La funzione χ

La funzione ϕ di Eulero è definita nel seguente modo:

$$\phi(n) = \#\{m \in \mathbb{N} \colon m < n \text{ e } (m,n) = 1\}$$

La ϕ è una funzione aritmetica moltiplicativa, cioè $\phi(mn) = \phi(m)\phi(n)$ se e solo se $(m,n) = 1$, con $n, m \in \mathbb{N}_0$. Inoltre, se $n = \prod_{i=1}^{h} p_i^{k_i}$, con p_i primi distinti e $k_i \in \mathbb{N}_0$, allora $\phi(n) = \prod_{i=1}^{h} p_i^{k_i-1}(p_i - 1)$. Quindi, essendo $p_i - 1 < p_i$ per ogni i, allora si ha che $\phi(n) < n$. Quindi, iterando la ϕ, giungo a 1, prima o poi, visto che per ogni $n > 1$ c'è almeno un numero coprimo con n. Ha senso quindi definire la funzione χ nel seguente modo:

$$\begin{cases} \chi(1) = 0 \\ \chi(n) = 1 + \chi(\phi(n)) \end{cases}$$

In questo modo, $\chi(2) = 1 + \chi(1) = 1$, $\chi(3) = 1 + \chi(2) = 1 + 1 = 2$ e così via.

Teorema 1. *Valgono le seguenti proprietà:*

1. $\chi(2n) = \chi(n)$ *per ogni* n *dispari maggiore di* 1
2. $\chi(2^n) = n$ *per ogni* n
3. $\chi(3^n) = n + 1$ *per ogni* $n > 1$

Dimostrazione. Vediamo punto per punto:

1. $\chi(2n) = 1 + \chi(\phi(2n)) = 1 + \chi(\phi(2)\phi(n)) = 1 + \chi(\phi(n)) = \chi(n)$
2. Vediamo per induzione:
   (a) $\chi(2^0) = \chi(1) = 0$
   (b) $\chi(2^1) = \chi(2) = 1$
   (c) $\chi(2^n) = 1 + \chi(2^{n-1}) = 1 + (n-1) = n$
3. Vediamo per induzione:
   (a) $\chi(3^1) = \chi(3) = 2$
   (b) $\chi(3^n) = 1 + \chi(2 \cdot 3^{n-1}) = 1 + \chi(3^{n-1}) = 1 + (n - 1 + 1) = n + 1$

□

Lo scopo della funzione è contare il numero di iterate della ϕ, prima che questa restituisca il valore 1. Indichiamo con ϕ^k la k-sima iterata della ϕ.

Teorema 2.

$$\phi^{\chi(n)}(n) = 1$$

Dimostrazione. Per induzione:

1. $\phi^{\chi(2)}(2) = \phi(2) = 1$
2. $\phi^{\chi(3)}(3) = \phi^2(3) = \phi(\phi(3)) = \phi(2) = 1$
3. $\phi^{\chi(n)}(n) = \phi^{\chi(n)-1}(\phi(n)) = \phi^{\chi(\phi(n))+1-1}(\phi(n)) = \phi^{\chi(\phi(n))}(\phi(n)) = 1$

$\square$

Inoltre $\phi^{\chi(n)-1}(n) > 1$. Si potrebbe dimostrare che per $n > 2$ si ha $\phi^{\chi(n)-1}(n) = 2$, dal fatto che $\phi(n) = 1 \Leftrightarrow n = 2$. Quindi sarebbe possibile definire una $\tilde{\chi}$ anche con dato iniziale $\tilde{\chi}(2) = 0$, contando quanti passi ci mettere per giungere a 2. In questo modo si ha che $\tilde{\chi}(n) = \chi(n) - 1$, ma $\tilde{\chi}(1)$ non avrebbe significato. Vediamo un'altra utile applicazione della funzione χ.

Teorema 3. *Siano $a, b \in \mathbb{N}_0$ tali che a è coprimo con $b, \phi(b), \phi^2(b), \ldots, \phi^{\tilde{\chi}(b)}$. Sia $H_0^{(a)} = 1$ e $H_n^{(a)} = a^{H_{n-1}^{(a)}}$. Allora $H_n^{(a)} \mod b$ è definitivamente costante.*

Dimostrazione. Osserviamo che essendo a coprimo con b e con $\phi(b)$, a deve essere necessariamente un numero dispari. Infatti $\phi(b)$ è pari e se a fosse pari, si avrebbe che $2|(a, \phi(b))$. Pertanto possiamo assumere a dispari. Quindi anche $H_n^{(a)}$ è dispari per ogni $n \geq 0$. Ricordo l'equazione di Eulero-Fermat:

$$a^{\phi(n)} \equiv_n 1 \quad \forall (n, a) = 1 \tag{1}$$

Vediamo cosa accade, usando l'equazione 1:

1. $H_1^{(a)} = a$ e non possiamo concludere nulla.
2. $H_2^{(a)} = a^a$ e possiamo usare 1: sia $a_1 = a \mod \phi(b)$. Allora $H_2^{(a)} = a^a = a^{a_1} \mod b$.
3. $H_3^{(a)} = a^{a^a}$ e possimo usare 1: sia $a_1 = a^a \mod \phi(b)$. Riutilizziamo 1 e otteniamo $a_2 = a \mod \phi^2(b)$. Quindi $a_1 = a_2^a \mod \phi(b)$. Allora $H_3^{(a)} = a^{a^a} \equiv_b a^{a_1} \equiv_b a^{a^{a_2}}$.
4. ...

$\square$

Detto questo, ho formulato alcune congetture:

1. $\chi(p^n) = n\chi(p-1) + 1$ per ogni $p > 2$ primo e $n > 0$
2. $\chi(2^n \cdot m) = n + \chi(m)$ per ogni $n > 0$
3. $\chi(p_1^{n_1} \cdot \ldots \cdot p_k^{n_k}) = n_1\chi(p_1 - 1) + \ldots + n_k\chi(p_k - 1) + 1$ con $p_i > 2$ primi distinti e $n_j > 0$
4. $\chi(2^n \cdot p_1^{n_1} \cdot \ldots \cdot p_k^{n_k}) = n + n_1\chi(p_1 - 1) + \ldots + n_k\chi(p_k - 1) + 1$ con $p_i > 2$ primi distinti e $n, n_j > 0$

Alcuni commenti: la 1 è già stata dimostrata nel caso in cui $p = 3$. Dalla 2 e dalla 3 segue immediatamente la 4. La 4 si può vedere come un caso particolare della 3, ma che funziona, con le dovute modifiche, anche nel caso della $\tilde{\chi}$.