# Introduzione alla Crittografia

Progetto Lauree Scientifiche

Liceo Scientifico "N. Tron", 30 gennaio 2007

# Riassunto

- Dati due numeri interi $a$ e $b$, diciamo che $a \equiv b \mod n$ se $a - b$ è un multiplo di $n$ o, equivalentemente, se $a = nq_a + r$ e $b = nq_b + r$.

# Riassunto

- Dati due numeri interi $a$ e $b$, diciamo che $a \equiv b \mod n$ se $a - b$ è un multiplo di $n$ o, equivalentemente, se $a = nq_a + r$ e $b = nq_b + r$. Dato un intero $a$, con $[a]_n$ indichiamo il resto di $a$ diviso $n$.

# Riassunto

- Dati due numeri interi $a$ e $b$, diciamo che $a \equiv b \mod n$ se $a - b$ è un multiplo di $n$ o, equivalentemente, se $a = nq_a + r$ e $b = nq_b + r$. Dato un intero $a$, con $[a]_n$ indichiamo il resto di $a$ diviso $n$.
- $\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n-1]\}$, con le operazioni di somma e moltiplicazione modulo $n$.

# Riassunto

- Dati due numeri interi $a$ e $b$, diciamo che $a \equiv b \mod n$ se $a - b$ è un multiplo di $n$ o, equivalentemente, se $a = nq_a + r$ e $b = nq_b + r$. Dato un intero $a$, con $[a]_n$ indichiamo il resto di $a$ diviso $n$.
- $\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n-1]\}$, con le operazioni di somma e moltiplicazione modulo $n$.
- Se $p$ è un numero primo, ogni elemento diverso da zero in $\mathbb{Z}_p$ è invertibile.

# Riassunto

- Dati due numeri interi $a$ e $b$, diciamo che $a \equiv b \mod n$ se $a - b$ è un multiplo di $n$ o, equivalentemente, se $a = nq_a + r$ e $b = nq_b + r$. Dato un intero $a$, con $[a]_n$ indichiamo il resto di $a$ diviso $n$.
- $\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n-1]\}$, con le operazioni di somma e moltiplicazione modulo $n$.
- Se $p$ è un numero primo, ogni elemento diverso da zero in $\mathbb{Z}_p$ è invertibile.
- In generale, un elemento $a \in \mathbb{Z}_n$ è invertibile se e solo se $(a, n) = 1$.

# Algoritmo di Euclide

- Per verificare se un elemento $a \in \mathbb{Z}_n$ è invertibile, si esegue l'Algoritmo di Eulide per trovare il M.C.D. tra $a$ e $n$.

# Algoritmo di Euclide

- Per verificare se un elemento $a \in \mathbb{Z}_n$ è invertibile, si esegue l'Algoritmo di Eulide per trovare il M.C.D. tra $a$ e $n$.
- Se $a$ è invertibile in $\mathbb{Z}_n$, per trovare il suo inverso si applica l'Algoritmo di Eulide esteso:

# Algoritmo di Euclide

- Per verificare se un elemento $a \in \mathbb{Z}_n$ è invertibile, si esegue l'Algoritmo di Eulide per trovare il M.C.D. tra $a$ e $n$.
- Se $a$ è invertibile in $\mathbb{Z}_n$, per trovare il suo inverso si applica l'Algoritmo di Eulide esteso:
  - si trova un elemento $u$ tale che $1 = au + nv$

# Algoritmo di Euclide

- Per verificare se un elemento $a \in \mathbb{Z}_n$ è invertibile, si esegue l'Algoritmo di Eulide per trovare il M.C.D. tra $a$ e $n$.
- Se $a$ è invertibile in $\mathbb{Z}_n$, per trovare il suo inverso si applica l'Algoritmo di Eulide esteso:
  - si trova un elemento $u$ tale che $1 = au + nv$
  - dalla formula precedente, si ottiene $au - 1$ è multiplo di $n$ e pertanto $au \equiv 1 \mod n$. Quindi $a^{-1} = u \mod n$.

# Algoritmo di Euclide

- Per verificare se un elemento $a \in \mathbb{Z}_n$ è invertibile, si esegue l'Algoritmo di Eulide per trovare il M.C.D. tra $a$ e $n$.
- Se $a$ è invertibile in $\mathbb{Z}_n$, per trovare il suo inverso si applica l'Algoritmo di Eulide esteso:
  - si trova un elemento $u$ tale che $1 = au + nv$
  - dalla formula precedente, si ottiene $au - 1$ è multiplo di $n$ e pertanto $au \equiv 1 \mod n$. Quindi $a^{-1} = u \mod n$.
  - Esempio: l'inverso di 5 in $\mathbb{Z}_9$ è 2. Infatti $1 = 5 \cdot 2 - 9 \cdot 1$, e quindi $5 \cdot 2 \equiv 1 \mod 9$.

# Quanti sono gli elementi invertibili?

- Se $p$ è primo, ogni elemento diverso da 0 è invertibile in $\mathbb{Z}_p$. Gli elementi invertibili sono $p - 1$.

# Quanti sono gli elementi invertibili?

- Se $p$ è primo, ogni elemento diverso da 0 è invertibile in $\mathbb{Z}_p$. Gli elementi invertibili sono $p - 1$.
- Se $n$ non è primo, gli elementi invertibili in $\mathbb{Z}_n$ sono gli elementi coprimi con $n$. Quanti sono?

# Quanti sono gli elementi invertibili?

- Se $p$ è primo, ogni elemento diverso da 0 è invertibile in $\mathbb{Z}_p$. Gli elementi invertibili sono $p - 1$.
- Se $n$ non è primo, gli elementi invertibili in $\mathbb{Z}_n$ sono gli elementi coprimi con $n$. Quanti sono?

# Funzione di Eulero

- Dato $n > 1$, introduciamo la funzione di Eulero $\varphi(n)$=numero di elementi $< n$ e coprimi con $n$.

# Funzione di Eulero

- Dato $n > 1$, introduciamo la funzione di Eulero $\varphi(n)$=numero di elementi $< n$ e coprimi con $n$.
- Se $p$ è primo $\varphi(p) = p - 1$.

# Funzione di Eulero

- Dato $n > 1$, introduciamo la funzione di Eulero $\varphi(n)$=numero di elementi $< n$ e coprimi con $n$.
- Se $p$ è primo $\varphi(p) = p - 1$.
- Se $n = pq$, gli elementi invertibili in $\mathbb{Z}_n$ sono

# Funzione di Eulero

- Dato $n > 1$, introduciamo la funzione di Eulero $\varphi(n)$=numero di elementi $< n$ e coprimi con $n$.
- Se $p$ è primo $\varphi(p) = p - 1$.
- Se $n = pq$, gli elementi invertibili in $\mathbb{Z}_n$ sono $pq - q - p + 1$, quindi $\varphi(n) = (p - 1)(q - 1)$

# Funzione di Eulero

- Dato $n > 1$, introduciamo la funzione di Eulero $\varphi(n)$=numero di elementi $< n$ e coprimi con $n$.
- Se $p$ è primo $\varphi(p) = p - 1$.
- Se $n = pq$, gli elementi invertibili in $\mathbb{Z}_n$ sono $pq - q - p + 1$, quindi $\varphi(n) = (p - 1)(q - 1)$
- Se $n = p^a$, con $a > 1$, gli elementi invertibili in $\mathbb{Z}_n$ sono

# Funzione di Eulero

- Dato $n > 1$, introduciamo la funzione di Eulero $\varphi(n)$=numero di elementi $< n$ e coprimi con $n$.
- Se $p$ è primo $\varphi(p) = p - 1$.
- Se $n = pq$, gli elementi invertibili in $\mathbb{Z}_n$ sono $pq - q - p + 1$, quindi $\varphi(n) = (p - 1)(q - 1)$
- Se $n = p^a$, con $a > 1$, gli elementi invertibili in $\mathbb{Z}_n$ sono $p^a - p^{(a-1)}$, quindi $\varphi(n) = p^{a-1}(p - 1)$.

# Funzione di Eulero

- Dato $n > 1$, introduciamo la funzione di Eulero $\varphi(n)$=numero di elementi $< n$ e coprimi con $n$.
- Se $p$ è primo $\varphi(p) = p - 1$.
- Se $n = pq$, gli elementi invertibili in $\mathbb{Z}_n$ sono $pq - q - p + 1$, quindi $\varphi(n) = (p-1)(q-1)$
- Se $n = p^a$, con $a > 1$, gli elementi invertibili in $\mathbb{Z}_n$ sono $p^a - p^{(a-1)}$, quindi $\varphi(n) = p^{a-1}(p-1)$.
- In generale, se $n = rs$ con $(r, s) = 1$, allora $\varphi(n) = \varphi(r)\varphi(s)$.

# Funzione di Eulero

- Esercizio: Calcolare $\varphi(8)$, $\varphi(35)$, $\varphi(24)$.
- Esercizio: se $\varphi(n) = n - 1$, cosa posso dire di $n$?
- Esercizio: Calcolare i possibili $n$ prodotto di due primi tali che $\varphi(n) = 192$. (Suggerimento: si ricordi che se $n = rs$ con $(r, s) = 1$, allora $\varphi(n) = \varphi(r)\varphi(s)$).

# Piccolo Teorema di Fermat

*Se $p$ è un numero primo, allora per ogni $a \in \mathbb{Z}_p$, $a \neq 0$, si ha*

$$a^{p-1} \equiv 1 \mod p$$

Dimostrazione: Consideriamo il sottoinsieme di $\mathbb{Z}_p$ formato dai multipli di $a$, $A = \{[a], [2a], [3a], \ldots, [(p-1)a]\}$.

# Piccolo Teorema di Fermat

*Se $p$ è un numero primo, allora per ogni $a \in \mathbb{Z}_p$, $a \neq 0$, si ha*

$$a^{p-1} \equiv 1 \mod p$$

Dimostrazione: Consideriamo il sottoinsieme di $\mathbb{Z}_p$ formato dai multipli di $a$, $A = \{[a], [2a], [3a], \ldots, [(p-1)a]\}$. L'insieme $A$ contiene $p-1$ elementi distinti e diversi da $[0]$.

# Piccolo Teorema di Fermat

*Se $p$ è un numero primo, allora per ogni $a \in \mathbb{Z}_p$, $a \neq 0$, si ha*

$$a^{p-1} \equiv 1 \mod p$$

Dimostrazione: Consideriamo il sottoinsieme di $\mathbb{Z}_p$ formato dai multipli di $a$, $A = \{[a], [2a], [3a], \ldots, [(p-1)a]\}$. L'insieme $A$ contiene $p-1$ elementi distinti e diversi da $[0]$. Perciò $A$ coincide con il sottoinsieme $B$ di $\mathbb{Z}_p$, $B = \{[1], [2], \ldots, [p-1]\}$.

# Piccolo Teorema di Fermat

*Se $p$ è un numero primo, allora per ogni $a \in \mathbb{Z}_p$, $a \neq 0$, si ha*

$$a^{p-1} \equiv 1 \mod p$$

Dimostrazione: Consideriamo il sottoinsieme di $\mathbb{Z}_p$ formato dai multipli di $a$, $A = \{[a], [2a], [3a], \ldots, [(p-1)a]\}$. L'insieme $A$ contiene $p-1$ elementi distinti e diversi da $[0]$. Perciò $A$ coincide con il sottoinsieme $B$ di $\mathbb{Z}_p$, $B = \{[1], [2], \ldots, [p-1]\}$. Quindi moltiplicando tra loro gli elementi in $A$ e in $B$ otteniamo lo stesso risultato.

$$a \cdot 2a \cdot 3a \ldots (p-1)a \equiv 1 \cdot 2 \cdot 3 \ldots (p-1) \mod p$$

# Piccolo Teorema di Fermat

*Se $p$ è un numero primo, allora per ogni $a \in \mathbb{Z}_p$, $a \neq 0$, si ha*

$$a^{p-1} \equiv 1 \mod p$$

Dimostrazione: Consideriamo il sottoinsieme di $\mathbb{Z}_p$ formato dai multipli di $a$, $A = \{[a], [2a], [3a], \ldots, [(p-1)a]\}$. L'insieme $A$ contiene $p-1$ elementi distinti e diversi da $[0]$. Perciò $A$ coincide con il sottoinsieme $B$ di $\mathbb{Z}_p$, $B = \{[1], [2], \ldots, [p-1]\}$. Quindi moltiplicando tra loro gli elementi in $A$ e in $B$ otteniamo lo stesso risultato.

$$a \cdot 2a \cdot 3a \ldots (p-1)a \equiv 1 \cdot 2 \cdot 3 \ldots (p-1) \mod p$$

Poiché $2, 3, \ldots, (p-1)$ sono invertibili, possiamo semplificare e si ottiene

$$a^{p-1} \equiv 1 \mod p$$

# Esempio

Esempio: Sia $p = 5$ e calcoliamo $a^4$ per $a = 1, 2, 3, 4$.

- $1^4 = 1 \equiv 1 \mod 5$
- $2^4 = 16 \equiv 1 \mod 5$
- $3^4 = 81 \equiv 1 \mod 5$
- $4^4 = 256 \equiv 1 \mod 5$.

# Esempio

Esempio: Sia $p = 5$ e calcoliamo $a^4$ per $a = 1, 2, 3, 4$.

- $1^4 = 1 \equiv 1 \mod 5$
- $2^4 = 16 \equiv 1 \mod 5$
- $3^4 = 81 \equiv 1 \mod 5$
- $4^4 = 256 \equiv 1 \mod 5$.

Esempio: Il teorema non vale se $n$ è non primo. Sia $n = 6$, $a = 2$; allora $2^5 = 32 \equiv 2 \mod 6$.

# Applicazioni

Problema: Come costruire funzioni invertibili da poter essere usate come buone chiavi crittografiche?

# Applicazioni

Problema: Come costruire funzioni invertibili da poter essere usate come buone chiavi crittografiche?

Esempio: Il metodo di Cesare e' una funzione $f(x) = x + n$ in $\mathbb{Z}_{21}$.

# Applicazioni

Problema: Come costruire funzioni invertibili da poter essere usate come buone chiavi crittografiche?

Esempio: Il metodo di Cesare e' una funzione $f(x) = x + n$ in $\mathbb{Z}_{21}$. La sua inversa è facilmente calcolabile, ed è $f(x) = x + m$ con $n + m = 21$, cioè $m$ è l'opposto di $n$ in $\mathbb{Z}_{21}$.

# Applicazioni

Problema: Come costruire funzioni invertibili da poter essere usate come buone chiavi crittografiche?

Esempio: Il metodo di Cesare e' una funzione $f(x) = x + n$ in $\mathbb{Z}_{21}$. La sua inversa è facilmente calcolabile, ed è $f(x) = x + m$ con $n + m = 21$, cioè $m$ è l'opposto di $n$ in $\mathbb{Z}_{21}$.

In punto cruciale consiste nel costruire funzioni le cui inverse siano difficili da calcolare in termini computazionali.

# Corollario 1

*Sia $p$ un numero primo e sia $r$ un intero tale che $(r, p-1) = 1$. Allora la funzione $f(x) = x^r$ è invertibile in $\mathbb{Z}_p$, e la sua inversa è data da $f^{-1}(x) = x^s$, dove $rs \equiv 1 \mod p-1$.*

# Corollario 1

*Sia $p$ un numero primo e sia $r$ un intero tale che $(r, p-1) = 1$. Allora la funzione $f(x) = x^r$ è invertibile in $\mathbb{Z}_p$, e la sua inversa è data da $f^{-1}(x) = x^s$, dove $rs \equiv 1 \mod p-1$.*

Dimostrazione: Verifichiamo che $f^{-1}f(x) = x$ per ogni intero $x$,

# Corollario 1

*Sia $p$ un numero primo e sia $r$ un intero tale che $(r, p-1) = 1$. Allora la funzione $f(x) = x^r$ è invertibile in $\mathbb{Z}_p$, e la sua inversa è data da $f^{-1}(x) = x^s$, dove $rs \equiv 1 \mod p-1$.*

Dimostrazione: Verifichiamo che $f^{-1}f(x) = x$ per ogni intero $x$, cioè che $x^{rs} \equiv x \mod p$ per ogni intero $x$.

# Corollario 1

*Sia $p$ un numero primo e sia $r$ un intero tale che $(r, p-1) = 1$. Allora la funzione $f(x) = x^r$ è invertibile in $\mathbb{Z}_p$, e la sua inversa è data da $f^{-1}(x) = x^s$, dove $rs \equiv 1 \mod p-1$.*

Dimostrazione: Verifichiamo che $f^{-1}f(x) = x$ per ogni intero $x$, cioè che $x^{rs} \equiv x \mod p$ per ogni intero $x$.
Poichè $rs \equiv 1 \mod p-1$, esiste un intero $b$ tale che
$rs = 1 + b(p-1)$;

# Corollario 1

*Sia $p$ un numero primo e sia $r$ un intero tale che $(r, p-1) = 1$. Allora la funzione $f(x) = x^r$ è invertibile in $\mathbb{Z}_p$, e la sua inversa è data da $f^{-1}(x) = x^s$, dove $rs \equiv 1 \mod p-1$.*

Dimostrazione: Verifichiamo che $f^{-1}f(x) = x$ per ogni intero $x$, cioè che $x^{rs} \equiv x \mod p$ per ogni intero $x$.
Poichè $rs \equiv 1 \mod p-1$, esiste un intero $b$ tale che $rs = 1 + b(p-1)$; dunque

$$x^{rs} = x^{1+b(p-1)} = x \cdot (x^{p-1})^b \equiv x \cdot 1 \mod p$$

dove l'ultimo passaggio segue dal Piccolo Teorema di Fermat

# Corollario 2

*Sia $n = pq$ con $p$ e $q$ primi distinti, e sia $r$ un intero tale che $(r, \varphi(n)) = 1$. Allora la funzione $f(x) = x^r$ è invertibile in $\mathbb{Z}_n$, e la sua inversa è data da $f^{-1}(x) = x^s$, dove $rs \equiv 1 \mod \varphi(n)$.*

# Corollario 2

*Sia $n = pq$ con $p$ e $q$ primi distinti, e sia $r$ un intero tale che $(r, \varphi(n)) = 1$. Allora la funzione $f(x) = x^r$ è invertibile in $\mathbb{Z}_n$, e la sua inversa è data da $f^{-1}(x) = x^s$, dove $rs \equiv 1 \mod \varphi(n)$.*

Dimostrazione: Verifichiamo che per ogni intero $x$ si ha $x^{rs} \equiv x \mod n$.

# Corollario 2

*Sia $n = pq$ con $p$ e $q$ primi distinti, e sia $r$ un intero tale che $(r, \varphi(n)) = 1$. Allora la funzione $f(x) = x^r$ è invertibile in $\mathbb{Z}_n$, e la sua inversa è data da $f^{-1}(x) = x^s$, dove $rs \equiv 1 \mod \varphi(n)$.*

Dimostrazione: Verifichiamo che per ogni intero $x$ si ha $x^{rs} \equiv x \mod n$. Ricordiamo che $\varphi(n) = (p-1)(q-1)$,

# Corollario 2

*Sia $n = pq$ con $p$ e $q$ primi distinti, e sia $r$ un intero tale che $(r, \varphi(n)) = 1$. Allora la funzione $f(x) = x^r$ è invertibile in $\mathbb{Z}_n$, e la sua inversa è data da $f^{-1}(x) = x^s$, dove $rs \equiv 1 \mod \varphi(n)$.*

Dimostrazione: Verifichiamo che per ogni intero $x$ si ha $x^{rs} \equiv x \mod n$. Ricordiamo che $\varphi(n) = (p-1)(q-1)$, quindi da $rs \equiv 1 \mod \varphi(n)$, segue che $(p-1)(q-1)$ divide $rs - 1$.

# Corollario 2

*Sia $n = pq$ con $p$ e $q$ primi distinti, e sia $r$ un intero tale che $(r, \varphi(n)) = 1$. Allora la funzione $f(x) = x^r$ è invertibile in $\mathbb{Z}_n$, e la sua inversa è data da $f^{-1}(x) = x^s$, dove $rs \equiv 1 \mod \varphi(n)$.*

Dimostrazione: Verifichiamo che per ogni intero $x$ si ha $x^{rs} \equiv x \mod n$. Ricordiamo che $\varphi(n) = (p-1)(q-1)$, quindi da $rs \equiv 1 \mod \varphi(n)$, segue che $(p-1)(q-1)$ divide $rs - 1$. In particolare $p - 1$ divide $rs - 1$, cioé

$$rs \equiv 1 \mod p - 1$$

# Corollario 2

*Sia $n = pq$ con $p$ e $q$ primi distinti, e sia $r$ un intero tale che $(r, \varphi(n)) = 1$. Allora la funzione $f(x) = x^r$ è invertibile in $\mathbb{Z}_n$, e la sua inversa è data da $f^{-1}(x) = x^s$, dove $rs \equiv 1 \mod \varphi(n)$.*

Dimostrazione: Verifichiamo che per ogni intero $x$ si ha $x^{rs} \equiv x \mod n$. Ricordiamo che $\varphi(n) = (p-1)(q-1)$, quindi da $rs \equiv 1 \mod \varphi(n)$, segue che $(p-1)(q-1)$ divide $rs - 1$. In particolare $p - 1$ divide $rs - 1$, cioé

$$rs \equiv 1 \mod p - 1$$

Dal Corollario 1 segue che $x^{rs} \equiv x \mod p$ per ogni intero $x$

# Corollario 2

*Sia $n = pq$ con $p$ e $q$ primi distinti, e sia $r$ un intero tale che $(r, \varphi(n)) = 1$. Allora la funzione $f(x) = x^r$ è invertibile in $\mathbb{Z}_n$, e la sua inversa è data da $f^{-1}(x) = x^s$, dove $rs \equiv 1 \mod \varphi(n)$.*

Dimostrazione: Verifichiamo che per ogni intero $x$ si ha $x^{rs} \equiv x \mod n$. Ricordiamo che $\varphi(n) = (p-1)(q-1)$, quindi da $rs \equiv 1 \mod \varphi(n)$, segue che $(p-1)(q-1)$ divide $rs - 1$. In particolare $p - 1$ divide $rs - 1$, cioé

$$rs \equiv 1 \mod p - 1$$

Dal Corollario 1 segue che $x^{rs} \equiv x \mod p$ per ogni intero $x$ e dunque $p$ divide $x^{rs} - x$.

# Corollario 2

*Sia $n = pq$ con $p$ e $q$ primi distinti, e sia $r$ un intero tale che $(r, \varphi(n)) = 1$. Allora la funzione $f(x) = x^r$ è invertibile in $\mathbb{Z}_n$, e la sua inversa è data da $f^{-1}(x) = x^s$, dove $rs \equiv 1 \mod \varphi(n)$.*

Dimostrazione: Verifichiamo che per ogni intero $x$ si ha $x^{rs} \equiv x \mod n$. Ricordiamo che $\varphi(n) = (p-1)(q-1)$, quindi da $rs \equiv 1 \mod \varphi(n)$, segue che $(p-1)(q-1)$ divide $rs - 1$. In particolare $p - 1$ divide $rs - 1$, cioé

$$rs \equiv 1 \mod p - 1$$

Dal Corollario 1 segue che $x^{rs} \equiv x \mod p$ per ogni intero $x$ e dunque $p$ divide $x^{rs} - x$. Lo stesso ragionamento si applica a $q$ e si conclude che anche $q$ divide $x^{rs} - x$.

# Corollario 2

*Sia $n = pq$ con $p$ e $q$ primi distinti, e sia $r$ un intero tale che $(r, \varphi(n)) = 1$. Allora la funzione $f(x) = x^r$ è invertibile in $\mathbb{Z}_n$, e la sua inversa è data da $f^{-1}(x) = x^s$, dove $rs \equiv 1 \mod \varphi(n)$.*

Dimostrazione: Verifichiamo che per ogni intero $x$ si ha $x^{rs} \equiv x \mod n$. Ricordiamo che $\varphi(n) = (p-1)(q-1)$, quindi da $rs \equiv 1 \mod \varphi(n)$, segue che $(p-1)(q-1)$ divide $rs - 1$. In particolare $p - 1$ divide $rs - 1$, cioé

$$rs \equiv 1 \mod p - 1$$

Dal Corollario 1 segue che $x^{rs} \equiv x \mod p$ per ogni intero $x$ e dunque $p$ divide $x^{rs} - x$. Lo stesso ragionamento si applica a $q$ e si conclude che anche $q$ divide $x^{rs} - x$. Siccome $p$ e $q$ sono primi distinti, si conclude che $n = pq$ divide $x^{rs} - x$,

# Corollario 2

*Sia $n = pq$ con $p$ e $q$ primi distinti, e sia $r$ un intero tale che $(r, \varphi(n)) = 1$. Allora la funzione $f(x) = x^r$ è invertibile in $\mathbb{Z}_n$, e la sua inversa è data da $f^{-1}(x) = x^s$, dove $rs \equiv 1 \mod \varphi(n)$.*

Dimostrazione: Verifichiamo che per ogni intero $x$ si ha $x^{rs} \equiv x \mod n$. Ricordiamo che $\varphi(n) = (p-1)(q-1)$, quindi da $rs \equiv 1 \mod \varphi(n)$, segue che $(p-1)(q-1)$ divide $rs - 1$. In particolare $p - 1$ divide $rs - 1$, cioé

$$rs \equiv 1 \mod p - 1$$

Dal Corollario 1 segue che $x^{rs} \equiv x \mod p$ per ogni intero $x$ e dunque $p$ divide $x^{rs} - x$. Lo stesso ragionamento si applica a $q$ e si conclude che anche $q$ divide $x^{rs} - x$. Siccome $p$ e $q$ sono primi distinti, si conclude che $n = pq$ divide $x^{rs} - x$, cioè $x^{rs} \equiv x \mod n$ per ogni intero $x$.

# Esercizi

- Verificare che la funzione $f(x) = 3x + 2$ non è invertibile in $\mathbb{Z}_9$.
- Verificare che la funzione $f(x) = 5x + 2$ è invertibile in $\mathbb{Z}_9$. Trovare la funzione inversa.
- Verificare se la funzione $f(x) = x^3$ è invertibile in $\mathbb{Z}_p$, con $p = 3, 5, 7, 11, 13$.
- Calcolare il massimo comun divisore di 672330 e 49531
- Calcolare l'inverso di 49531 modulo 672330

# Esercizi

- Sia $n > 1$; dimostare che se $(a, n) \neq 1$, allora esiste un intero $b$ tale che $ab \equiv 0 \mod n$.
- Dimostrare che se $p$ è primo e $a \neq 0$, allora gli elementi di $\mathbb{Z}_p$ $[a], [2a], [3a] \ldots, [(p-1)a]$ sono distinti e diversi da $[0]$.
- Se $n = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$, dimostare che $\varphi(n) = p_1^{a_1-1} p_2^{a_2-1} \ldots p_r^{a_r-1}(p_1 - 1)(p_2 - 1)\ldots(p_r - 1)$. Suggerimento: Se $n = rs$ con $(r, s) = 1$, allora $\varphi(n) = \varphi(r)\varphi(s)$.
- Sia $n > 1$ e sia $x$ un elemento invertibile in $\mathbb{Z}_n$. Allora $x^{\varphi(n)} \equiv 1 \mod n$. Suggerimento: vedi G. Alberti , es. 5.6.

# Esercizi

- Dimostare che se $n = p^h$ con $p$ primo e $h > 1$, allora la funzione $f(x) = x^r$ non è invertibile in $\mathbb{Z}_n$ per alcun esponente $h$. Suggerimento: calcolare $f(x)$ per $x = p^{h-1}$ e $x = 1$.
- Dimostrare che se $n$ non è prodotto di primi distinti, allora la funzione $f(x) = x^r$ non è invertibile in $\mathbb{Z}_n$ per alcun esponente $h$. Suggerimento: vedi G. Alberti, es. 5.11.
- Scrivere un script in Pari/Gp che, fissati due interi $x$ e $n$ con $n > 1$, dica se $x$ è invertibile in $\mathbb{Z}_n$ e in caso affermativo ne calcoli l'inverso.