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
- 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

ordine di un elemento

- $(G, \cdot)$ un gruppo moltiplicativo di ordine n
- 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 $mg = 0$)

- 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
- $o(2) = o(U(\mathbb{Z}_9)) = 6$
- ogni elemento di $U(\mathbb{Z}_9)$ si ottiene come una potenza dell'elemento 2
- si dice che 2 genera $U(\mathbb{Z}_9)$

gruppi ciclici

- Definizione
  Un gruppo G con n elementi tale esiste un elemento $g \in G$ con $o(g) = n$ si dice ciclico, e g si dice un generatore del gruppo
  - $U(\mathbb{Z}_9)$ è ciclico – p. es. $U(\mathbb{Z}_8)$ non lo è
  - i gruppi $U(\mathbb{Z}_p)$, p primo, sono gruppi ciclici
  - se $GF(p^m)$ è un campo finito, il gruppo moltiplicativo $(GF(p^m) - \{0\}, \cdot)$ è un gruppo ciclico
  - in questi due esempi, i generatori si chiamano radici primitive, o elementi primitivi

logaritmo discreto

- sia G un gruppo ciclico di ordine n, sia g un generatore di G
- dato $y \neq 1 \in G$
- bisogna determinare l'unico intero x con $1 \leq x \leq n-1$ tale che

$$g^x = y$$

- ex: in $U(\mathbb{Z}_9)$ con $g = 2$, se $y = 7$ si ha $x = 4$, perché $2^4 = 7$.
- l'intero x si chiama il logaritmo discreto di y in base g, e si denota con $\log_g y$
- ex: in $U(\mathbb{Z}_9)$, $4 = \log_2 7$

logaritmo discreto come funzione unidirezionale

- in generale, lavoreremo con il gruppo $U(\mathbb{Z}_p) = \mathbb{Z}_p^*$
- dati g generatore di $\mathbb{Z}_p^*$ e x tale che $1 \leq x \leq p-1$, calcolare $y = g^x$ è computazionalmente facile
- ($y \equiv g^x \pmod{p}$ – si usa l'algoritmo square-and-multiply)
- si ritiene che, dati g generatore di $\mathbb{Z}_p^*$ e $y \in \mathbb{Z}_p^*$, determinare $x = \log_g y$ sia difficile (sotto opportune ipotesi su p)
- in particolare, p devessere grande (2048 bit), $p \approx 2^{2047}$
- dati g e y posso trovare x tale che $g^x = y$ per tentativi – calcolando g^x per tutti gli x, $1 \leq x \leq p-1$
- ma il numero di tentativi è enorme

cifratura RSA e logaritmo discreto

- nella cifratura RSA, la funzione è del tipo

$$x \longrightarrow x^e \pmod{N}$$

- nel problema del logaritmo discreto, la funzione è del tipo

$$x \longrightarrow g^x \pmod{p}$$