Facile e Difficile

Crittografia

Luciano Margara

Unibo

2022

Facile e Difficile (computazionalmente)

Cosa è facile e cosa è difficile da calcolare?

Numero di cifre di alcune funzioni

n	$\lvert\log_2(n)\rvert$	$\lvert n\rvert$	$\lvert n^2\rvert$	$\lvert n^5\rvert$	$\lvert 2^n\rvert$	$\lvert n^n\rvert$
1	1	1	1	1	1	1
100.000	2	6	11	26	30.103	500.001
200.000	2	6	11	27	60.206	1.060.206
300.000	2	6	11	28	90.309	1.643.137
400.000	2	6	12	29	120.412	2.240.824
500.000	2	6	12	29	150.515	2.849.486
600.000	2	6	12	29	180.618	3.466.891
700.000	2	6	12	30	210.721	4.091.569
800.000	2	6	12	30	240.824	4.722.472
900.000	2	6	12	30	270.927	5.358.819
1.000.000	2	7	13	31	301.030	6.000.001

Valore di alcune funzioni

n	$\log_2(n)$	n	n^2	n^5	2^n
10	3	10	100	100.000	1024
100	6	100	10.000	10.000.000.000	x
1000	9	1000	1.000.000	1.000.000.000.000.000	y

$x = 126765060022822940149670320537 6$

$y = 107150860718626732094842504906000181056$

$140481170553360744375038837035105112493612249319837881569585812759467291755314682518714528569231404359845775746985748039345677748242309854210746050623711418779541821530464749835819412673987675591655439460770629145711964776865421676604298316526243868372056680693 76$

Vita dell'Universo

Secondo alcune stime, il sole si spegnerà tra 4 miliardi di anni, ovvero tra 126.144.000.000.000.000.000 microsecondi

Fattorizzazione di numeri

Input: $n \quad (= p_1^{k_1} \cdot \ldots \cdot p_m^{k_m})$
Output: $p_1, k_1, \ldots, p_m, k_m$
Numero di cifre (in base b) di $n = \log_b(n)$

Fattorizzazione di numeri: algoritmo migliore

$$T(n) = \mathrm{e}^{\left(\sqrt[3]{\frac{64}{9}\cdot\ln(n)\cdot\ln(\ln(n))^2}\right)}$$

Se n è un numero di 3000 cifre binarie, allora

$$T(n) = 9.31119 \cdot 10^{50}$$

Elevamento a potenza e Logaritmo

$$a = \mathrm{b}^c$$

Elevamento a potenza: dati b e c calcolare a
Logaritmo: dati a e b calcolare c
Nei numeri reali calcolare il logaritmo è facile !

Logaritmo discreto

Sia p un numero primo
Sia $\mathbb{Z}_p^* = \{1, \ldots, p-1\}$ il gruppo degli interi modulo p con l'operazione di moltiplicazione modulo p
Siano $a, b, c \in \mathbb{Z}_p^*$

$$a = \mathrm{b}^c \mod p$$

Elevamento a potenza: dati b e c calcolare a
Logaritmo: dati a e b calcolare c

Logaritmo discreto: Esempio

$p = 17$
$\mathbb{Z}_{17}^* = \{1, \ldots, 16\}$

$$13 = 3^4 \mod 17$$

Elevamento a potenza: dati 3 e 4 calcolare 13
Logaritmo: dati 13 e 3 calcolare 4
Questo problema è difficile !

Facile vs difficile

Facile: tutto ciò che possiamo calcolare in tempo polinomiale

Difficile: tutto ciò che sappiamo calcolare in tempo esponenziale ma non sembra possibile calcolare in tempo polinomiale

Impossibile: tutto ciò che non sappiamo calcolare

Impossibile: Equazioni diofantee

$$3x^2 - 7y^2z^3 = 18$$
$$-7y^2 + 8z^2 = 0$$

Trovare soluzioni per intere per le variabili x, y, z

Impossibile: non esistono algoritmi per risolvere un sistema di equazioni diofantee