Aritmetica modulare

L'aritmetica modulare studia quelle particolari situazioni nelle quali i numeri interi "si avvolgono su sé stessi" ogni volta che raggiungono i multipli di un determinato numero *n*, detto *modulo*.
Questa importante branca della matematica viene detta anche *aritmetica dell'orologio*, perché la sua applicazione più nota riguarda la rappresentazione delle ore, a cicli di 12 o di 24.

L'aritmetica modulare si basa sul concetto di *congruenza modulo n*.
Dati tre numeri naturali, *a*, *b*, *n*, con $n \neq 0$, si dice che *a* e *b* sono *congrui modulo n* se, divisi per *n*, producono lo stesso resto. Scelto un modulo *n*, si ottiene una partizione dell'insieme dei numeri naturali in classi di equivalenza: se *a* e *b* sono *congrui modulo n* si dice anche che *a* e *b* appartengono alla stessa *classe di resto modulo n*.
Nel caso dell'orologio, ad esempio, si può dire che 14 e 2 sono *congrui modulo 12* o che appartengono alla stessa *classe di resto modulo 12*, perché sia 14 che 2, divisi per 12, forniscono come resto 2.

Una proprietà interessante della relazione di congruenza è la sua invarianza rispetto alle usuali operazioni aritmetiche tra numeri naturali. Ovvero se si esegue la stessa operazione aritmetica su due numeri congrui modulo *n*, i due valori risultanti sono ancora congrui tra loro modulo *n*.
Ad esempio, se sommiamo 5 a ciascuno dei due numeri 14 e 2 (che, come abbiamo visto, sono congrui modulo 12) otteniamo: 14 + 5 = 19; 2 + 5 = 7; ebbene, anche 19 e 7 sono congrui modulo 12, dato che, se vengono divisi per 12, forniscono entrambi come resto 7.

Nelle applicazioni di matematica magica, il ricorso all'aritmetica modulare consente di ottenere diversi effetti piuttosto sorprendenti. Le sue proprietà, infatti, anche se piuttosto semplici, non sono di immediata rilevazione.