Matematica Discreta - addendum

Giuseppe Lancia

Dipartimento di Matematica e Informatica
Università di Udine

Indice

Capitolo 1

La matematica degli interi

In questo capitolo ci occupiamo di alcune proprietà dei numeri interi che sono alla base della cosiddetta *Teoria dei Numeri*. Quest'ultima è una branca della matematica tra le più antiche, e i cui problemi, generalmente di formulazione molto semplice, risultano spesso estremamente difficili da risolvere. Non a caso, molte questioni la cui soluzione appariva difficile 2000 o più anni fa, sono tuttoggi ancora irrisolte. Tra esse, in particolare, troviamo alcune importanti congetture riguardo ai numeri primi.

1.1 MCD e mcm

Innanzitutto ricordiamo il concetto di divisibilità fra interi, introdotto nella sezione **??**. Siano a e b due interi. Diciamo che a *divide* b (o che a è un *divisore* di b, o che b è un *multiplo* di a) se esiste un intero m tale che $b = am$. Per indicare che a divide b, usiamo la notazione $a \mid b$. Se a non è un divisore di b, allora scriviamo $a \nmid b$. Questo significa che, nella divisione intera di b per a, si ha $b = qa + r$ con $0 < r < a$.

Esercizio 1.1. Sia r il resto della divisione di b per a. Supponiamo che $c \mid a$ e $c \mid b$. Dimostrare che $c \mid r$.

Esercizio 1.2. Dimostrare che, (i) per ogni intero a, si ha $a - 1 \mid a^2 - 1$; (ii) più in generale, dimostrare che per ogni intero a e naturale positivo n, si ha $a - 1 | a^n - 1$.

Dati due interi a e b, resta definito l'insieme dei loro divisori comuni. Il massimo di tale insieme, è detto il loro *Massimo Comun Divisore*, ed è denotato con $\mathrm{MCD}(a, b)$. Ad esempio:

$$\mathrm{MCD}(1,6) = 1, \quad \mathrm{MCD}(2,6) = 2, \quad \mathrm{MCD}(3,6) = 3, \quad \mathrm{MCD}(4,6) = 2, \quad \mathrm{MCD}(5,6) = 1, \quad \mathrm{MCD}(6,6) = 6.$$

Due numeri per i quali il massimo comun divisore è 1 si dicono *relativamente primi*, o *coprimi*. Inoltre, risulta conveniente definire $MCD(a, 0) = a$ per ogni intero $a \geq 0$.

In modo simile alla nozione di MCD, si definisce il *minimo comune multiplo* di due interi, denotato con

$\mathrm{mcm}(a,b)$. Come tutti avranno immaginato, si tratta del più piccolo fra i multipli comuni positivi di a e b. Ad esempio:

$$\mathrm{mcm}(1,6)=6,\quad \mathrm{mcm}(2,6)=6,\quad \mathrm{mcm}(3,6)=6,\quad \mathrm{mcm}(4,6)=12,\quad \mathrm{mcm}(5,6)=30,\quad \mathrm{mcm}(6,6)=6.$$

1.1.1 L'algoritmo di Euclide per il MCD

Siano a e b due interi positivi. Descriviamo un algoritmo per il calcolo di $\mathrm{MCD}(a,b)$ dovuto ad Euclide.

Algorithm 1 MCD

```
0.  if a > b then si scambino fra loro a e b;
1.  loop
2.      r := b mod a;
3.      if r = 0 then
4.          return a /* a è ora il MCD */;
5.      else
6.          b := a;
7.          a := r;
8.      endif
9.  forever
```

La procedura divide il maggiore dei due numeri per il minore, e rimpiazza il maggiore con il minore, e il minore con il resto di tale divisione. Questo processo va ripetuto finchè il resto non diventa zero. Ad esempio supponiamo che sia $a=18$ e $b=300$. Abbiamo $300=16\times 18+12$, per cui b diventa 18 e a diventa 12. A questo punto, $18=1\times 12+6$, per cui b diventa 12 e a diventa 6. Infine $12=2\times 6+0$, sicchè il procedimento si arresta e restituisce $\mathrm{MCD}(18,300)=6$.

Veniamo ora alla correttezza dell'algoritmo. Vanno verificate due cose: (i) che l'algoritmo termina sempre; (ii) che il risultato restituito dopo la terminazione è effettivamente il MCD dei due numeri di ingresso.

Per quel che riguarda la finitezza, si noti che, ad ogni iterazione, il massimo tra a e b decresce e resta positivo, e quindi questo processo non può ripetersi all'infinito. Per la correttezza del risultato, si noti che, posto $r = b \bmod a$,

1. ogni divisore comune di a e di b è anche un divisore di r (si veda l'esercizio 1.1).
2. se c divide r e c divide a, allora $c \mid b$, come è immediato verificare.

In virtù di questa osservazione, i divisori comuni di a e b sono gli stessi dei divisori comuni di r e a, e quindi l'iterazione generica dell'algoritmo (che rimpiazza (a,b) con (r,a)) è corretta, così come è corretta l'ultima iterazione, in cui il MCD viene calcolato effettivamente.

Facciamo un esempio un po' più complesso: abbiamo $\mathrm{MCD}(89,55)=\mathrm{MCD}(55,34)=\mathrm{MCD}(34,21)=\mathrm{MCD}(21,13)=\mathrm{MCD}(13,8)=\mathrm{MCD}(8,5)=\mathrm{MCD}(5,3)=\mathrm{MCD}(3,2)=\mathrm{MCD}(2,1)=1$.

Abbiamo visto come l'algoritmo di Euclide termini in ogni caso. Ci chiediamo ora quante iterazioni siano necessarie per sua terminazione. Chiaramente, il numero di iterazioni dipenderà dai valori in ingresso e vogliamo formalizzare questa dipendenza il più accuratamente possibile. Una prima osservazione è la seguente: *Ad ogni iterazione, almeno uno dei due valori a, b decresce di almeno un'unità.* In base a questa osservazione, dopo al massimo $a + b$ iterazioni l'algoritmo deve terminare, e quindi abbiamo ottenuto una prima stima secondo la quale il numero massimo di iterazioni ha lo stesso ordine di grandezza dei numeri di cui vogliamo calcolare il MCD. Si tratta di una stima pressochè inutile qualora a o b siano dei numeri particolarmente grandi. Ad esempio, se si tratta di numeri di 100 cifre decimali, sappiamo che non ci vorranno più di circa 10^{100} iterazioni prima di conoscere il risultato, ma ciò non ci rende particolarmente felici nel momento in cui stiamo per lanciare l'algoritmo.

Una stima molto più stretta è basata su questa osservazione: *Ad ogni iterazione, il prodotto dei due valori a, b perlomeno si dimezza.* Per dimostare ciò, si noti come la coppia (a, b) viene rimpiazzata dalla coppia (r, a), dove r è il resto della divisione di b per a. Essendo $r < a$, si ha $b \geq a + r > 2r$, da cui, moltiplicando per a, si ottiene $ar < \frac{1}{2}ab$. In base a questa osservazione, detti a e b i valori iniziali, dopo k iterazioni, il prodotto dei due valori correnti sarà al massimo $ab/2^k$. Siccome questo valore è almeno 1, otteniamo che $ab \geq 2^k$, ossia

$$k \leq \log_2(ab) = \log_2 a + \log_2 b.$$

Abbiamo quindi ottenuto una nuova stima del numero di iterazioni dell'algoritmo di Euclide, che ci dice, fondamentalmente, che esso è proporzionale non già ai valori di ingresso, ma *al loro logaritmo.* In particolare, se come nell'esempio precedente i valori d'ingresso avessero 100 cifre decimali, dovremmo attenderci al massimo circa $2 \times \log_2 10^{100}$ iterazioni. Questo valore è inferiore a 1000 iterazioni, il che, rispetto alle 10^{100} della stima precedente, ci fa provare un certo sollievo al momento di lanciare l'algoritmo.

Esercizio 1.3. Si esegua l'algoritmo di Euclide su due numeri di Fibonacci consecutivi. Quante iterazioni risultano necessarie?

Il teorema di Bezout

Teorema **1**: (Bezout). Siano a e b numeri naturali e sia $d = \text{MCD}(a, b)$. Allora esistono due numeri interi x e y tali che $d = ax + by$.

Dim: Per dimostrare questo teorema utilizziamo l'algoritmo di Euclide per il MCD. Supponiamo che l'algoritmo esegua P iterazioni e denotiamo con a_i, b_i, r_i, per $i = 1, 2, \ldots, P$ i valori del divisore, dividendo e resto all'iterazione i-ma, con $a_1 = a$ e $b_1 = b$. In generale, abbiamo $a_{i+1} = r_i$, $b_{i+1} = a_i = r_{i-1}$, e l'algoritmo termina con $r_P = 0$, restituendo $\text{MCD}(a, b) = a_P = r_{P-1}$.

Sia $q_i = b_i \text{ div } a_i$. Abbiamo allora

$$r_1 = -q_1 a_1 + b_1 = ax_1 + by_1$$

proseguendo,

$$r_2 = -q_2 a_2 + b_2 = -q_2 r_1 + a = -q_2(ax_1 + by_1) + a = a(-q_2 x_1 + 1) + b(-q_2 y_1) = ax_2 + by_2,$$

e, in generale, $r_i = -q_i r_{i-1} + r_{i-2}$, per cui

$$r_3 = -q_3 r_2 + r_1 = -q_3(ax_2 + by_2) + (ax_1 + by_1) = a(-q_3 x_2 + x_1) + b(-q_3 y_2 + y_1) = ax_3 + by_3.$$

Proseguendo in questo modo, arriviamo a $r_{P-1} = ax_{P-1} + by_{P-1}$, ossia $\text{MCD}(a,b) = xa + yb$ per $x = x_{P-1}$ e $y = y_{P-1}$. ♣

L'equazione $\text{MCD}(a,b) = ax + by$ per opportune coppie (anche non uniche) di interi x, y, è detta *identità di Bezout*. Dal teorema di Bezout segue come corollario il seguente lemma.

Lemma 2: Due numeri naturali a e b sono coprimi se e solo se esistono interi x e y tali che $ax + by = 1$.

Dim: Se a e b sono coprimi, allora $\text{MCD}(a,b) = 1$ e quindi esistono x, y tali che $ax + by = 1$. Viceversa, se a e b non sono coprimi, allora sia $d > 1$ un loro divisore comune. Ponendo $a = a'd$ e $b = b'd$, si ha, per ogni x e y interi, $ax + by = d(a'x + b'y)$ che, essendo $d > 1$, non può mai valere 1. ♣

1.2 Numeri primi e loro distribuzione

Un numero naturale $p > 1$ si dice *primo* se i suoi unici divisori positivi sono 1 e p stesso. I primi primi sono

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, \ldots$$

Se $p > 1$ non è primo, allora si dice che p è un numero *composto*. In questo caso, esistono numeri naturali $a > 1$ e $b > 1$ tali che $p = ab$. Si noti che, per convenzione, 1 non è nè primo nè composto.

I numeri primi hanno sempre affascinato i matematici, sin dai tempi antichi. In tempi più recenti, con l'avvento dei computers e lo studio della codifica e protezione delle informazioni, si è scoperto che essi possono risultare particolarmente utili allo sviluppo di efficaci sistemi di *crittografia*. In particolare, sono stati sviluppati degli algoritmi di crittografia la cui robustezza si basa sull'assunto che è difficile, anche utilizzando dei potenti computers, decidere se un numero "sufficientemente grande" è composto o meno. Inoltre, alcuni di questi sistemi di crittografia richiedono di poter generare numeri primi "particolarmente grandi". La crittografia è stata quindi il motore di numerose ricerche relativamente al problema di come decidere se un numero sia primo o meno e di come generare numeri primi di molte cifre. Su entrambi i problemi sono stati ottenuti risultati notevoli (come ad esempio la costruzione di numeri primi con centinaia di cifre decimali), il cui studio risulta però troppo complesso per essere affrontato in questo testo introduttivo.

Abbiamo visto in sezione **??** come esistano infiniti numeri primi. Una domanda interessante sorge rispetto alla loro densità: quanti numeri composti si trovano, mediamente, tra due numeri primi? È facile dimostrare il seguente risultato:

Teorema **3**: Per ogni $k \geq 1$, esiste un blocco di k numeri naturali consecutivi tale che nessuno di essi è un numero primo.

Dim: Sia $n = k + 1$. Consideriamo i numeri

$$n! + 2, n! + 3, \ldots, n! + n.$$

Il primo di essi è divisibile per 2, il secondo per 3, e così via fino all'ultimo che è divisibile per n. Quindi, sono tutti numeri composti, e ce ne sono $n - 1 = k$. ♣

Per quanto esistano queste isole di numeri composti arbitrariamente larghe, in realtà esse non si presentano così spesso (in effetti, la costruzione utilizzata nella dimostrazione del teorema restituisce dei numeri enormi, e viene da chiedersi quanto, mediamente, siano lunghe le sequenze di numeri composti comprese nell'intervallo $1, \ldots, N$ al variare di N). È stato dimostrato che per ogni $k \geq 1$, esistono numeri primi di k cifre, ma questo risultato lascia spazio a potenziali isole la cui lunghezza è dell'ordine di N stesso. Un risultato più preciso è il seguente:

TEOREMA **4**: **(Teorema dei numeri primi)** Sia $\pi(N)$ il numero di primi nell'intervallo $1, 2, \ldots, N$. Allora

$$\pi(N) \sim \frac{N}{\ln N}.$$

Quindi, una frazione di $1/\ln N$ dei numeri è fatta di numeri primi. Si noti che N è esponenziale rispetto a $\ln N$ e quindi la stragrande maggioranza dei numeri è costituita da numeri composti. Inoltre, il teorema ci dà (approssimativamente, e per N "sufficientemente grande") la probabilità che, preso a caso un numero tra 1 e N, esso sia composto. Ad esempio, se $N = 10000$, la probabilità che un numero casuale sia composto è circa $1/9.21$, ossia tra il 10% e l'11%.

Possiamo usare il teorema dei numeri primi per cercare di dare una risposta alla seguente domanda:

Quanti numeri primi esistono di k cifre decimali ciascuno?

Per rispondere a questa domanda, possiamo sottrarre i numeri primi nell'intervallo $\{1, \ldots, 10^{k-1}\}$ da quelli nell'intervallo $\{1, \ldots, 10^k\}$. In base al teorema dei numeri primi, tale quantità è circa

$$\frac{10^k}{k \ln 10} - \frac{10^{k-1}}{(k-1)\ln 10} = \frac{(9k-10)10^{k-1}}{k(k-1)\ln 10}.$$

Essendo

$$\frac{9k-10}{k-1} = 9 - \frac{1}{k-1}$$

molto prossimo a 9 per k sufficientemente grande, ricaviamo che il numero di primi di k cifre è circa

$$9 \times \frac{10^{k-1}}{k \ln 10}.$$

Siccome esistono in tutto $10^k - 10^{k-1} = 9 \cdot 10^{k-1}$ numeri di k cifre, abbiamo che la frazione di essi data dai numeri primi è

$$\frac{1}{k \ln 10} \simeq \frac{1}{2.3k}.$$

Quindi, tra gli interi di k cifre, circa uno ogni $2.3k$ è primo. (Ovviamente si tratta di una stima approssimativa, che diventa via via più precisa al crescere di k).

Numeri di Fermat e primi di Mersenne ***

Alcune interessanti congetture sui primi. Riportiamo in questa sezione alcune congetture che riguardano i numeri primi. Nonostante per qualcuna di esse (grazie soprattutto al massiccio uso di potenti computers) si siano ottenuti dei progressi, su molte altre siamo sostanzialmente fermi al momento in cui esse furono formulate (in alcuni casi, centinaia di anni fa):

- *(Congettura di Goldbach) Ogni numero naturale pari > 2 può essere espresso come somma di due primi.* Ad esempio, $8 = 3 + 5$; $16 = 3 + 13$; $80 = 37 + 43$; ecc. Questa congettura è stata verificata essere soddisfatta da tutti i naturali fino a circa 10^{18}.
- *(Congettura di Lemoine) Ogni numero naturale dispari > 5 può essere espresso come somma di un primo con il doppio di un primo.* In termini algebrici, viene congetturato che l'equazione $2n+1 = x+2y$ ha sempre soluzioni x, y nell'insieme dei numeri primi, per $n > 2$. Ad esempio $47 = 13 + 2 \times 17 = 37 + 2 \times 5 = 41 + 2 \times 3 = 43 + 2 \times 2$. Questa congettura è stata verificata essere soddisfatta da tutti i naturali fino a circa 10^9.
- *(I Primi gemelli) Esistono infinite coppie $(a_1, b_1), (a_2, b_2), \ldots,$ di numeri primi tali che $b_i - a_i = 2$ per ogni i.* Ad esempio, le prime coppie di questo tipo sono

  $$(3,5), (5,7), (11,13), (17,19), (41,43), (71,73), (101,103), (107,109), (137,139), \ldots$$

  Ad oggi, è stato verificato che esistono $808,675,888,577,436$ coppie di primi gemelli $\leq 10^{18}$. Inoltre, sono stati individuati primi gemelli con più di $100,000$ cifre.
- *(Congettura di Legendre) Per ogni naturale $n > 1$ esiste sempre almeno un numero primo compreso nell'intervallo tra n^2 e $(n+1)^2$.*
- *(Numeri di Mersenne) Esistono infiniti primi di Mersenne* (i.e., della forma $2^n - 1$). Nel senso opposto a questa congettura ve n'è poi una che ipotizza che gli unici numeri primi di Fermat (i.e., della forma $2^{2^n} + 1$) si abbiano in corrispondenza di $n = 0, 1, 2, 3, 4$.

1.3 Fattorizzazione in primi

Sia n un numero naturale maggiore di 1. Se n non è un numero primo, n è comunque esprimibile come un prodotto di un numero finito di fattori primi (dove per "prodotto" di un singolo fattore si intende il fattore stesso). Questo prodotto viene detto una *fattorizzazione* di n in primi. Diciamo che due fattorizzazioni sono uguali se contengono gli stessi primi, ognuno ripetuto lo stesso numero di volte. In particolare, questo significa che dati due prodotti $p_1 \cdot p_2 \cdots p_k$ e $q_1 \cdot q_2 \cdots q_r$, essi sono la stessa fattorizzazione se $k = r$ ed è possibile riordinare i termini p_i, chiamando $p'_1 \cdot p'_2 \cdots p'_k$ il prodotto riordinato, in modo tale che risulti $p'_i = q_i$ per $i = 1, \ldots, k$.

TEOREMA **5**: (Esistenza della fattorizzazione) Ogni numero naturale $n \geq 2$ è esprimibile come un prodotto di un numero finito di fattori primi.

Dim: Per induzione. Il caso base è $n = 2$: siccome 2 è primo, allora n coincide con la sua fattorizzazione, data da un unico fattore. Supponiamo ora vero l'asserto per ogni numero in $2, 3, \ldots, n-1$ e dimostriamolo per n. Se n è primo, allora n coincide con la sua fattorizzazione, data da un unico fattore. Altrimenti,

siano a, b, entrambi minori di n, tali che $n = ab$. Per induzione, esiste una fattorizzazione in primi di a, sia essa $a = p_1 \cdot p_2 \cdots p_k$ e una di b, sia essa $b = q_1 \cdot q_2 \cdots q_r$. Ma allora esiste la fattorizzazione di n data da $n = p_1 \cdot p_2 \cdots p_k \cdot q_1 \cdot q_2 \cdots q_r$. ♣

Dimostreremo ora il *Teorema Fondamentale dell'Aritmetica*, che afferma che la fattorizzazione di un numero in fattori primi è di fatto unica. Per questa dimostrazione, abbiamo però bisogno di un risultato preliminare.

TEOREMA **6**: Sia p un numero naturale, $p > 1$. p è primo se e solo se per ogni coppia di numeri naturali a e b, se $p|ab$ allora $p|a$ oppure $p|b$.

Dim: ($\Rightarrow$) Supponiamo che p sia primo, che $p|ab$ e che $p \nmid a$. Si ottiene che $\text{MCD}(a, p) = 1$, in quanto, essendo p un numero primo, il massimo comun divisore può essere solo 1 oppure p, ma non può essere p, visto che $p \nmid a$. Per il teorema di Bezout, esistono interi x e y tali che $1 = ax + py$. Allora $b = b \cdot 1 = abx + pby$. Siccome $p|ab$, otteniamo che $p|b$.

($\Leftarrow$) Supponiamo che p abbia la proprietà suddetta e scriviamo $p = ab$, con $0 < a < p$. Siccome $p \nmid a$, deve essere $p|b$, quindi $b = pc$ per qualche $c \in \mathbb{Z}$. Ne segue $p = ab = apc$, ossia $0 = p(1 - ac)$. Ma allora $ac = 1$ e quindi $a = 1$. In conclusione, p non ha divisori propri maggiori di 1 e minori di p stesso, e quindi è primo. ♣

COROLLARIO **7:** Sia p un numero primo e supponiamo che $p|a_1 a_2 \cdots a_r$. Allora $p|a_i$ per almeno un i , $1 \leq i \leq r$.

Dim: La dimostrazione è facile per induzione su r. ♣

TEOREMA **8**: (Teorema fondamentale dell'aritmetica) Ogni numero naturale $n \geq 2$ è esprimibile in un unico modo come un prodotto di un numero finito di fattori primi.

Dim: Abbiamo già dimostrato l'esistenza della fattorizzazione, per cui ci basta fare vedere che la fattorizzazione è unica. Supponiamo per assurdo che esistano dei numeri maggiori di 1 che ammettono fattorizzazioni diverse. In particolare, sia $\bar{n}$ il minimo tra tali controesempi. Indichiamo due fattorizzazioni diverse di $\bar{n}$ con

$$\bar{n} = p_1 \cdot p_2 \cdots p_k = q_1 \cdot q_2 \cdots q_r.$$

Siccome $p_k|q_1 \cdot q_2 \cdots q_r$, allora, in base al teorema 6, p_k divide almeno uno dei q_i. Ma, essendo tutti i q_i primi, ciò vuol dire che $p_k = q_t$ per un $t \in \{1, 2, \ldots, r\}$. Senza perdita di generalità, supponiamo $t = r$. Ma allora, dividendo entrambe le fattorizzazioni per $p_k (= q_r)$ e detto $\hat{n} = p_1 \cdot p_2 \cdots p_{k-1}$, si ha

$$\hat{n} = p_1 \cdot p_2 \cdots p_{k-1} = q_1 \cdot q_2 \cdots q_{r-1}$$

dove le fattorizzazioni $p_1 \cdot p_2 \cdots p_{k-1}$ e $q_1 \cdot q_2 \cdots q_{r-1}$ sono diverse perchè erano diverse le fattorizzazioni di $\bar{n}$. Ma allora $\bar{n}$ non sarebbe il più piccolo controesempio, in quanto $\hat{n} < \bar{n}$. Assurdo. ♣

Per convenzione, quando si indica una fattorizzazione di un numero, i fattori vengono sempre elencati in ordine non-decrescente. Inoltre, vengono raggruppati i fattori uguali, e la loro molteplicità diventa l'esponente del corrispondente fattore. Alcuni esempi: $100 = 2^2 \cdot 5^2$; $150 = 2 \cdot 3^2 \cdot 5$; $30492 = 2^2 \cdot 3^3 \cdot 7 \cdot 11^2$ ecc.

Si può poi pensare di estendere la fattorizzazione a *tutti* i numeri primi, in modo tale che ogni numero può essere rappresentato come il prodotto di tutti i primi, ciascuno elevato ad un opportuno esponente. Tale esponente risulterà 0 per quasi tutti i fattori, e sarà diverso da 0 solo per un numero finito di fattori. Quindi, per ogni naturale $n \geq 2$ esistono naturali $k_1, k_2, \ldots$ tali che

$$n = 2^{k_1} \times 3^{k_2} \times 5^{k_3} \times 7^{k_4} \times 11^{k_5} \times \cdots$$

Quando è nota la fattorizzazione in primi di due numeri a e b, diventa molto facile calcolare il loro MCD e mcm. Infatti, supponiamo che le fattorizzazioni in primi siano $a = p_1^{n_1} \times p_2^{n_2} \times \cdots \times p_k^{n_k}$ e $b = p_1^{m_1} \times p_2^{m_2} \times \cdots \times p_k^{m_k}$ (dove la fattorizzazione è stata estesa in modo da coinvolgere gli stessi divisori primi. Chiaramente, alcuni degli esponenti n_i e m_i possono essere nulli, in corrispondenza dei fattori primi che dividono solo uno dei due numeri). Abbiamo allora

$$\mathrm{MCD}(a,b) = p_1^{\min(n_1,m_1)} \times p_2^{\min(n_2,m_2)} \times \cdots \times p_k^{\min(n_k,m_k)}$$

$$\mathrm{mcm}(a,b) = p_1^{\max(n_1,m_1)} \times p_2^{\max(n_2,m_2)} \times \cdots \times p_k^{\max(n_k,m_k)}$$

Ad esempio, sia $a = 18 = 2 \times 3^2$ e $b = 60 = 2^2 \times 3 \times 5$. Abbiamo allora $\mathrm{MCD}(18, 60) = 2 \times 3 = 6$ e $\mathrm{mcm}(18, 60) = 2^2 \times 3^2 \times 5 = 180$.

Esercizio 1.4. Dimostrare che per qualsiasi coppia di interi a e b si ha $\mathrm{MCD}(a,b) \times \mathrm{mcm}(a,b) = a\,b$.

Esercizio 1.5. Dimostrare che se $a \,|\, b$ e $a \,|\, c$, allora (i) $a \,|\, b + c$ e $a \,|\, b - c$; (ii) $a \,|\, b \bmod c$.

Per quel che riguarda la fattorizzazione in primi del fattoriale di n, abbiamo il seguente teorema (noto come Teorema di Legendre),

Teorema **9**: Il numero $n!$ contiene il fattore primo p esattamente

$$\sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor$$

volte.

Dim: Innanzitutto, esattamente $\lfloor \frac{n}{p} \rfloor$ dei fattori di $n! = 1 \cdot 2 \cdot 3 \cdots n$ sono divisibili per p. Inoltre, $\lfloor \frac{n}{p^2} \rfloor$ di tali fattori sono divisibili anche per p^2, altri $\lfloor \frac{n}{p^3} \rfloor$ sono divisibili anche per p^3 e così via. ♣

Ad esempio, nello sviluppo di 15!, il fattore primo 3 compare $\lfloor \frac{15}{3} \rfloor + \lfloor \frac{15}{9} \rfloor = 5 + 1 = 6$ volte. Similmente, il 2 compare $7 + 3 + 1 = 11$ volte, il 5 compare 3 volte, il 7 compare 2 volte, mentre l'11 e il 13 compaiono una volta ciascuno. Quindi $15! = 2^{11} \times 3^6 \times 5^3 \times 7^2 \times 11 \times 13$.

Esercizio 1.6. Con quanti zeri termina il numero 56! ?

1.4 Il piccolo teorema di Fermat

TEOREMA **10**: **(Piccolo teorema di Fermat)** Sia p un numero primo e $a \in \mathbb{Z}$. Se $p \nmid a$, allora $a^{p-1} \equiv 1 (\text{mod } p)$.

Dim: Siccome p ed a sono coprimi, i numeri $\{0, a, 2a, \ldots, (p-1)a\}$ sono congruenti modulo p (non necessariamente in quest'ordine) con tutti i possibili resti $\{0, 1, 2, \ldots, p-1\}$. Siccome (si veda anche l'esercizio XXX) $x' \equiv x''(\text{mod } p)$ e $y' \equiv y''(\text{mod } p)$ implicano $x'y' \equiv x''y''(\text{mod } p)$, allora

$$a \cdot 2a \cdots (p-1)a \equiv 1 \cdot 2 \cdots (p-1) \pmod{p}$$

e quindi

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}.$$

Abbiamo allora che $p \,|\, (p-1)! \cdot (a^{p-1} - 1)$, e, visto che $p \nmid (p-1)!$, deve essere $p \,|\, a^{p-1} - 1$. Quindi $a^{p-1} \equiv 1(\text{mod } p)$. ♣

COROLLARIO 11**:**

1.5 Pari e Dispari

Ci sono alcuni problemi della matematica combinatorica la cui soluzione più semplice ed elegante è quella di ricorrere ad argomenti di *parità* e/o *simmetria*. Il concetto di parità è ben noto, e sappiamo che gli interi si ripartiscono in due classi, i numeri pari e quelli dispari. Diciamo che due numeri hanno la stessa parità se appartengono alla medesima classe, ossia se sono entrambi pari o entrambi dispari. Il concetto apparentemente elementare di parità è alle volte indispensabile nella risoluzione di problemi che, qualora venissero affrontati senza farvi ricorso, possono risultare di complessità estrema. L'unico modo per convincersi di ciò è quello di fare degli esempi, per cui, cominciamo.

1.5.1 Il segno delle permutazioni.

Sia $\mathcal{S}_n$ l'insieme di tutte le permutazioni dei numeri $\{1, 2, \ldots, n\}$. Data una permutazione $\pi = (\pi_1, \ldots, \pi_n) \in \mathcal{S}_n$, una *trasposizione* τ_{ab}, con $a, b \in \{1, 2, \ldots, n\}$ e $a \neq b$ è una funzione che trasforma π in una nuova permutazione, identica a π eccezion fatta per gli elementi π_a e π_b che vengono scambiati fra loro. In particolare, supponendo $a < b$,

$$\tau_{ab}(\pi) = (\pi_1, \ldots, \pi_{a-1}, \pi_b, \pi_{a+1}, \ldots, \pi_{b-1}, \pi_a, \pi_{b+1}, \ldots, \pi_n).$$

Ogni permutazione $\sigma \in \mathcal{S}_n$ può essere ottenuta (in più modi) da π con una sequenza di trasposizioni. Infatti, con una trasposizione, possiamo far sì che π_1 diventi uguale a σ_1. Con un'ulteriore trasposizione portiamo σ_2 in posizione 2, e così via, finchè π coincide con σ. Ad esempio, se $\pi = (2, 1, 3, 6, 5, 4)$ e $\sigma = (3, 1, 4, 5, 6, 2)$ possiamo trasformare π in σ con 3 trasposizioni come segue:

$$(\mathbf{2}, 1, \mathbf{3}, 6, 5, 4) \mapsto (3, 1, \mathbf{2}, 6, 5, \mathbf{4}) \mapsto (3, 1, 4, \mathbf{6}, \mathbf{5}, 2) \mapsto (3, 1, 4, 5, 6, 2)$$

Facciamo ora vedere che se σ può essere ottenuta da π con k trasposizioni, allora ogni modo di ottenere σ da π richiede un numero di trasposizioni che ha la stessa parità di k. Senza perdita di generalità(eventualmente rinominando gli elementi delle due permutazioni) pssiamo sempre assumere che σ sia la permutazione identica. Abbiamo il seguente teorema.

TEOREMA **12**: Data una permutazione π, o tutti i modi di trasformare π nella permutazione identica richiedono un numero pari di trasposizioni, o richiedono tutti un numero dispari di trasposizioni.

Dim: Consideriamo in π tutte le coppie $\{\pi_i, \pi_j\}$ tali che $i < j$ ma $\pi_i > \pi_j$. Chiamiamo ogni coppia di questo tipo un'*inversione*. Si tratta di una coppia di elementi che compaiono in un ordine diverso nella permutazione di partenza e in quella di arrivo. Supponiamo che vengano trasposti due qualsiasi elementi π_i e π_j. Ogni elemento in posizione k con $i < k < j$:

- se non faceva inversione con nessuno dei due ora la fa con tutti e due.
- se faceva inversione solo con uno dei due, allora adesso la fa solo con l'altro.
- se faceva inversione con entrambi, ora non la fa con nessuno dei due.

Quindi, relativamente agli elementi tra i e j, il numero complessivo di inversioni mantiene la stessa parità. Similmente, gli elementi in posizione $k < i$ o $k > j$ non possono dare luogo a nuove inversioni in quanto rimangono nello stesso ordine relativamente a π_i e π_j. Infine, la coppia $\{\pi_i, \pi_j\}$ se era un'inversione ora non lo è più, mentre se non lo era ora lo diventa. In conclusione, il numero totale di inversioni cambia di parità. Questo implica che se la permutazione di partenza aveva un numero dispari di inversioni, sarà necessario un numero dispari di trasposizioni per eliminarle tutte, mentre se le inversioni erano in numero pari, servirà un numero pari di trasposizioni. ♣

In base a quanto appena osservato, le permutazioni si ripartiscono in due classi, chiamate rispettivamente permutazioni pari e permutazioni dispari. Le permutazioni pari sono tutte quelle ottenibili con un numero pari di trasposizioni a partire dalla permutazione identica mentre le restanti permutazioni sono dispari. Essendoci una corrispondenza biunivoca tra le due classi, esistono $n!/2$ permutazioni pari ed altrettante permutazioni dispari. Per convenzione, le permutazioni pari sono dette di segno +1, mentre quelle dispari di segno -1.

Esempio. Il gioco del 15 In un popolare gioco di ingegno, all'interno di una piccola cornice di plastica quadrata di lato 4, si trovano 15 tasselli quadrati di lato 1, numerati da 1 a 15, ed una posizione libera (detta il "buco"). Ogni tassello adiacente al buco può essere fatto slittare nel buco stesso. Questa mossa ha l'effetto di muovere il tassello, ma, alternativamente, può essere vista come una mossa che muove il buco. Il buco può perciò muoversi al massimo in 4 posizioni rispetto alla posizione corrente, ossia in alto, in basso, a sinistra o a destra. Ad esempio, spostando il buco in alto possiamo effettuare la seguente mossa

1	2	3	4
5		6	8
9	10	7	11
13	14	15	12

$\mapsto$

1		3	4
5	2	6	8
9	10	7	11
13	14	15	12

◇

Immaginiamo ora che qualcuno ci presenti una configurazione che è stata ottenuta a partire dalla configurazione ordinata applicando un buon numero di mosse casuali. La configurazione ordinata è quella in cui la casella in alto a sinista è 1, i valori crescono spostandosi da sinistra a destra e da una riga alla successiva, e la casella in basso a destra è il buco. L'obiettivo è quello di riportare tutti i tasselli nella configurazione ordinata tramite una sequenza di mosse (più breve possibile). Supponiamo ora che ci venga presentata la configurazione

	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15

e che ci venga chiesto di risolverla. Possiamo provare fin che vogliamo ma non potremo mai riportare i tasselli nella configurazione ordinata. Per convincerci di ciò consideriamo la permutazione di 16 elementi ottenuta leggendo una configurazione riga per riga, dall'alto in basso, e chiamando "16" il buco. Ogni mossa del buco corrisponde a una trasposizione. Ad esempio, data la configurazione

5	1	12	3
4	15	6	2
8	9		11
7	13	14	10

equivalente alla permutazione

$$(5, 1, 12, 3, 4, 15, 6, 2, 8, 9, \mathbf{16}, 11, 7, 13, 14, 10)$$

ogni mossa del buco è una trasposizione:

- Mossa a sinistra: $(5, 1, 12, 3, 4, 15, 6, 2, 8, \mathbf{16}, 9, 11, 7, 13, 14, 10)$
- Mossa a destra: $(5, 1, 12, 3, 4, 15, 6, 2, 8, 9, 11, \mathbf{16}, 7, 13, 14, 10)$
- Mossa in alto: $(5, 1, 12, 3, 4, 15, \mathbf{16}, 2, 8, 9, 6, 11, 7, 13, 14, 10)$
- Mossa in basso: $(5, 1, 12, 3, 4, 15, 6, 2, 8, 9, 14, 11, 7, 13, \mathbf{16}, 10)$

In particolare, quindi, ad ogni mossa *la parità della permutazione corrente cambia*. Nel nostro specifico esempio, la permutazione di arrivo è pari, mentre quella di partenza è dispari (ci sono esattamente 15 inversioni). Se coloriamo le 16 posizioni dei tasselli di bianco e nero, come le caselle di una scacchiera, notiamo che il buco deve passare dall'angolo alto a sinistra a quello basso a destra, che hanno lo stesso colore, e quindi deve essere mosso un numero pari di volte. Questo implica che la parità della permutazione di partenza sarà la stessa di quella di arrivo. Siccome la permutazione di partenza è dispari e quella di arrivo è pari, il problema non ammette soluzione.

Esempio. Ordinamento a blocchi. Consideriamo il seguente puzzle: è data una permutazione di n elementi, che vogliamo ordinare tramite una sequenza di mosse. Ad ogni mossa, possiamo prendere un

blocco consecutivo di 3 elementi ed invertirne l'ordine. Ad esempio, possiamo passare da $(2, \mathbf{1}, \mathbf{3}, \mathbf{5}, 4, 6, 7)$ a $(2, 5, 3, 1, 4, 6, 7)$. Immaginiamo che partendo dalla permutazione ordinata, qualcuno abbia effettuato un gran numero di mosse e ci abbia poi presentato la permutazione mescolata risultante, apparentemente casuale. Il gioco richiede ora di trovare una sequenza di mosse (tanto più corta tanto meglio) che riporti la permutazione mescolata nella permutazione originale. Ad esempio, se ci viene presentata la permutazione $(3, 4, 1, 2, 7, 8, 5, 6)$, possiamo ordinarla in 4 mosse come segue:

$$(3, 4, 1, 2, 7, \mathbf{8}, \mathbf{5}, \mathbf{6}) \mapsto (3, 4, 1, 2, \mathbf{7}, \mathbf{6}, \mathbf{5}, 8) \mapsto (\mathbf{3}, \mathbf{4}, \mathbf{1}, 2, 5, 6, 7, 8) \mapsto (1, \mathbf{4}, \mathbf{3}, \mathbf{2}, 5, 6, 7, 8) \mapsto (1, 2, 3, 4, 5, 6, 7, 8)$$

Supponiamo ora che il nostro avversario ci presenti la permutazione $(1, 4, 6, 2, 5, 7, 3, 8)$ e ci sfidi a risolverla. Anche qui, possiamo dimostrare che è impossibile ordinarla, e che quindi l'avversario ci sta imborogliando. La dimostrazione è la seguente. Ogni mossa coinvolge tre elementi consecutivi, dei quali quello in posizione centrale sta fermo, mentre gli altri due si scambiano di posto. In particolare, ogni elemento che si muove, lo fa di due caselle, e quindi passa da una posizione (di indice) pari ad una pari, o da una dispari ad una dispari. Quindi, se la permutazione mescolata è stata ottenuta dalla permutazione identica, i numeri dispari devono sempre e comunque occupare posizioni di indice dispari, e quelli pari posizioni di indice pari. Ora, nella nostra permutazione il numero 6 si trova in posizione 3 (oppure il 7 in posizione 6), e quindi non è possibile riordinare questa permutazione con mosse legali. ◇

Esempio. Pavimentazione di rettangoli. Tiling con pezzi del domino. Rimuovere caselle. Tiling con le L. ◇

Esempio. Le lampadine. Ci sono n lampadine, inizialmente tutte spente. Ad ogni iterazione, possiamo azionare l'interruttore di esattamente $n-1$ lampadine, e questa operazione può essere ripetuta più volte, con l'obiettivo finale di accendere tutte le lampadine. Dimostrare che ciò è possibile se e solo se n è pari.

(i) Sia n pari. Per $i = 1, \ldots, n$ ripetiamo l'operazione : "aziona tutti gli interruttori tranne l'i-esimo". In questo modo, ogni lampadina viene azionata (accesa/spenta) $n-1$ volte (un numero dispari) e quindi, siccome all'inizio era spenta, alla fine è accesa.

(ii) Supponiamo ora che n sia dispari ma che, per assurdo, esista una soluzione. Sia k_i il numero di volte in cui l'interruttore i viene premuto nella soluzione. Siccome alla fine la lampadina i è accesa, k_i deve essere dispari. Chiamiamo $K = \sum_{i=1}^{n} k_i$. Siccome K è la somma di un numero dispari di termini dispari, K è dispari. Ma K è anche il numero complessivo di interruttori premuti, e ad ogni iterazione vengono premuti $n-1$ interruttori. Quindi, K è un multiplo di $n-1$. Ma $n-1$ è un numero pari e K deve essere pari, da cui l'assurdo. ◇

Esempio. Il giro del cavallo. Nel gioco degli scacchi, il cavallo effettua una caratteristica mossa "ad L". In particolare, dette (x, y) le coordinate della casella in cui si trova, il cavallo può muovere verso ciascuna (ammesso che esista) tra 8 caselle del tipo $(x \pm \delta_x, y \pm \delta_y)$, con $\delta_x, \delta_y \in \{1, 2\}$ e $\delta_x \neq \delta_y$.

Supponiamo ora di avere a disposizione una scacchiera 7×7 e di aver posizionato il cavallo in riga 1, colonna 2. Ci chiediamo se, partendo da lì ed effettuando sempre mosse ad L, si possa riuscire a visitare una ed una sola volta tutte le caselle della scacchiera. Vogliamo dimostrare che questo è impossibile.

La soluzione migliore è ricorrere ad un argomento di parità. Supponiamo che le caselle siano colorate, nel

classico modo, nere e bianche. Senza perdita di generalità, supponiamo che la casella $(1, 1)$ sia nera e quindi la $(1, 2)$ è bianca. Siccome il lato della scacchiera è un numero dispari, ci sono in tutto un numero dispari di caselle. In particolare, ci sono 25 caselle nere e 24 bianche. Dopo aver posizionato il cavallo sulla casella iniziale, dobbiamo effettuare 48 mosse, visto che ad ogni mossa viene visitata una nuova casella. Siccome ad ogni mossa il colore della casella di arrivo è diverso da quello della casella di partenza, dopo un numero pari di mosse il cavallo ha visitato un numero uguale di caselle bianche e nere. Quindi, avrebbe visitato 24 caselle bianche e 24 nere. Ma la casella iniziale era bianca, e quindi ci sarebbero 25 caselle bianche, assurdo. $\diamond$