CAPITOLO 1
I NUMERI NATURALI
1.1 Il sistema decimale

Originati dall'esigenza di *contare*, i numeri naturali rappresentano un *modello* adeguato per la rappresentazione astratta di insiemi di oggetti, e possono essere rappresentati in molti modi, di cui quello largamente più diffuso è il *sistema decimale* posizionale, o *in base dieci*, rappresentato dalle cifre da 0 a 9.

Questo significa che, ad esempio, il numero 731 è diverso dal 137, pur essendo costituiti dalle stesse cifre, perché $731 = 700 + 30 + 1 = 7 \cdot 10^2 + 3 \cdot 10^1 + 1 \cdot 10^0$, mentre $137 = 100 + 30 + 7 = 1 \cdot 10^2 + 3 \cdot 10^1 + 7 \cdot 10^0$.

Osservando il modo con cui i due numeri sono stati rappresentati nel sistema decimale, è possibile dare una regola generale per la rappresentazione di qualsiasi numero intero:

$$z = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_1 \cdot 10 + a_0 ,$$

dove i *coefficienti*, ovvero i termini $a_i \in \{0,1,...,9\}$, appartengono cioè all'insieme delle cifre da 0 a 9.

Notiamo che

731 : 10 = 73 e *resto* 1,
73 : 10 = 7 e *resto* 3,
7 : 10 = 0 e *resto* 7,

e quindi, i coefficienti sono i resti delle successive divisioni del numero dato per 10.

Questo spiega il senso della rappresentazione usuale di un numero naturale di n+1 cifre:

$$z = a_n a_{n-1} ... a_1 a_0 .$$

Come è facile intuire, è possibile rappresentare i numeri naturali in una base *qualsiasi*, una volta accettato che le cifre nella rappresentazione numerica sono i resti delle successive divisioni per la *base*.

Per esempio, in base 3 si ha:

731 : 3 = 243 e resto 2,
243 : 3 = 81 e resto 0,
81 : 3 = 27 e resto 0,
27 : 3 = 9 e resto 0,
9 : 3 = 3 e resto 0,
3 : 3 = 1 e resto 0,
1 : 3 = 0 e resto 1.

e quindi

$$731 = 1 \cdot 3^6 + 0 \cdot 3^5 + 0 \cdot 3^4 + 0 \cdot 3^3 + 0 \cdot 3^2 + 0 \cdot 3^1 + 2 \cdot 3^0 = 1000002$$

Per inciso, l'ultima rappresentazione suggerisce anche come passare dalla base 3 alla base 10.

Il vantaggio più grande apportato dalla notazione *posizionale* rispetto a quella *additiva* (tipo quello dei numeri *romani*, dove MCMXCVI = 1000 (M) + 900 (CM) + 90 (XC) + 5 (V) + 1 (I)), si riscontra nei *calcoli* con le operazioni aritmetiche fondamentali.

Nel sistema posizionale le regole di calcolo possono essere raccolte nelle famose *tavole*, che una volta memorizzate, permettono di svolgere calcoli con relativa semplicità.

1.2 Numeri primi

Tra i numeri naturali assumono una grande importanza i cosiddetti *numeri primi*, ovvero quei numeri maggiori di 1, che non ammettono divisori diversi da se stesso e da 1.

I numeri che non sono primi si dicono *composti*. In generale, un numero *a* è multiplo di *b* se esiste un numero naturale *c* tale che $a = bc$: in questo caso si dice che *b* divide *a* e si indica $b \mid a$.

Dalla definizione di multiplo di un numero naturale seguono i seguenti fatti:

- $d \mid a, \quad d \mid b \quad \Rightarrow d \mid a + b$,
- $d \mid a \quad \Rightarrow d \mid ac, \quad \forall c \in N$,

- $d \mid a, \quad a \mid b, \quad \Rightarrow d \mid b$.

Caratterizziamo ulteriormente i numeri primi attraverso alcuni importanti risultati.

Teorema della fattorizzazione unica: *ogni numero naturale maggiore di 1 si può esprimere in un solo modo come prodotto di potenze di numeri primi.* Si tratta di un teorema fondamentale dell'aritmetica, di cui dimostreremo tra breve soltanto l'unicità.
La ricerca dei numeri primi all'interno dell'insieme dei numeri naturali suscita da sempre un grande interesse.
Esaminiamo un metodo molto antico, ideato dal grande scienziato *Eratostene.*
Il metodo, denominato *crivello di Eratostene*, consente, fissato un numero naturale *N*, di determinare tutti i numeri primi non superiori a *N.* In che modo? Semplicemente *cancellando i multipli dei numeri il cui quadrato non supera N.* Vediamo come funziona con un semplice esempio: determiniamo i numeri primi minori di $N = 36$. Cancelliamo i multipli dei numeri da 2 a 6 (in quanto il quadrato di 7 supera 40):

1 **2** **3** ~~4~~ **5** ~~6~~
7 ~~8~~ ~~9~~ ~~10~~ **11** ~~12~~
13 ~~14~~ ~~15~~ ~~16~~ **17** ~~18~~
19 ~~20~~ ~~21~~ ~~22~~ **23** ~~24~~
~~25~~ ~~26~~ ~~27~~ ~~28~~ **29** ~~30~~
31 ~~32~~ ~~33~~ ~~34~~ ~~35~~ ~~36~~

Il metodo ideato da Eratostene si basa sul fatto che un numero composto minore o uguale a 36, *è divisibile per un numero minore o uguale a 6.* Dimostriamo questo fatto considerando il numero $n = ab \le 36$: se quanto detto non fosse vero, risulterebbe $a > 6 \wedge b > 6$ e quindi $n = ab > 36$, in contraddizione con la scelta di $n = ab \le 36$.
Adesso occupiamoci di stabilire *quanti sono* i numeri primi. La risposta a questa domanda fu data, sempre nell'antichità, dal matematico **Euclide**, ed è contenuta nel teorema che porta il suo nome, di cui, oltre all'enunciato, daremo anche una dimostrazione.

Teorema (Euclide). I numeri primi sono *infiniti*.
Dimostrazione. Supponiamo *per assurdo* che l'insieme dei numeri primi contenga un numero finito di elementi, e sia *p* il maggiore di questi (consideriamo nota la proprietà di *ordinamento* dell'insieme dei numeri naturali). Moltiplichiamo tutti i numeri primi ed aggiungiamo al risultato 1. Il numero $n = 2 \cdot 3 \cdot 5 \cdot \ldots \cdot p + 1$ così ottenuto dovrebbe essere non primo, in quanto *il più grande* numero primo è *p*, e chiaramente $n > p$. Tuttavia, se osserviamo attentamente il numero *n*, notiamo che questo può essere scritto nella forma $n = 2(3 \cdot 5 \cdot \ldots \cdot p) + 1 \Rightarrow 2 \nmid n$, ma anche $n = 3(2 \cdot 5 \cdot \ldots \cdot p) + 1 \Rightarrow 3 \nmid n$, oppure, in generale se *q* è un qualsiasi numero primo minore o uguale a *p*, $n = q(2 \cdot 3 \cdot 5 \cdot \ldots \cdot p) + 1 \Rightarrow q \nmid n$, dove il prodotto tra parentesi, ovviamente, non contiene il fattore *q*.
Da questo segue che *n* non è divisibile per nessuno dei numeri primi dell'insieme. Si presentano quindi due possibilità, che portano comunque ad una contraddizione: se *n* è primo, allora deve appartenere all'insieme dei numeri primi, ma $n > p$ in contraddizione con la massimalità di *p*; se *n* è non primo, allora deve scomporsi nel prodotto di primi, ma non essendo divisibile per nessuno dei numeri primi dell'insieme, deve necessariamente esistere un numero primo più grande di tutti i numeri primi dell'insieme, ancora in contraddizione con la massimalità di *p*.
L'insieme dei numeri primi *non* può quindi contenere un numero finito di elementi, come volevasi dimostrare.
Il numero costruito nella dimostrazione suggerisce un metodo per costruire *una successione* di numeri primi.
Purtroppo, ancora non sono state trovate formule per la generazione di numeri primi. Restano tuttora irrisolti due problemi sui numeri primi:

- (*congettura di Goldbach*, 1742): Ogni numero pari diverso da due può essere espresso come somma di due numeri primi,
- esistono infinite coppie di numeri primi *gemelli*, ovvero della forma $p, p+2$.

1.3 Massimo comun divisore ed algoritmo euclideo

Come noto, dati due numeri $a, b \neq 0 \in Z$, l'insieme dei numeri *interi*, si definisce *massimo comun divisore* il maggiore dei loro divisori comuni. Si considera nota la regola per il calcolo del MCD attraverso la scomposizione in fattori primi (giustificata, adesso, dal teorema della fattorizzazione unica): ad esempio, se $a = 18 = 2 \cdot 3^2$, $b = 24 = 2^3 \cdot 3$, allora $MCD(18,24) = 2 \cdot 3 = 6$.

Esiste un metodo "antico" per il calcolo del MCD: il cosiddetto *algoritmo euclideo*, basato su un procedimento *iterativo*.

Supponiamo di voler determinare il MCD $(24,15)$.

$$24 = 1 \text{ x } 15 + 9$$
$$15 = 1 \text{ x } 9 + 6$$
$$9 = 1 \text{ x } 6 + 3$$
$$6 = 2 \text{ x } 3 + 0.$$

Quando l'ultimo resto è zero, il resto precedente è il MCD; nell'esempio sopra, il MCD $(24,15)$ è 3.

In generale, il procedimento iterativo può essere schematizzato così:

$$MCD(a,b):$$
$$a = q_1 b + r_1$$
$$b = q_2 r_1 + r_2$$
$$r_1 = q_3 r_2 + r_3$$
$$\ldots$$
$$r_{n-1} = q_{n+1} r_n + 0 \Rightarrow MCD(a,b) = r_n,$$

dal momento che $r_n = r_n \cdot 1 + 0$.

Dobbiamo giustificare l'algoritmo euclideo. Dimostriamo le seguenti proprietà.

Proprietà 1: se $d \mid a$ e $d \mid b$, $a = bq + r$, allora $d \mid r$.

Dimostrazione. $d \mid a \Rightarrow \exists a' : a = da'$, $d \mid b \Rightarrow \exists b' : b = db'$. Di conseguenza $r = a - qb = da' - qdb' = d(a' - qb') \Rightarrow d \mid r$.

Proprietà 2: se $d \mid r$ e $d \mid b$, $a = bq + r$, allora $d \mid a$.

Dimostrazione. $d \mid r \Rightarrow \exists r' : r = dr'$, $d \mid b \Rightarrow \exists b' : b = db'$. Di conseguenza $a = qb + r = qdb' + dr' = d(qb' + r') \Rightarrow d \mid a$.

Di conseguenza, $MCD(a,b) = MCD(b,r_1)$ e, in definitiva, $MCD(b,r_1) = MCD(r_1,r_2)$, fino a $MCD(r_n,0) = r_n$. Quindi $MCD(a,b) = \ldots = MCD(r_n,0) = r_n$ e l'algoritmo euclideo è pienamente giustificato.

Diretta conseguenza dell'algoritmo euclideo è la seguente proprietà.

Proprietà 3: se $d = MCD(a,b)$, allora esistono due numeri interi *k* e *l* tali che $d = ka + lb$.

La dimostrazione di questa proprietà poggia sul seguente procedimento.

$$24 = 1 \cdot 15 + 9 \Rightarrow 9 = 24 - 1 \cdot 15$$

$$15 = 1 \cdot 9 + 6 \Rightarrow 6 = 15 - 1 \cdot (24 - 1 \cdot 15)$$

$$9 = 1 \cdot 6 + 3 \Rightarrow 3 = 24 - 1 \cdot 15 - 1 \cdot \left[15 - 1 \cdot (24 - 1 \cdot 15)\right] \Rightarrow \quad 3 = 2 \cdot 24 - 3 \cdot 15 \Rightarrow \quad k = 2 \quad l = -3$$

$$6 = 2 \cdot 3 + 0$$

Corollario della proprietà 3 è la
Proprietà 4: se $1 = MCD(a,b)$, allora esistono due numeri interi *k* e *l* tali che $1 = ka + lb$.
Quest'ultima proprietà è fondamentale per la dimostrazione del teorema della fattorizzazione unica. Per questo scopo dimostriamo il seguente fatto.
Lemma: se *p* è primo e $p \mid ab$, allora $p \mid a$ o $p \mid b$.
Dimostrazione. Facciamo vedere, per esempio, che se *p* non divide *a*, necessariamente deve dividere *b*. Infatti, se $p \nmid a \Rightarrow MCD(a,p) = 1 \Rightarrow \exists k,l \in Z$ tali che $ka + lp = 1$, in virtù della proprietà 4. Moltiplicando per *b* l'ultima espressione e ricordando che $p \mid ab \Rightarrow ab = sp$, otteniamo $kab + lbp = b \Rightarrow ksp + lbp = b \Rightarrow (ks + lb)p = b \Rightarrow p \mid b$, come volevasi dimostrare.
Il lemma può essere generalizzato al prodotto di un numero *qualsiasi* di interi, e porta alla conclusione che se *p* divide tale prodotto, allora dovrà dividere *almeno uno* dei fattori.
Esercizio. Dimostrare che se $p \mid abc$, allora o $p \mid a$, o $p \mid b$, o $p \mid c$.

L'unicità della fattorizzazione di un numero naturale
A questo possiamo dimostrare l'*unicità* della fattorizzazione di un numero naturale maggiore di 1.
Dimostrazione (teorema della fattorizzazione unica). Per assurdo supponiamo che un numero naturale maggiore di uno possa essere fattorizzato in due modi diversi, cioè che esistano due diversi insiemi di numeri primi, $(p_1,...,p_r)$ e $(q_1,...,q_s)$, tali che $N = p_1p_2...p_r = q_1q_2...q_s$. Partiamo da p_1: poiché divide N, e $N = q_1q_2...q_s$, per il lemma precedente esiste $k \in 1,...,s$ tale che p_1 divide q_k. Ma quest'ultimo è primo, quindi necessariamente $p_1 = q_k$. Togliamo questi due fattori dalla lista $N = p_1p_2...p_r = q_1q_2...q_s$, e ripetiamo il ragionamento per p_2, per p_3, fino all'ultimo p_r. In questo modo, avendoli eliminati dalla lista $p_1p_2...p_r = q_1q_2...q_s$, il membro di sinistra è uguale a uno. E quello di destra? Dovrà per forza essere anch'esso uguale a uno, essendo $(q_1,...,q_s)$ primi, quindi maggiori di uno. Abbiamo quindi dimostrato che, a meno dell'ordine, la scomposizione di un numero composto è unica.

1.4 Equazioni diofantee
Vogliamo cercare le soluzioni intere delle equazioni algebriche, in una o più incognite, a coefficienti interi: le cosiddette *equazioni diofantee*. Consideriamo l'equazione $ax + by = c$, e dimostriamo il seguente fatto.
Proposizione. L'equazione diofantea $ax + by = c$ ammette soluzioni intere se e soltanto se $MCD(a,b) \mid c$.
Dimostrazione ($\Rightarrow$). Sia $d = MCD(a,b)$, allora $d \mid a$ e $d \mid b$, di conseguenza $a = a'd$ e $b = b'd$.
Dunque se $x := m$ e $y := n$ sono soluzioni intere, allora $a'dn + b'dn = c \Rightarrow c \mid d$.
($\Leftarrow$). Viceversa, se $d \mid c \Rightarrow c = dq$. Per la proprietà 3 $\exists k,l \in Z$ tali che $ak + bl = d$. Se moltiplichiamo per *q* ambo i membri dell'ultima equazione otteniamo

$$(ak + bl)q = dq = c \Rightarrow a(kq) + b(lq) = c \Rightarrow \begin{cases} x := kq \\ y := lq \end{cases}$$ una coppia di soluzioni intere.

Ad esempio, l'equazione $3x + 6y = 22$ non ammette soluzioni intere perché $MCD(3,6) = 3 \nmid 22$.
La proposizione appena vista permette di stabilire se un'equazione diofantea ammette soluzioni intere, inoltre ci suggerisce un metodo per determinarle.
Infatti, se (x',y') e (x^*,y^*) rappresentano due coppie di soluzioni dell'equazione $ax + by = c$, allora la coppia $(x_0 = x' - x^*, y_0 = y' - y^*)$ è soluzione della cosiddetta equazione *omogenea* $ax + by = 0$ (verificare!). Quindi, una soluzione dell'equazione di partenza può essere sempre vista

come la somma tra una soluzione *particolare* (x^*, y^*), e *le* soluzioni dell'equazione omogenea, ovvero tutte le coppie della forma $(x_0 = bn; y_0 = -an)$, con $n \in Z$ (verificare).

Vediamo con un esempio come funziona il meccanismo.

Problema. Si determinino le soluzioni intere dell'equazione $17x - 15y = 5$.

Soluzione. Innanzitutto si individuano le soluzioni dell'*equazione omogenea* associata:

$17x - 15y = 0 \Rightarrow \begin{cases} x_0 = 15n \\ y_0 = 17n \end{cases}$ $n \in Z$ e si osserva che $MCD(17,15) = 1$ divide il termine noto, per cui esistono infinite soluzioni intere dell'equazione diofantea; cerchiamo una soluzione particolare sfruttando la proprietà dell'algoritmo euclideo,

$17 = 1 \cdot 15 + 2$

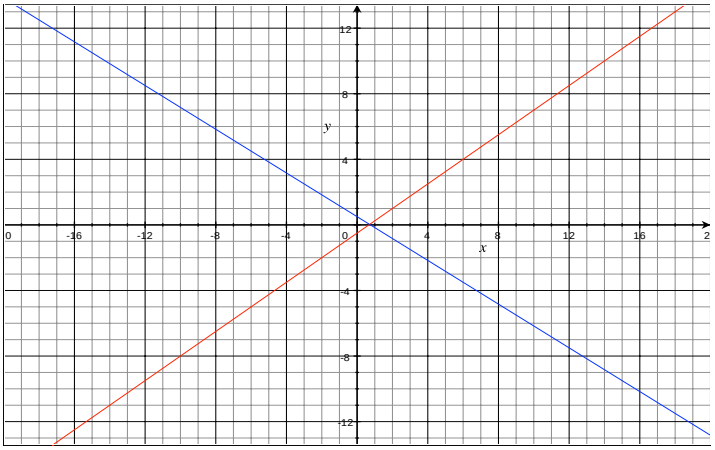
$15 = 7 \cdot 2 + 1 \Rightarrow 1 = 15 - 7 \cdot 2 = 15 - 7(17 - 1 \cdot 15) = 17(-7) + 15(8)$

quindi, $x = -7, y = -8$ sono soluzioni dell'equazione $17x - 15y = 1$; di conseguenza una soluzione particolare dell'equazione $17x - 15y = 5$ si otterrà moltiplicando per 5 le soluzioni trovate:

$\begin{cases} x' = -35 \\ y' = -40 \end{cases}$. Le soluzioni, della forma $\begin{cases} x = x' + x_0 \\ y = y' + y_0 \end{cases}$, sono $\begin{cases} x = -35 + 15n \\ y = -40 + 17n \end{cases}$.

Se rappresentiamo su un diagramma cartesiano la retta di equazione $ax + by = c$, le soluzioni intere si troveranno nei punti a coordinate intere.

Ad esempio, l'equazione $3x - 4y = 2$ (retta colorata in rosso) ammette soluzioni intere, mentre l'equazione $4x + 6y = 3$ (retta colorata in blu) no, come è possibile vedere anche dalla loro rappresentazione grafica: a differenza della seconda, la prima retta passa per punti a coordinate intere.



Per comprendere meglio l'utilità delle equazioni diofantee, proviamo a risolvere il seguente:

Problema. Un uovo deve cuocere in 9 minuti. Com'è possibile misurare questo tempo con due clessidre da 5 e 7 minuti?

Soluzione. Si capovolgono le clessidre contemporaneamente e, esaurita la clessidra da 5 minuti, mettiamo l'uovo nell'acqua. Esaurita anche la clessidra da 7 minuti, l'uovo sta cuocendo da due minuti: capovolgiamo quest'ultima e saranno trascorsi 9 minuti dall'immissione dell'uovo nell'acqua.

Le equazioni diofantee costituiscono un *modello* per risolvere problemi di questo tipo. Infatti, se interpretiamo le soluzioni intere come il numero dei capovolgimenti delle due clessidre, i coefficienti *a*, *b* come il tempo misurabile con le singole clessidre, ed il termine noto *c* come il tempo che vogliamo misurare, allora

$$9 = 5x + 7y$$

è l'equazione le cui soluzioni, se esistono, ci dicono come utilizzare le due clessidre per misurare il tempo di cottura.

Vediamo come. Le soluzioni dell'equazione omogenea sono $x_0 = 7n, y_0 = -5n$. Poiché $MCD(5,7) = 1$, l'equazione $5x + 7y = 1$ ammette soluzioni intere, quindi una soluzione particolare si otterrà moltiplicando per 9 una soluzione dell'equazione $5x + 7y = 1$.

Determiniamo quest'ultima:

$7 = 1 \cdot 5 + 2$

$5 = 2 \cdot 2 + 1 \Rightarrow 1 = 5 - 2 \cdot 2 = 5 - 2 \cdot (7 - 1 \cdot 5) = 3 \cdot 5 - 2 \cdot 7 \Rightarrow x^* = 3 \cdot 9 = 27, y^* = -2 \cdot 9 = -18$.

Le soluzioni, che rappresentano quindi i tempi interi che si possono misurare con le clessidre da 5 e da 7 minuti, sono quindi $x = 7n + 27, y = -5n - 18$. In particolare, per $n = -4$ otteniamo $x = -1, y = 2$. Come possiamo mettere in relazione questo risultato con la sequenza di capovolgimenti determinata all'inizio? Come possiamo interpretare, ad esempio, la soluzione $x = 6, y = -3$?

A questo punto ci chiediamo: è possibile misurare qualsiasi intervallo di tempo (in minuti *interi*) con due clessidre di diversa durata? No. Il metodo funziona soltanto se l'intervallo di tempo divide il massimo comun divisore delle durate delle singole clessidre.