Il Teorema cinese del resto

Il Teorema cinese del resto

Due numeri x e y si dicono congrui modulo n - e si scrive $x \equiv y \pmod{n}$ - se, quando li divido per n, hanno lo stesso resto. Ad esempio $17 \equiv 12 \pmod{5}$ perchè sia 17 che 12 danno resto 2 quando vengono divisi per 5. In quali casi è possibile ricostruire un numero a partire a partire dai resti della sua divisione con altri numeri? Una risposta a questa domanda è data dal *Teorema cinese del resto*, di cui qui presentiamo un caso particolare.

Teorema

Siano n_1, n_2, n_3 numeri primi distinti e sia $N = n_1 \cdot n_2 \cdot n_3$. Per ogni scelta di resti a_1, a_2, a_3, con $0 \leq a_i < n_i$, esiste un unico intero x, con $0 \leq x < N$, tale che

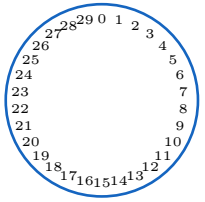
$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ x \equiv a_3 \pmod{n_3} \end{cases}$$

Cosa significa? Immaginiamo di voler individuare un numero x tra 0 e $N-1$ sapendo soltanto "che resto dà" quando lo dividiamo per n_1, per n_2 e per n_3. Il teorema afferma che questa informazione basta e avanza: non esistono due numeri diversi compresi tra 0 e $N-1$, che condividano *tutti e tre* questi resti contemporaneamente. Conoscere i tre resti equivale dunque a conoscere il numero stesso: in un certo senso, la terna (a_1, a_2, a_3) è una specie di "carta d'identità" del numero x.

Serve davvero che i numeri siano primi? In realtà no, per avere le stesse conclusioni del teorema è sufficiente che n_1, n_2 e n_3 siano a due a due coprimi (ovvero non abbiano fattori comuni). Quando i numeri non sono a due a due coprimi, è possibile sia che non ci siano soluzioni del tutto, sia che venga meno l'unicità della soluzione tra 0 e $N-1$.
Il teorema, nella sua formulazione più generale, non richiede che i numeri coinvolti siano a due a due coprimi.

Il gioco dei dischi

Scegliamo tre numeri primi distinti n_1, n_2 e n_3 e immaginiamo di avere un disco che contiene tutti i numeri da 0 a $N = n_1 n_2 n_3 - 1$ disposti lungo la circonferenza. Sopra di esso immaginiamo di avere, per ciascun n_i, un disco nero forato i cui fori sono disposti a intervalli regolari di n_i posizioni. Ogni disco può essere ruotato liberamente attorno al centro comune e lascia visibili tutti e soli gli interi che sono congrui tra loro modulo l'intero considerato. Quando i tre dischi vengono sovrapposti al disco principale, un numero resta visibile *solo se*, in corrispondenza della sua posizione, c'è un foro in *ognuno* dei tre dischi; altrimenti viene coperto dal nero di almeno uno di essi.



Disco principale (0–29)


Disco $n_1 = 2$


Disco $n_2 = 3$


Disco $n_3 = 5$

Come si gioca

La persona pensa un numero x tra 0 e $N-1$ senza dirlo a nessuno e calcola i resti a_i della divisione di x per ciascun n_i. Il disco corrispondente al valore n_i viene poi ruotato in modo che uno dei suoi fori passi sopra la casella pari al resto a_i calcolato per il valore n_i. Rimarrà un solo numero scoperto: quello pensato!

Esempio

Se la persona pensa $x = 17$, si ha $17 \equiv 1 \pmod{2}$, $17 \equiv 2 \pmod{3}$, $17 \equiv 2 \pmod{5}$. Ruotando i tre dischi in modo che il il disco relativo al 2 abbia un foro in corrispondenza del numero 1, quello relativo al 3 in corrispondenza del 2 e quello relativo al 5 in corrispondenza del 2, l'unico numero rimasto scoperto sul disco principale sarà proprio il 17.

Perché funziona. Per il teorema, x è l'*unico* numero tra 0 e $N-1$ che soddisfa contemporaneamente $x \equiv a_1 \pmod{n_1}$, $x \equiv a_2 \pmod{n_2}$, $x \equiv a_3 \pmod{n_3}$. Sovrapponendo i tre dischi ruotati come sopra, ogni altra casella verrà coperta da almeno un disco, mentre l'unica scoperta da tutti e tre sarà esattamente quella del numero pensato.