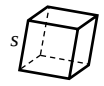
Corso matematica Data:



$A = 6 \cdot s^2$

Caccia ai divisori!

Trovare tutti i divisori di un numero naturale è un compito facile ma che può richiedere molto tempo.

Ad esempio, per trovare tutti i divisori di 100 dovremmo eseguire 100 divisioni:

100 : 1 =	100 : 2 =	100 : 3 =	100 : 4 =
…	100 : 98 =	100 : 99 =	100 : 100 =

C'è un modo di trovare i divisori che ci evita di effettuare tutte queste divisioni?

Osserviamo alcuni insiemi di divisori:

$D_{12} = \{ 1; 2; 3; 4; 6; 12 \}$

$D_{39} = \{ 1; 3; 13; 39 \}$

$D_{13} = \{ 1; 13 \}$

$D_{25} = \{ 1; 5; 25 \}$

$D_{81} = \{ 1; 3; 9; 27; 81 \}$

$D_{100} = \{ 1; 2; 4; 5; 10; 20; 25; 50; 100 \}$

Possiamo tracciare una specie di asse di simmetria. I divisori sono sempre presenti a coppie. Con l'eccezione di quando un divisore fa coppia con se stesso (il divisore moltiplicato per se stesso è uguale al numero di cui si cercano i divisori. Es. $5 \cdot 5 = 25$, $9 \cdot 9 = 81$, $10 \cdot 10 = 100$).

$1 \cdot 88 = 88$

$4 \cdot 22 = 88$

$D_{88} = \{ 1; 2; 4; 8; 11; 22; 44; 88 \}$

$8 \cdot 11 = 88$

$2 \cdot 44 = 88$

Quindi, di solito, quando troviamo un divisore, ne troviamo automaticamente anche un altro.
Fino a quando allora dobbiamo eseguire divisioni per cercare divisori? Qual è il numero spartiacque? Come trovarlo?

È il numero naturale più vicino al numero che ……

……

Questo numero può essere trovato eseguendo la ……

Esempi:

Quindi, ad esempio, per trovare i divisori di 200, basta cercare i divisori fino a $\sqrt{200} = 14{,}142135623... \cong 14$

Si può poi fare un'altra importante ottimizzazione: se un numero non è divisibile per n, non lo sarà nemmeno per i multipli di n.

Quindi per cercare i divisori di 200 ci basta eseguire le seguenti divisioni:

200 : 2 = 100 ∈ N	200 : 3 = $66,\overline{6}$ ∉ N	200 : 4 = 50 ∈ N
200 : 5 = 40 ∈ N	200 : 7 = $28,\overline{571428}$ ∉ N	200 : 8 = 25 ∈ N
200 : 10 = 20 ∈ N	200 : 11 = $18,\overline{18}$ ∉ N	200 : 13 = $15,\overline{384615}$ ∉ N

Cercare i divisori di un numero resta comunque impresa ardua; per numeri sufficientemente grandi anche un computer può fare fatica. Su questo fatto si basano alcuni algoritmi di sicurezza informatica.

Ad esempio, nel 2020, per scoprire che il numero:

2140324650240744961264423072839333563008614715144755017797754920881418023447140136643345519095804679610992851872470914587687396261921557363047454770520805119056493106687691590019759405693457452230589325976697471681738069364894699871578494975937497937

è fattorizzabile in

6413528947707158027879019017057738908482501474294344720811685963202453234463023862359875266834770873766192558569463979885336733372027594978156556226010605355114227940760344767554666784520987023841729210037080257448673296881877565718986258036932062711

ci sono voluti l'equivalente di 2500 anni CPU (il che significa che un computer del 2020 di media potenza, lavorando da solo, ci avrebbe messo 2500 anni a trovarlo).