ordine di un gruppo

- G un gruppo finito: ordine di $G = o(G) =$ numero di elementi di G
- l'insieme degli invertibili di $\mathbb{Z}_n$ è un gruppo rispetto al prodotto (mod n)
- si denota con $U(\mathbb{Z}_n)$ e ha ordine $\phi(n)$
- esempio: $U(\mathbb{Z}_9) = \{1, 2, 4, 5, 7, 8\}$, ha $\phi(9) = 6$ elementi

funzione ϕ di Eulero

- funzione ϕ di Eulero, o funzione toziente
- è definita sugli interi positivi
- $\phi(n)$ è il numero di interi positivi $\leq n$ che sono coprimi con n
- $\phi(n) = |\{k \in \mathbb{N}, \quad k \leq n \quad | \quad (k, n) = 1\}|$
  - se p è primo, $\phi(p) = p - 1$
  - se p è primo, $\phi(p^k) = p^k - p^{k-1}$
  - se n, m sono coprimi, allora $\phi(n \cdot m) = \phi(m)\phi(n)$
- in questo modo, si può calcolare la funzione di Eulero di ogni intero
- purché se ne conosca la fattorizzazione
- se $n = p_1^{\alpha_1} \dots p_s^{\alpha_s}$
- $\phi(n) = \phi(p_1^{\alpha_1}) \dots \phi(p_s^{\alpha_s}) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \dots (p_s^{\alpha_s} - p_s^{\alpha_s - 1})$

ordine di un elemento

- $(G, \cdot)$ un gruppo moltiplicativo di ordine M
- l'ordine di un elemento $g \in G$, $o(g)$, è il minimo intero positivo m tale che
$$g^m = 1$$

- (se $(G, +)$ è un gruppo additivo, l'ordine di un elemento $g \in G$ è il minimo intero positivo m tale che $mg = 0$)
- esempio: in $U(\mathbb{Z}_9)$, calcoliamo $o(2)$
$2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 16 = 7, 2^5 = 2 \cdot 7 = 14 = 5,$
$2^6 = 2 \cdot 5 = 10 = 1$ quindi l'ordine di 2 è 6.
- per gli altri elementi, si ha
$o(1) = 1, o(4) = 3, o(5) = 6, o(7) = 3, o(8) = 2$

Teorema (Lagrange)

Se G è un gruppo di ordine M, allora l'ordine di ogni elemento di G divide M

- quindi in particolare si ha $g^M = 1 \quad \forall g \in G$
- se si applica il Teorema di Lagrange al gruppo $U(\mathbb{Z}_n)$ si ottiene

Teorema (Eulero)

Se $(a, n) = 1$, allora $a^{\phi(n)} \equiv 1$ (mod n).

se consideriamo $U(\mathbb{Z}_p)$, p primo, si ha il piccolo teorema di Fermat

Teorema (Fermat)

se p è primo, e $p \not| a$, allora $a^{p-1} \equiv 1$ (mod p)

- quindi se $p \not| a$, si ha $a^p \equiv a$ (mod p)
- anche se $p|a$ si ha $a^p \equiv a (\equiv 0)$ (mod p)
- dunque $\forall a \in \mathbb{N}$ e $m \equiv 1$ mod $p-1$ si ha $a^m \equiv a$ (mod p)

ci servirà il seguente corollario del teorema di Eulero:

Corollario

se $n = pq$, p, q numeri primi, $a \in \mathbb{N}$, sia $m \equiv 1$ (mod $\phi(n)$) allora si ha $a^m \equiv a$ (mod n)

la dimostrazione usa il teorema cinese dei resti