q - 1 = \ (mod\ p);$$

non può ammettere soluzioni diverse dalle potenze di a:

$$x^q - 1 = (x-1)\cdot(x-a)\cdot(x-a^2)\cdots(x-a^{q-1}) = 0\ (mod\ p);$$

- ovvero in $\mathbb{Z}$:

$$x^q - 1 = (x-1)\cdot(x-a)\cdot(x-a^2)\cdots(x-a^{q-1}) = p\cdot N.$$

Unicità delle radici dell'unità - cont

- L'equazione diofantea

$$x^q - 1 = \ (mod\ p);$$

non può ammettere soluzioni diverse dalle potenze di a:

$$x^q - 1 = (x-1)\cdot(x-a)\cdot(x-a^2)\cdots(x-a^{q-1}) = 0\ (mod\ p);$$

- ovvero in $\mathbb{Z}$:

$$x^q - 1 = (x-1)\cdot(x-a)\cdot(x-a^2)\cdots(x-a^{q-1}) = p\cdot N.$$

- Infatti p è primo e tutti i fattori $(x - a_k)$ sono (in valore assoluto) minori di p (e dunque primi con p).
In realtà avevamo già visto che $\mathbb{Z}_p^*$ è un campo e quindi se il prodotto di due elementi è nullo deve esserlo almeno uno di loro.

Unicità delle radici dell'unità - cont

- L'equazione diofantea

$$x^q - 1 = \ (mod\ p);$$

non può ammettere soluzioni diverse dalle potenze di a:

$$x^q - 1 = (x-1)\cdot(x-a)\cdot(x-a^2)\cdots(x-a^{q-1}) = 0\ (mod\ p);$$

- ovvero in $\mathbb{Z}$:

$$x^q - 1 = (x-1)\cdot(x-a)\cdot(x-a^2)\cdots(x-a^{q-1}) = p\cdot N.$$

- Infatti p è primo e tutti i fattori $(x - a_k)$ sono (in valore assoluto) minori di p (e dunque primi con p).
  In realtà avevamo già visto che $\mathbb{Z}_p^*$ è un campo e quindi se il prodotto di due elementi è nullo deve esserlo almeno uno di loro.
- In generale in ogni campo, la decomposizione di un polinomio (non solo di $x^q - 1$) è unica e quindi ci sono solo q radici. Ma non ci serve dimostrarlo.

Il massimo periodo di un elemento in un anello primale (che è un campo) coincide con la funzione di Eulero $p-1$

- Lo dimostreremo per assurdo. Supponiamo che esista un periodo massimo τ minore di $\phi = p-1$ e un elemento elemento g di tale periodo.

Il massimo periodo di un elemento in un anello primale (che è un campo) coincide con la funzione di Eulero $p-1$

- Lo dimostreremo per assurdo. Supponiamo che esista un periodo massimo τ minore di $\phi = p-1$ e un elemento elemento g di tale periodo.
- Consideriamo un elemento a che non è una potenza di g di periodo q.

Il massimo periodo di un elemento in un anello primale (che è un campo) coincide con la funzione di Eulero $p-1$

- Lo dimostreremo per assurdo. Supponiamo che esista un periodo massimo τ minore di $\phi = p-1$ e un elemento elemento g di tale periodo.
- Consideriamo un elemento a che non è una potenza di g di periodo q.
- Se q non è un divisore di τ allora il MCD di q e τ ($M = MCD(q, \tau)$) è diverso da q e quindi il periodo di a^M è q/M che è primo con τ. L'elemento $b = a^M \cdot g$ ha periodo $\tau \cdot q/M > \tau$. Il che è impossibile.

Il massimo periodo di un elemento in un anello primale (che è un campo) coincide con la funzione di Eulero $p-1$

- Lo dimostreremo per assurdo. Supponiamo che esista un periodo massimo τ minore di $\phi = p-1$ e un elemento elemento g di tale periodo.
- Consideriamo un elemento a che non è una potenza di g di periodo q.
- Se q non è un divisore di τ allora il MCD di q e τ ($M = MCD(q, \tau)$) è diverso da q e quindi il periodo di a^M è q/M che è primo con τ. L'elemento $b = a^M \cdot g$ ha periodo $\tau \cdot q/M > \tau$. Il che è impossibile.
- Se q è un divisore di τ allora a e $b = g^{\tau/q}$ hanno lo stesso periodo. Ma allora:

$$a^q - 1 = (a-1)\cdot(a-b)\cdot(a-b^2)\cdots(a-b^{q-1}) = 0 \pmod{p};$$

essendo $\mathbb{Z}_p^*$ un campo, uno dei fattori deve annullarsi, ma questo è impossibile perché per ipotesi a non è una potenza di g e quindi di b.

Theorema: “Ogni anello primale è ciclico”

- Abbiamo visto che esiste sempre un elemento di periodo massimo e quindi pari alla funzione di Eulero. Dunque esiste almeno un generatore.

Theorema: “Ogni anello primale è ciclico”

- Abbiamo visto che esiste sempre un elemento di periodo massimo e quindi pari alla funzione di Eulero. Dunque esiste almeno un generatore.
- Quindi il gruppo è ciclico.

Theorema: "Ogni anello primale è ciclico"

- Abbiamo visto che esiste sempre un elemento di periodo massimo e quindi pari alla funzione di Eulero. Dunque esiste almeno un generatore.
- Quindi il gruppo è ciclico.
- Se esiste un generatore g allora ne esistono $\phi(p-1)$ perchè tutte le potenze g^k ad un esponente k primo con $p-1$ hanno lo stesso periodo di g pari a $p-1$.

Teorema (di Gauss): Per ogni primo p dispari il gruppo moltiplicativo associato $(\mathbb{Z}^*_{p^h}, X)$ è ciclico.

- Anche per questo teorema serve qualche lemma preliminare.

Teorema (di Gauss): Per ogni primo p dispari il gruppo moltiplicativo associato $(\mathbb{Z}^*_{p^h}, X)$ è ciclico.

- Anche per questo teorema serve qualche lemma preliminare.
- Lemma 1: "Immersione dei periodi": Se un elemento ha periodo τ in $\mathbb{Z}^*_n$ ha un periodo almeno uguale in $\mathbb{Z}^*_{n \cdot m}$.

Teorema (di Gauss): Per ogni primo p dispari il gruppo moltiplicativo associato $(\mathbb{Z}^*_{p^h}, X)$ è ciclico.

- Anche per questo teorema serve qualche lemma preliminare.
- Lemma 1: "Immersione dei periodi": Se un elemento ha periodo τ in $\mathbb{Z}^*_n$ ha un periodo almeno uguale in $\mathbb{Z}^*_{n\cdot m}$.
- Lemma 2: Esistono elementi di periodo p^{h-1} in $(\mathbb{Z}^*_{p^h}, X)$

Lemma 1: Se un elemento ha periodo τ in $\mathbb{Z}_n^*$ ha un periodo maggiore o uguale in $\mathbb{Z}_{n \cdot m}^*$.

- a ha periodo τ in $\mathbb{Z}_n^*$ implica:

$$\begin{cases} a^{\tau} & \equiv & 1 & (mod\ n), \\ a^{k} & \not\equiv & 1 & (mod\ n) \quad (per\ k < \tau); \end{cases}$$

Lemma 1: Se un elemento ha periodo τ in $\mathbb{Z}_n^*$ ha un periodo maggiore o uguale in $\mathbb{Z}_{n \cdot m}^*$.

- a ha periodo τ in $\mathbb{Z}_n^*$ implica:

$$\begin{cases} a^{\tau} & \equiv & 1 & (mod\ n), \\ a^{k} & \not\equiv & 1 & (mod\ n) \quad (per\ k < \tau); \end{cases}$$

- In $\mathbb{Z}$ diviene:

$$\begin{cases} a^{\tau} & = & \gamma n + 1, & \\ a^{k} & = & \alpha n + \beta & \neq \quad n \cdot m\alpha' + 1 \quad (per\ k < \tau); \end{cases}$$

con $1 < \beta < n$.

Lemma 1: Se un elemento ha periodo τ in $\mathbb{Z}_n^*$ ha un periodo maggiore o uguale in $\mathbb{Z}_{n \cdot m}^*$.

- a ha periodo τ in $\mathbb{Z}_n^*$ implica:

$$\begin{cases} a^{\tau} & \equiv & 1 & (mod\ n), \\ a^{k} & \not\equiv & 1 & (mod\ n) \quad (per\ k < \tau); \end{cases}$$

- In $\mathbb{Z}$ diviene:

$$\begin{cases} a^{\tau} & = & \gamma n + 1, \\ a^{k} & = & \alpha n + \beta & \neq & n \cdot m\alpha' + 1 \quad (per\ k < \tau); \end{cases}$$

  con $1 < \beta < n$.
- Quindi gli a^k (per $k < \tau$) non sono congrui all'unità rispetto nessun multiplo di n, ma non sappiamo se $a^{\tau} \equiv 1\ (mod\ n \cdot m)$

Corollario: esistono elementi di periodo $p-1$ in $\mathbb{Z}^*_{p^h}$

- Per il lemma precedente (nel caso $n = p^h$ ed $m = p$) il periodo di un generatore g_1 di $\mathbb{Z}^*_p$ in $\mathbb{Z}^*_{p^h}$ è maggiore di $p-1$. Ma tutti i periodi devono essere divisori di $\phi(p^h) = p^{h-1}(p-1)$, quindi il periodo è multiplo multiplo di $p-1$ o di p. Deve essere un multiplo di $p-1$ perché g_1^{p-1} è congruo ad uno modulo p mentre g_1^p è congruo a g_1.

Corollario: esistono elementi di periodo $p-1$ in $\mathbb{Z}^*_{p^h}$

- Per il lemma precedente (nel caso $n = p^h$ ed $m = p$) il periodo di un generatore g_1 di $\mathbb{Z}^*_p$ in $\mathbb{Z}^*_{p^h}$ è maggiore di $p-1$. Ma tutti i periodi devono essere divisori di $\phi(p^h) = p^{h-1}(p-1)$, quindi il periodo è multiplo multiplo di $p-1$ o di p. Deve essere un multiplo di $p-1$ perché g_1^{p-1} è congruo ad uno modulo p mentre g_1^p è congruo a g_1.
- Se il periodo τ è esattamente uguale a $p-1$ il corollario è dimostrato.

Corollario: esistono elementi di periodo $p-1$ in $\mathbb{Z}^*_{p^h}$

- Per il lemma precedente (nel caso $n = p^h$ ed $m = p$) il periodo di un generatore g_1 di $\mathbb{Z}^*_p$ in $\mathbb{Z}^*_{p^h}$ è maggiore di $p-1$. Ma tutti i periodi devono essere divisori di $\phi(p^h) = p^{h-1}(p-1)$, quindi il periodo è multiplo multiplo di $p-1$ o di p. Deve essere un multiplo di $p-1$ perché g_1^{p-1} è congruo ad uno modulo p mentre g_1^p è congruo a g_1.
- Se il periodo τ è esattamente uguale a $p-1$ il corollario è dimostrato.
- Se il periodo τ di g_1 è multiplo di $(p-1)$: $\tau = (p-1) * m$ (e quindi m è una potenza di p), allora il periodo di $b = g_1^m$ è $p-1$

In $G = \mathbb{Z}^*_{p^h}$ esistono elementi di periodo p^{h-1}

- Vedremo che tutti gli elementi della forma $\alpha p + 1$ con α primo con p dispari, hanno periodo p^{h-1}. Tratteremo le potenze di due a parte.

In $G = \mathbb{Z}^*_{p^h}$ esistono elementi di periodo p^{h-1}

- Vedremo che tutti gli elementi della forma $\alpha p + 1$ con α primo con p dispari, hanno periodo p^{h-1}. Tratteremo le potenze di due a parte.
- Il periodo di $\alpha p + 1$ è p^{h-1}:

$$(\alpha p + 1)^{p^{h-1}} = 1 + \alpha p \cdot p^{h-1} + \cdots \equiv 1 \ (mod\ p^h);$$

e inoltre per $k < p$:

$$(\alpha p + 1)^{k p^{h-2}} \equiv 1 + \alpha p \cdot k \cdot p^{h-2} + \cdots \ (mod\ p^h);$$

$$(\alpha p + 1)^{k p^{h-2}} \equiv 1 + \alpha \cdot k \cdot p^{h-1} + \cdots p^h \ (mod\ p^h);$$

In $G = \mathbb{Z}^*_{p^h}$ esistono elementi di periodo p^{h-1}

- Vedremo che tutti gli elementi della forma $\alpha p + 1$ con α primo con p dispari, hanno periodo p^{h-1}. Tratteremo le potenze di due a parte.
- Il periodo di $\alpha p + 1$ è p^{h-1}:

$$(\alpha p + 1)^{p^{h-1}} = 1 + \alpha p \cdot p^{h-1} + \cdots \equiv 1 \ (mod\ p^h);$$

e inoltre per $k < p$:

$$(\alpha p + 1)^{k p^{h-2}} \equiv 1 + \alpha p \cdot k \cdot p^{h-2} + \cdots \ (mod\ p^h);$$

$$(\alpha p + 1)^{k p^{h-2}} \equiv 1 + \alpha \cdot k \cdot p^{h-1} + \cdots p^h \ (mod\ p^h);$$

- Per $1 < k < p$: $\alpha \cdot k \not\equiv p \ (mod\ p)$; quindi

$$(\alpha p + 1)^{k p^{h-2}} \not\equiv 1 \ (mod\ p^h);$$

Gli elementi di $G = \mathbb{Z}^*_{p^h}$ con periodo $p^{h-1} + 1$ sono $\alpha p + 1$ con $1 < \alpha < p$

- Dimostriamo per induzione una formula generale:
  $a^p = (\alpha p^k + 1)^p \equiv 1 + p \cdot \alpha p^k = 1 + \alpha \cdot p^{k+1}$

Gli elementi di $G = \mathbb{Z}^*_{p^h}$ con periodo $p^{h-1} + 1$ sono $\alpha p + 1$ con $1 < \alpha < p$

- Dimostriamo per induzione una formula generale:
  $a^p = (\alpha p^k + 1)^p \equiv 1 + p \cdot \alpha p^k = 1 + \alpha \cdot p^{k+1}$
- Caso $k = 1$: elevando ad una potenza minore di p:

$$(\alpha p + 1)^m = 1 + \alpha \cdot m \cdot p + a \cdot p^2 + \cdots \ (mod\ p^h);$$

per $m < p$, $\alpha' = \alpha \cdot m \not\equiv 0\ (mod\ p)$, quindi è ancora un termine del tipo $\alpha' p + 1$

Gli elementi di $G = \mathbb{Z}^*_{p^h}$ con periodo $p^{h-1} + 1$ sono $\alpha p + 1$ con $1 < \alpha < p$

- Dimostriamo per induzione una formula generale:
  $a^p = (\alpha p^k + 1)^p \equiv 1 + p \cdot \alpha p^k = 1 + \alpha \cdot p^{k+1}$
- Caso $k = 1$: elevando ad una potenza minore di p:

  $$(\alpha p + 1)^m = 1 + \alpha \cdot m \cdot p + a \cdot p^2 + \cdots \ (mod\ p^h);$$

  per $m < p$, $\alpha' = \alpha \cdot m \not\equiv 0\ (mod\ p)$, quindi è ancora un termine del tipo $\alpha' p + 1$
- Caso $k = 1$: elevando a p:

  $$(\alpha p + 1)^p = 1 + \alpha \cdot p \cdot p + a \cdot p^2 + \cdots \equiv 1 + p^2 \alpha\ (mod\ p^h);$$

Dimostriamo per induzione
$a^p = (\alpha p^k + 1)^p \equiv 1 + p \cdot \alpha p^{k+1}$ cont

- Formula di ricorrenza su k: Elevando ad una potenza m minore di p si ottiene un elemento dello stesso tipo

$$(\alpha p^k + 1)^m = 1 + \alpha \cdot m \cdot p^k + \cdots = 1 + \alpha' p^k + \cdots \ (mod\ p^h);$$

perché per $m < p$:

$$(\alpha m \equiv \alpha' \neq 0\ (mod\ p).$$

Dimostriamo per induzione
$a^p = (\alpha p^k + 1)^p \equiv 1 + p \cdot \alpha p^{k+1}$ cont

- Formula di ricorrenza su k: Elevando ad una potenza m minore di p si ottiene un elemento dello stesso tipo

$$(\alpha p^k + 1)^m = 1 + \alpha \cdot m \cdot p^k + \cdots = 1 + \alpha' p^k + \cdots \ (mod\ p^h);$$

perché per $m < p$:

$$(\alpha m \equiv \alpha' \neq 0\ (mod\ p).$$

- Formula di ricorrenza su k: Elevando ad una potenza p:

$$(\alpha p^k + 1)^p = 1 + \alpha \cdot p \cdot p^k + \cdots = 1 + \alpha p^{k+1} + \cdots \ (mod\ p^h);$$

Th. di Gauss: $\mathbb{Z}^*_{p^h}$ è ciclico

- Nei lemmi precedenti abbiamo costruito elementi b di periodo $p-1$ e $\alpha \cdot p-1$ di periodo p^{h-1}.

Th. di Gauss: $\mathbb{Z}^*_{p^h}$ è ciclico

- Nei lemmi precedenti abbiamo costruito elementi b di periodo $p-1$ e $\alpha \cdot p - 1$ di periodo p^{h-1}.
- Essendo $p-1$ e p^{h-1} primi tra loro, per il teorema sul periodo del prodotto, l'elemento $b(\alpha \cdot p - 1)$ ha periodo $p^{h-1}(p-1)$ che è pari alla funzione di Eulero di p^h.

Th. di Gauss: $\mathbb{Z}^*_{p^h}$ è ciclico

- Nei lemmi precedenti abbiamo costruito elementi b di periodo $p-1$ e $\alpha \cdot p - 1$ di periodo p^{h-1}.
- Essendo $p-1$ e p^{h-1} primi tra loro, per il teorema sul periodo del prodotto, l'elemento $b(\alpha \cdot p - 1)$ ha periodo $p^{h-1}(p-1)$ che è pari alla funzione di Eulero di p^h.
- Quindi $\mathbb{Z}^*_{p^h}$ è ciclico

Th. di Gauss: $\mathbb{Z}^*_{p^h}$ è ciclico

- Nei lemmi precedenti abbiamo costruito elementi b di periodo $p-1$ e $\alpha \cdot p - 1$ di periodo p^{h-1}.
- Essendo $p-1$ e p^{h-1} primi tra loro, per il teorema sul periodo del prodotto, l'elemento $b(\alpha \cdot p - 1)$ ha periodo $p^{h-1}(p-1)$ che è pari alla funzione di Eulero di p^h.
- Quindi $\mathbb{Z}^*_{p^h}$ è ciclico
- Il teorema vale per p primo dispari. Vedremo il caso pari in seguito.

Secondo Th. di Gauss: $\mathbb{Z}^*_{2\cdot p^h}$ è ciclico

- La funzione di Eulero di $2 \cdot p^h$ (con p primo dispari) è pari a $\phi(2 \cdot p^h) = \phi(2) \cdot \phi(p^h)$

Secondo Th. di Gauss: $\mathbb{Z}^*_{2\cdot p^h}$ è ciclico

- La funzione di Eulero di $2 \cdot p^h$ (con p primo dispari) è pari a $\phi(2 \cdot p^h) = \phi(2) \cdot \phi(p^h)$
- Essendo $\phi(2) = 1$ anche $\phi(2 \cdot p^h) = \phi(p^h)$.

Secondo Th. di Gauss: $\mathbb{Z}^*_{2\cdot p^h}$ è ciclico

- La funzione di Eulero di $2 \cdot p^h$ (con p primo dispari) è pari a $\phi(2 \cdot p^h) = \phi(2) \cdot \phi(p^h)$
- Essendo $\phi(2) = 1$ anche $\phi(2 \cdot p^h) = \phi(p^h)$.
- Per il teorema dell'immersione dei periodi i generatori di $\mathbb{Z}^*_{p^h}$ hanno lo stesso periodo in $\mathbb{Z}^*_{2\cdot p^h}$. Quindi il massimo periodo è uguale alla funzione di Eulero.

Secondo Th. di Gauss: $\mathbb{Z}^*_{2\cdot p^h}$ è ciclico

- La funzione di Eulero di $2 \cdot p^h$ (con p primo dispari) è pari a $\phi(2 \cdot p^h) = \phi(2) \cdot \phi(p^h)$
- Essendo $\phi(2) = 1$ anche $\phi(2 \cdot p^h) = \phi(p^h)$.
- Per il teorema dell'immersione dei periodi i generatori di $\mathbb{Z}^*_{p^h}$ hanno lo stesso periodo in $\mathbb{Z}^*_{2\cdot p^h}$. Quindi il massimo periodo è uguale alla funzione di Eulero.
- Resta da analizzare il caso delle potenze del due.

Ciclicità in $\mathbb{Z}^*_{2\cdot p^h}$

- Essendo il modulo pari, le potenze dei numeri pari in $\mathbb{Z}^*_{2\cdot p^h}$ sono pari e le potenze dei dispari sono dispari.

Ciclicità in $\mathbb{Z}^*_{2\cdot p^h}$

- Essendo il modulo pari, le potenze dei numeri pari in $\mathbb{Z}^*_{2\cdot p^h}$ sono pari e le potenze dei dispari sono dispari.
- Quindi se esiste un generatore di $\mathbb{Z}^*_{p^h}$ dispari questo genera tutto $\mathbb{Z}^*_{2p^h}$.

Ciclicità in $\mathbb{Z}^*_{2\cdot p^h}$

- Essendo il modulo pari, le potenze dei numeri pari in $\mathbb{Z}^*_{2\cdot p^h}$ sono pari e le potenze dei dispari sono dispari.
- Quindi se esiste un generatore di $\mathbb{Z}^*_{p^h}$ dispari questo genera tutto $\mathbb{Z}^*_{2p^h}$.
- I generatori pari di $\mathbb{Z}^*_{p^h}$ generano tutti i pari di $\mathbb{Z}_{2p^h}$, perché le potenze del generatore devono essere distinte.

Ciclicità in $\mathbb{Z}^*_{2\cdot p^h}$

- Essendo il modulo pari, le potenze dei numeri pari in $\mathbb{Z}^*_{2\cdot p^h}$ sono pari e le potenze dei dispari sono dispari.
- Quindi se esiste un generatore di $\mathbb{Z}^*_{p^h}$ dispari questo genera tutto $\mathbb{Z}^*_{2p^h}$.
- I generatori pari di $\mathbb{Z}^*_{p^h}$ generano tutti i pari di $\mathbb{Z}_{2p^h}$, perché le potenze del generatore devono essere distinte.
- Se anche tutti i generatori g di $\mathbb{Z}^*_{p^h}$ fossero pari, esisterebbe sempre $g + p^h$ in $\mathbb{Z}^*_{2\cdot p^h}$ che genera tutti i dispari:

$$(g+p^h)^k \equiv g^k + \binom{k}{1}(g)^{k-1}\cdot p^h + \cdots + \binom{k}{k-1} g\cdot (p^h)^{k-1} + (p^h)^k;$$

tutti i termini escluso il primo e l'ultimo sono multipli di $2p^h$ e quindi nulli. Quindi:

$$(g + p^h)^k \equiv g^k + (p^h)^k \equiv g^k + p^h.$$

Ciclicità in $\mathbb{Z}^*_{2\cdot p^h}$

- Essendo il modulo pari, le potenze dei numeri pari in $\mathbb{Z}^*_{2\cdot p^h}$ sono pari e le potenze dei dispari sono dispari.
- Quindi se esiste un generatore di $\mathbb{Z}^*_{p^h}$ dispari questo genera tutto $\mathbb{Z}^*_{2p^h}$.
- I generatori pari di $\mathbb{Z}^*_{p^h}$ generano tutti i pari di $\mathbb{Z}_{2p^h}$, perché le potenze del generatore devono essere distinte.
- Se anche tutti i generatori g di $\mathbb{Z}^*_{p^h}$ fossero pari, esisterebbe sempre $g + p^h$ in $\mathbb{Z}^*_{2\cdot p^h}$ che genera tutti i dispari:

$$(g+p^h)^k \equiv g^k + \binom{k}{1}(g)^{k-1}\cdot p^h + \cdots + \binom{k}{k-1} g\cdot (p^h)^{k-1} + (p^h)^k;$$

tutti i termini escluso il primo e l'ultimo sono multipli di $2p^h$ e quindi nulli. Quindi:

$$(g + p^h)^k \equiv g^k + (p^h)^k \equiv g^k + p^h.$$

- Infatti $(p^h)^2 \equiv [(p^h - 1) + 1]p^h \equiv p^h$ e quindi $(p^h)^k \equiv p^h$.

Ciclicità degli anelli $\mathbb{Z}_{2^h}^*$

- Tutti gli $\mathbb{Z}_{2^h}^*$ hanno cardinalità 2^{h-1} e contengono solo i dispari tra 1 e $2^h - 1$.
  $\mathbb{Z}_2^*$ possiede solo l'elemento unità:

$$\mathbb{Z}_2^* = \{1\}$$

Ciclicità degli anelli $\mathbb{Z}_{2^h}^*$

- Tutti gli $\mathbb{Z}_{2^h}^*$ hanno cardinalità 2^{h-1} e contengono solo i dispari tra 1 e $2^h - 1$.
  $\mathbb{Z}_2^*$ possiede solo l'elemento unità:

$$\mathbb{Z}_2^* = \{1\}$$

- $\mathbb{Z}_{2^2}^* = \mathbb{Z}_4^*$ possiede due soli elementi:

$$\mathbb{Z}_4^* = \{1, 3\}$$

Ciclicità degli anelli $\mathbb{Z}^*_{2^h}$

- Tutti gli $\mathbb{Z}^*_{2^h}$ hanno cardinalità 2^{h-1} e contengono solo i dispari tra 1 e $2^h - 1$.
  $\mathbb{Z}^*_2$ possiede solo l'elemento unità:

$$\mathbb{Z}^*_2 = \{1\}$$

- $\mathbb{Z}^*_{2^2} = \mathbb{Z}^*_4$ possiede due soli elementi:

$$\mathbb{Z}^*_4 = \{1, 3\}$$

- Entrambi gli elementi hanno periodo due.

$$3^2 = 9 = 1 = 1^2 \ (mod\ 4).$$

  Dunque 3 è un generatore.

Ciclicità degli anelli $\mathbb{Z}_{2^h}^*$

- Tutti gli $\mathbb{Z}_{2^h}^*$ hanno cardinalità 2^{h-1} e contengono solo i dispari tra 1 e $2^h - 1$.
  $\mathbb{Z}_2^*$ possiede solo l'elemento unità:

$$\mathbb{Z}_2^* = \{1\}$$

- $\mathbb{Z}_{2^2}^* = \mathbb{Z}_4^*$ possiede due soli elementi:

$$\mathbb{Z}_4^* = \{1, 3\}$$

- Entrambi gli elementi hanno periodo due.

$$3^2 = 9 = 1 = 1^2 \ (mod\ 4).$$

  Dunque 3 è un generatore.
- $\mathbb{Z}_{2^3}^* = \mathbb{Z}_8^*$ possiede quattro elementi:

$$\mathbb{Z}_8^* = \{1, 3, 5, 7\}\,;$$

  ed hanno tutti periodo 2, quindi non esiste un generatore e $\mathbb{Z}_8^*$ non è ciclico.

Ciclicità degli anelli $\mathbb{Z}_{2^h}^*$

- Il problema è che $(2+1)^2 = 3^2 = 9 = 1+8 = 1+2^3$:

$$(2+1)^2 = 4+4+1 = 8+1 \neq 4+1+8*k;$$

Ciclicità degli anelli $\mathbb{Z}_{2^h}^*$

- Il problema è che $(2+1)^2 = 3^2 = 9 = 1+8 = 1+2^3$:

$$(2+1)^2 = 4+4+1 = 8+1 \neq 4+1+8*k;$$

- Quindi si passa da $2+1$ a 2^3+1 mentre per gli altri primi dispari $(\alpha p+1)^p = 1+\alpha \cdot p^2 + k \cdot p^3$

Ciclicità degli anelli $\mathbb{Z}_{2^h}^*$

- Il problema è che $(2+1)^2 = 3^2 = 9 = 1+8 = 1+2^3$:

$$(2+1)^2 = 4+4+1 = 8+1 \neq 4+1+8*k;$$

- Quindi si passa da $2+1$ a 2^3+1 mentre per gli altri primi dispari $(\alpha p+1)^p = 1+\alpha \cdot p^2 + k \cdot p^3$
- Da 2^2+1 in su (2^i+1) al quadrato si trasformano in termini $(2^{i+1}+1)$

$$(2^i+1)^2 = 1+2\cdot 2^i + 2^{2i}$$

Ciclicità degli anelli $\mathbb{Z}^*_{2^h}$

- Il problema è che $(2+1)^2 = 3^2 = 9 = 1+8 = 1+2^3$:

$$(2+1)^2 = 4+4+1 = 8+1 \neq 4+1+8*k;$$

- Quindi si passa da $2+1$ a 2^3+1 mentre per gli altri primi dispari $(\alpha p+1)^p = 1+\alpha \cdot p^2 + k \cdot p^3$
- Da 2^2+1 in su (2^i+1) al quadrato si trasformano in termini $(2^{i+1}+1)$

$$(2^i+1)^2 = 1+2\cdot 2^i + 2^{2i}$$

- Quindi $(2^{i+1}+1)$ (per $I \geq 2$) ha periodo 2^{h-i} in $\mathbb{Z}^*_{2^h}$

$$(2^i+1)^{2^{h-i}} = 1+\cdot 2^i \cdot 2^{h-i} + \cdots \equiv 1\ (mod\ 2^h)$$

Ciclicità degli anelli $\mathbb{Z}^*_{2^h}$

- Il problema è che $(2+1)^2 = 3^2 = 9 = 1+8 = 1+2^3$:

$$(2+1)^2 = 4+4+1 = 8+1 \neq 4+1+8*k;$$

- Quindi si passa da $2+1$ a 2^3+1 mentre per gli altri primi dispari $(\alpha p+1)^p = 1+\alpha \cdot p^2 + k \cdot p^3$
- Da 2^2+1 in su (2^i+1) al quadrato si trasformano in termini $(2^{i+1}+1)$

$$(2^i+1)^2 = 1+2\cdot 2^i + 2^{2i}$$

- Quindi $(2^{i+1}+1)$ (per $I \geq 2$) ha periodo 2^{h-i} in $\mathbb{Z}^*_{2^h}$

$$(2^i+1)^{2^{h-i}} = 1+\cdot 2^i \cdot 2^{h-i} + \cdots \equiv 1 \,(mod\ 2^h)$$

- 3 ha sempre periodo 2^{h-2} come $4+1$. Quindi tutti i numeri hanno periodo 2^{h-2} e $\mathbb{Z}^*_{2^h}$ non è ciclico per $h > 2$.

Ciclicità degli anelli $\mathbb{Z}_n^*$

- Abbiamo visto che si possono costruire i generatori di tutti i gruppi moltiplicativi $\mathbb{Z}_p^*$, $\mathbb{Z}_{p^h}^*$, $\mathbb{Z}_{2p^h}^*$, $\mathbb{Z}_2^*$ e $\mathbb{Z}_4^*$.

Ciclicità degli anelli $\mathbb{Z}_n^*$

- Abbiamo visto che si possono costruire i generatori di tutti i gruppi moltiplicativi $\mathbb{Z}_p^*$, $\mathbb{Z}_{p^h}^*$, $\mathbb{Z}_{2p^h}^*$, $\mathbb{Z}_2^*$ e $\mathbb{Z}_4^*$.
- Vedremo che tutti gli altri $\mathbb{Z}_n^*$ non possono essere ciclici. Qualunque prodotto di due dispari che non siano potenze dello stesso primo si può scrivere come prodotto di due dispari primi tra loro, ad esempio:

$$n_1 \cdot n_2 = \frac{n_1 \cdot n_2}{(M)^2} \cdot M^2 = \left(\frac{n_1}{M}\right) \cdot (n_2 \cdot M);$$

in cui M è il massimo comune divisore di n_1 ed n_2.

Ciclicità degli anelli $\mathbb{Z}_n^*$

- Abbiamo visto che si possono costruire i generatori di tutti i gruppi moltiplicativi $\mathbb{Z}_p^*$, $\mathbb{Z}_{p^h}^*$, $\mathbb{Z}_{2p^h}^*$, $\mathbb{Z}_2^*$ e $\mathbb{Z}_4^*$.
- Vedremo che tutti gli altri $\mathbb{Z}_n^*$ non possono essere ciclici. Qualunque prodotto di due dispari che non siano potenze dello stesso primo si può scrivere come prodotto di due dispari primi tra loro, ad esempio:

$$n_1 \cdot n_2 = \frac{n_1 \cdot n_2}{(M)^2} \cdot M^2 = \left(\frac{n_1}{M}\right) \cdot (n_2 \cdot M);$$

  in cui M è il massimo comune divisore di n_1 ed n_2.
- Vedremo che in questo caso non può esistere un generatore perché esistono quattro radici distinte dell'unità.

Radici quadrate dell'unità in $\mathbb{Z}^*_{n_1 \cdot n_2}$

- Per $n = n_1 \cdot n_2$ si possono trovare 4 radici quadrate dell'unità:

$$\begin{cases} x_1 \overset{def}{=} & 1, \\ x_2 \overset{def}{=} & n-1, \\ x_3 \overset{def}{=} & \frac{(n_1-n_2)}{(n_1+n_2)} = (n_1+n_2)^{-1} \cdot (n_1-n_2), \\ x_4 \overset{def}{=} & n - x_3; \end{cases}$$

$n_1 + n_2 \in \mathbb{Z}^*_{n_1 \cdot n_2}$ perché essendo n_1 ed n_2 primi tra loro, anche la loro somma e la loro differenza sono prime rispetto ad entrambi e quindi anche rispetto al loro prodotto.

Radici quadrate dell'unità in $\mathbb{Z}^*_{n_1 \cdot n_2}$

- Per $n = n_1 \cdot n_2$ si possono trovare 4 radici quadrate dell'unità:

$$\begin{cases} x_1 \stackrel{def}{=} & 1, \\ x_2 \stackrel{def}{=} & n-1, \\ x_3 \stackrel{def}{=} & \frac{(n_1-n_2)}{(n_1+n_2)} = (n_1+n_2)^{-1} \cdot (n_1-n_2), \\ x_4 \stackrel{def}{=} & n - x_3; \end{cases}$$

  $n_1 + n_2 \in \mathbb{Z}^*_{n_1 \cdot n_2}$ perché essendo n_1 ed n_2 primi tra loro, anche la loro somma e la loro differenza sono prime rispetto ad entrambi e quindi anche rispetto al loro prodotto.

- infatti:

$$\begin{cases} (x_1) = 1^2 = 1 & \equiv 1 \pmod{n}, \\ (x_2) = (n-1)^2 = n^2 + 2n + 1 & \equiv 1 \pmod{n}, \\ (x_3) = \left(\frac{(n_1-n_2)}{(n_1+n_2)}\right)^2 = \frac{(n_1^2+n_2^2-2n)}{n_1^2+n_2^2+2n} \equiv \frac{(n_1^2+n_2^2)}{n_1^2+n_2^2} & \equiv 1 \pmod{n}, \\ (x_4) = (n-x_3)^2 = n - 2n \cdot x_3 + (x_3)^2 \equiv (x_3)^2 & \equiv 1 \pmod{n}. \end{cases}$$

Radici quadrate non banali dell'unità in $\mathbb{Z}^*_{n_1 \cdot n_2}$ e generatori

- Abbiamo visto che esistono almeno due radici quadrate non banali dell'unità che denominiamo r_1 ed r_2. Se esistesse un generatore g esisterebbe una potenza di g uguale ad ognuna delle quattro radici quadrate r:

$$r = g^k.$$

Radici quadrate non banali dell'unità in $\mathbb{Z}^*_{n_1 \cdot n_2}$ e generatori

- Abbiamo visto che esistono almeno due radici quadrate non banali dell'unità che denominiamo r_1 ed r_2. Se esistesse un generatore g esisterebbe una potenza di g uguale ad ognuna delle quattro radici quadrate r:

$$r = g^k.$$

- Il quadrato di r deve essere unitario:

$$r^2 = 1 = g^{2k};$$

quindi $2k = 0 \ (mod \ \phi(n))$.

Radici quadrate non banali dell'unità in $\mathbb{Z}^*_{n_1 \cdot n_2}$ e generatori

- Abbiamo visto che esistono almeno due radici quadrate non banali dell'unità che denominiamo r_1 ed r_2. Se esistesse un generatore g esisterebbe una potenza di g uguale ad ognuna delle quattro radici quadrate r:

$$r = g^k.$$

- Il quadrato di r deve essere unitario:

$$r^2 = 1 = g^{2k};$$

quindi $2k = 0 \ (mod \ \phi(n))$.

- Essendo ϕ pari esistono solo due valori di k ammissibili:

$$\begin{cases} k = 0 & => \quad r = 1, \\ k = \phi(n)/2 & => \quad r = r_i. \end{cases}$$

ma le radici sono almeno quattro.

Radici quadrate non banali dell'unità in $\mathbb{Z}^*_{n_1 \cdot n_2}$ e generatori

- Abbiamo visto che esistono almeno due radici quadrate non banali dell'unità che denominiamo r_1 ed r_2. Se esistesse un generatore g esisterebbe una potenza di g uguale ad ognuna delle quattro radici quadrate r:

$$r = g^k.$$

- Il quadrato di r deve essere unitario:

$$r^2 = 1 = g^{2k};$$

quindi $2k = 0 \ (mod \ \phi(n))$.

- Essendo ϕ pari esistono solo due valori di k ammissibili:

$$\begin{cases} k = 0 & => \quad r = 1, \\ k = \phi(n)/2 & => \quad r = r_i. \end{cases}$$

ma le radici sono almeno quattro.

- Quindi non può esistere un generatore. Se n è prodotto di due dispari (qualunque essi siano) $\mathbb{Z}^*_n$ non può essere ciclico.

Enunciamo il teorema di Gauss

- Tutti e soli gli anelli ciclici sono $\mathbb{Z}_2^*$, $\mathbb{Z}_4^*$, $\mathbb{Z}_{p^h}^*$ e $\mathbb{Z}_{2\cdot p^h}^*$ con p primo dispari.

Enunciamo il teorema di Gauss

- Tutti e soli gli anelli ciclici sono $\mathbb{Z}_2^*$, $\mathbb{Z}_4^*$, $\mathbb{Z}_{p^h}^*$ e $\mathbb{Z}_{2\cdot p^h}^*$ con p primo dispari.
- Negli anelli ciclici valgono diverse proprietà:

Enunciamo il teorema di Gauss

- Tutti e soli gli anelli ciclici sono $\mathbb{Z}_2^*$, $\mathbb{Z}_4^*$, $\mathbb{Z}_{p^h}^*$ e $\mathbb{Z}_{2\cdot p^h}^*$ con p primo dispari.
- Negli anelli ciclici valgono diverse proprietà:
  - Il periodo massimo di $\mathbb{Z}_n^*$ coincide con $\phi(n)$

Enunciamo il teorema di Gauss

- Tutti e soli gli anelli ciclici sono $\mathbb{Z}_2^*$, $\mathbb{Z}_4^*$, $\mathbb{Z}_{p^h}^*$ e $\mathbb{Z}_{2\cdot p^h}^*$ con p primo dispari.
- Negli anelli ciclici valgono diverse proprietà:
  - Il periodo massimo di $\mathbb{Z}_n^*$ coincide con $\phi(n)$
  - Tutte le equazioni del tipo $x^k = 1$ ammettono esattamente k soluzioni potenze generate da una di loro

Enunciamo il teorema di Gauss

- Tutti e soli gli anelli ciclici sono $\mathbb{Z}_2^*$, $\mathbb{Z}_4^*$, $\mathbb{Z}_{p^h}^*$ e $\mathbb{Z}_{2\cdot p^h}^*$ con p primo dispari.
- Negli anelli ciclici valgono diverse proprietà:
  - Il periodo massimo di $\mathbb{Z}_n^*$ coincide con $\phi(n)$
  - Tutte le equazioni del tipo $x^k = 1$ ammettono esattamente k soluzioni potenze generate da una di loro
  - Il gruppo moltiplicativo $G = (\mathbb{Z}_n^*, x)$ è isomorfo a $G = (\mathbb{Z}_{\phi(n)}, +)$.

Enunciamo il teorema di Gauss

- Tutti e soli gli anelli ciclici sono $\mathbb{Z}_2^*$, $\mathbb{Z}_4^*$, $\mathbb{Z}_{p^h}^*$ e $\mathbb{Z}_{2\cdot p^h}^*$ con p primo dispari.
- Negli anelli ciclici valgono diverse proprietà:
  - Il periodo massimo di $\mathbb{Z}_n^*$ coincide con $\phi(n)$
  - Tutte le equazioni del tipo $x^k = 1$ ammettono esattamente k soluzioni potenze generate da una di loro
  - Il gruppo moltiplicativo $G = (\mathbb{Z}_n^*, x)$ è isomorfo a $G = (\mathbb{Z}_{\phi(n)}, +)$.
- Vediamo adesso come cambiano queste proprietà legate all'algoritmo RSA nel caso generale.

Massimo periodo di un anello

Robert Carmichael si pose il problema di calcolare il massimo periodo nel caso generale di un anello $\mathbb{Z}_n^*$. Come vedremo rispose pienamente al problema.

Robert Carmichael
(1879 ? 1967 USA)

Massimo periodo di un anello

Robert Carmichael si pose il problema di calcolare il massimo periodo nel caso generale di un anello $\mathbb{Z}_n^*$. Come vedremo rispose pienamente al problema.

Robert Carmichael
(1879 ? 1967 USA)

- Utilizziamo la decomposizione di n in fattori primi:

$$n = \left((p_1)^{h_1} \cdot (p_2)^{h_2} \cdots (p_i)^{h_i} \cdots (p_m)^{h_m}\right) = n_1 \cdot n_2 \cdots n_i \cdots n_m;$$

in cui $n_i \stackrel{def}{=} (p_i)^{h_i}$, (cioè $n_1 \stackrel{def}{=} (p_1)^{h_1}$, $n_2 \stackrel{def}{=} (p_2)^{h_2}$ etc).

Massimo periodo di un anello

Robert Carmichael si pose il problema di calcolare il massimo periodo nel caso generale di un anello $\mathbb{Z}_n^*$. Come vedremo rispose pienamente al problema.

Robert Carmichael
(1879 ? 1967 USA)

- Utilizziamo la decomposizione di n in fattori primi:

$$n = \left((p_1)^{h_1} \cdot (p_2)^{h_2} \cdots (p_i)^{h_i} \cdots (p_m)^{h_m}\right) = n_1 \cdot n_2 \cdots n_i \cdots n_m;$$

in cui $n_i \stackrel{def}{=} (p_i)^{h_i}$, (cioè $n_1 \stackrel{def}{=} (p_1)^{h_1}$, $n_2 \stackrel{def}{=} (p_2)^{h_2}$ etc).

- Teorema di Carmichael: "Il massimo periodo eguaglia il minimo comune multiplo delle funzioni di Eulero della sua decomposizione in potenze di fattori primi"

Teorema di Carmichael

- Il periodo massimo in $\mathbb{Z}_n^*$ è uguale alla funzione di Carlmichael $\lambda(n)$.

Teorema di Carmichael

- Il periodo massimo in $\mathbb{Z}_n^*$ è uguale alla funzione di Carlmichael $\lambda(n)$.
- La funzione di Carmichael $\lambda(n)$ è il minimo comune multiplo tra le funzioni di Eulero della decomposizione canonica di n in fattori primi:

$$\lambda(n) \stackrel{def}{=} mcm(\phi(n_1), \phi(n_2), \ldots, \phi(n_m)),$$

cioè:

$$\lambda(n) \stackrel{def}{=} mcm\left(\phi\left((p_1)^{h_1}\right), \phi\left((p_2)^{h_2}\right), \ldots, \phi\left((p_m)^{h_m}\right)\right)$$

Teorema di Carmichael

- Il periodo massimo in $\mathbb{Z}_n^*$ è uguale alla funzione di Carlmichael $\lambda(n)$.
- La funzione di Carmichael $\lambda(n)$ è il minimo comune multiplo tra le funzioni di Eulero della decomposizione canonica di n in fattori primi:

$$\lambda(n) \stackrel{def}{=} mcm(\phi(n_1), \phi(n_2), \ldots, \phi(n_m)),$$

cioè:

$$\lambda(n) \stackrel{def}{=} mcm\left(\phi\left((p_1)^{h_1}\right), \phi\left((p_2)^{h_2}\right), \ldots, \phi\left((p_m)^{h_m}\right)\right)$$

- Per definizione è un numero minore o uguale alla funzione di Eulero. Quando almeno due fattori sono dispari la funzione di Carmichael è minore o uguale alla metà della funzione di Eulero.

Teorema di Carmichael

- Il periodo massimo in $\mathbb{Z}_n^*$ è uguale alla funzione di Carlmichael $\lambda(n)$.
- La funzione di Carmichael $\lambda(n)$ è il minimo comune multiplo tra le funzioni di Eulero della decomposizione canonica di n in fattori primi:

$$\lambda(n) \stackrel{def}{=} mcm(\phi(n_1), \phi(n_2), \ldots, \phi(n_m)),$$

cioè:

$$\lambda(n) \stackrel{def}{=} mcm\left(\phi\left((p_1)^{h_1}\right), \phi\left((p_2)^{h_2}\right), \ldots, \phi\left((p_m)^{h_m}\right)\right)$$

- Per definizione è un numero minore o uguale alla funzione di Eulero. Quando almeno due fattori sono dispari la funzione di Carmichael è minore o uguale alla metà della funzione di Eulero.
- In realtà nel caso di numeri pari al posto della funzione di Eulero $\phi(2^h)$ occorre mettere $\lambda(2^h)$ che per $h = 2$ vale 2 e per $h > 2$ vale $2^{(h-2)}$.

Teorema di Carmichael - Dimostrazione

- Dimostreremo il teorema in due passi:

Teorema di Carmichael - Dimostrazione

- Dimostreremo il teorema in due passi:
- Mostreremo che $\lambda(n)$ è una ciclicità per ogni elemento di $\mathbb{Z}_n^*$;

Teorema di Carmichael - Dimostrazione

- Dimostreremo il teorema in due passi:
- Mostreremo che $\lambda(n)$ è una ciclicità per ogni elemento di $\mathbb{Z}_n^*$;
- Mostreremo che esiste un elemento di periodo $\lambda(n)$.

"$\lambda(n)$ è una ciclicità per ogni elemento di $\mathbb{Z}_n^*$"

- Essendo $n_1, n_2, \ldots, n_m$ primi tra loro, l'eguaglianza $x \equiv a^\lambda$ (in $\mathbb{Z}_n^*$) equivale al sistema:

$$\begin{cases} x = a^\lambda & \equiv & x_1 & (mod & n_1), \\ x = a^\lambda & \equiv & x_2 & (mod & n_2), \\ \ldots & & \ldots & & \\ x = a^\lambda & \equiv & x_m & (mod & n_m). \end{cases}$$

"$\lambda(n)$ è una ciclicità per ogni elemento di $\mathbb{Z}_n^*$"

- Essendo $n_1, n_2, \ldots, n_m$ primi tra loro, l'eguaglianza $x \equiv a^\lambda$ (in $\mathbb{Z}_n^*$) equivale al sistema:

$$\begin{cases} x = a^\lambda & \equiv & x_1 & (mod & n_1), \\ x = a^\lambda & \equiv & x_2 & (mod & n_2), \\ \ldots & & \ldots & & \\ x = a^\lambda & \equiv & x_m & (mod & n_m). \end{cases}$$

- Siccome λ è multiplo di tutti i $\phi(n_i)$, tutti gli $x_i = \left(a^{\phi(n_i)}\right)^{\lambda(n)/\phi(n_i)} = (1)^{\lambda(n)/\phi(n_i)}$ sono congruenti all'unità:

$$\begin{cases} x & \equiv & 1 & (mod & n_1), \\ x & \equiv & 1 & (mod & n_2), \\ \ldots & & \ldots & & \\ x & \equiv & 1 & (mod & n_m). \end{cases}$$

"$\lambda(n)$ è una ciclicità per ogni elemento di $\mathbb{Z}_n^*$"

- Essendo $n_1, n_2, \ldots, n_m$ primi tra loro, l'eguaglianza $x \equiv a^\lambda$ (in $\mathbb{Z}_n^*$) equivale al sistema:

$$\begin{cases} x = a^\lambda & \equiv & x_1 & (mod & n_1), \\ x = a^\lambda & \equiv & x_2 & (mod & n_2), \\ \ldots & & \ldots & & \\ x = a^\lambda & \equiv & x_m & (mod & n_m). \end{cases}$$

- Siccome λ è multiplo di tutti i $\phi(n_i)$, tutti gli $x_i = \left(a^{\phi(n_i)}\right)^{\lambda(n)/\phi(n_i)} = (1)^{\lambda(n)/\phi(n_i)}$ sono congruenti all'unità:

$$\begin{cases} x & \equiv & 1 & (mod & n_1), \\ x & \equiv & 1 & (mod & n_2), \\ \ldots & \ldots & & & \\ x & \equiv & 1 & (mod & n_m). \end{cases}$$

- Per il teorema cinese dei resti il sistema ammette un'unica soluzione, che quindi è $x = 1$. Essendo vero per ogni a il periodo massimo è al più λ

"Esiste un elemento di periodo $\lambda(n)$"

- Sappiamo dal teorema di Gauss che per ogni gruppo ciclico $G_i = \mathbb{Z}^*_{n_i} = \mathbb{Z}^*_{(p_i)^{h_i}}$ esiste un generatore g_i di periodo $\phi(n_i)$.

"Esiste un elemento di periodo $\lambda(n)$"

- Sappiamo dal teorema di Gauss che per ogni gruppo ciclico $G_i = \mathbb{Z}^*_{n_i} = \mathbb{Z}^*_{(p_i)^{h_i}}$ esiste un generatore g_i di periodo $\phi(n_i)$.
- Definiamo dei nuovi Λ_i in maniera ricorsiva:

$$\begin{cases} \Lambda_1 & \stackrel{def}{=} & MCD(\phi(n_1), \phi(n_1)) = 1, \\ \Lambda_2 & \stackrel{def}{=} & MCD(\tau_1, \phi(n_2)), \\ \cdots & \cdots & \cdots, \\ \Lambda_{i+1} & \stackrel{def}{=} & MCD(\tau_1 \cdot \tau_2 \cdots \tau_i, \phi(n_{i+1})). \end{cases}$$

"Esiste un elemento di periodo $\lambda(n)$"

- Sappiamo dal teorema di Gauss che per ogni gruppo ciclico $G_i = \mathbb{Z}^*_{n_i} = \mathbb{Z}^*_{(p_i)^{h_i}}$ esiste un generatore g_i di periodo $\phi(n_i)$.
- Definiamo dei nuovi Λ_i in maniera ricorsiva:

$$\begin{cases} \Lambda_1 & \stackrel{def}{=} & MCD(\phi(n_1), \phi(n_1)) = 1, \\ \Lambda_2 & \stackrel{def}{=} & MCD(\tau_1, \phi(n_2)), \\ \cdots & \cdots & \cdots, \\ \Lambda_{i+1} & \stackrel{def}{=} & MCD(\tau_1 \cdot \tau_2 \cdots \tau_i, \phi(n_{i+1})). \end{cases}$$

- (g_i) ha (almeno) periodo $\phi(n_i)$ e quindi esiste (g'_i) di periodo esatto $\phi(n_i)$; mentre $a_i \stackrel{def}{=} (g'_i)^{\Lambda_i}$ ha periodo $\tau_i = \phi(n_i)/\Lambda_i$.

"Esiste un elemento di periodo $\lambda(n)$"

- Sappiamo dal teorema di Gauss che per ogni gruppo ciclico $G_i = \mathbb{Z}^*_{n_i} = \mathbb{Z}^*_{(p_i)^{h_i}}$ esiste un generatore g_i di periodo $\phi(n_i)$.
- Definiamo dei nuovi Λ_i in maniera ricorsiva:

$$\begin{cases} \Lambda_1 & \stackrel{def}{=} & MCD(\phi(n_1), \phi(n_1)) = 1, \\ \Lambda_2 & \stackrel{def}{=} & MCD(\tau_1, \phi(n_2)), \\ \cdots & \cdots & \cdots, \\ \Lambda_{i+1} & \stackrel{def}{=} & MCD(\tau_1 \cdot \tau_2 \cdots \tau_i, \phi(n_{i+1})). \end{cases}$$

- (g_i) ha (almeno) periodo $\phi(n_i)$ e quindi esiste (g'_i) di periodo esatto $\phi(n_i)$; mentre $a_i \stackrel{def}{=} (g'_i)^{\Lambda_i}$ ha periodo $\tau_i = \phi(n_i)/\Lambda_i$.
- Tutti i τ_i sono per definizione primi tra loro.

"Esiste un elemento di periodo $\lambda(n)$"

- Sappiamo dal teorema di Gauss che per ogni gruppo ciclico $G_i = \mathbb{Z}^*_{n_i} = \mathbb{Z}^*_{(p_i)^{h_i}}$ esiste un generatore g_i di periodo $\phi(n_i)$.
- Definiamo dei nuovi Λ_i in maniera ricorsiva:

$$\begin{cases} \Lambda_1 & \stackrel{def}{=} & MCD(\phi(n_1), \phi(n_1)) = 1, \\ \Lambda_2 & \stackrel{def}{=} & MCD(\tau_1, \phi(n_2)), \\ \cdots & \cdots & \cdots, \\ \Lambda_{i+1} & \stackrel{def}{=} & MCD(\tau_1 \cdot \tau_2 \cdots \tau_i, \phi(n_{i+1})). \end{cases}$$

- (g_i) ha (almeno) periodo $\phi(n_i)$ e quindi esiste (g'_i) di periodo esatto $\phi(n_i)$; mentre $a_i \stackrel{def}{=} (g'_i)^{\Lambda_i}$ ha periodo $\tau_i = \phi(n_i)/\Lambda_i$.
- Tutti i τ_i sono per definizione primi tra loro.
- Il prodotto di tutti i periodi τ_i è uguale a λ:

$$\tau \stackrel{def}{=} \tau_1 \cdots \tau_m = \phi(n_1) \cdot \left(\frac{\phi(n_2}{\Lambda_2}\right) \cdots \left(\frac{\phi(n_m}{\Lambda_m}\right) = \lambda(n).$$

Costruzione di un elemento di periodo massimo $\lambda(n)$

- Costruiamo l'elemento di periodo massimo a:

$$a \stackrel{def}{=} a_1 \cdot a_2 \cdots a_m;$$

Costruzione di un elemento di periodo massimo $\lambda(n)$

- Costruiamo l'elemento di periodo massimo a:

$$a \stackrel{def}{=} a_1 \cdot a_2 \cdots a_m;$$

- Esplicitando gli a_i:

$$a \stackrel{def}{=} \left(g_1'\right)^{\Lambda_1} \cdot \left(g_2'\right)^{\Lambda_2} \cdots \left(g_m'\right)^{\Lambda_m}.$$

Costruzione di un elemento di periodo massimo $\lambda(n)$

- Costruiamo l'elemento di periodo massimo a:

$$a \stackrel{def}{=} a_1 \cdot a_2 \cdots a_m;$$

- Esplicitando gli a_i:

$$a \stackrel{def}{=} \left(g_1'\right)^{\Lambda_1} \cdot \left(g_2'\right)^{\Lambda_2} \cdots \left(g_m'\right)^{\Lambda_m}.$$

- Essendo tutti i periodi degli a_i, primi tra loro, il periodo del prodotto è uguale al prodotto dei periodi che per costruzione coincide con $\lambda(n)$

Conseguenze su RSA

- La sequenza cifrata c è una potenza della sequenza in chiaro t:

$$c = t^k.$$

in cui $k \in \mathbb{Z}^*_{n_1 \cdot n_2}$ cioè primo con n_1 ed n_2 .

Conseguenze su RSA

- La sequenza cifrata c è una potenza della sequenza in chiaro t:

$$c = t^k.$$

  in cui $k \in \mathbb{Z}^*_{n_1 \cdot n_2}$ cioè primo con n_1 ed n_2 .
- La funzione inversa è

$$\forall t : t = (c)^x = (t^k)^x = t^{kx}.$$

Conseguenze su RSA

- La sequenza cifrata c è una potenza della sequenza in chiaro t:

$$c = t^k.$$

  in cui $k \in \mathbb{Z}^*_{n_1 \cdot n_2}$ cioè primo con n_1 ed n_2 .
- La funzione inversa è

$$\forall t : t = (c)^x = (t^k)^x = t^{kx}.$$

- Quindi possiamo scegliere x in modo che $kx - 1$ sia un multiplo del periodo massimo di $\mathbb{Z}^*_{n_1 \cdot n_2}$ cioè:

$$k \cdot x = 1 \ (mod \ \lambda(n_1 \cdot n_2)).$$

Conseguenze su RSA

- La sequenza cifrata c è una potenza della sequenza in chiaro t:

$$c = t^k.$$

  in cui $k \in \mathbb{Z}^*_{n_1 \cdot n_2}$ cioè primo con n_1 ed n_2 .
- La funzione inversa è

$$\forall t : t = (c)^x = (t^k)^x = t^{kx}.$$

- Quindi possiamo scegliere x in modo che $kx - 1$ sia un multiplo del periodo massimo di $\mathbb{Z}^*_{n_1 \cdot n_2}$ cioè:

$$k \cdot x = 1 \ (mod \ \lambda(n_1 \cdot n_2)).$$

- $\lambda(n_1 \cdot n_2) \stackrel{def}{=} mcm(n_1 - 1, n_2 - 1)$ è significativamente minore di $\phi(n_1)\phi(n_2) = (n_1 - 1) \cdot (n_2 - 1)$. Essendo i due numeri dispari il rapporto minimo è 2.

Conseguenze su RSA

- La sequenza cifrata c è una potenza della sequenza in chiaro t:

$$c = t^k.$$

  in cui $k \in \mathbb{Z}^*_{n_1 \cdot n_2}$ cioè primo con n_1 ed n_2 .
- La funzione inversa è

$$\forall t : t = (c)^x = (t^k)^x = t^{kx}.$$

- Quindi possiamo scegliere x in modo che $kx - 1$ sia un multiplo del periodo massimo di $\mathbb{Z}^*_{n_1 \cdot n_2}$ cioè:

$$k \cdot x = 1 \ (mod \ \lambda(n_1 \cdot n_2)).$$

- $\lambda(n_1 \cdot n_2) \stackrel{def}{=} mcm(n_1 - 1, n_2 - 1)$ è significativamente minore di $\phi(n_1)\phi(n_2) = (n_1 - 1) \cdot (n_2 - 1)$. Essendo i due numeri dispari il rapporto minimo è 2.
- Quindi l'attaccante per ispezionare l'insieme delle possibili chiavi segrete (le x) nell'intervallo $(1, n - 1)$ può trovarne $\phi(n)/\lambda(n)$ diverse, ma equivalenti.

Proprietà dei numeri di Carmichael

- Un numero n si dice numero di Carmichael quando qualsiasi elemento a di $\mathbb{Z}_n^*$ supera il test di Fermat di pseudo-primalità: $a^{n-1} = 1$. Questo significa che tutti i periodi sono divisori di $n-1$, e quindi λ divide $n-1$ cioè che tutti i $p_i - 1$ devono dividere $n-1$:

$$p_i - 1 | n-1 \Leftrightarrow \lambda(n) | n-1$$

Proprietà dei numeri di Carmichael

- Un numero n si dice numero di Carmichael quando qualsiasi elemento a di $\mathbb{Z}_n^*$ supera il test di Fermat di pseudo-primalità: $a^{n-1} = 1$. Questo significa che tutti i periodi sono divisori di $n-1$, e quindi λ divide $n-1$ cioè che tutti i $p_i - 1$ devono dividere $n-1$:

$$p_i - 1 | n-1 \Leftrightarrow \lambda(n) | n-1$$

- Quindi i numeri di Carmichael sono dispari: se n-1 fosse dispari qualsiasi $p-1$ (di un fattore dispari) non potrebbe essere un suo divisore.

Proprietà dei numeri di Carmichael

- Un numero n si dice numero di Carmichael quando qualsiasi elemento a di $\mathbb{Z}_n^*$ supera il test di Fermat di pseudo-primalità: $a^{n-1} = 1$. Questo significa che tutti i periodi sono divisori di $n-1$, e quindi λ divide $n-1$ cioè che tutti i $p_i - 1$ devono dividere $n-1$:

$$p_i - 1 | n-1 \Leftrightarrow \lambda(n) | n-1$$

- Quindi i numeri di Carmichael sono dispari: se n-1 fosse dispari qualsiasi $p-1$ (di un fattore dispari) non potrebbe essere un suo divisore.
- I numeri di Carmichael sono aquadratici.
  Se infatti non lo fossero ($n = p^h \cdot m$), n-1 sarebbe divisibile per $\phi(p) = p^h(p-1)$, il che è impossibile perché Il resto della divisione di (n-1) per p è sempre $p-1$ (n è multiplo di p).

Proprietà dei numeri di Carmichael utile per RSA

- I numeri di Carmichael non possono essere prodotto di due primi $n \neq p \cdot q$ (hp $p > q$):

$$p-1|n-1 \Rightarrow p-1|n-1-(p-1) = n-p = pq-p = p(q-1) \Rightarrow$$

$$p-1|q-1$$

impossibile.

Proprietà dei numeri di Carmichael utile per RSA

- I numeri di Carmichael non possono essere prodotto di due primi $n \neq p \cdot q$ (hp $p > q$):

$$p-1|n-1 \Rightarrow p-1|n-1-(p-1) = n-p = pq-p = p(q-1) \Rightarrow$$

$$p-1|q-1$$

impossibile.

- Questo è positivo per la robustezza di RSA perché non c'è il rischio di scegliere un particolare $n = p \cdot q$ e q per il quale l'attaccante può trovare la chiave segreta risolvendo $\alpha \cdot k = 1 \ mod(n-1)$.

Proprietà dei numeri di Carmichael utile per RSA

- I numeri di Carmichael non possono essere prodotto di due primi $n \neq p \cdot q$ (hp $p > q$):

  $$p-1|n-1 \Rightarrow p-1|n-1-(p-1) = n-p = pq-p = p(q-1) \Rightarrow$$

  $$p-1|q-1$$

  impossibile.
- Questo è positivo per la robustezza di RSA perché non c'è il rischio di scegliere un particolare $n = p \cdot q$ e q per il quale l'attaccante può trovare la chiave segreta risolvendo $\alpha \cdot k = 1 \ mod(n-1)$.
- I numeri di Carmichael possono, invece, essere prodotti di tre primi. Es: 561=3*11*17; 1105=5*17*13 etc. Questa è un'ulteriore ragione per usare sempre la decomposizione in due soli primi nell'agoritmo RSA: $n = p \cdot q$

Proprietà dei numeri di Carmichael utile per RSA

- I numeri di Carmichael non possono essere prodotto di due primi $n \neq p \cdot q$ (hp $p > q$):

  $$p-1|n-1 \Rightarrow p-1|n-1-(p-1) = n-p = pq-p = p(q-1) \Rightarrow$$

  $$p-1|q-1$$

  impossibile.
- Questo è positivo per la robustezza di RSA perché non c'è il rischio di scegliere un particolare $n = p \cdot q$ e q per il quale l'attaccante può trovare la chiave segreta risolvendo $\alpha \cdot k = 1 \ mod(n-1)$.
- I numeri di Carmichael possono, invece, essere prodotti di tre primi. Es: 561=3*11*17; 1105=5*17*13 etc. Questa è un'ulteriore ragione per usare sempre la decomposizione in due soli primi nell'agoritmo RSA: $n = p \cdot q$
- I primi numeri di Carmicael sono 561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841

Messaggio

- Gli anelli primali $\mathbb{Z}_p$ sono ciclici (cioè $G = (\mathbb{Z}_p^*, x)$ è ciclico); possono quindi essere generati esponenziando alcuni loro elementi detti generatori

Messaggio

- Gli anelli primali $\mathbb{Z}_p$ sono ciclici (cioè $G = (\mathbb{Z}_p^*, x)$ è ciclico); possono quindi essere generati esponenziando alcuni loro elementi detti generatori
- Negli anelli primali le "radici dell'unità" sono uniche e quindi sono tutte potenze di una di esse

Messaggio

- Gli anelli primali $\mathbb{Z}_p$ sono ciclici (cioè $G = (\mathbb{Z}_p^*, x)$ è ciclico); possono quindi essere generati esponenziando alcuni loro elementi detti generatori
- Negli anelli primali le "radici dell'unità" sono uniche e quindi sono tutte potenze di una di esse
- Abbiamo visto quali anelli sono ciclici (cioè posseggono un generatore) ed in generale qual è il massimo periodo di un elemento in un anello: $\lambda(n)$.

Messaggio

- Gli anelli primali $\mathbb{Z}_p$ sono ciclici (cioè $G = (\mathbb{Z}_p^*, x)$ è ciclico); possono quindi essere generati esponenziando alcuni loro elementi detti generatori
- Negli anelli primali le "radici dell'unità" sono uniche e quindi sono tutte potenze di una di esse
- Abbiamo visto quali anelli sono ciclici (cioè posseggono un generatore) ed in generale qual è il massimo periodo di un elemento in un anello: $\lambda(n)$.
- La funzione di Carmichael $\lambda(n)$ ci dice quanto sia veramente vasto l'insieme degli esponenti da esplorare per tentare di ottenere il messaggio in chiaro e quindi trovare la chiave privata (segreta) data la chiave pubblica.

Messaggio

- Gli anelli primali $\mathbb{Z}_p$ sono ciclici (cioè $G = (\mathbb{Z}_p^*, x)$ è ciclico); possono quindi essere generati esponenziando alcuni loro elementi detti generatori
- Negli anelli primali le "radici dell'unità" sono uniche e quindi sono tutte potenze di una di esse
- Abbiamo visto quali anelli sono ciclici (cioè posseggono un generatore) ed in generale qual è il massimo periodo di un elemento in un anello: $\lambda(n)$.
- La funzione di Carmichael $\lambda(n)$ ci dice quanto sia veramente vasto l'insieme degli esponenti da esplorare per tentare di ottenere il messaggio in chiaro e quindi trovare la chiave privata (segreta) data la chiave pubblica.
- Nella cifratura RSA si usa sempre il prodotto di due soli primi e non tre, anche per evitare di imbattersi in numeri di Carmichael.

Messaggio

- Gli anelli primali $\mathbb{Z}_p$ sono ciclici (cioè $G = (\mathbb{Z}_p^*, x)$ è ciclico); possono quindi essere generati esponenziando alcuni loro elementi detti generatori
- Negli anelli primali le "radici dell'unità" sono uniche e quindi sono tutte potenze di una di esse
- Abbiamo visto quali anelli sono ciclici (cioè posseggono un generatore) ed in generale qual è il massimo periodo di un elemento in un anello: $\lambda(n)$.
- La funzione di Carmichael $\lambda(n)$ ci dice quanto sia veramente vasto l'insieme degli esponenti da esplorare per tentare di ottenere il messaggio in chiaro e quindi trovare la chiave privata (segreta) data la chiave pubblica.
- Nella cifratura RSA si usa sempre il prodotto di due soli primi e non tre, anche per evitare di imbattersi in numeri di Carmichael.
- Gli anelli a potenze del 2, $\mathbb{Z}^*_{2 \cdot p^h}$ non sono ciclici (escludendo $\mathbb{Z}_2^*$ e $\mathbb{Z}_4^*$); il loro massimo periodo è $\lambda(2^h) = 2^{h-2}$.

Esercizio per la prossima lezione

Studiamo $\mathbb{Z}_{527}^*$

Esercizio per la prossima lezione

Studiamo $\mathbb{Z}_{527}^*$

- Decomporre $n = 527$ in fattori usando il metodo di Fermat.

Esercizio per la prossima lezione

Studiamo $\mathbb{Z}_{527}^*$

- Decomporre $n = 527$ in fattori usando il metodo di Fermat.
- Calcolare funzione di Carmichael $\lambda(n)$.

Esercizio per la prossima lezione

Studiamo $\mathbb{Z}_{527}^*$

- Decomporre $n = 527$ in fattori usando il metodo di Fermat.
- Calcolare funzione di Carmichael $\lambda(n)$.
- Trovare un elemento di massimo periodo in $\mathbb{Z}_{527}^*$.

Esercizio per la prossima lezione

Studiamo $\mathbb{Z}^*_{527}$

- Decomporre $n = 527$ in fattori usando il metodo di Fermat.
- Calcolare funzione di Carmichael $\lambda(n)$.
- Trovare un elemento di massimo periodo in $\mathbb{Z}^*_{527}$.
- Costruire una coppia di chiavi pubblica k e privata α che realizzino la cifratura a chiave pubblica tramite l'algoritmo RSA.

Esercizio per la prossima lezione

Studiamo $\mathbb{Z}^*_{527}$

- Decomporre $n = 527$ in fattori usando il metodo di Fermat.
- Calcolare funzione di Carmichael $\lambda(n)$.
- Trovare un elemento di massimo periodo in $\mathbb{Z}^*_{527}$.
- Costruire una coppia di chiavi pubblica k e privata α che realizzino la cifratura a chiave pubblica tramite l'algoritmo RSA.
- Cifrare con la chiave pubblica il messaggio dato dalla sequenza m dei numeri numeri 120, 131, 63, 92

Esercizio per la prossima lezione

Studiamo $\mathbb{Z}^*_{527}$

- Decomporre $n = 527$ in fattori usando il metodo di Fermat.
- Calcolare funzione di Carmichael $\lambda(n)$.
- Trovare un elemento di massimo periodo in $\mathbb{Z}^*_{527}$.
- Costruire una coppia di chiavi pubblica k e privata α che realizzino la cifratura a chiave pubblica tramite l'algoritmo RSA.
- Cifrare con la chiave pubblica il messaggio dato dalla sequenza m dei numeri numeri 120, 131, 63, 92
- Verificare che α, la chiave privata, funziona.

Esercizio per la prossima lezione

Studiamo $\mathbb{Z}^*_{527}$

- Decomporre $n = 527$ in fattori usando il metodo di Fermat.
- Calcolare funzione di Carmichael $\lambda(n)$.
- Trovare un elemento di massimo periodo in $\mathbb{Z}^*_{527}$.
- Costruire una coppia di chiavi pubblica k e privata α che realizzino la cifratura a chiave pubblica tramite l'algoritmo RSA.
- Cifrare con la chiave pubblica il messaggio dato dalla sequenza m dei numeri numeri 120, 131, 63, 92
- Verificare che α, la chiave privata, funziona.
- Trovare tutte le (quattro) radici dell'unità e mostrare come si poteva scomporre n conoscendone una non banale.