MATHEMATICAL.
OLYMPIAD.CH
MATHEMATIK-OLYMPIADE
OLYMPIADES DE MATHÉMATIQUES
OLIMPIADI DELLA MATEMATICA

Teoria dei numeri I

Thomas Huber

Aggiornato: 3 agosto 2021
vers. 1.1.0

Indice

1 Divisibilità

In quel che segue, a e b sono numeri interi. Se esiste $k \in \mathbb{Z}$ con $a = kb$, allora si dice che a è *divisibile* per b oppure che b è un *divisore* di a. In simboli: $b \mid a$. Ogni intero n è divisibile per ± 1 e $\pm n$, e ogni numero intero è un divisore di 0. Se si considerano i divisori di $a > 0$, ci si riferisce di solito ai divisori *positivi* di a. Si dice che $p \in \mathbb{N}$ è un *numero primo*, o semplicemente *primo*, se p e 1 sono gli unici divisori di p (tuttavia 1 non è considerato un numero primo).

Valgono le seguenti semplici ma importanti proprietà:

- $a \mid b$ e $b \mid c \quad \Longrightarrow \quad a \mid c$
- se $a \mid b_1, \ldots, a \mid b_n$, allora presi degli interi qualsiasi $c_1, \ldots, c_n$ abbiamo

$$a \mid \sum_{i=1}^{n} b_i c_i.$$

- $a \mid b$ e $c \mid \mathrm{d} \quad \Longrightarrow \quad ac \mid bd$
- p primo e $p \mid ab \quad \Longrightarrow \quad p \mid a$ o $p \mid b$
- $a \in \mathbb{N}$, $b \in \mathbb{Z}$ e $a \mid b \quad \Longrightarrow \quad b = 0$ o $a \leq |b|$

Esempio 1 *Trovare tutti i numeri naturali x, y con*

$$x^2 - y! = 2001.$$

Soluzione. 2001 è divisibile per 3, ma non per 9. Se $y \geq 3$, allora $y!$ è divisibile per 3, dunque anche x. Allora x^2 è divisibile per 9. Per $y \geq 6$, $y!$ è anche divisibile per 9, quindi dovrebbe valere lo stesso per 2001, ma non è il caso. Restano le possibilità $y = 1, 2, 3, 4, 5$. Testando tutti i casi troviamo l'unica soluzione $(x, y) = (45, 4)$. □

Se abbiamo due interi, possiamo effettuare la divisione con resto. Più precisamente:

Teorema 1.1 (Divisione con resto) *Siano a, b numeri interi con $b > 0$. Allora esistono unici due numeri interi q e r con $0 \leq r < b$, tali che*

$$a = qb + r,$$

laddove r si chiama resto *della divisione e vale $r = 0$ se e solo se $b \mid a$ (q è invece noto con il nome di* quoziente*).*

Uno dei risultati più importanti di tutta la teoria dei numeri asserisce che ogni numero naturale possiede un'unica *decomposizione* o *fattorizzazione* in numeri primi.

Teorema 1.2 (Teorema fondamentale dell'aritmetica) *Per ogni numero naturale a esistono dei numeri primi $p_1, p_2, \ldots, p_r$ e dei numeri interi $n_1, n_2, \ldots, n_r$, tali che*

$$a = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}.$$

I valori p_i e n_i sono determinati univocamente da a.

Possiamo dimostrare questo teorema per induzione grazie alla divisione con resto, ma qui non entreremo nei dettagli. Il caso $a = 1$ corrisponde al *prodotto vuoto* a secondo membro, vale a dire che non vi è alcun fattore primo e che $r = 0$.

Osservazione *Sia $a = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$ la fattorizzazione in primi del numero naturale a. Allora accade che:*

- *a possiede esattamente $(n_1 + 1)(n_2 + 1) \cdots (n_r + 1)$ divisori positivi distinti.*
- *a è la potenza m-esima di un numero naturale se e solo se tutti gli esponenti n_k sono divisibili per m.*

Come ulteriore applicazione presentiamo ancora un risultato classico di Euclide:

Teorema 1.3 *Esitono infiniti numeri primi.*

Dimostrazione. Supponiamo per assurdo che esistano solo un numero finito di primi $p_1, p_2, \ldots, p_n$ e consideriamo il numero $N = p_1 p_2 \cdots p_n + 1$. Siccome $N > 1$, esiste per il teorema 1.2 un divisore primo q di N. Tuttavia N non è divisibile per alcuno dei primi p_k, poiché altrimenti risulterebbe $p_k \mid 1$, che è assurdo. Dunque q è diverso da $p_1, p_2, \ldots, p_n$. Contraddizione. □

2 mcd e mcm

Dati due numeri interi a, b, $\mathrm{mcd}(a, b)$ indica il *massimo comune divisore* di a e b; detto altrimenti, il più grande numero positivo che è sia un divisore di a sia un divisore di b. $\mathrm{mcm}(a, b)$ indica il *minimo comune multiplo*, cioè il più piccolo numero positivo che possiede sia a sia b come divisori. In modo analogo si definiscono mcd e mcm di più di due numeri. Inoltre, spesso si utilizzano le notazioni abbreviate $(a_1, a_2, \ldots, a_n)$ e $[a_1, a_2, \ldots, a_n]$ per il mcd e il mcm, rispettivamente. Formalmente possiamo caratterizzare il mcd con le due seguenti affermazioni equivalenti:

1) $c = \mathrm{mcd}(a, b)$

2) $c > 0$ è un divisore di a e di b e per ogni numero positivo x vale

$$x \mid a, x \mid b \quad \Longrightarrow \quad x \mid c.$$

Analogamente per il mcm. Se $\mathrm{mcd}(a,b) = 1$, allora a e b si dicono *coprimi*. Valgono i seguenti fatti:

- $\mathrm{mcd}(a,b) = \mathrm{mcd}(b,a)$
- $\mathrm{mcd}(a,b,c) = \mathrm{mcd}(\mathrm{mcd}(a,b),c)$
- $c \mid ab$ e $\mathrm{mcd}(a,c) = 1 \quad \Longrightarrow \quad c \mid b$
- $a \mid c$, $b \mid c$ e $\mathrm{mcd}(a,b) = 1 \quad \Longrightarrow \quad ab \mid c$
- Posto $d = \mathrm{mcd}(a,b)$ esistono numeri interi coprimi x e y tali che $a = xd$ e $b = yd$. Inoltre avremo $\mathrm{mcm}(a,b) = xyd$ (cf. proposizione 2.1).
- Se a, b sono coprimi e ab è una potenza m-esima, allora a e b sono entrambi potenze m-esime.

Mediante l'applicazione della fattorizzazione in numeri primi è possibile determinare esplicitamente mcd e mcm:

Teorema 2.1 *Siano $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ e $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}$ le fattorizzazioni di a e b con numeri primi p_k ed esponenti $\alpha_k, \beta_k \geq 0$. Vale che*

$$\mathrm{mcd}(a,b) = p_1^{\min\{\alpha_1,\beta_1\}} p_2^{\min\{\alpha_2,\beta_2\}} \cdots p_r^{\min\{\alpha_r,\beta_r\}}$$
$$\mathrm{mcm}(a,b) = p_1^{\max\{\alpha_1,\beta_1\}} p_2^{\max\{\alpha_2,\beta_2\}} \cdots p_r^{\max\{\alpha_r,\beta_r\}}$$

Inoltre, grazie alla formula $\min\{x,y\} + \max\{x,y\} = x + y$, segue subito che

$$\mathrm{mcd}(a,b) \cdot \mathrm{mcm}(a,b) = ab.$$

Esempio 2 *(Russia 1995) Siano m e n numeri naturali tali che*

$$\mathrm{mcd}(m,n) + \mathrm{mcm}(m,n) = m + n.$$

Dimostrare che uno dei due numeri divide l'altro.

Soluzione. Scrivendo $m = ad, n = bd$, otteniamo $\mathrm{mcm}(m,n) = abd$ per la proposizione 2.1 e l'equazione si trasforma in $d + abd = ad + bd$ o $d(ab - a - b + 1) = 0$. Fattorizzando il lato sinistro, troviamo $d(a-1)(b-1) = 0$, dunque vale che $a = 1$ o $b = 1$. Nel primo caso, abbiamo come conseguenza che $m = d$, dunque $m \mid n$. Nel secondo caso troviamo allo stesso modo che $n \mid m$. □

Mediante le formule della proposizione 2.1 è in principio sempre possibile calcolare il mcd. Il problema risiede soprattutto nel fattorizzare grandi numeri. C'è tuttavia un metodo di calcolo semplice e molto efficiente, noto come *algoritmo di* EUCLIDE. Si basa sulla seguente proposizione.

Teorema 2.2 *Dati numeri interi qualsiasi a, b e n, vale la seguente uguaglianza:*

$$(a, b) = (a, b + na). \tag{1}$$

Dimostrazione. È sufficiente dimostrare l'asserzione per $n = \pm 1$, poiché il caso generale segue da una sua applicazione ripetuta. Se c è un divisore comune di a e b, allora c divide anche $b \pm a$, perciò vale $(a, b) \mid (a, b \pm a)$. D'altra parte, sia c un divisore comune di a e $b + a$ e $b - a$. Allora c divide anche $(b + a) - a = b$ e $(b - a) + a = b$. Di conseguenza $(a, b \pm a) \mid (a, b)$. □

Per dare un esempio, calcoliamo $(2541, 1092)$ applicando l'uguaglianza (1) fino a quando il risultato non diventa evidente:

$$\begin{aligned}(2541, 1092) &= (2541 - 2 \cdot 1092, 1092) = (357, 1092)\\ &= (1092 - 3 \cdot 357, 357) = (21, 357)\\ &= (357 - 17 \cdot 21, 21) = (0, 21) = 21.\end{aligned}$$

È chiara l'idea: si proseguono i calcoli con il resto della divisione del numero più grande con quello più piccolo. Tutto ciò è formalizzato nell'algoritmo di EUCLIDE:

Algoritmo 2.3 (EUCLIDE) *Calcolo di (a, b) per $a, b \geq 0$.*

1. *Si pone $a_1 = \max\{a, b\}$, $a_2 = \min\{a, b\}$ e $n = 2$.*
2. *Si scrive $a_{n-1} = q_n a_n + a_{n+1}$ con $0 \leq a_{n+1} < a_n$ (divisione con resto).*
3. *Se $a_{n+1} = 0$, allora vale $(a, b) = a_n$, altrimenti si aumenta n di 1 e si ripete il passo 2.*

La correttezza di questo algoritmo segue immediatamente dall'uguaglianza (1). Per il nostro esempio dobbiamo eseguire i seguenti calcoli:

$$\begin{aligned}2541 &= 2 \cdot 1092 + 357\\ 1092 &= 3 \cdot 357 + 21\\ 357 &= 17 \cdot 21 + 0.\end{aligned}$$

Poiché il resto dell'ultima divisione è 0, abbiamo che $(2541, 1092) = 21$.

Teorema 2.4 (BÉZOUT) *Se a, b sono coprimi, allora esistono numeri interi x, y tali che*

$$xa + yb = 1.$$

Generalizzando: posto $d = \mathrm{mcd}(a, b)$ esistono numeri interi x, y tali che

$$xa + yb = d.$$

Dimostrazione. Questo teorema segue dall'algoritmo euclideo. Dall'ultima riga dell'algoritmo si ottiene infatti l'uguaglianza $\mathrm{mcd}(a, b) = a_n$. Inserendo quest'espressione di a_n nella $(n-1)$-esima riga, e in seguito le espressioni ottenute di a_k nella $(k-1)$-esima riga per k sempre più piccolo, si giunge infine a un'uguaglianza della forma $\mathrm{mcd}(a, b) = xa + yb$. □

Nel nostro esempio si ottiene successivamente:

$$\begin{aligned} 21 &= 1 \cdot 1092 - 3 \cdot 357 \\ &= 1 \cdot 1092 - 3(2541 - 2 \cdot 1092) \\ &= (-3) \cdot 2541 + 7 \cdot 1092. \end{aligned}$$

Accenniamo ora a un'applicazione del precedente risultato: l'equazione lineare di DIOFANTO in due variabili.

Teorema 2.5 *Siano a, b, c numeri interi. L'equazione*

$$ax + by = c$$

possiede una soluzione (x, y) con $x, y \in \mathbb{Z}$ se e solo se $d = \mathrm{mcd}(a, b) \mid c$. Se questo è il caso e (x_0, y_0) è una soluzione, allora tutte le soluzioni sono date da

$$(x, y) = \left(x_0 + k \cdot \frac{b}{d}\,,\; y_0 - k \cdot \frac{a}{d} \right), \qquad k \in \mathbb{Z}.$$

Dimostrazione. Supponiamo che (x, y) sia una soluzione. Allora d è un divisore del membro di sinistra, dunque anche di c. D'altra parte, se $d \mid c$, allora l'esistenza di una soluzione (x_0, y_0) segue direttamente dal teorema di BÉZOUT. Ora, se (x, y) è un'ulteriore soluzione, allora vale $a(x - x_0) + b(y - y_0) = c - c = 0$, quindi

$$\frac{a}{d} \cdot (x - x_0) = -\frac{b}{d} \cdot (y - y_0).$$

Poiché a/d e b/d sono coprimi, osserviamo che $(x - x_0)$ è divisibile per b/d e che $(y - y_0)$ è divisibile per a/d. Ne consegue immediatamente che tutte le soluzioni devono essere della forma proposta. È poi facile verificare che sono effettivamente soluzioni sostituendole nell'equazione. □

3 Stime

Una competenza molto importante per risolvere i problemi di teoria dei numeri è saper stimare certe grandezze. Spesso possiamo ridurre il problema a qualche caso particolare facile da risolvere. Si tratta di comparare la crescita delle grandezze coinvolte in un'equazione. Presentiamo ora alcuni esempi, mediante i quali sarà più chiaro che cosa intendiamo.

Esempio 3 *Trovare tutti i numeri naturali n tali che $n^2+11 \mid n^3+13$.*

Che cos'ha a che fare questo con le stime? Vediamolo subito.

Dimostrazione. Il numero n^2+11 è un divisore di n^3+13, quindi anche di $n(n^2+11)-(n^3+13) = 11n-13$. Chiaramente $n=1$ non è una soluzione. Per $n \geq 2$ vale $11n-13 > 0$, e siccome questo numero deve essere divisibile per n^2+11 ricaviamo

$$n^2 + 11 \leq 11n - 13.$$

Ecco la stima. Poiché il primo membro è quadratico in n, il secondo solamente lineare, quest'equazione può essere soddisfatta solo per valori piccoli di n. È equivalente a $n^2 - 11n + 24 = n(n-11)+24 \leq 0$. Per $n \geq 12$ vale sempre $n(n-11)+24 \geq 12 \cdot 1 + 24 > 0$, di conseguenza abbiamo $n \leq 11$. Testando i vari casi si ottengono le soluzioni $n=3$ e $n=8$. □

Il passo decisivo è stata quest'osservazione: da $a \mid b$ e $b > 0$ segue $|a| \leq b$. Questa idea ricorre molto spesso, anche nei problemi IMO. Ricordatevela!

Il secondo caso di applicazione sfrutta il fatto che tra due quadrati *consecutivi* (o più in generale tra due n-esime potenze consecutive), non ce ne sono altri. Ciò può essere utile qualora si abbia a che fare con una grandezza che è vicina a un quadrato ed è essa stessa un quadrato. Nonostante questa formulazione possa sembrare triviale a priori, si rivela straordinariamente utile in pratica.

Esempio 4 *(Germania 1995) Trovare tutte le coppie (x,y) di numeri interi non-negativi che soddisfano la seguente equazione:*

$$x^3 + 8x^2 - 6x + 8 = y^3.$$

Soluzione. Qui non è possibile trovare una buona stima sulla crescita. L'idea è la seguente: il membro di sinistra deve essere una terza potenza (cioè y^3), tuttavia è anche abbastanza vicino x^3. Vogliamo quantificare quanto appena detto, quindi cerchiamo nei dintorni di x:

$$(x+2)^3 = x^3 + 6x^2 + 12x + 8,$$
$$(x+3)^3 = x^3 + 9x^2 + 27x + 27.$$

Osservando i coefficienti di x^2 nelle due espressioni, vediamo che la prima sembra essere più piccola e la seconda più grande del lato sinistro della nostra equazione. Effettuiamo qualche calcolo:

$$(x+2)^3 < x^3+8x^2-6x+8 \Leftrightarrow 2x^2-18x>0 \Leftrightarrow x>9,$$
$$(x+3)^3 > x^3+8x^2-6x+8 \Leftrightarrow x^2+33x+15>0 \quad \text{vale per ogni } x \geq 0.$$

Dunque per $x>9$ il lato sinistro si trova fra due terze potenze e deve essere lui stesso una terza potenza. Contraddizione. Ne segue che $x \leq 9$ e testando i vari casi giungiamo alle due soluzioni $(0,2)$ e $(9,11)$. □

Vediamo ora un terzo metodo di stima che può risultare utile per alcuni problemi di calcolo del mcd.

Teorema 3.1 *Siano a,b,c tre numeri interi. Allora $(a,bc) \leq (a,b)\cdot(a,c)$, con uguaglianza se b e c sono coprimi. (Esistono anche altri casi di uguaglianza, tuttavia è più semplice trattarli singolarmente che cercare un criterio generale.)*

Dimostrazione. Poniamo $d=(a,bc)$. Esistono due numeri interi (non necessariamente unici) d_1,d_2 tali che $d=d_1d_2$ e $d_1 \mid b, d_2 \mid c$. Inoltre, abbiamo che $d_1 \mid a$ e $d_2 \mid a$ poiché $d_1d_2=d \mid a$. Otteniamo dunque

$$(a,bc)=d=d_1d_2 \leq (a,b)\cdot(a,c).$$

Questo dimostra la prima parte della proposizione. Per la seconda parte supponiamo che b,c siano coprimi. Ne deduciamo che $d_1=(a,b)$ e $d_2=(a,c)$ sono a loro volta coprimi, poiché se k è un divisore comune di d_1 e d_2, allora k è pure un divisore comune di b e c, pertanto $k=1$. Ora, essendo d_1 e d_2 primi tra loro ed essendo pure divisori di a, il loro prodotto d_1d_2 divide a. Chiaramente d_1d_2 divide bc. Infine ricaviamo $d_1d_2 \leq (a,bc) \leq (a,b)\cdot(a,c)=d_1d_2$, che è quanto che volevamo. □

Riguardo ai casi di uguaglianza, osserviamo che $(16,2\cdot 4)=(16,2)\cdot(16,4)$ sebbene 2 e 4 non sono primi tra loro, tuttavia $(4,2\cdot 4)=4<8=(4,2)\cdot(4,4)$.

Questa diseguaglianza è particolarmente utile qualora si voglia dimostrare che due numeri sono primi tra loro. Se uno dei due termini è un prodotto, è possibile utilizzarla per scomporre il calcolo in tanti calcoli più semplici. Vediamo subito come procedere grazie a un esempio concreto.

Esempio 5 *Siano m,n due numeri interi coprimi. Allora mn e $m+n$ sono anch'essi primi tra loro.*

Soluzione. Grazie alla diseguaglianza appena dimostrata, otteniamo $(mn,m+n) \leq (m,m+n)\cdot(n,m+n)$. Pertanto, se riusciamo a dimostrare che $(m,m+n)=(n,m+n)=1$, abbiamo concluso. Sfruttando l'algoritmo di Euclide si trova $(m,m+n)=(m,n)=1$. Allo stesso modo si procede per l'altro termine, giungendo così alla soluzione. □