2. Numeri interi, numeri primi e divisibilità

2.1 Divisibilità, primi e fattorizzazione

Uno dei concetti più importanti e basilari che riguardano i numeri interi è quello di *divisibilità*. Dati due interi a e b, diciamo che a divide b (si scrive $a \mid b$) se b è multiplo di a, ovvero, detto in altre parole, se esiste un intero k tale che $b = ka$. Per esempio, 4 divide 12 perché $12 = 3 \cdot 4$; inoltre 7 divide -35 perché $-35 = (-5) \cdot 7$; invece 6 non divide 9 perché il rapporto $\frac{9}{6}$ non è intero.
I numeri interi possono avere molti divisori[1]; per esempio i divisori di 12 sono $1, 2, 3, 4, 6, 12$ e i loro opposti $-1, -2, -3, -4, -6, -12$. In effetti qualsiasi intero positivo n ha sicuramente come divisori positivi 1 e n (ogni numero è infatti divisibile per 1 e per se stesso). Se un intero positivo $n > 1$ non ha nessun divisore positivo diverso da 1 e n lo chiamiamo *numero primo*. Ecco l'elenco dei numeri primi più piccoli:

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ \ldots$$

Esempio 2.1. Trovare tutti i numeri primi p tali che anche $p + 5$ sia un numero primo.

[1] Lo 0 ha addirittura infiniti divisori, ovvero tutti i numeri interi non nulli. Per $n \neq 0$ invece i divisori di n sono compresi tra $-n$ e n, quindi sono in numero finito.

Soluzione. A prima vista un problema del genere potrebbe sembrare difficile: i numeri primi infatti si comportano bene con i prodotti (essendo definiti attraverso la nozione di divisibilità), ma non con le somme.
In generale se non si sa da dove iniziare per risolvere un problema può essere utile controllare a mano cosa succede nei casi piccoli, per potersi fare un'idea generale di come funzionino le cose. Nel nostro caso, proviamo a sostituire a p alcuni primi piccoli:

- $p = 2 \Rightarrow p + 5 = 7$ (primo!)
- $p = 3 \Rightarrow p + 5 = 8$ (non primo)
- $p = 5 \Rightarrow p + 5 = 10$ (non primo)
- $p = 7 \Rightarrow p + 5 = 12$ (non primo)
- ...

Come è facile osservare, ogni primo $p > 2$ è dispari, quindi $p + 5$ è pari e dunque non è un numero primo. L'unica soluzione allora è $p = 2$. □

I primi in un certo senso costituiscono i "mattoni" dei numeri interi. Ogni intero maggiore di 1, infatti, può essere scritto in un modo unico come prodotto di numeri primi[2]. Ecco per esempio le fattorizzazioni di alcuni numeri naturali:

$$\begin{array}{lll} 2 = 2 & 7 = 7 & 12 = 2^2 \cdot 3 \\ 3 = 3 & 8 = 2^3 & 13 = 13 \\ 4 = 2^2 & 9 = 3^2 & 14 = 2 \cdot 7 \\ 5 = 5 & 10 = 2 \cdot 5 & 15 = 3 \cdot 5 \\ 6 = 2 \cdot 3 & 11 = 11 & 16 = 2^4 \end{array}$$

Affinché un intero a (diverso da zero) divida un intero b, è necessario e sufficiente che *ogni* primo della fattorizzazione di a compaia anche in quella di b con esponente uguale o maggiore. Ad esempio $28 \mid 168$ perché $28 = 2^2 \cdot 7$ e $168 = 2^3 \cdot 3 \cdot 7$: osserviamo infatti che il 2 compare con esponente 2 in 28 e 3 in 168 ($2 \leq 3$) e il 7 compare con esponente 1 in entrambi ($1 \leq 1$). Al contrario $18 = 2 \cdot 3^2$ non divide $132 = 2^2 \cdot 3 \cdot 11$ (il 3 compare con esponente 2 in 18 e solo con esponente 1 in 132).

Esempio 2.2 (Archimede 2009, biennio e triennio)**.** Quale dei seguenti numeri è un divisore di $3^5 \cdot 4^4 \cdot 5^3$?
(A) 42, (B) 45, (C) 52, (D) 85, (E) 105.

[2] L'abbiamo già detto nell'Esempio 1.3, parlando di induzione estesa.

Soluzione. Scomponiamo in fattori primi le cinque possibili risposte:

$$42 = 2 \cdot 3 \cdot 7, \quad 45 = 3^2 \cdot 5, \quad 52 = 2^2 \cdot 13, \quad 85 = 5 \cdot 17, \quad 105 = 3 \cdot 5 \cdot 7.$$

Come si può facilmente osservare, di questi numeri l'unico che divide $3^5 \cdot 4^4 \cdot 5^3$ è 45. □

Esempio 2.3 (Provinciali 2010)**.** In una scatola ci sono venti palline numerate da 1 a 20. Ciascun numero è presente in una e una sola di queste palline. Quante palline diverse dobbiamo estrarre come minimo, per essere sicuri che il prodotto dei loro numeri sia un multiplo di 12?
(A) 7, (B) 11, (C) 12, (D) 15, (E) 18.

Soluzione. Immaginiamo di capovolgere il problema, cercando quante possono essere al massimo le palline in modo che il prodotto non sia multiplo di 12. La fattorizzazione di 12 è $2^2 \cdot 3$, quindi il prodotto delle palline estratte deve non essere multiplo di $2^2 = 4$, oppure deve non essere multiplo di 3 (serve che almeno una di queste due condizioni sia soddisfatta). Affinché non sia multiplo di 4 possiamo al massimo scegliere tutti i numeri dispari (che non danno fattori 2) più un qualsiasi numero pari non multiplo di 4 (che dà un unico fattore 2); i numeri dispari tra 1 e 20 sono 10, quindi in questo caso possiamo estrarre al massimo 11 palline. Invece, affinché il prodotto non sia multiplo di 3 possiamo scegliere tutti i numeri non multipli di 3, che sono 14, e nessun altro (altrimenti il prodotto sarebbe per forza multiplo di 3). In conclusione, per massimizzare il numero di palline ci conviene evitare che il prodotto sia multiplo di 3, il che ci consente di estrarne 14.
Estraendo almeno 15 palline, quindi, è inevitabile che il prodotto sia multiplo di 12. Il minimo è proprio 15 perché, come abbiamo visto, estraendo soltanto 14 palline è possibile che su nessuna di esse vi sia un multiplo di 3. □

Supponiamo di avere tre interi a, b, c (con $a \neq 0$) tali che $a \mid b$ e $a \mid c$. Possiamo affermare che $a \mid b + c$? Sì, perché sommando multipli di a otteniamo ancora un multiplo di a. Per la stessa ragione, se sommiamo m volte un multiplo di a e n volte un altro multiplo di a, otteniamo sempre un numero multiplo di a:

$$m \cdot (ka) + n \cdot (ha) = (mk + nh)\, a.$$

In altre parole,

$$\text{se } a \mid b \text{ e } a \mid c \text{ allora } a \mid mb + nc \text{ per qualsiasi scelta degli interi } m, n.$$

Per esempio se sappiamo che $a \mid 42$ e $a \mid 18$, utilizzando la proprietà appena trovata per $m = 1$ e $n = -2$ otteniamo che $a \mid 42 - 2 \cdot 18$, ovvero $a \mid 6$.

Esempio 2.4 (Provinciali 2010)**.** Per quanti interi relativi n si ha che $\dfrac{3n}{n+5}$ è intero e divisibile per 4?
(A) 1, (B) 2, (C) 4, (D) 8, (E) più di 8.

Soluzione. Tralasciamo per il momento la divisibilità per 4 e concentriamoci sul fatto che quel rapporto debba essere intero. Ciò si traduce nel fatto che $n+5 \mid 3n$. Abbiamo visto in precedenza che a $3n$ possiamo aggiungere (o togliere) un qualsiasi multiplo di $n+5$ e la divisibilità continua a valere. Se ad esempio togliessimo $n+5$ otterremmo che

$$n+5 \mid 3n-(n+5) \quad \Longrightarrow \quad n+5 \mid 2n-5.$$

Questo risultato non sembra particolarmente utile, ma se al posto di togliere $n+5$ togliamo $3\cdot(n+5)$ ricaviamo qualcosa di più interessante:

$$n+5 \mid 3n-3(n+5) \quad \Longrightarrow \quad n+5 \mid -15$$

quindi $n+5$ deve essere un divisore di 15, il che ci porta a dover esaminare solo un numero finito di possibilità per n (i divisori di 15 diminuiti di 5).
Consideriamo ora il fatto che la frazione debba essere multipla di 4. Il denominatore $n+5$ è un divisore di 15, per cui non può contenere fattori 2; è quindi sufficiente imporre che $3n$ sia un multiplo di 4, ovvero che n stesso lo sia.
Dobbiamo in conclusione trovare tutti gli n multipli di 4 tali che $n+5$ sia un divisore di 15, cioè $n+5$ può assumere i valori $1, 3, 5, 15, -1, -3, -5, -15$; i possibili n multipli di 4 sono quindi $-4, 0, -8, -20$. Verifichiamo infine che ognuno di questi valori di n soddisfi tutte le richieste del problema[3]:

n	$\frac{3n}{n+5}$
-4	-12
0	0
-8	8
-20	4

La risposta è quindi 4. □

[3]In questo caso la verifica non è necessaria, perché le condizioni che abbiamo imposto su n sono anche sufficienti. Tuttavia non fa mai male controllare che le soluzioni trovate rispettino le richieste, soprattutto quando questa verifica è particolarmente semplice e veloce. Comunque, bisogna sempre prestare attenzione: è facile trovare condizioni necessarie e poi dimenticarsi di controllare che i casi a cui ci si riduce in questo modo siano effettivamente soluzioni del problema.

2.2 Criteri di divisibilità

Per risolvere alcuni problemi possono tornare utili delle semplici regole che permettono rapidamente di stabilire se un numero sia o meno divisibile per un altro. Quello che segue è un elenco dei criteri di divisibilità più utili; torneremo a parlare più approfonditamente di questo argomento nel prossimo capitolo.

- *Divisibilità per* 2: un numero è multiplo di 2 (ovvero è pari) se e solo se la sua ultima cifra è pari.
- *Divisibilità per* 3: un numero è multiplo di 3 se e solo se la somma delle sue cifre è multipla di 3.
- *Divisibilità per* 4: un numero è multiplo di 4 se e solo se il numero formato dalle sue ultime due cifre è multiplo di 4.
- *Divisibilità per* 5: un numero è multiplo di 5 se e solo se la sua ultima cifra è multipla di 5 (cioè è 5 oppure 0).
- *Divisibilità per* 9: un numero è multiplo di 9 se e solo se la somma delle sue cifre è multipla di 9.
- *Divisibilità per* 11: un numero è multiplo di 11 se e solo se la somma delle sue cifre a segni alterni è multipla di 11. Per esempio 30118 è multiplo di 11 perché anche $3 - 0 + 1 - 1 + 8 = 11$ è multiplo di 11.

Esempio 2.5. Partendo dal numero $n = 123456789$, si possono effettuare più volte due operazioni, in qualsiasi ordine: la prima consiste nel raddoppiare il numero; la seconda consiste nel sostituirlo con la somma delle sue cifre. Qual è il più piccolo numero che è possibile ottenere?

Soluzione. L'idea di sommare le cifre ci ricorda i criteri di divisibilità per 3 e per 9. Applicandoli al numero n di partenza scopriamo che $1+2+3+4+5+6+7+8+9 = 45$, quindi n è multiplo di 9.
Se effettuassimo la prima mossa su un qualsiasi numero k multiplo di 9 otterremmo un numero ancora multiplo di 9 (staremmo infatti moltiplicando per 2); anche applicando la seconda mossa otterremmo un numero che, per quanto afferma il criterio di divisibilità per 9, deve essere ancora multiplo di 9. Quindi in nessun modo è possibile "uscire" dall'insieme dei numeri divisibili per 9.
Ci resta infine da capire qual è il minimo numero ottenibile. Entrambe le mosse, se applicate ad un numero positivo, restituiscono un numero positivo; d'altra parte il più piccolo numero positivo multiplo di 9 è 9 stesso, che può essere ottenuto

effettuando due volte la seconda mossa:

$$123456789 \longrightarrow 45 \longrightarrow 9.$$

Quindi il minimo numero ottenibile è effettivamente 9. □

Esempio 2.6. Determinare tutti i numeri primi palindromi con un numero pari di cifre.

Soluzione. Per cominciare, ricordiamo che un numero palindromo è un numero che rimane uguale leggendolo da destra a sinistra; per esempio 44 e 23932 sono palindromi, mentre 5525 non lo è.
I numeri palindromi di due cifre sono abbastanza pochi da poter essere elencati completamente:

$$11, 22, 33, 44, 55, 66, 77, 88, 99.$$

Si vede facilmente che sono tutti multipli di 11 e pertanto 11 è l'unico ad essere primo. Il più piccolo numero palindromo di quattro cifre è 1001 che, curiosamente, è a sua volta multiplo di 11. Potremmo cominciare a pensare allora che tutti i numeri palindromi con un numero pari di cifre siano multipli di 11, ma come dimostrarlo? A pensarci bene abbiamo a disposizione un criterio di divisibilità per 11 che sembra proprio fare al caso nostro: per un numero di quattro cifre, infatti, accade che la prima e la quarta cifra vengano sommate una volta con segno positivo e una volta con segno negativo, e lo stesso vale per la seconda e la terza cifra; ma la prima e la quarta cifra sono uguali tra loro, come anche la seconda e la terza, quindi la somma è nulla. Per esempio, dato il numero palindromo 3883, la somma delle cifre a segni alterni vale $3 - 8 + 8 - 3 = 0$, quindi 11 divide 3883.
Ormai possiamo cominciare a ragionare più in generale. Se il numero di cifre è pari la prima e l'ultima vengono sommate con segni opposti, la seconda e la penultima anche, e così via. Il risultato quindi è sempre 0 ed ogni numero risulta multiplo di 11. In conclusione 11 è l'unico numero primo palindromo con un numero pari di cifre. □

2.3 Divisione euclidea, MCD, mcm

Finora abbiamo esaminato cosa accade quando un numero intero è multiplo di un altro. In generale, dati due interi positivi a e b, possiamo effettuare la divisione con resto (o divisione euclidea) tra a e b ottenendo un quoziente q e un resto r in modo che

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

In particolare, se $r = 0$ allora $a = q \cdot b$, ovvero $b \mid a$.
Chiamiamo ora massimo comun divisore (MCD) tra due interi a, b (non entrambi nulli) il più grande intero d che divide sia a che b. Il minimo comune multiplo (mcm) è invece il più piccolo intero positivo c multiplo sia di a che di b (stavolta nessuno tra a e b può essere nullo). Indichiamo con (a, b) il massimo comun divisore tra a e b e con $[a, b]$ il loro minimo comune multiplo.
Esamineremo ora varie proprietà del MCD.

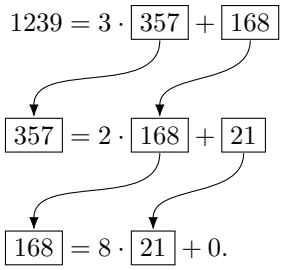
- Per qualsiasi intero a, $(a, 1) = 1$ (infatti nessun intero maggiore di 1 può dividere 1).
- Per qualsiasi $a > 0$ intero, $(a, 0) = a$ (infatti ogni intero non nullo divide 0).
- Per qualsiasi $a > 0$ intero, $(a, a) = a$.
- Il massimo comun divisore non dipende dal *segno* dei due interi: $(a, b) = (-a, b) = (a, -b) = (-a, -b)$.
- Per qualsiasi a, b interi non entrambi nulli, $(a, b) = (b, a)$ (infatti la definizione che abbiamo dato di MCD è simmetrica tra a e b).
- Non abbiamo definito $(0, 0)$ perché qualsiasi numero intero (non nullo) divide 0 e quindi non può esistere un divisore che sia massimo.

Per esercizio potete verificare quali di queste proprietà valgono anche per il minimo comune multiplo e, per quelle che non valgono, trovare relazioni analoghe che siano verificate dal mcm.
Facciamo un esempio: se $a = 40 = 2^3 \cdot 5$ e $b = 60 = 2^2 \cdot 3 \cdot 5$, allora si ha $(a, b) = 20 = 2^2 \cdot 5$; nel massimo comun divisore, infatti, ogni numero primo viene "preso" con l'esponente minimo tra quelli con cui compare in a e b. Al contrario, nel minimo comune multiplo ogni primo viene preso con l'esponente massimo: $\left[2^3 \cdot 5,\ 2^2 \cdot 3 \cdot 5\right] = 2^3 \cdot 3 \cdot 5 = 120$.
Un'ulteriore proprietà del MCD, che risulta ovvia pensando a come si determina il massimo comun divisore tramite la fattorizzazione, è la seguente: se d divide sia a che b allora divide (a, b).
Per calcolare il massimo comun divisore generalmente non si ricorre alla fattorizzazione dei due numeri dati[4]. Fin dall'antichità si conosce un metodo molto più

[4]Questa operazione infatti può risultare molto lunga; attualmente non si conosce (ammesso che esista) un algoritmo che permetta, ad esempio, di finire di fattorizzare un numero di 10000 cifre prima che il Sole diventi una gigante rossa[5].

[5]Non preoccupatevi, mancano ancora 5 miliardi di anni.

rapido, chiamato *algoritmo di Euclide*, che consiste nell'effettuare ripetutamente la divisione con resto utilizzando come dividendo e divisore quelli che al passo precedente erano il divisore e il resto. Ecco come si può procedere se si vuole determinare per esempio $(1239, 357)$:



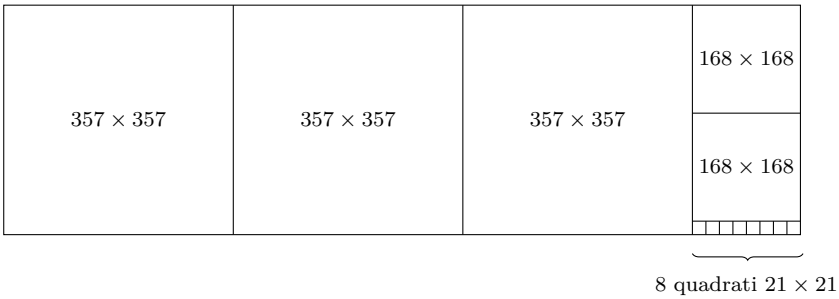
Prima di tutto scriviamo la divisione di 1239 per 357, ottenendo quoziente 3 e resto 168; a questo punto effettuiamo nuovamente la divisione tra il divisore (357) e il resto (168) della divisione precedente, che porta ad un quoziente uguale a 2 e ad un resto uguale a 21; infine la divisione tra il nuovo divisore (168) e il nuovo resto (21) dà quoziente 8 e resto 0. Arrivati a 0, ci fermiamo. Il massimo comun divisore risulta essere l'ultimo resto diverso da zero, ovvero nel nostro caso 21.

Cerchiamo di capire perché funziona l'algoritmo di Euclide. Immaginiamo di avere due interi positivi a e b, con $a > b$. Abbiamo visto nella Sezione 2.1 che se $d \mid a$ e $d \mid b$ allora $d \mid a - b$; viceversa, se $d \mid b$ e $d \mid a - b$ allora $d \mid b + (a - b) = a$. Questo ci porta ad affermare che i divisori comuni tra a e b sono uguali ai divisori comuni tra $a - b$ e b. In particolare, anche il massimo comun divisore sarà lo stesso: $(a, b) = (a - b, b)$.

L'algoritmo di Euclide non fa altro che iterare questo procedimento: togliamo tante volte b da a, finché non rimane un numero naturale che sia minore di b (ovvero il resto r della divisione tra a e b: $a - q \cdot b = r$). A questo punto ci troviamo con i numeri b e r, il cui MCD è rimasto ancora quello tra a e b, e continuiamo a ripetere il procedimento. Quando infine troviamo un resto uguale a zero (il che prima o poi deve succedere perché ad ogni passaggio i resti diminuiscono strettamente), siamo arrivati ad avere due numeri a' e b' che sono uno multiplo dell'altro, ovvero $b' \mid a'$; ma allora il massimo comun divisore è b', cioè l'ultimo resto diverso da zero.

Possiamo interpretare visualmente l'algoritmo di Euclide come un modo iterativo di tassellare un rettangolo di dimensione $a \times b$ con quadrati: ad ogni passo aggiungiamo il quadrato più grande possibile che tocchi il vertice in alto a sinistra dell'area (rettangolare) rimanente. I primi q quadrati hanno dimensione $b \times b$ e si posizionano in modo da occupare un rettangolo $qb \times b$, lasciando libero un rettangolo $(a - qb) \times b = r \times b$. La procedura continua con l'aggiunta quadrati sempre più piccoli, finché il

rettangolo iniziale viene riempito completamente. Il MCD è la lunghezza del lato dei quadrati più piccoli. Questa tassellazione è mostrata nella figura seguente per $a = 1239$ e $b = 357$.



Si noti che il numero di quadrati di ciascuna dimensione è dato dai quozienti delle divisioni dell'algoritmo di Euclide: in questo esempio ci sono 3 quadrati 357×357, poi 2 quadrati 168×168, ed infine 8 quadrati 21×21. Il MCD è uguale a 21.

Esempio 2.7. Dimostrare che due numeri di Fibonacci consecutivi sono *coprimi*, ovvero hanno MCD uguale a 1 (per la definizione dei numeri di Fibonacci vedi l'Esempio 1.2).

Soluzione. Chiamiamo F_n l'n-esimo numero di Fibonacci. Per le proprietà che abbiamo visto $(F_{n-1}, F_n) = (F_{n-1} + F_n, F_n)$. Ma per definizione dei numeri di Fibonacci, $F_{n+1} = F_n + F_{n-1}$, quindi l'uguaglianza dei due MCD diventa $(F_{n-1}, F_n) = (F_{n+1}, F_n)$.
La tesi risulta quindi vera per induzione: il passo base è $(0, 1) = 1$; abbiamo poi dimostrato che se una coppia di numeri di Fibonacci consecutivi ha MCD uguale a 1, allora lo stesso vale per la coppia successiva (questo è il passo induttivo).
Questa dimostrazione si può interpretare in termini dell'algoritmo di Euclide per calcolare (F_{n+1}, F_n). Infatti al primo passo ci si riduce a $(F_{n+1} - F_n, F_n) = (F_{n-1}, F_n)$, poi a (F_{n-1}, F_{n-2}), e così via fino a $(F_1, F_0) = 1$. □

Esempio 2.8. Dati due interi positivi a e b, dimostrare che $(a, b) \cdot [a, b] = a \cdot b$.

Soluzione. Per dimostrare un'uguaglianza tra interi positivi possiamo verificare che, dato qualsiasi numero primo p, esso compaia con lo stesso esponente nella fattorizzazione di entrambi i numeri (infatti abbiamo visto che ogni numero intero positivo ha un'unica fattorizzazione). Immaginiamo che nella fattorizzazione di