

# Elementi di Teoria dei Numeri

Iniziamo con il richiamare la definizione di quoziente e resto nella divisione di due numeri interi  $a$  e  $b$ . Chiameremo quoziente e resto nella divisione di  $a$  per  $b$  due numeri  $q$  e  $r$  che soddisfano le seguenti condizioni:

- $a = qb + r$ ;
- $0 \leq r < b$ .

La prima condizione scritta non è sufficiente per garantire l'unicità del quoziente e del resto nella divisione di  $a$  per  $b$ , infatti se consideriamo ad esempio:  $a = 10$  e  $b = 3$  risulta:  $a = 2b + 4$  e anche  $a = 4b + 1$ ; imponendo che venga soddisfatta anche la seconda condizione i numeri  $q$  e  $r$  che soddisfano la prima condizione invece diventano unici.

Diremo che  $b$  divide  $a$ , e anche che  $a$  è un multiplo di  $b$ , se nella divisione di  $a$  per  $b$  il resto  $r$  è 0, nel seguito scriveremo  $b|a$ . Tutti i numeri compresi tra 1 e  $a$  che dividono  $a$  vengono detti divisori di  $a$ . Un numero intero  $p$  che ammette quale unici divisori 1 e  $p$  viene detto numero primo.

È possibile dimostrare che i numeri primi sono infiniti, ad esempio utilizzando il seguente procedimento (dovuto a Euclide): ammettiamo per assurdo che l'insieme dei numeri primi sia un insieme finito, composto dai numeri  $\{p_1, p_2, \dots, p_k\}$ , costruiamo il numero  $N = p_1 \cdot p_2 \cdot \dots \cdot p_k + 1$ , tale numero non è divisibile per  $p_j$  per ogni  $j$ , infatti dividendo  $N$  per  $p_j$  otteniamo quale resto 1. Quindi anche il numero  $N$  è un numero primo contro l'ipotesi fatta.

Come possiamo determinare se il numero intero  $N$  è un numero intero? Il procedimento più semplice per controllare la primalità di un numero  $N$  è ovviamente la divisione del numero  $N$  per tutti i numeri interi compresi tra 2 e  $N - 1$ . Facendo semplici considerazioni possiamo però migliorare tale procedimento, riducendo notevolmente i calcoli.

Per prima cosa notiamo che se  $N$  non è pari, sicuramente non sarà divisibile per nessun numero pari, quindi nella ricerca che dobbiamo fare possiamo escludere tutti i numeri pari. La divisione deve essere limitata a tutti i numeri interi dispari più piccoli di  $N$ . Notiamo anche che se  $k$  divide il numero intero  $N$ , allora  $\frac{N}{k} = h$  divide  $N$ , quindi ogni volta che troviamo un divisore di  $N$  riusciamo a trovare immediatamente un secondo divisore. Possiamo supporre che  $k \leq h$ , utilizzando tale considerazione la ricerca dei divisori di  $N$  risulta notevolmente limitata. Infatti dobbiamo cercare i possibili divisori di  $N$  non tra tutti i numeri minori di  $N - 1$ , ma

solo tra i numeri dispari che sono minori di  $\sqrt{N}$ . Se vogliamo limitare maggiormente la ricerca possiamo non prendere un qualsiasi numero dispari, ma solo tra i numeri primi minori di  $\sqrt{N}$ . Dalle considerazioni prima fatte è immediato concludere che dato  $N$  intero, se  $N$  è un quadrato il numero dei suoi divisori è dispari, mentre in tutti gli altri casi dato il numero  $N$  il numero dei divisori di  $N$  è pari.

Uno dei problemi ancora aperti della matematica è il seguente:

*Come sono distribuiti i numeri primi nell'insieme  $\mathbb{N}$  dei numeri interi?*

Esiste a tale proposito un'ipotesi, detta ipotesi di Riemann, che, se dimostrata, permetterebbe di caratterizzare tutti i numeri primi, questo è uno dei così detti problemi del millennio.

Per i numeri interi vale il seguente teorema:

**Teorema fondamentale dell'aritmetica.** Dato un numero intero  $N$  esiste un'unica scomposizione del numero dato nel seguente modo:

$$N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_j^{\alpha_j},$$

tale scrittura è unica a meno di permutazione dei termini che la compongono.

È possibile dimostrare le seguenti proposizioni:

- se il numero primo  $p$  divide il prodotto  $ab$  e  $p$  non divide  $a$  allora  $p$  divide  $b$ ;
- se il numero primo  $p$  divide la somma  $a + b$  e  $p$  divide  $a$  allora  $p$  divide anche  $b$ ;
- più in generale se  $n$  divide la somma  $a + b$  e  $n$  divide  $a$  allora  $n$  divide anche  $b$ .

Utilizzando il teorema fondamentale dell'aritmetica possiamo risolvere il seguente problema:

*Dato un numero intero  $N$  determinare il numero dei suoi divisori.*

Utilizzando il teorema fondamentale dell'aritmetica possiamo dire che  $N = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ , ogni divisore  $d$  di  $N$  potrà essere scritto nella forma  $d = p_1^{\beta_1} \cdots p_k^{\beta_k}$ , con  $0 \leq \beta_j \leq \alpha_j$ . Allora il numero dei possibili divisori di  $N$  si potrà ottenere andando a determinare quante sono le possibili scelte delle potenze  $\beta_j$ . Tale numero è pari a:

$$d(N) = (\alpha_1 + 1) \cdots (\alpha_k + 1).$$

Un secondo problema che possiamo risolvere utilizzando il teorema fondamentale dell'aritmetica è il seguente:

*Dato un numero intero  $N$  qual è la somma dei suoi divisori?*

Utilizzando la notazione precedente sappiamo che dovremmo calcolare la somma:

$$\sum p_1^{\beta_1} \cdots p_k^{\beta_k}$$

tale somma deve essere estesa a tutti i possibili valori distinti che può assumere la  $k$ -pla  $(\beta_1, \dots, \beta_k)$ .

Tale somma si può scrivere come:

$$S(N) = (1 + p_1 + \cdots + p_1^{\alpha_1}) \cdots (1 + p_k + \cdots + p_k^{\alpha_k}),$$

infatti tale prodotto contiene tutti i possibili prodotti di potenze dei valori  $p_j$ , che sono tutti i possibili divisori del numero iniziale  $N$ . Tale somma può essere facilmente calcolata ricordando che in ogni parentesi compare la somma dei termini di una progressione geometrica, possiamo quindi concludere che:

$$S(N) = \frac{p_1^{\alpha_1} - 1}{p_1 - 1} \cdots \frac{p_k^{\alpha_k} - 1}{p_k - 1}.$$

**MCD.** Dati due numeri interi  $a, b$  chiameremo **Massimo Comune Divisore** tra  $a$  e  $b$ , un numero intero  $d$  che soddisfi le seguenti condizioni:

1.  $d|a, d|b$ ;
2. se  $d'|a, d'|b$  allora  $d'|d$ .

Nel seguito indicheremo il **MCD** tra due numeri  $a$  e  $b$  nel seguente modo  $(a, b)$ .

**Algoritmo di Euclide per il calcolo di MCD.** Per calcolare esplicitamente  $(a, b)$  possiamo procedere nel seguente modo:

1. calcoliamo quoziente e resto della divisione di  $a$  per  $b$ , siano  $q_0$  e  $r_0$ . Per quanto detto in precedenza risulta  $0 \leq r_0 < b$ ,
2. se  $r_0 = 0$  allora  $(a, b) = b$ , in caso contrario sostituiamo  $a$  con  $b$ ,  $b$  con  $r_0$  e ritorniamo al punto precedente.

Il procedimento precedente avrà termine in un numero finito di passi, infatti detto  $r_k$  il  $k$ -esimo resto ottenuto diverso da 0 sappiamo che  $0 \leq r_k < r_{k-1} < r_0$  quindi al più in  $r_0$  passi otterremo  $(a, b)$ .

**Esempio.** Calcoliamo  $(156, 42)$  utilizzando il procedimento descritto in precedenza:

$$\begin{aligned} 156 &= 3 \cdot 42 + 30 \\ 42 &= 1 \cdot 30 + 12 \\ 30 &= 2 \cdot 12 + 6 \\ 12 &= 2 \cdot 6. \end{aligned}$$

Quindi  $(156, 42) = 6$ .

Tale procedimento può essere applicato per determinare il MCD tra due polinomi.

Da quanto illustrato in precedenza possiamo trarre un'altra importante conclusione. Partendo dalla penultima relazione scritta e procedendo a ritroso, possiamo scrivere:

$$\begin{aligned} 6 &= 30 - 2 \cdot 12 \\ 12 &= 42 - 1 \cdot 30 \Rightarrow 6 = 30 - 2 \cdot (42 - 1 \cdot 30) = 3 \cdot 30 - 2 \cdot 42 \\ 30 &= 156 - 3 \cdot 42 \Rightarrow 6 = 3 \cdot (156 - 3 \cdot 42) - 2 \cdot 42 = 3 \cdot 156 - 11 \cdot 42 \\ 6 &= 3 \cdot 156 - 11 \cdot 42. \end{aligned}$$

Abbiamo ricavato, in un caso particolare, una proprietà che può risultare molto utile, ovvero il **Teorema di Bézout**.

**Teorema di Bézout.** Dati due numeri  $a$  e  $b$ , esistono due numeri interi  $x$  e  $y$  tali che risulti:

$$(a, b) = ax + by.$$

La dimostrazione può essere effettuata utilizzando l'algoritmo euclideo per il calcolo del massimo comune divisore, come abbiamo fatto in precedenza. In particolare il procedimento illustrato permette di determinare esplicitamente i valori di  $x$ ,  $y$ .

Passiamo ora ad illustrare un procedimento per risolvere le equazioni diofantee lineari. Un'equazione in un numero qualsiasi di indeterminate e di qualsiasi grado

viene detta equazione diofantea se le soluzioni della stessa vengono cercate tra quelle intere. La teoria relativa alle equazioni diofantee è per il momento incompleta, infatti non esiste un procedimento unico per risolvere una qualsiasi equazione diofantea e non è stato ancora individuata una qualche condizione che permetta di decidere a priori, senza risolverla, se un'equazione di questo tipo ammetta soluzioni oppure non le ammetta. Un esempio famoso di equazione diofantea è la seguente:

**Ultimo teorema di Fermat.** L'equazione  $x^n + y^n = z^n$  ammette soluzioni intere se e solo se  $n = 2$ .

L'enunciato di questo teorema, noto appunto come ultimo teorema di Fermat, è molto semplice, ma solo negli ultimi anni dello scorso millennio è stato dimostrato da un matematico inglese, Andrew Wiles, dopo uno studio particolare di molti anni.

Un'equazione lineare diofantea è del tipo  $ax + by = c$ . Iniziamo con il notare che data un'equazione diofantea lineare, se questa ammette una soluzione, ad esempio  $(x_0, y_0)$ , allora ne ammette infinite. Infatti tutte le coppie del tipo:  $(x_0 + kb, y_0 - ka)$ ,  $k \in \mathbb{Z}$  sono a loro volta soluzioni. Sappiamo che  $(x_0, y_0)$  è soluzione, quindi vale la seguente relazione:  $ax_0 + by_0 = c$ . Sostituiamo nell'equazione iniziale la coppia indicata, otteniamo:

$$a(x_0 + kb) + b(y_0 - ka) = ax_0 + kab + by_0 - kab = (ax_0 + by_0) + (kab - kab) = c,$$

quindi anche questa coppia è una soluzione dell'equazione iniziale. Il problema proposto quindi consiste nel trovare una soluzione particolare del problema proposto, tutte le altre soluzioni si possono ottenere utilizzando il procedimento prima descritto.

L'equazione di partenza ammette soluzioni intere se risulta soddisfatta la seguente semplice condizione:  $(a, b) | c$ .

Infatti, ammettiamo che valga la condizione prima scritta, per il teorema di Bézout esistono due numeri  $(x_0, y_0)$  tali che risulta soddisfatta la condizione:  $(a, b) = ax_0 + by_0$ . Dato che  $c = c'(a, b)$ , allora risulta:  $c'(ax_0 + by_0) = a(c'x_0) + b(c'y_0) = c'(a, b) = c$ , quindi la coppia  $(c'x_0, c'y_0)$  è soluzione dell'equazione di partenza.

È possibile dimostrare che la condizione indicata è una condizione non solo sufficiente, ma anche necessaria per poter garantire l'esistenza di soluzioni dell'equazione prima indicata. Il procedimento illustrato in precedenza illustra anche un metodo esplicito per poter ottenere le soluzioni dell'equazione diofantea indicata.

Terminiamo questa breve esposizione indicando alcune considerazioni che possono essere utili per risolvere equazioni diofantee:

- sia  $f(x_1, x_2, \dots, x_n) = 0$  un'equazione diofantea, allora per le possibili soluzioni

deve valere, comunque si scelga il numero intero  $n$  la seguente relazione:

$$[f(x_1, x_2, \dots, x_n)] \equiv [0] \pmod{n}.$$

In alcuni casi questa semplice considerazione può essere utile per individuare informazioni sulle soluzioni dell'equazione proposta.

- In alcuni casi può essere utile riscrivere l'equazione di partenza nel seguente modo:  $f'(x_1, \dots, x_n) = N$ , con  $N$  numero intero. Scomponendo opportunamente il polinomio a primo membro ed il numero  $N$  in fattori primi, ogni fattore di  $N$  dovrà dividere un fattore della scomposizione del polinomio a primo membro.
- Un caso particolare è dato dall'equazione diofantea del tipo:

$$xy + bx + cy + d = 0.$$

Per prima cosa si deve ricavare una delle due indeterminate:  $y(x + c) = -d - bx$ ,  $y = -\frac{bx + d}{x + c}$ , il secondo membro di tale relazione può essere scritto nel seguente modo:  $y = -b + \frac{bc - d}{x + c}$ . Questo permette di concludere che l'equazione di partenza ammette soluzioni se  $(x + c)|(bc - d)$ , cosa che permette di terminare le eventuali coppie soluzioni dell'equazione.