Giorno 30: classi di resto

Gli interi $\mathbb{Z}$ non formano campo. Abbiamo una somma ben fatta, il prodotto è associativo, commutativo, ha 1 come elemento neutro ma non abbiamo inverso rispetto al prodotto. Ad esempio $2 \in \mathbb{Z}$ non ha reciproco, visto che $\frac{1}{2}$ non è intero.

Se prendiamo un numero intero $n \in \mathbb{Z}$ possiamo definire equivalenti 2 intero a, b se e solo se esiste un $k \in \mathbb{Z}$ tale che $b = a + kn$. Questa è una relazione di equivalenza e le corrispondenti classi di equivalenza $[a] = \{\dots, a-2n, a-n, a, a+n, a+2n, \dots\}$. In pratica $[0]$ sono i multipli di n, $[1]$ sono i numeri $kn+1$, e via così.

Questo è quello che facciamo all'asilo quando impariamo a leggere l'orologio analogico, in quel caso con $n = 12$ (o $n = 24$). Se parliamo di $n = 12$ (che già non si dovrebbe), passate 10 ore dopo le 5 non sono le 15, sono le 3, o meglio la classe $[3] = \{\dots, -9, 3, 15, 27, \dots\}$ che sono quando l'orologio segna le 3.

> **Nota:** La prossima volta che incontro una maestra che chiede che senso abbia insegnare a leggere l'orologio analogico ai bambini quando sui telefonini c'è l'orologio digitale, la sprango.

Quando sommiamo le ore non sommiamo i numeri. Se calcoliamo 5+10 sull'orologio non fa 15, fa $[15 \mod 12] = [3]$. Quindi possiamo definire l'insieme delle classi di equivalenza $\mathbb{Z}_n$, che ha n elementi, e ridefiniamo le operazioni come

$$[a] + [b] = [a+b] = [a+b \mod n] \qquad [a][b] = [ab] = [ab \mod n] \tag{1}$$

Uno può dimostrare che queste nuove operazioni ereditano da $\mathbb{Z}$ le proprietà, associativa, esistenza degli elementi neutri $[0]$ e $[1]$ e dell'opposto $[-a] = [-a \mod n] = [n-a]$. Per ora non ci pronunciamo sul reciproco.

Facciamo 3 esempi.

> **Nota:** $(n = 2)$: in $\mathbb{Z}_2$ abbiamo 2 classi $[0]$ e $[1]$. Sono i pari e i dispari. Le somme sono
>
> $$\begin{array}{ll} [0]+[0]=[0] & [0]+[1]=[1] \\ [1]+[0]=[1] & [1]+[1]=[0] \end{array} \tag{2}$$
>
> mentre i prodotti sono
>
> $$\begin{array}{ll} [0][0]=[0] & [0][1]=[0] \\ [1][0]=[0] & [1][1]=[1] \end{array} \tag{3}$$
>
> Si noti che $[1]$ è il reciproco di 1, quindi Z_2 è un campo.
>
> $(n = 3)$: in $\mathbb{Z}_3$ abbiamo 3 classi $[0]$, $[1]$ e $[2]$. Le somme sono
>
> $$\begin{array}{lll} [0]+[0]=[0] & [0]+[1]=[1] & [0]+[2]=[2] \\ [1]+[0]=[1] & [1]+[1]=[2] & [1]+[2]=[0] \\ [2]+[0]=[2] & [2]+[1]=[0] & [2]+[2]=[1] \end{array} \tag{4}$$
>
> mentre i prodotti sono
>
> $$\begin{array}{lll} [0][0]=[0] & [0][1]=[0] & [0][2]=[0] \\ [1][0]=[0] & [1][1]=[1] & [1][2]=[2] \\ [2][0]=[0] & [2][1]=[2] & [2][2]=[1] \end{array} \tag{5}$$

Si noti che [2] è il reciproco di [2], quindi Z_3 è un campo con 3 elementi.

Quindi siamo tentati di dire che $\mathbb{Z}_n$ è un campo, non sapessimo che la natura è maligna.

($n = 4$): in $\mathbb{Z}_4$ abbiamo 4 classi [0], [1], [2] e [3]. Le somme sono

$$\begin{array}{cccc} [0]+[0]=[0] & [0]+[1]=[1] & [0]+[2]=[2] & [0]+[3]=[3] \\ [1]+[0]=[1] & [1]+[1]=[2] & [1]+[2]=[3] & [1]+[3]=[0] \\ [2]+[0]=[2] & [2]+[1]=[3] & [2]+[2]=[0] & [2]+[3]=[1] \\ [3]+[0]=[3] & [3]+[1]=[0] & [3]+[2]=[1] & [3]+[3]=[2] \end{array} \tag{6}$$

mentre i prodotti sono

$$\begin{array}{cccc} [0][0]=[0] & [0][1]=[0] & [0][2]=[0] & [0][3]=[0] \\ [1][0]=[0] & [1][1]=[1] & [1][2]=[2] & [1][3]=[3] \\ [2][0]=[0] & [2][1]=[2] & [2][2]=[0] & [2][3]=[2] \\ [3][0]=[0] & [3][1]=[3] & [3][2]=[2] & [3][3]=[1] \end{array} \tag{7}$$

Si noti che [3] è il reciproco di [3], ma non esiste il reciproco di [2], quindi $\mathbb{Z}_4$ non è un campo. Si noti che $[2][2] = [0]$, cioè $[2]|[0]$, esistono divisori dello zero.

Quando non esiste il reciproco di ogni elemento non nullo, quell'insieme si chiama un *anello*. Ogni $\mathbb{Z}_n$ è un *anello* ma qualcuno (ad esempio $\mathbb{Z}_2$ e $\mathbb{Z}_3$) è anche un campo.

In un anello, può capitare che alcuni elementi siano invertibili (e altri no se no sarebbe un campo). Gli elementi invertibili si chiamano *unità*. In $\mathbb{Z}$, sia 1 che -1 sono unità. In un campo ogni elemento non nullo è una unità.

Ovviamente abbiamo sempre che $[0][a] = [0]$. Ma in un anello può capitare che esistano 2 elementi entrambi non nulli tali che $[a][b] = [0]$. Abbiamo visto che $[2][2] = [0]$ in $\mathbb{Z}_4$. Analogamente, $[3][2] = [0]$ in $\mathbb{Z}_6$. In questi casi diciamo che quell'anello ammette *divisori dello zero*. Quindi [2] è divisore dello zero in $\mathbb{Z}_4$, in $\mathbb{Z}_6$ e [3] è anche divisore dello zero in $\mathbb{Z}_6$ (e in $\mathbb{Z}_9$).

In realtà se $n = ab$ (con $[a]$ e $[b]$ non nulli e non unità in $\mathbb{Z}_n$) allora $[a]$ e $[b]$ sono divisori dello zero in $\mathbb{Z}_n$. Se consideriamo un primo p, allora in $\mathbb{Z}_p$ non possiamo costruire divisori dello zero in questo modo. Questo purtroppo non impedisce che possano esistere divisori dello zero construiti in questo modo. Uno deve *dimostrare* che in $\mathbb{Z}_p$ non esistono divisori dello zero (che è abbastanza laborioso in generale, mentre è facile controllarlo in $\mathbb{Z}_5$ o in $\mathbb{Z}_{17}$ dove basta provarlo per tutti gli elementi che oltretutto sono finiti).

Poi è abbastanza facile mostrare che se X è un campo allora non esistono divisori dello zero.

Nota: dim: se X è un campo consideriamo l'equazione $ax = 0$ con $a \neq 0$. Siccome siamo in un campo e $a \neq 0$ allora esiste a^{-1} e possiamo moltiplicare ambo i membri (a sinistra) per a^{-1} e otteniamo l'equazione equivalente $x = a^{-1}0 = 0$. Quindi l'unica possibilità è che $x = 0$ e quindi non sono divisori dello zero. In un campo non ci sono divisori dello zero.

Notate bene: ho detto che campo è X? No. Quello che ho scritto vale in *ogni* campo, non ha nessuna importanza cosa siano gli elementi di X. La generalità del risultato viene *completamente* dal fatto che è un ragionamento astratto.

Questo basta a concludere che $\mathbb{Z}_n$ non è un campo quando $n \in \mathbb{Z}$ non è primo. Comunque (anche se è un po' più complicato da dimostrare) è vero che se consideriamo un primo $p \in \mathbb{Z}$, allora $\mathbb{Z}_p$ è un campo (cioè $\mathbb{Z}_p$ è un campo se e solo se $p \in \mathbb{Z}$ è primo).

Tanto per essere chiari se chiedete ad un matematico di mostrare se $\mathbb{Z}_{72871}$ è un campo, gli scatta nel cervello il; teorema $\mathbb{Z}_p$ è un campo se e solo se p è primo e la risposta è: basta controllare se p è primo. Per un matematico la matematica non è rispondere al problema è fare il teorema che ti consente di rispondere a classi di domande. Vi ricordate quando abbiamo definito numeri per poter risolvere classi di equazioni? Quella è matematica, non passare la maturità.

> **Nota:** Come esercizio sui quantificatori è vero che se uno fa matematica poi risolve facilmente i problemi, ma risolvere i problemi non è fare matematica più di quanto fare l'amore sia riprodursi.
>
> Come probabilmente Feynmann non ha mai detto:
>
> *La fisica è come il sesso: certo, può dare qualche risultato concreto, ma non è per questo che la facciamo.*

Comunque era per mostrare che ci sono campi che non sono $\mathbb{Q}$ o $\mathbb{R}$. Ira prendete $\mathbb{Z}_{13}$ e considerate l'equazione $[7]x = [2]$. Siccome so che $\mathbb{Z}_{13}$ è un campo, allora $[7]$ deve ammettere un inverso. Infatti $[7][2] = [14] = [1]$, quindi in $\mathbb{Z}^{13}$ abbiamo che $[7]^{-1} = [2]$. Quindi l'equazione ha soluzione $x = [2][2] = [4]$, e *vedrete che* $[4]$ *è la soluzione cercata*.

> **Nota:** Significa *controllate* che $[7][4] = [2]$ in $\mathbb{Z}_{13}$.

Ora brindate, sapete risolvere equazioni *in un campo qualunque*.