Capitolo 3

Aritmetica e Algebra

3.1 Il Teorema di Cantor-Bernstein

Teorema 3.1 (Cantor-Bernstein)**.** *Se $f : A \to B$ e $g : B \to A$ sono due mappe iniettive, esiste corrispondenza biunivoca tra A e B.*

Dimostrazione. Diciamo che $x \in A$ ha un *precedente* $y \in B$ se $x = g(y)$. Analogamente, diciamo che $y \in B$ ha un *precedente* $z \in A$ se $y = f(z)$. Notiamo che, per l'iniettività di f e g, se un elemento ha un precedente, questo è unico. E' dunque lecito risalire la catena dei precedenti $(x, y, z, \ldots)$ fino, eventualmente, a determinare un elemento che non ha precedenti, che chiamiamo *primo precedente*. Definiamo ora A_A come l'insieme dei punti di A che hanno un primo precedente in A; A_B come l'insieme dei punti di A che hanno un primo precedente in B e A_C come l'insieme dei punti di A che non hanno un primo precedente, ossia come l'insieme dei punti di A per cui la catena dei precedenti non termina. E' a questo punto semplice verificare che la funzione

$$h(x) = \begin{cases} f(x) & \text{se} \quad x \in A_A \cup A_C, \\ g^{-1}(x) & \text{se} \quad x \in A_B \end{cases}$$

è una mappa biettiva tra A e B. Infatti, h è iniettiva su $A_A \cup A_C$ per l'iniettività di f, ed è iniettiva su A_B poiché $A_B \subseteq g(B)$ e g è iniettiva. Se $y \in B$ ha un primo precedente in A oppure non ha un primo precedente, certamente $y \in f(A_A \cup A_C)$; se $y \in B$ ha un primo precedente in B, allora $x = g(y) \in A$ ha la medesima proprietà, per cui $x \in A_B$: $h : A \to B$ risulta perciò sia iniettiva che suriettiva.

In alternativa, posto $C_0 = A \setminus g(B)$, $C_{n+1} = g(f(C_n))$ e $C = \bigcup_{n \in N} C_n$, si provi che

$$h(x) = \begin{cases} f(x) & \text{se} \quad x \in C, \\ g^{-1}(x) & \text{se} \quad x \notin C \end{cases}$$

è una mappa biunivoca tra A e B. □

3.2 Rappresentazione degli interi in varie basi

Introduzione al logaritmo come lunghezza della rappresentazione b-aria.

3.3 Divisori e numeri primi

Dati due numeri interi d ed n, diciamo che d è un divisore di n o che d *divide* n, in simboli $d|n$, se

$$\exists\, a \in \mathbb{Z} :\ a \cdot d = n,$$

ossia se $n \in d\mathbb{Z}$. Equivalentemente, diciamo che n è un *multiplo* di d.
In caso negativo, ossia se $n \notin d\mathbb{Z}$, diciamo che d non divide n, in simboli $d \nmid n$.
Denotiamo con $d(n)$ la *funzione dei divisori*, definita come:

$$d(n) = |\{m \in \mathbb{N} :\ m|n\}|,$$

e diciamo che un numero naturale p è *primo* se ammette esattamente due divisori, ossia se verifica:

$$d(p) = 2.$$

Diciamo inoltre che due numeri naturali a e b sono *coprimi* se non ammettono divisori comuni all'infuori di 1, e denotiamo con $\mathcal{P}$ l'insieme dei numeri primi:

$$\mathcal{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \ldots\}.$$

Dato un numero $q \in \mathbb{Q}$, definiamo la sua *parte intera inferiore* $\lfloor q \rfloor$ e la sua *parte intera superiore* $\lceil q \rceil$ come:

$$\lfloor q \rfloor = \max\{n \in \mathbb{Z} : n \leq q\}, \qquad \lceil q \rceil = \min\{n \in \mathbb{Z} : n \geq q\},$$

la sua *parte frazionaria* $\{q\}$ come:

$$\{q\} = q - \lfloor q \rfloor.$$

Dimostreremo i seguenti fatti:

(I) se un numero primo p divide un prodotto di due interi ab, p divide almeno uno tra a e b;

(II) $\mathcal{P}$ è un insieme infinito;

(III) ogni numero naturale $n > 2$ può essere espresso in modo unico come prodotto di potenze di numeri primi - questo è il Teorema di fattorizzazione unica,

(IV) a, b coprimi $\longrightarrow d(ab) = d(a) \cdot d(b)$.

Esercizio 3.2. *Si dimostri che ogni numero naturale $n \geq 3$, ad eccezione delle potenze di 2, può essere espresso come somma di due o più interi positivi consecutivi.*

Dimostrazione. Considerato che la somma dei numeri naturali da 1 a k è pari a $\frac{k(k+1)}{2}$, vogliamo provare che tutti i numeri naturali positivi n possono essere espressi come

$$\frac{j(j+1)}{2} - \frac{k(k+1)}{2} = n,$$

con $j \geq k + 2 \geq 2$. L'ultima identità è equivalente a:

$$4j(j+1) - 4k(k+1) = 8n,$$

$$(2j+1)^2 - (2k+1)^2 = 8n,$$

$$(j+k+1)(j-k) = 2n.$$

I due fattori che compaiono a membro sinistro sono sempre l'uno pari e l'altro dispari, ed entrambi ≥ 2. Ciò comporta che il membro destro ammette almeno un divisore primo dispari, per cui se n è una potenza di 2, l'equazione non ammette certamente soluzioni. Viceversa, se $n \geq 3$ non è una potenza di due, n ammette certamente un divisore primo p dispari e $\leq \frac{n}{2}$: in tali ipotesi $\frac{2n}{p}$ è pari e $\geq (p+1)$. Ponendo $(j-k) = p$ e $(j+k) = \frac{2n}{p} - 1$ abbiamo che $j = \frac{p-1}{2} + \frac{n}{p}$ e $k = \frac{n}{p} - \frac{p+1}{2}$ sono soluzioni della nostra equazione, con $(j-k) = p \geq 3$. □

3.4 Relazioni e classi di equivalenza

Una *relazione di equivalenza* $\sim$ su un insieme A è una relazione

- riflessiva: $\forall a \in A,\ a \sim a$;
- simmetrica: $a \sim b \longrightarrow b \sim a$;
- transitiva: $a \sim b, b \sim c \longrightarrow a \sim c$.

Dato un insieme A e una relazione di equivalenza $\sim$ su di esso, l'*insieme quoziente* $A/_\sim$ è definito come:

$$A/_\sim \doteqdot \{[a] : a \in A\}.$$

Gli elementi dell'insieme quoziente sono detti *classi di equivalenza*:

$$[a] = \{b \in A :\ b \sim a\}.$$

3.5 Frazioni continue

NB: chiarire il fatto che i convergenti sono frazioni ridotte.

Chiamiamo *frazione continua* un numero razionale della forma[1]:

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \ldots}},$$

dove a_0 è un intero e tutti gli altri a_j sono numeri interi postivi. Per questioni tipografiche, talvolta tale espressione si indica come:

$$[a_0; a_1, a_2, \ldots, a_n] \quad \text{oppure come} \quad a_0 + \frac{1}{a_0+}\,\frac{1}{a_0+}\ldots\frac{1}{a_n}.$$

Gli a_j sono detti *termini* o *quozienti parziali* della frazione continua, mentre i numeri razionali:

$$q_0 = a_0, \quad q_1 = [a_0; a_1], \quad q_2 = [a_0; a_1, a_2], \quad \ldots$$

sono detti *convergenti* della frazione continua. Notiamo che si ha:

$$[a_0; a_1, \ldots, a_n, 1] = [a_0; a_1, \ldots, a_n + 1];$$

per questioni di unicità della rappresentazione supporremo perciò che l'ultimo termine di una frazione continua associata ad un elemento di $\mathbb{Q}^+ \setminus \mathbb{N}$ non sia mai 1.

[1] Temporaneamente, supporremo che le frazioni annidate siano in quantità finita. Vedremo successivamente che il concetto di frazione continua con una infinità di termini è ben fondato, ed anzi fornisce un metodo per rappresentare ogni numero reale.

Teorema 3.3. *Ogni numero razionale $q \in \mathbb{Q}^+$ può essere espresso in modo unico in forma di frazione continua.*

Consideriamo quanto accade nella ripetizione di due operazioni: prendere la parte intera di un numero e prendere il reciproco della sua parte frazionaria. A partire da $q = \frac{24}{7}$, ad esempio, otteniamo:

$$\frac{24}{7} = 3 + \frac{3}{7}, \qquad \frac{7}{3} = 2 + \frac{1}{3},$$

da cui:

$$\frac{24}{7} = 3 + \frac{1}{2 + \frac{1}{3}} = [3; 2, 3].$$

Notiamo che le parti frazionarie in gioco sono sempre numeri strettamente minori di 1, e che i numeratori di tali parti frazionarie costituiscono una sequenza strettamente decrescente: se, infatti, ad un certo passo abbiamo una parte frazionaria $\frac{a}{b}$ con $a < b$, la parte frazionaria al passo successivo ha numeratore $b - \left\lfloor \frac{b}{a} \right\rfloor a < a$. Ciò comporta che ad un certo passo la parte frazionaria presa in considerazione abbia numeratore pari ad 1, concludendo l'algoritmo: ciò prova che ogni $q \in \mathbb{Q}^+$ ammette una rappresentazione in forma di frazione continua.

Lemma 3.4. *Se due frazioni continue di $n+1$ termini $[a_0; a_1, \ldots, a_n] = q_a$ e $[b_0; b_1, \ldots, b_n] = q_b$ coincidono per i primi n termini e si verifica $a_n > b_n$, allora $q_a > q_b$ oppure $q_a < q_b$, a seconda che, rispettivamente, n sia pari oppure dispari.*

E' semplice dimostrare tale risultato per induzione su n: il caso-base $n = 0$ è immediato,
e la disuguaglianza

$$[c_0; c_1, \ldots, c_{n-1}, c] < [c_0; c_1, \ldots, c_{n-1}, d]$$

è equivalente, attraverso la sottrazione di c_0 ad ambo i membri, alla disuguaglianza:

$$[0; c_1, \ldots, c_{n-1}, c] < [0; c_1, \ldots, c_{n-1}, d],$$

a sua volta equivalente, reciprocando ambo i membri, alla disuguaglianza:

$$[c_1; \ldots, c_{n-1}, c] > [c_1; \ldots, c_{n-1}, d],$$

che consiste nel raffronto di due frazioni continue con un termine in meno al punto di partenza.
Più in generale, due frazioni continue che differiscono per almeno un termine rappresentano numeri razionali distinti. Supponiamo, per assurdo, che si abbia:

$$[a_0; a_1, \ldots, a_n, b_0, \ldots, b_m] = [a_0; a_1, \ldots, a_n, c_0, \ldots, c_r],$$

con $b_0 \neq c_0$. Sottraendo il medesimo numero intero ad ambo i membri e reciprocando $n+1$ volte si ha:

$$[b_0; \ldots, b_m] = [c_0; \ldots, c_r],$$

ma ciò è impossibile, in quanto i due membri hanno diverse parti intere inferiori, ragion per cui non possono rappresentare il medesimo numero. Abbiamo provato che ogni numero razionale positivo può essere rappresentato in modo unico in forma di frazione continua.

Teorema 3.5. *Siano h_m e k_m, rispettivamente, numeratore e denominatore dell'm-esimo convergente della frazione continua $[a_0; a_1, \ldots, a_n]$. Per ogni intero $x \geq 1$ si ha:*

$$[a_0; a_1, \ldots, a_n, x] = \frac{x\, h_n + h_{n-1}}{x\, k_n + k_{n-1}}.$$

Dimostrazione. Dimostriamo il Teorema per induzione su n, lasciando il caso-base $n = 2$ come esercizio per il lettore. Siano p_m e q_m numeratore e denominatore dell'm-esimo convergente di $[a_1; \ldots, a_n, x]$; si ha:

$$[a_0; a_1, \ldots, a_n, x] = a_0 + \frac{q_n}{p_n} = \frac{a_0 p_n + q_n}{p_n},$$

ma per ipotesi induttiva si hanno pure $p_n = x \cdot p_{n-1} + p_{n-2}$ e $q_n = x \cdot q_{n-1} + q_{n-2}$, da cui:

$$[a_0; a_1, \ldots, a_n, x] = \frac{x(a_0 p_{n-1} + q_{n-1}) + (a_0 p_{n-2} + q_{n-2})}{x k_n + k_{n-1}} = \frac{x\, h_n + h_{n-1}}{x\, k_n + k_{n-1}}.$$

□

Teorema 3.6. *Se $\frac{h_m}{k_m}$ e $\frac{h_{m+1}}{k_{m+1}}$ sono convergenti successivi della medesima frazione continua,*

$$h_{m+1}\, k_m - h_m\, k_{m+1} = (-1)^m.$$

Dimostrazione. Sia $A_m = h_{m+1}\, k_m - h_m\, k_{m+1}$. In virtù del Teorema precedente,

$$h_{m+1} = a_m h_m + h_{m-1}, \qquad k_{m+1} = a_m k_m + k_{m-1},$$

da cui discende immediatamente $A(m) = -A(m-1)$. □

Corollario 3.7. *Se $q \in \mathbb{Q}^+$ è un numero razionale la cui frazione continua consta di n termini, detto k_m il denominatore dell'm-esimo convergente, si ha:*

$$q = a_0 - \sum_{j=1}^{n} \frac{(-1)^j}{k_{j-1} k_j}.$$

Dimostrazione. Con le notazioni del Teorema precedente si ha infatti:

$$q = \frac{h_n}{k_n} = a_0 + \sum_{j=1}^{n} \left(\frac{h_j}{k_j} - \frac{h_{j-1}}{k_{j-1}} \right) = a_0 + \sum_{j=1}^{n} \frac{A(j-1)}{k_{j-1} k_j}.$$

□

Corollario 3.8. *Se la frazione continua di $q \in \mathbb{Q}^+$ consta di almeno $k+2$ termini e $\frac{p_k}{q_k}$ è il k-esimo convergente, vale:*

$$\frac{1}{q_k(q_k + q_{k+1})} \leq \left| q - \frac{p_k}{q_k} \right| < \frac{1}{q_k\, q_{k+1}}.$$

Dimostrazione. In virtù del Corollario (3.7) q è certamente compreso tra $\frac{p_k}{q_k}$ e $\frac{p_{k+1}}{q_{k+1}}$, ragion per cui:

$$\left| q - \frac{p_k}{q_k} \right| < \left| \frac{p_{k+1}}{q_{k+1}} - \frac{p_k}{q_k} \right| = \frac{1}{q_{k+1} q_k},$$

dove l'ultima identità segue dal Teorema (3.6). D'altro canto, se a, b, c, d sono quattro interi positivi, il rapporto $\frac{a+c}{b+d}$ è sempre compreso tra $\frac{a}{b}$ e $\frac{c}{d}$, per cui la sequenza:

$$\frac{p_k}{q_k}, \frac{p_k + p_{k+1}}{q_k + q_{k+1}}, \frac{p_k + 2p_{k+1}}{q_k + 2q_{k+1}}, \ldots, \frac{p_k + a_k\, p_{k+1}}{q_k + a_k\, q_{k+1}} = \frac{p_{k+2}}{q_{k+2}}$$

risulta monotona. Inoltre, $\frac{p_k}{q_k}$ e $\frac{p_{k+2}}{q_{k+2}}$ giacciono sempre dalla stessa parte rispetto a q, per cui:

$$\left|q - \frac{p_k}{q_k}\right| \geq \left|\frac{p_k + p_{k+1}}{q_k + q_{k+1}} - \frac{p_k}{q_k}\right| = \frac{1}{q_k(q_k + q_{k+1})},$$

dove l'ultima identità segue nuovamente dal Teorema (3.6). □

Corollario 3.9. *Se $\frac{p_k}{q_k}$ è il k-esimo convergente della frazione continua di $\alpha \in \mathbb{Q}^+$, che consta di almeno $k+2$ termini, si ha:*

$$|q_k\alpha - p_k| > |q_{k+1}\alpha - p_{k+1}|.$$

Dimostrazione. In virtù del Corollario (3.8), si ha:

$$|q_k\alpha - p_k| \geq \frac{1}{q_k + q_{k+1}} \geq \frac{1}{q_{k+2}} > |q_{k+1}\alpha - p_{k+1}|.$$

□

Teorema 3.10 (Hurwitz)**.** *Tra due convergenti successivi di $\alpha \in (\mathbb{R} \setminus \mathbb{Q})^+$, almeno uno soddisfa la disuguaglianza:*

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{2\,q^2}.$$

Dimostrazione. Supponiamo, per assurdo, che sia $\frac{p_k}{q_k}$ che $\frac{p_{k+1}}{q_{k+1}}$ violino la suddetta disuguaglianza. In tali ipotesi si ha:

$$\frac{1}{q_k q_{k+1}} = \left|\frac{p_k}{q_k} - \frac{p_{k+1}}{q_{k+1}}\right| = \left|\alpha - \frac{p_k}{q_k}\right| + \left|\alpha - \frac{p_{k+1}}{q_{k+1}}\right| \geq \frac{1}{2q_k^2} + \frac{1}{2q_{k+1}^2},$$

da cui segue:

$$2q_k q_{k+1} \geq q_k^2 + q_{k+1}^2,$$

ossia $0 \geq (q_{k+1} - q_k)^2$, che comporta $k = 0$ e $q_k = 1$: in tal caso, tuttavia, $\left|\alpha - \frac{p_0}{q_0}\right| < \frac{1}{2}$. □

Teorema 3.11 (Hurwitz)**.** *Tra tre convergenti successivi di $\alpha \in (\mathbb{R} \setminus \mathbb{Q})^+$, almeno uno soddisfa la disuguaglianza:*

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{\sqrt{5}\,q^2}.$$

Dimostrazione. Analogamente a prima, supponiamo che la disuguaglianza sia violata da tre convergenti successivi $\frac{p_k}{q_k}, \frac{p_{k+1}}{q_{k+1}}, \frac{p_{k+2}}{q_{k+2}}$. Valgono allora:

$$\frac{1}{q_k q_{k+1}} > \frac{1}{\sqrt{5}q_k^2} + \frac{1}{\sqrt{5}q_{k+1}^2}, \quad \frac{1}{q_{k+1} q_{k+2}} > \frac{1}{\sqrt{5}q_{k+1}^2} + \frac{1}{\sqrt{5}q_{k+2}^2},$$

per cui, posto $\lambda_1 = \frac{q_{k+1}}{q_k}$ e $\lambda_2 = \frac{q_{k+2}}{q_{k+1}}$, vale la disuguaglianza:

$$\lambda_i^2 - \sqrt{5}\lambda_i + 1 < 0,$$

da cui discende $\lambda_i \in \left(\frac{\sqrt{5}-1}{2}, \frac{\sqrt{5}+1}{2}\right)$. Ma allora:

$$\lambda_2 = \frac{q_{k+2}}{q_{k+1}} = a_{k+1} + \frac{1}{\lambda_1} > 1 + \frac{2}{\sqrt{5}+1} = \frac{\sqrt{5}+1}{2},$$

che contraddice quanto stabilito precedentemente. □

Teorema 3.12. *Se α è un numero irrazionale positivo e due interi coprimi p, q realizzano:*

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{2q^2},$$

allora $\frac{p}{q}$ è un convergente della frazione continua di α.

Dimostrazione. Sia $[a_0; a_1, \ldots, a_n]$ la frazione continua di $\frac{p}{q}$: valgono allora $p = p_n$ e $q = q_n$. Posto:

$$\beta = \frac{p_{n-1} - \alpha q_{n-1}}{\alpha q_n - p_n},$$

si ha:

$$\alpha = \frac{\beta p_n + p_{n-1}}{\beta q_n + q_{n-1}}, \tag{3.1}$$

e inoltre:

$$\left|\alpha - \frac{p}{q}\right| = \frac{1}{q_n(\beta q_n + q_{n-1})}.$$

Per ipotesi il membro destro è minore o uguale a $\frac{1}{2q_n^2}$, il che comporta:

$$\beta \geq 2 - \frac{q_{n-1}}{q_n} > 1.$$

Posto dunque $\beta = [a_{n+1}; \ldots]$, in virtù della (3.1) si ha che la frazione continua di α è data dalla concatenazione della frazione continua di $\frac{p}{q}$ con quella di β, ossia:

$$\alpha = [a_0; a_1, \ldots, a_n, a_{n+1}, \ldots],$$

il che prova che $\frac{p}{q}$ è un convergente di α. □

Teorema 3.13 (Hurwitz)**.**

Corollario 3.14. *Se due elementi di $\mathbb{Q}^+$ hanno in comune i primi n termini delle rispettive frazioni continue, distano meno di $\frac{2}{F_n^2}$, ove F_n è l'n-esimo numero di Fibonacci.*

Dimostrazione. Tale risultato è una diretta conseguenza del Corollario (3.8): se infatti $\alpha, \beta \in \mathbb{Q}^+$ hanno in comune i primi n termini delle rispettive frazioni continue, $a_0, \ldots, a_{n-1}$, allora hanno in comune anche i denominatori $k_0 = 1, \ldots, k_{n-1}$ dei primi n convergenti, e, detto $\gamma = [a_0; a_1, \ldots, a_{n-1}]$, vale:

$$|\alpha - \beta| \leq |\alpha - \gamma| + |\beta - \gamma| \leq \frac{2}{k_{n-1}^2} \leq \frac{2}{F_n^2}.$$

□

PROPRIETÀ DELLE FRAZIONI CONTINUE LETTE A ROVESCIO.
DEFINIZIONE DEI NUMERI DI FIBONACCI.

Esercizio 3.15. *Sia $[a_0; a_1, \ldots, a_n]$ la frazione continua associata a un numero razionale $\frac{p}{q} > 1$. Si determini la frazione continua di $\frac{p}{p-q}$.*

Hint: $\frac{p}{p-q} = 1 + \frac{1}{\frac{p}{q}-1}$.

FRAZIONI CONTINUE DEGLI ALGEBRICI DI GRADO 2.

Teorema 3.16. *Se α è un numero irrazionale positivo, $\frac{p_k}{q_k}$ è un convergente della sua frazione continua e due interi coprimi p, q realizzano:*

$$|q\alpha - p| < |q_k\alpha - p_k|,$$

allora si ha $q \geq q_{k+1}$.

Dimostrazione. □

Teorema 3.17. *Se un numero irrazionale positivo α e due interi coprimi p, q realizzano:*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2},$$

allora $\frac{p}{q}$ è un convergente della frazione continua di α.

Dimostrazione. Poiché i denominatori dei convergenti di α determinano una successione crescente, per un qualche numero naturale k si ha certamente:

$$q_k \leq q < q_{k+1}.$$

□

3.6 Algoritmo di Euclide e lemma di Bézout

Dati due numeri interi a e b, il loro *massimo comun divisore* è definito come:

$$\gcd(a, b) = \max\{d \in \mathbb{N} : d|a, d|b\},$$

e talvolta, per brevità, indicato semplicemente come (a, b). Notiamo che, per come abbiamo precedentemente definito il concetto di coprimalità, cui a, b coprimi $\iff \gcd(a, b) = 1$.
Qual è un algoritmo efficiente per la determinazione del massimo comun divisore?
Chiaramente la complessità del calcolo è limitata da $\min(a, b)$ test di divisibilità, in quanto

$$\gcd(a, b) \leq \min(a, b),$$

ma è possibile essere più astuti, semplicemente considerando il seguente

Lemma 3.18.

$$a > b,\ d|a,\ d|b \longrightarrow d|(a - b).$$

Dimostrazione.

$$d|a \longrightarrow a = d \cdot a_1,$$
$$d|b \longrightarrow b = d \cdot b_1,$$
$$a - b = d \cdot (a_1 - b_1).$$

□

Se, dati due numeri naturali positivi a e b definiamo $(a \bmod b)$ come il resto nella divisione intera di a per b, ossia:

$$a \bmod b = a - \left\lfloor \frac{a}{b} \right\rfloor b.$$

Notiamo che si ha $0 \leq (a \bmod b) \leq (b-1)$. Nelle ipotesi del lemma si verifica:

(Euclide). $\gcd(a,b) = \gcd(a-b,b) = \gcd(a \bmod b, b),$

osservazione che dà luogo all'algoritmo di Euclide:

$$\gcd(101,75) = \gcd(75,26) = \gcd(26,23) = \gcd(23,3) = \gcd(3,2) = 1,$$

tramite il quale è possibile calcolare il massimo comun divisore in modo molto più efficiente rispetto allo stilare elenchi di divisori.
Riportiamo un corollario immediato ma estremamente importante dell'algoritmo di Euclide:
interi consecutivi sono sempre coprimi. Vale inoltre il seguente risultato:

Teorema 3.19 (Bézout)**.** *Comunque dati due numeri naturali positivi a e b per cui si abbia $\gcd(a,b) = 1$, esistono due numeri naturali positivi c e d che realizzano:*

$$\begin{cases} c \cdot a - d \cdot b &= 1 \\ c &< b \\ d &< a. \end{cases}$$

Dimostrazione. Portiamo a termine l'algoritmo di Euclide per il calcolo del massimo comun divisore tenendo traccia dei quozienti parziali: poiché $\gcd(a,b) = 1$, l'algoritmo termina in un numero finito di passi, fornendo una scrittura del numero razionale $\frac{a}{b}$ in forma di frazione continua. Ad esempio:

$$\gcd(\overset{1}{101},75) = \gcd(\overset{2}{75},26) = \gcd(\overset{1}{26},23) = \gcd(\overset{7}{23},3) = \gcd(\overset{1}{3},2) = \gcd(\overset{2}{2},1) = 1$$

$$\frac{101}{75} = 1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{7 + \frac{1}{1 + \frac{1}{2}}}}}} = [1;2,1,7,1,2].$$

Tuttavia, se $\frac{x}{y}$ e $\frac{z}{w}$ sono convergenti successivi di una qualsiasi frazione continua, allora:

$$|x \cdot w - y \cdot z| = 1, \quad x < z, \quad y < w.$$

Consideriamo allora il numero razionale associato alla frazione continua di $\frac{a}{b}$, privata dell'ultimo termine. Nel nostro caso otteniamo, senza colpo ferire, una soluzione del sistema iniziale:

$$[1,2,1,7,1] = \frac{35}{26},$$

$$26 \cdot 101 - 35 \cdot 75 = 1;$$

e nel caso avessimo ottenuto una soluzione per $c \cdot a - d \cdot b = -1$ sarebbe stato sufficiente operare le sostituzioni $c \leftarrow (b - c), d \leftarrow (a - d)$. □

Lemma 3.20 (Euclide)**.** *Se n, a, b sono tre interi positivi tali per cui $\gcd(n, a) = 1$ e $n|(ab)$, allora $n|b$.*

Dimostrazione. In virtù del Teorema di Bézout esistono due interi positivi x, y per cui:

$$nx + ay = 1.$$

Moltiplicando ambo i membri per b, si ha:

$$nbx + aby = b.$$

n divide banalmente il primo addendo, e divide il secondo in quanto $n|(ab)$.
Segue che $n|b$, come volevasi dimostrare. □

Corollario 3.21. *Se un numero primo p divide il prodotto di due o più interi non nulli, p divide almeno uno dei fattori.*

Dimostrazione. Supponiamo $p|(a_1 \cdot \ldots \cdot a_{n-1} \cdot a_n)$. Se $p \nmid a_n$, $\gcd(p, a_n)$ è un divisore positivo di p diverso da p, ossia necessariamente 1. Il lemma precedente comporta allora $p|(a_1 \cdot \ldots \cdot a_{n-1})$, ed è semplice concludere per induzione su n. □

Muniti del Lemma di Euclide, notiamo, inoltre, che esiste un'unica coppia di interi (c, d) che soddisfa le richieste del Teorema di Bézout. Supponiamo, per assurdo, $(c_1, d_1) \neq (c_2, d_2)$ e

$$ac_1 - bd_1 = ac_2 - bd_2 = 1, \qquad 1 \leq c_1, c_2 \leq b, \qquad 1 \leq d_1, d_2 \leq a.$$

Per sottrazione si ha:

$$a(c_1 - c_2) = b(d_1 - d_2).$$

a divide il membro sinistro dell'ultima identità, dunque divide il destro. Poiché $\gcd(a, b) = 1$, si ha che a divide $|d_1 - d_2|$. Tuttavia $|d_1 - d_2| \leq (a - 1)$, per cui $a||d_1 - d_2| \Rightarrow d_1 = d_2$. Analogamente, $b||c_1 - c_2|$ comporta $c_1 = c_2$.

Notiamo inoltre che tutte le soluzioni intere (u, v) dell'equazione

$$u \cdot a - v \cdot b = 1$$

dipendono dalla soluzione fondamentale (c, d) determinata dal Teorema di Bézout attraverso le relazioni:

$$u = c + k \cdot b, \quad v = d + k \cdot a.$$

E' infatti immediato verificare che quelle appena riportate sono soluzioni, poiché:

$$a(c + kb) - b(d + ka) = ac - bd = 1.$$

Viceversa, se (u, v) è soluzione si ha:

$$(u - c) \cdot a = (v - d) \cdot b,$$

dunque a divide $(v - d)$ e b divide $(u - c)$, per cui u è della forma $k_1 b + c$ e v è della forma $k_2 a + d$. Ma allora:

$$1 = u \cdot a - v \cdot b = (k_1 - k_2)ab + (ac - bd) = (k_1 - k_2)ab + 1,$$

per cui $k_1 = k_2$.

Lemma 3.22. *Se a e b sono due interi non nulli,*

$$a\,\mathbb{Z} + b\,\mathbb{Z} = (a, b)\,\mathbb{Z}.$$

Dimostrazione. Poiché ogni elemento di $a\mathbb{Z}$, così come ogni elemento di $b\mathbb{Z}$, è multiplo di $\gcd(a, b)$, vale l'inclusione:

$$a\,\mathbb{Z} + b\,\mathbb{Z} \subseteq (a, b)\,\mathbb{Z},$$

per cui è sufficiente dimostrare l'inclusione opposta. Posto $A = \frac{a}{(a,b)}, B = \frac{b}{(a,b)}$, si ha $\gcd(A, B) = 1$, ed è sufficiente provare che ogni intero può essere espresso come $xA + yB$ per una qualche coppia di interi (x, y). D'altro canto, in virtù del Teorema di Bézout, l'intero 1 può essere certamente espresso in tale forma, per cui ogni intero può essere espresso in tale forma, e il Lemma è provato. □

ALBERO DI STERN-BROCOT E MAPPE BIETTIVE TRA $\mathbb{Q}$ ED $\mathbb{N}$, TRA $\mathbb{N}^{\mathbb{N}}$ E $\mathbb{R}$.

3.7 L'infinità dei numeri primi

Teorema 3.23. *L'insieme dei numeri primi è infinito.*

Dimostrazione. Di questo importante fatto riportiamo più dimostrazioni. La prima è dovuta ed Euclide. Supponiamo, per assurdo, che l'insieme dei numeri primi sia finito, costituito dagli elementi $p_1 < p_2 < \ldots < p_n$. Consideriamo il numero naturale:

$$N = 1 + \prod_{j=1}^{n} p_j.$$

Si ha certamente $N > p_n$, ma nessuno dei p_j con $1 \leq j \leq n$ può dividere N: l'insieme dei divisori di N è allora costituito unicamente da 1 e N. Ciò, tuttavia, comporta che N sia primo, contro l'assunzione che p_n fosse il più grande numero primo.

Una tecnica dimostrativa quasi analoga discende dalla considerazione che gli insiemi dei divisori primi di due numeri naturali consecutivi sono necessariamente disgiunti. In particolare, la sequenza definita da:

$$a_1 = n, \quad a_2 = n + 1, \quad a_{k+1} = 1 + \prod_{j=1}^{k} a_j,$$

con $n \geq 2$, ha la proprietà che ogni a_k ammette almeno un divisore primo che non divide alcuno degli a_j precedenti. Segue che i numeri primi devono essere almeno tanti quanti i termini della successione, ossia

infiniti.

Una terza strada consiste nell'esibire una sequenza infinita di numeri naturali coprimi a 2 a 2: se i numeri primi fossero finiti, una sequenza con tale proprietà non potrebbe certamente esistere. Si consideri, ad esempio, la sequenza definita da $a_j = 2^{2^j} + 1$. Se $k > j$, si ha:

$$a_k = (a_j - 1)^{2^{k-j}} + 1,$$

dunque:

$$\gcd(a_j, a_k) = \gcd(a_j, 2) = 1.$$

Una quarta strada è quella di considerare che la più grande potenza di un primo p che divide $n!$ ha esponente pari a:

$$\sum_{j=1}^{+\infty} \left\lfloor \frac{n}{p^j} \right\rfloor.$$

Tale esponente risulta superiormente limitato dalla quantità $\frac{n}{p-1}$, dunque, a maggior ragione, da n. Se i numeri primi fossero finiti e il loro prodotto fosse pari a P, per ogni numero naturale n si avrebbe allora:

$$n! \leq P^n,$$

ma tale disuguaglianza è falsa già quando $n \geq 3P$. Questo tipo di approccio precorre di fatto le idee contenute nella dimostrazione dovuta a Chebyshev del postulato di Bertrand.

Una quinta dimostrazione è dovuta a Dustin J. Mixon. Supponiamo per assurdo che i numeri primi siano finiti, $p_1 < \ldots < p_N$. Preso un numero naturale K abbastanza grande da garantire che si abbia $2^K > 1 + (K+1)^N$, consideriamo la funzione

$$f : [2, 2^K] \to [0, K]^N$$

che associa ad un numero naturale n la N-upla $(k_1, \ldots, k_N)$ data dalla fattorizzazione di n in primi:

$$n = p_1^{k_1} \cdot \ldots \cdot p_N^{k_N}.$$

Non può aversi $k_j > K$, altrimenti si avrebbe $n > 2^K$. D'altro canto, la cardinalità del dominio di f è più grande di quella dell'immagine, per cui f non può essere iniettiva: la supposizione che esistano solo una quantità finita di numeri primi va dunque a contradddire il teorema di fattorizzazione unica. □

3.8 Il Teorema di fattorizzazione unica

Teorema 3.24. *Dato un numero naturale $n > 2$, esiste un unico insieme $\mathcal{P}_n = \{p_1, \ldots, p_k\} \subset \mathcal{P}$ e un unico insieme $\{m_1, \ldots, m_k\} \subset \mathbb{N}_0^k$ per cui si ha:*

$$n = p_1^{m_1} \cdot \ldots \cdot p_k^{m_k}.$$

In tale contesto definiamo le funzioni aritmetiche ω e Ω nel modo seguente:

$$\omega(n) = k, \qquad \Omega(n) = \sum_{j=1}^{k} m_j.$$

Dimostrazione. L'esistenza di una fattorizzazione è garantita dal seguente algoritmo:

- Si elencano i divisori di n ad eccezione di 1 ed n;
- Se non se ne trovano, allora n è primo: si ritorna tale primo;
- Se $d > 1$ è un divisore proprio di n, si ritorna una fattorizzazione di d per una fattorizzazione di $\frac{n}{d}$.

Poiché i fattori di cui andiamo a considerare le fattorizzazioni sono più piccoli del numero di partenza, l'algoritmo termina necessariamente: l'esistenza di una fattorizzazione è garantita, non resta che provarne l'unicità. Supponiamo che si abbia:

$$p_1^{m_1} \cdot \ldots \cdot p_k^{m_k} = n = q_1^{u_1} \cdot \ldots \cdot q_l^{u_l},$$

ove i q_j sono tutti primi e costituiscono l'insieme $\mathcal{Q}_n \subset \mathcal{P}$. Abbiamo visto che se un numero primo divide un prodotto deve necessariamente dividere uno dei fattori: questo comporta che gli insiemi $\mathcal{P}_n$ e $\mathcal{Q}_n$ debbano necessariamente coincidere. In tal caso si ha:

$$p_1^{m_1} \cdot \ldots \cdot p_k^{m_k} = n = p_1^{u_1} \cdot \ldots \cdot p_k^{u_k}.$$

Supponiamo che per un qualche $j \in [1, k]$ si abbia $m_j \neq u_j$: in tal caso, dividendo il membro destro e il membro sinistro della precedente identità per $p_j^{\min(u_j, m_j)}$, si ottiene da una parte un multiplo di p_j e dall'altro un numero che non è diviso da p_j, con un assurdo che conclude la dimostrazione. □

Definizione 3.25. *Dato un numero primo p e un intero non nullo n, definiamo ora l'altezza o norma p-adica di n, in simboli $\nu_p(n)$, come:*

$$\nu_p(n) = \max\{a \in \mathbb{N} : p^a \mid n\}.$$

Siano ora a e b due interi positivi. Invitiamo il lettore a dimostrare i seguenti risultati:

- $\nu_p(a \pm b) \geq \min(\nu_p(a), \nu_p(b))$,
- $\nu_p(a \cdot b) = \nu_p(a) + \nu_p(b)$,
- $\gcd(a, b) = \prod_{p \in \mathcal{P}} p^{\min(\nu_p(a), \nu_p(b))}$.

Lemma 3.26. *Se d, n sono numeri naturali maggiori di 2 e vale $d|n$, i divisori primi di d costituiscono un sottoinsieme dei divisori primi di n. In tali ipotesi, per ogni numero primo p che divide n si ha $\nu_p(d) \leq \nu_p(n)$. Inoltre, ogni divisore di n è della forma*

$$d = \prod_{p_i \in I} p_i^{\nu_i},$$

dove

$$I \subseteq \{p \in \mathcal{P} : p|n\}, \qquad \nu_i \leq \nu_{p_i}(n).$$

Dimostrazione. La prima asserzione è giustificata dalla transitività della divisibilità: se $p|d$ e $d|n$, necessariamente $p|n$. Analogamente, se $p^a|d$ e $d|n$, allora $p^a|n$, per cui $\nu_p(n) \geq \nu_p(d)$. In ultima istanza, se $I \subseteq \{p \in \mathcal{P} : p|n\}$ e per ogni $i \in [1, |I|]$ si ha $\nu_i \leq \nu_{p_i}(n)$, allora:

$$\frac{n}{\prod_{p_i \in I} p_i^{\nu_i}} = \prod_{p|n} p^{\nu_p(n) - \nu_p(d)} \in \mathbb{N},$$

per cui $d|n$. □

Se $p_1, p_2, \ldots, p_{\omega(n)}$ sono i divisori primi di n, abbiamo allora che i divisori di n sono in corrispondenza biunivoca con gli elementi dell'insieme:

$$[0, \nu_{p_1}(n)] \times \ldots \times [0, \nu_{p_{\omega(p)}}(n)],$$

di cardinalità

$$\prod_{n=1}^{\omega(n)} (1 + \nu_{p_i}(n)) .$$

Se denotiamo con $d(n)$ il numero di divisori positivi di n, abbiamo allora:

$$d(n) = \prod_{n=1}^{\omega(n)} (1 + \nu_{p_i}(n)) \geq 2^{\omega(n)}.$$

Proviamo che la funzione $d : \mathbb{N} \to \mathbb{N}$ ha un'importante proprietà: se a e b sono due interi positivi coprimi,

$$d(ab) = d(a) \cdot d(b).$$

Dimostrazione. È sufficiente provare che ogni divisore di ab può essere associato in modo biunivoco a una coppia di interi positivi, che sono l'uno un divisore di a e l'altro un divisore di b - questi due insiemi sono disgiunti, in quanto $\gcd(a, b) = 1$. L'associazione più naturale:

$$d \longrightarrow (\gcd(a, d), \gcd(b, d))$$

è effettivamente biunivoca, in virtù del fatto che:

$$d|ab \quad \Longrightarrow \quad d = \gcd(a, d) \cdot \gcd(b, d).$$

Sia infatti $\mathcal{P}_A$ l'insieme dei divisori primi di a e $\mathcal{P}_B$ l'insieme dei divisori primi di b. Poiché, in virtù del Lemma di Euclide, ogni divisore primo di n deve appartenere necessariamente a $\mathcal{P}_A$ o a $\mathcal{P}_B$, e poiché tali insiemi sono disgiunti, si ha:

$$\{p \in \mathcal{P} : p|n\} = \mathcal{P}_A \cup \mathcal{P}_B.$$

Dato che i divisori primi di d sono un sottoinsieme dei divisori primi di n, è sempre possibile partizionarli a seconda che appartengano a $\mathcal{P}_A$ oppure a $\mathcal{P}_B$:

$$\prod_{p|d} p^{\nu_p(d)} = \left(\prod_{\substack{p|d \\ p \in \mathcal{P}_A}} p^{\nu_p(d)} \right) \cdot \left(\prod_{\substack{p|d \\ p \in \mathcal{P}_B}} p^{\nu_p(d)} \right).$$

Dato che, indipendentemente dall'appartenenza a $\mathcal{P}_A$ o a $\mathcal{P}_B$, ogni divisore primo primo di d realizza $\nu_p(d) \leq \nu_p(n)$,

$$\gcd(d, a) = \prod_{\substack{p|d \\ p \in \mathcal{P}_A}} p^{\min(\nu_p(d), \nu_p(a))} = \prod_{\substack{p|d \\ p \in \mathcal{P}_A}} p^{\min(\nu_p(d), \nu_p(n))} = \prod_{\substack{p|d \\ p \in \mathcal{P}_A}} p^{\nu_p(d)},$$

e l'uguaglianza $d = \gcd(a, d) \cdot \gcd(b, d)$ è provata. □

Chiamiamo *moltiplicativa* una qualunque funzione $f : \mathbb{N} \to \mathbb{N}$ che goda di tale proprietà, e *completamente moltiplicativa* una qualunque funzione $g : \mathbb{N} \to \mathbb{N}$ che realizza $g(ab) = g(a) \cdot g(b)$ per qualunque coppia (a, b) di interi positivi. In virtù del Teorema di fattorizzazione unica, i valori assunti da una funzione moltiplicativa su $\mathbb{N}$ dipendono unicamente dai valori assunti sulle potenze dei primi, mentre i valori assunti da una funzione completamente moltiplicativa dipendono unicamente dai valori assunti sui primi:

$$f(n) = \prod_{p|n} f(p^{\nu_p(n)}), \qquad g(n) = \prod_{p|n} g(p)^{\nu_p(n)}.$$

Dato che abbiamo provato che la funzione $d : \mathbb{N} \to \mathbb{N}$ è moltiplicativa, e dato che l'insieme dei divisori di p^a è costituito dagli $(a+1)$ interi $1, p, \ldots, p^a$, abbiamo una riprova di quanto già dimostrato:

Corollario 3.27.

$$d(n) = \prod_{p|n} (\nu_p(n) + 1)\,.$$

Poiché per ogni numero naturale positivo n si ha $2^n \geq n+1$, vale:

$$d(n) \leq \prod_{p|n} 2^{\nu_p(n)} = 2^{\Omega(n)},$$

donde:

$$2^{\omega(n)} \leq d(n) \leq 2^{\Omega(n)}.$$

ACHTUNG: BISOGNA INTRODURRE ALMENO IL CONCETTO DI POLINOMIO, SE NON GIÀ QUELLO DI ANELLO. PER GIUSTIFICARE IL FATTO CHE UN POLINOMIO NON PUÒ AVERE PIÙ RADICI DEL SUO GRADO, BISOGNA INTRODURRE RUFFINI O IL CONCETTO DI INTEGRITÀ DI UN ANELLO.

Teorema 3.28 (Legendre)**.** *Nessun polinomio non constante a coefficienti interi può assumere su* $\mathbb{N}$ *unicamente valori primi.*

Dimostrazione. Posto che si abbia $q(1) = p$, in virtù del fatto che per ogni coppia (x, y) di interi distinti si ha $(x-y)|(p(x)-p(y))$, p divide $q(kp+1)$ per ogni intero k. Ma in tal caso $q(x)$ assume il valore p infinite volte, e ciò può accadere solo se $q(x)$ è costantemente uguale a p. □

UNA PARENTESI SULLA DIFFICOLTÀ DEL PROBLEMA DI FATTORIZZAZIONE. ALGORITMO DI NEWTON. PIÙ AVANTI, QUADRATIC SIEVE. TEST DI PRIMALITÀ.

3.9 Nozioni fondamentali sui gruppi

Un *gruppo* è un insieme G dotato di un'operazione binaria associativa $\circ : G \times G \to G$, ove

- $\exists e \in G : \ \forall g \in G,\ e \circ g = g \circ e = g$;
- $\forall (g,h) \in G \times G,\ g \circ h \in G$;
- $\forall g \in G\ \exists h \in G : \ g \circ h = e$.

Un gruppo si dice *commutativo* (o *abeliano*) se tale è l'operazione $\circ$, ossia se

$$\forall (g,h) \in G \times G, \quad g \circ h = h \circ g.$$

L'*ordine* di un gruppo è la sua cardinalità; H si dice *sottogruppo* di G, in simboli $H \leq G$, se è al contempo un gruppo rispetto a $\circ$ e un sottoinsieme di G. Il sottogruppo generato da un elemento g, in simboli $< g >$, è dato da[2]:

$$< g >= \{\ldots, g^{-1} \circ g^{-1},\ g^{-1}, e,\ g,\ g \circ g,\ g \circ g \circ g, \ldots\}.$$

L'*ordine di un elemento* è l'ordine del sottogruppo generato, e un gruppo si dice *ciclico* se è generato da un certo elemento g, che in tal caso viene detto *generatore*. Uno strumento fondamentale nella teoria dei gruppi è il

Teorema 3.29 (Lagrange). *Se G è un gruppo finito, l'ordine di ogni suo elemento divide l'ordine del gruppo:*

$$o(g) \mid o(G).$$

Dimostrazione. Osserviamo preliminarmente che $o(g)$ è finito, e che

$$g^a = g^b,\ a > b \longrightarrow\ g^{a-b} = e$$

garantisce che valga l'identità:

$$o(g) = \min\{n \in \mathbb{N} \setminus \{0\} :\ g^n = e\}.$$

Proviamo ora che $g^{o(G)} = e$. Nel caso di gruppi abeliani è sufficiente considerare che, fissato $g \in G$, la mappa

$$x \to x \circ g$$

manda iniettivamente G in se stesso, alché il prodotto degli elementi nell'immagine coincide con il prodotto degli elementi del dominio:

$$\prod_{h \in G} h = \prod_{h \in G} h \circ g = g^{o(G)} \prod_{h \in G} h$$

e la tesi segue immediatamente. A questo punto:

$$g^{o(g)} = e,\ g^{o(G)} = e \ \to g^{\gcd(o(g), o(G))} = e \ \to o(g) = \gcd(o(g), o(G)) \ \to o(g) \mid o(G).$$

Nel caso di gruppi non abeliani è opportuno definire il concetto di *laterale sinistro*:

$$aH \doteqdot \{a \circ h : h \in H\}.$$

Per ogni elemento $a \in G$, il laterale $a < g >$ consta di $o(g)$ elementi; ogni elemento di G appartiene ad un laterale della suddetta forma (in particolare $h \in (hg^{-1}) < g >$) e, inoltre:

$$a \in b < g > \to a = b \circ g^m \to a < g >= b < g >;$$

segue che tutti i possibili laterali sinistri distinti della forma $a < g >$ partizionano G come insieme, e dunque:

$$o(g) \mid o(G)$$

come voluto. □

Altri risultati notevoli sono i seguenti:

[2] Denotiamo con g^{-1} l'inverso di g, ossia l'unico $h \in G :\ h \circ g = e$.

Teorema 3.30. *Se $H \leq G$, $o(H) \mid o(G)$.*

Dimostrazione. E' sufficiente partizionare G in laterali di H come già fatto per il Teorema di Lagrange. □

Teorema 3.31. *Ogni gruppo avente per ordine un numero primo è ciclico.*

Dimostrazione. Preso $g \in G$ diverso dall'elemento neutro, $o(g) = p$ per il Teorema di Lagrange, dunque $< g >= G$. □

Teorema 3.32 (Cauchy)**.** *Se G è un gruppo finito, per ogni primo p che divida l'ordine di G esiste un elemento $g \in G$ che realizza $o(g) = p$.*

Dimostrazione. Chiamiamo X l'insieme delle p-uple $(g_1, \ldots, g_p)$ di elementi di G con la proprietà:

$$g_1 \cdot g_2 \cdot \ldots \cdot g_p = e.$$

La cardinalità di X è pari a $o(G)^{p-1}$, in quanto possiamo liberamente scegliere le prime $p-1$ componenti di ogni p-upla, e a tal punto la scelta dell'ultima componente è forzata. In particolare, p divide $|X|$. Diciamo ora che due p-uple sono equivalenti se si corrispondono a meno di una rotazione delle componenti:

$$(g_1, \ldots, g_{p-1}, g_p) \sim (g_p, g_1, \ldots, g_{p-1}).$$

Questa è chiaramente una relazione di equivalenza tra gli elementi di X, e la classe di equivalenza di ogni elemento può avere unicamente cardinalità p o cardinalità 1; quest'ultima eventualità si verifica quando tutte le componenti di una p-upla sono tra loro uguali. Poiché le classi di equivalenza partizionano l'insieme X e la p-upla $(e, \ldots, e) \in X$ ha una classe d'equivalenza costituita da un solo elemento, esistono almeno altre $p-1$ classi di equivalenza con cardinalità 1: ciò comporta che in G vi siano almeno $p-1$ elementi di ordine p. □

3.10 Gruppi notevoli e congruenze

Preso un numero naturale $m \geq 2$, consideriamo la relazione di equivalenza[3] $\equiv_m$ su $\mathbb{Z}$ definita come segue:

$$a \equiv_m b \iff m|(a-b);$$

l'insieme quoziente

$$\mathbb{Z}/_{\equiv_m} = \{[0], [1], \ldots, [m-1]\}$$

si denota usualmente con

$$\mathbb{Z}/_{m\mathbb{Z}},$$

inoltre la relazione[4] $a \equiv_m b$ si scrive più comunemente come

$$a \equiv b \pmod{m}$$

[3] *Semel in vita*, è opportuno verificare che sia tale.
[4] "a e b hanno in medesimo resto nella divisione per m", ossia $(a-b) \in [0]$.

e le classi di equivalenza sono anche dette *classi residue modulo* m. Quello che ha rilevanza cruciale è che

$$(\mathbb{Z}/_{m\mathbb{Z}}, +)$$

è un gruppo ciclico (dunque abeliano) di ordine m, in quanto

- l'usuale operazione di somma è *compatibile* con il passaggio al quoziente, ossia $x \in [y], z \in [w] \to (x+z) \in [y+w]$;
- la classe $[0] = [m]$ è elemento neutro;
- l'inverso della classe $[a]$ è la classe $[m-a]$;
- $[1]^k = [1] + [1] + \ldots + [1] = [k]$.

Se ora introduciamo la funzione *totient* di Eulero attraverso

$$\varphi(n) = |\{1 \leq a < n : \ \gcd(a,n) = 1\}|$$

abbiamo che nel gruppo additivo $\mathbb{Z}/_{m\mathbb{Z}}$ vi sono esattamente $\varphi(d)$ elementi di ordine d per ogni intero d che divida m, ordine del gruppo, da cui:

- $(\mathbb{Z}/_{m\mathbb{Z}}, +)$ ha esattamente $\varphi(m)$ generatori;
- $\forall m \in \mathbb{N}, \ m = \sum_{d|m} \varphi(d)$.

Analogamente, preso un numero naturale m, l'insieme dei numeri coprimi con m, quozientato rispetto alla relazione $\equiv_m$, si denota con

$$\mathbb{Z}/_{m\mathbb{Z}}{}^*$$

e tale insieme risulta un gruppo abeliano rispetto all'usuale prodotto, in quanto:

- il prodotto di due interi coprimi con m è coprimo con m (supposto infatti $d|m$ e $p|m|ab$ si ha $p|a$ o $p|b$, entrambe impossibili in quanto $p|a, p|m \to p|\gcd(a,m) = 1$) e tale condizione non muta sommando o sottraendo multipli di m;
- il prodotto è compatibile con $\equiv_m$ in quanto $(k_1 m + a) \cdot (k_2 m + b) = (k_1 k_2 m + a k_2 + b k_1) \cdot m + ab$ ed è dunque lecito scrivere $[a] \cdot [b] = [ab]$;
- la classe $[1]$ è elemento neutro per il prodotto;
- l'inverso della classe $[a]$ è rintracciabile attraverso l'algoritmo di Euclide: per il lemma di Bèzout esistono infatti $k_1 < a$ e $k_2 < m$ per cui $k_1 \cdot m - k_2 \cdot a = -1$, e da tale identità si deduce $m|(k_2 a - 1)$, ossia $[k_2 a] = [1]$, ossia $[k_2] = [a]^{-1}$.

Nel caso in cui $m = p \in \mathcal{P}$ avvengono diversi fatti interessanti:

Lemma 3.33 (piccolo Teorema di Fermat)**.** $a^p \equiv a \pmod{p}$

Dimostrazione. $\mathbb{Z}/_{p\mathbb{Z}}{}^*$ è un gruppo di ordine $p-1$, dunque per il Teorema di Lagrange ogni intero a non divisibile per p realizza $a^{p-1} \equiv 1 \pmod{p}$. □

Lemma 3.34 (Wilson)**.** $n \in \mathcal{P} \iff n|\,((n-1)! + 1)$

Dimostrazione. Supponiamo che un numero primo p divida propriamente n: in tal caso $p \leq n-1$ e dunque $p|(n-1)!$, da cui l'impossibilità di $p|n|\left((n-1)!+1\right)$. Viceversa, consideriamo ${\mathbb{Z}/_{p\mathbb{Z}}}^*$: ogni classe $[a]$ è distinta dalla propria inversa, eccetto le classi $[1]$ e $[p-1]$, dunque

$$[(p-1)!] = [1]\cdot[2]\cdot\ldots\cdot[p-2]\cdot[p-1] = [1]\cdot[p-1]$$

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

□

Lemma 3.35. *${\mathbb{Z}/_{p\mathbb{Z}}}^*$ è un gruppo ciclico.*

Dimostrazione. La tesi è semplice da provare nei casi $p=2$ o $p=3$ per diretta costruzione della tabella moltiplicativa, possiamo dunque supporre $p \geq 5$. Proviamo ora che in ${\mathbb{Z}/_{p\mathbb{Z}}}^*$ vi sono al più $\varphi(d)$ elementi di ordine d per ogni numero naturale d che sia un divisore proprio dell'ordine del gruppo. Poichè possiamo dotare ${\mathbb{Z}/_{\equiv_p}}$ sia di struttura additiva che moltiplicativa, l'anello dei polinomi a coefficienti in ${\mathbb{Z}/_{p\mathbb{Z}}}$, che si denota con

$$\mathbb{F}_p[x]$$

eredita da $\mathbb{Z}[x]$, anello dei polinomi a coefficienti interi, la proprietè di essere *euclideo*:

$$\exists \partial : \mathbb{F}_p[x] \to \mathbb{N} \text{ tale che } \forall u, v \in \mathbb{Z}[x]\ \exists\, k, r \in \mathbb{Z}[x] : u - k\cdot v = r, \partial r < \partial v,$$

ove la funzione ∂ viene detta *grado*, e nel nostro caso coincide con l'usuale definizione di grado di un polinomio. Si ha in particolare che:

- $x^p - x \equiv \prod_{g\in{\mathbb{Z}/_{p\mathbb{Z}}}}(x-g) \pmod{p}$;
- per ogni elemento $u \in \mathbb{F}_p[x]$, il numero di radici in ${\mathbb{Z}/_{p\mathbb{Z}}}$ di u non supera il grado di u.

Proviamo ora che tutti gli elementi di ordine d in ${\mathbb{Z}/_{p\mathbb{Z}}}^*$, con d divisore proprio di $\varphi(p) = p-1$, sono radici di un elemento di $\mathbb{F}_p[x]$ di grado $\varphi(d)$. Si ha infatti:

$$o(g) = d \longrightarrow g^d - 1 \equiv 0 \pmod{p} \text{ e } \forall q \neq d : q|d,\ \ g^q - 1 \not\equiv 0 \pmod{p}.$$

Tuttavia se u e v sono due elementi di un anello euclideo di polinomi, e le radici di u sono un sottoinsieme delle radici di v, allora u divide v, ossia esiste w tale che $v = u\cdot w$. Introduciamo ora la funzione di Möebius $\mu(n) : \mathbb{N} \to \{-1, 0, 1\}$:

$$\mu(1) = 1, \quad \forall p \in \mathcal{P}\ \mu(p) = -1 \text{ e } \forall n > 1\ \mu(p^n) = 0, \quad \gcd(a,b) = 1 \to \mu(a\cdot b) = \mu(a)\cdot\mu(b).$$

Questa funzione gode di un'interessante proprietè:

$$\sum_{d|n}\mu(d) = \begin{cases} 1 & \text{se } n = 1 \\ 0 & \text{altrimenti} \end{cases},$$

dalla quale segue, per il principio di inclusione-esclusione, che ogni elemento di ordine d in ${\mathbb{Z}/_{p\mathbb{Z}}}^*$ è radice del polinomio

$$p_d(x) = \frac{\prod_{q|d:\mu(q)=1}(x^{d/q}-1)}{\prod_{q|d:\mu(q)=-1}(x^{d/q}-1)} \in \mathbb{F}_p[x].$$

Ora la funzione grado soddisfa $\partial(u\cdot v) = \partial u + \partial v$, dunque

$$\partial p_d = d\sum_{q|d}\frac{\mu(q)}{q},$$

ma è certamente lecito restringere la somma nel membro destro ai divisori di d della forma $p_1 \cdot p_2 \cdot \ldots \cdot p_k$, in quanto la funzione di Möebius è nulla sugli interi che sono multipli di un quadrato di un primo. Segue:

$$d \sum_{q|d} \frac{\mu(q)}{q} = d \cdot \prod_{p \in \mathcal{P}: p|d} \left(1 - \frac{1}{p}\right) = \varphi(d),$$

dunque in $G = \mathbb{Z}/_{p\mathbb{Z}}{}^*$ non possono esistere più di $\varphi(d)$ elementi di ordine d. Ricordando ora che

$$o(G) = p - 1 = \sum_{d|(p-1)} \varphi(d),$$

abbiamo che in G vi sono almeno $\varphi(p-1) > 1$ generatori, ed in realtè ve ne sono esattamente $\varphi(p-1)$, in quanto l'esistenza di un singolo generatore garantisce che in G vi siano esattamente $\varphi(d)$ elementi di ordine d. In particolare:

$$o(g) = p - 1,\ \gcd(n, p-1) = 1 \ \longrightarrow\ o(g^n) = p - 1.$$

□

Provata dunque l'esistenza di un generatore in $\mathbb{Z}/_{p\mathbb{Z}}{}^*$, ci chiediamo quale sia un algoritmo efficiente per determinarne esplicitamente uno. Al giorno d'oggi si ritiene che la scansione sequenziale delle classi $[2], [3], \ldots$ attraverso il criterio:

$$\forall q \in \mathcal{P} : q|(p-1) \quad g^{\frac{p-1}{q}} \not\equiv 1 \pmod{p} \iff o(g) = p - 1$$

sia la migliore strada perseguibile, in quanto Chen ha provato che, assumendo l'ipotesi di Riemann generalizzata, per p sufficientemente grande, esiste un generatore di $\mathbb{Z}/_{p\mathbb{Z}}{}^*$ entro le prime $2\log^2 p$ classi.

Rimuovendo ora l'ipotesi di primalitè di m, resta il fatto che $\mathbb{Z}/_{m\mathbb{Z}}{}^*$ è un gruppo abeliano di ordine $\varphi(m)$, da cui, come conseguenza del Teorema di Lagrange, il seguente

Lemma 3.36 (Eulero)**.**

$$m \nmid a \ \rightarrow\ a^{\varphi(m)} \equiv 1 \pmod{m}.$$

E' inoltre interessante ricordare che:

Lemma 3.37. *Preso un numero naturale $m > 1$, nè pari nè divisibile per 5, la lunghezza del periodo dell'espressione decimale del numero $\frac{1}{m}$ è un divisore di $\varphi(m)$, in particolare coincide con l'ordine della classe $[10]$ in $\mathbb{Z}/_{m\mathbb{Z}}{}^*$.*

Dimostrazione. Detta l la lunghezza del periodo si ha $m|(10^l - 1)$, ed anzi l è il minimo intero per cui ciè accade, da cui, immediatamente, la tesi. □

E' a questo punto lecito chiedersi se e quando $\mathbb{Z}/_{m\mathbb{Z}}{}^*$ sia un gruppo ciclico. Valgono i seguenti risultati:

Lemma 3.38. *$\mathbb{Z}/_{m\mathbb{Z}}{}^*$ è un gruppo ciclico se e solo se $m = 2, 4, 2\,p^n$ o p^n per p primo dispari.*

Dimostrazione. Forniamo solo uno sketch della dimostrazione, rimandando ai riferimenti bibliografici per ulteriori delucidazioni. Se m è prodotto di due distinti primi dispari p e q, per ogni intero a coprimo con m si ha:

$$a^{p-1} \equiv 1 \pmod{p} \qquad a^{q-1} \equiv 1 \pmod{q}$$

dunque $a^{\gcd(p-1,q-1)} \equiv 1 \pmod{m}$ e il massimo ordine di un elemento di $\mathbb{Z}/_{m\mathbb{Z}}{}^*$ è al più metè dell'ordine del gruppo. I casi $m = 2$ ed $m = 4$ sono banali e il caso $m = 2\,p^n$ è sostanzialmente analogo al caso $m = p^n$, mentre nel caso $m = p^n$ si fa ricorso alla tecnica del *sollevamento henseliano*: un generatore per

$\mathbb{Z}/_{p^h\mathbb{Z}}{}^*$ può essere traslato fino a ottenere un generatore di $\mathbb{Z}/_{p^{h+1}\mathbb{Z}}{}^*$.
Proviamo il passo base dell'induzione: sia g un generatore (ossia un elemento di ordine massimo) di $\mathbb{Z}/_{p\mathbb{Z}}{}^*$. Si ha:

$$\left|\mathbb{Z}/_{p^2\mathbb{Z}}{}^*\right| = \varphi(p^2) = p(p-1).$$

Per ogni numero primo q che divide $(p-1)$ si ha:

$$g^{\frac{p(p-1)}{q}} \not\equiv 1 \pmod{p^2},$$

in quanto:

$$g^{\frac{p(p-1)}{q}} \equiv g^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}$$

è un'identità assicurata dal fatto che g è generatore di $\mathbb{Z}/_{p\mathbb{Z}}{}^*$. Tale identità continua inoltre ad essere verificata rimpiazzando g con $g+kp$. Consideriamo allora $g^{(p-1)} \pmod{p^2}$: se questa quantitè è diversa da 1, g è un generatore per $\mathbb{Z}/_{p^2\mathbb{Z}}{}^*$. In caso contrario, facendo ricorso al binomio di Newton, si ha:

$$(g+kp)^{p-1} \equiv g^{p-1} + kp(p-1)g^{p-2} \equiv 1 - p\,k\,g^{-1} \pmod{p^2}.$$

In tal caso, appena $k \not\equiv 0 \pmod{p}$, l'ultimo addendo del membro destro è non nullo, e ciè permette di concludere che $g+kp$ è un generatore di $\mathbb{Z}/_{p^2\mathbb{Z}}{}^*$. La tecnica del sollevamento henseliano permette inoltre di provare che: □

Lemma 3.39. *Preso $n \geq 3$, il massimo ordine di un elemento di $\mathbb{Z}/_{2^n\mathbb{Z}}{}^*$ è pari a 2^{n-2}, ossia a metè dell'ordine del gruppo; inoltre la classe $[5]$ ha esattamente tale ordine, ed ogni elemento di $\mathbb{Z}/_{2^n\mathbb{Z}}{}^*$ puè essere espresso come $[\pm 5^k]$.*

Esaminiamo ora, attraverso alcuni esempi, delle proprietè generali delle *congruenze*, ossia delle identità che hanno luogo dall'applicazione della relazione $\equiv_m$. Consideriamo in primo luogo equazioni di primo grado della forma $a \cdot x + b \equiv 0 \pmod{m}$:

$$2 \cdot x + 15 \equiv -1 \pmod{101}.$$

Per compatibilitè del prodotto e della somma con la relazione di equivalenza $\equiv_{101}$ è lecito scrivere:

$$[2] \cdot [x] + [15] = [100], \qquad [2] \cdot [x] = [85].$$

Poichè 101 è un numero primo, ogni classe distinta dalla classe $[0]$ è invertibile (moltiplicativamente), da cui:

$$[x] = [85] \cdot [2]^{-1}.$$

Per ogni p primo dispari, l'inversa della classe $[2]$ in $\mathbb{Z}/_{p\mathbb{Z}}{}^*$ è la classe $\left[\frac{p+1}{2}\right]$, dunque:

$$[x] = [85] \cdot [51] = [4335] = [93] \qquad x \equiv 93 \pmod{101},$$

risultato a cui saremmo potuti pervenire in maniera più rapida attraverso:

$$[x] = [-16] \cdot [2]^{-1} = [-8] = [93].$$

Ma come trattare le congruenze lineari nel caso in cui appaiano classi non invertibili?
I due risultati che seguono sono fondamentali:

Lemma 3.40.

$$a \cdot x \equiv 0 \pmod{ab} \iff x \equiv 0 \pmod{b}.$$

Lemma 3.41. *Se* $\gcd(a,b)=1$, *allora*

$$x \equiv m \pmod{ab} \longleftrightarrow \begin{cases} x \equiv m \pmod{a} \\ x \equiv m \pmod{b} \end{cases}$$

Consideriamo, ad esempio, l'equazione

$$6x \equiv -11 \pmod{70}.$$

La classe $[6]$ non appartiene al gruppo $\mathbb{Z}/_{70\mathbb{Z}}{}^*$ in quanto $\gcd(6,70)=2\neq 1$, tuttavia l'equazione risulta equivalente al sistema

$$\begin{cases} 6x+11 \equiv 0 \pmod{2} \\ 6x+11 \equiv 0 \pmod{35} \end{cases}$$

che è impossibile, visto che la prima equazione si riduce a $1\equiv 0 \pmod 2$.
In generale, un'equazione della forma

$$ax+b\equiv 0 \pmod{p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}}$$

risulta equivalente ad un sistema di equazioni del tipo

$$ax+b\equiv 0 \pmod{p_i^{\alpha_i}}.$$

Se $p_i \nmid a$, la classe $[a]$ appartiene a $\mathbb{Z}/_{p_i^{\alpha_i}\mathbb{Z}}{}^*$, e si ha $x\equiv -b\cdot a^{-1} \pmod{p_i^{\alpha_i}}$. Se $p_i|a$ ma $p_i\nmid b$, l'equazione è impossibile; se $p_i|a$ e $p_i|b$ l'equazione è equivalente a

$$\frac{a}{p_i}\cdot x+\frac{b}{p_i}\equiv 0 \pmod{p_i^{\alpha_i-1}};$$

resta da provare il seguente fatto:

Teorema 3.42 (Teorema cinese del resto)**.** *Se* $\forall i\neq j$ *si ha* $\gcd(m_i,m_j)=1$, *il sistema*

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \dots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

è equivalente ad un'unica equazione della forma

$$x\equiv a \pmod{m_1\cdot m_2\cdot \ldots \cdot m_k}.$$

Dimostrazione. Detto M il prodotto di tutti gli m_i, chiamiamo S_1 il sistema

$$S_1: \begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv 0 \pmod{M/m_1} \end{cases}$$

Dalla seconda equazione abbiamo $x=k_1\cdot \frac{M}{m_1}$, e affinchè una siffatta x soddisfi anche la prima equazione dev'essere

$$k_1 \equiv a_1 \cdot \left(\frac{M}{m_1}\right)^{-1} \pmod{m_1},$$

dove l'ipotesi di coprimalitè degli m_i garantisce l'esistenza della classe inversa di $\left[\frac{M}{m_1}\right]$ in $\mathbb{Z}/_{m_1\mathbb{Z}}{}^*$, che per brevitè denominiamo K_1. Abbiamo che tutte e sole le x che risolvono S_1 sono della forma

$$x \equiv a_1 K_1 \frac{M}{m_1} \pmod{M},$$

denominiamo dunque X_1 il più piccolo numero naturale congruo a $a_1 K_1 \frac{M}{m_1}$ modulo M, e procediamo analogamente per $X_2, X_3, \ldots, X_k$. Poichè

$$x \equiv 0 \pmod{M/m_i} \longrightarrow \forall j \neq i \quad x \equiv 0 \pmod{m_j},$$

il numero $a \doteqdot X_1 + X_2 + \ldots + X_k$ è soluzione del sistema iniziale, e tutte le soluzioni sono della forma $a + kM$, in quanto:

- $x \equiv a \pmod{M}$ implica $x \equiv a \pmod{m_i}$ per ogni i;
- $\forall j \neq i \; X_i \equiv 0 \pmod{m_j}$ e $X_i \equiv a_1 \pmod{m_i}$ garantiscono che, $\forall i$, $a \equiv a_i \pmod{m_i}$;
- se U e V sono due distinte soluzioni del sistema iniziale, $\forall i \quad U - V \equiv 0 \pmod{m_i}$, e dunque $M|(U - V)$.

□

Dal Teorema cinese del resto discende un importante risultato di struttura:

Lemma 3.43. *Se $m = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, l'ordine moltiplicativo della classe $[a]$ in $\mathbb{Z}/_{m\mathbb{Z}}{}^*$ è pari al minimo comune multiplo di $(n_1, \ldots, n_k)$, dove n_i è l'ordine della classe $[a]$ in $\mathbb{Z}/_{p_i^{\alpha_i}\mathbb{Z}}{}^*$.*

3.10.1 Criteri di divisibilità

Muniti delle più importanti nozioni di teoria dei gruppi, analizziamo ora alcuni criteri di divisibilità. Assumendo che $a_1 a_2 \ldots a_{l(n)}$ sia la rappresentazione decimale del numero naturale

$$n = a_1 \cdot 10^{l(n)-1} + a_2 \cdot 10^{l(n)-2} + \ldots + 10 \cdot a_{l(n)-1} + a_{l(n)},$$

allora:

$$2|n \longleftrightarrow a_{l(n)} = 0, 2, 4, 6, 8 \qquad 3|n \longleftrightarrow 3| \left(\sum_{i=1}^{l(n)} a_i\right)$$

$$4|n \longleftrightarrow 4| \left(2\, a_{l(n)-1} + a_{l(n)}\right) \quad 5|n \longleftrightarrow a_{l(n)} = 0, 5 \qquad ,$$

$$9|n \longleftrightarrow 9| \left(\sum_{i=1}^{l(n)} a_i\right) \qquad 11|n \longleftrightarrow 11| \left(\sum_{i=1}^{l(n)} (-1)^i\, a_i\right)$$

in quanto:

- $n \equiv a_{l(n)} \pmod{10}$ implica $n \equiv a_{l(n)} \pmod{2}$ e $n \equiv a_{l(n)} \pmod{5}$;
- $10^k \equiv 1 \pmod{3}$ e $10^k \equiv 1 \pmod{3}$ implicano $n \equiv \sum_{i=1}^{l(n)} a_i \pmod{3}$ e $n \equiv \sum_{i=1}^{l(n)} a_i \pmod{9}$;
- $10^k \equiv (-1)^k \pmod{11}$ implica $n \equiv \pm \sum_{i=1}^{l(n)} (-1)^i\, a_i \pmod{11}$;
- $\forall j \geq k$, $10^k \equiv 0 \pmod{2^k}$ e $\pmod{5^k}$ implicano che 2^k (5^k) divide n se e solo se le ultime k cifre dell'espressione decimale di n costituiscono un multiplo di 2^k (5^k).

Notiamo inoltre che:

$$7|(10\cdot a+b) \longrightarrow 7|(50\cdot a+5\cdot b) \longrightarrow 7|(a-2\cdot b),$$

segue che n è un multiplo di 7 se e solo se lo è

$$\left\lfloor \frac{n}{10} \right\rfloor - 2\cdot a_{l(n)},$$

e ciè costituisce un criterio di divisibilità per 7:

$$12334 \to 1225 \to 112 \to 7, \qquad 7 \,|\, 12334,$$

$$12345 \to 1224 \to 114 \to 3, \qquad 7 \nmid 12345.$$

Analogamente per il 13:

$$13|(10\cdot a+b) \longrightarrow 13|(40\cdot a+4\cdot b) \longrightarrow 13|(a+4\cdot b),$$

$$13 \,|\, n \longleftrightarrow 13 \,|\, \left(\left\lfloor \frac{n}{10} \right\rfloor + 4\cdot a_{l(n)}\right)$$

$$12324 \to 1248 \to 156 \to 39, \qquad 13 \,|\, 12324,$$

$$12345 \to 1254 \to 141 \to 18 \qquad 13 \nmid 12345.$$

Per il 17 si ha:

$$17|(100\cdot a+b) \longrightarrow 17|(1600\cdot a+16\cdot b) \longrightarrow 13|(2\cdot a-b),$$

$$17 \,|\, n \longleftrightarrow 17 \,|\, \left(2\cdot \left\lfloor \frac{n}{100} \right\rfloor - a_{l(n)}\right)$$

$$12342 \to 204 \to 0, \qquad 17 \,|\, 12342,$$

$$12345 \to 201 \to 3 \qquad 17 \nmid 12345.$$

Per il 19 si ha:

$$19|(10\cdot a+b) \longrightarrow 19|(20\cdot a+2\cdot b) \longrightarrow 19|(a+2\cdot b),$$

$$19 \,|\, n \longleftrightarrow 19 \,|\, \left(\left\lfloor \frac{n}{10} \right\rfloor + 2\cdot a_{l(n)}\right)$$

$$12331 \to 1235 \to 133 \to 19, \qquad 19 \,|\, 12331,$$

$$12345 \to 1244 \to 132 \to 17 \qquad 19 \nmid 12345.$$

Per il 23 si ha:

$$23|(10\cdot a+b) \longrightarrow 23|(70\cdot a+7\cdot b) \longrightarrow 23|(a+7\cdot b),$$

$$23 \,|\, n \longleftrightarrow 23 \,|\, \left(\left\lfloor \frac{n}{10} \right\rfloor + 7\cdot a_{l(n)}\right)$$

$$12351 \to 1242 \to 138 \to 69 \qquad 23 \,|\, 12351,$$

$$12345 \to 1269 \to 189 \to 81 \qquad 23 \nmid 12345.$$

Lasciamo al lettore il compito di generalizzare quanto esposto ad altri primi e a basi differenti da quella decimale.

Esercizio 3.44 (IMO 2005, problema 4)**.** *Per $n \geq 1$, sia*

$$a_n = 2^n + 3^n + 6^n - 1.$$

Si determinino tutti i numeri naturali coprimi con ogni a_n.

Dimostrazione. Restringiamo immediatamente la nostra indagine ai numeri primi p che ipotizziamo non dividere alcun termine della successione, denotando con U il loro insieme. Notiamo subito che $2 \notin U$, in quanto a_n è sempre pari, e che $3 \notin U$, in quanto a_{2n} è sempre un multiplo di 3:

$$a_{2n} \equiv 4^n - 1 \equiv 0 \pmod 3.$$

Analogamente, a_{2n+1} è sempre un multiplo di 5:

$$a_{2n+1} \equiv 2^{2n+1} + 3^{2n+1} \equiv (2+3)(2^{2n} + \ldots + 3^{2n}) \equiv 0 \pmod 5,$$

per cui neppure 5 appartiene a U. In generale, per ogni numero primo $p \geq 5$ si ha

$$2^{p-1} \equiv 3^{p-1} \equiv 6^{p-1} \equiv 1 \pmod p,$$

per cui, con lieve abuso di notazione, possiamo scrivere:

$$a_{p-2} \equiv 2^{-1} + 3^{-1} + 6^{-1} + 1 \equiv \frac{1}{2} + \frac{1}{3} + \frac{1}{6} - 1 \equiv 0 \pmod p,$$

provando che p divide a_{p-2}.
Da ciò segue che l'unico numero naturale coprimo con tutti i termini della successione è 1. □

3.11 L'infinità dei primi in alcune progressioni aritmetiche

Teorema 3.45. *Sia p un numero primo. Esistono infiniti primi della forma $kp+1$.*

Dimostrazione. Proviamo preliminarmente che, se a ed n sono due numeri naturali maggiori di 2, allora:

$$n \mid \varphi(a^n \pm 1).$$

Tale risultato segue immediatamente dal Teorema di Lagrange e dal fatto che l'ordine di a in $\mathbb{Z}^*_{/(a^n-1)\mathbb{Z}}$ è esattamente pari ad n, mentre in $\mathbb{Z}^*_{/(a^n+1)\mathbb{Z}}$ è esattamente pari a $2n$. Supponiamo ora che si abbia $a \not\equiv -1 \pmod p$: in tal caso, in virtù del piccolo Teorema di Fermat p non divide a^p+1, ma in virtù del lemma iniziale p divide $\varphi(a^p+1)$. Poiché

$$\varphi(a^p+1) = \prod_{\substack{q\in\mathcal{P}\\ q\mid(a^p+1)}} (q-1)\, q^{(\nu_q(a^p+1)-1)},$$

esiste necessariamente un[5] divisore primo q di (a^p+1) tale per cui p divide $(q-1)$: ciò comporta che tale q sia della forma $kp+1$. Poniamo ora:

$$A_\nu = (p+1)^{2^\nu p} + 1,$$

e notiamo che, se $\nu_1 > \nu_2 > 1$, si ha:

$$A_{\nu_1} = (A_{\nu_2} - 1)^{2^{\nu_1-\nu_2}} + 1,$$

per cui:

$$\gcd(A_{\nu_1}, A_{\nu_2}) = \gcd(2, A_{\nu_2}) = 2.$$

Ciò comporta che i primi dispari che figurano nella fattorizzazione di A_{ν_1} siano tutti distinti da quelli che figurano nella fattorizzazione di A_{ν_2}: poiché ogni A_ν ammette un divisore primo della forma $kp+1$, il Teorema è provato. □

Lemma 3.46. *Se $q(x) \in \mathbb{Z}[x]$ è un polinomio non costante, nelle fattorizzazioni di*

$$q(1),\ q(2),\ q(3),\ \ldots$$

figurano infiniti primi.

Dimostrazione. Supponiamo, per assurdo, che i primi figurano nelle fattorizzazioni siano un numero finito, $p_1, \ldots, p_k$, e denotiamo con P il loro prodotto. Poiché q è non costante, possiamo scegliere un numero intero n in modo che si abbia $q(n) = a \neq 0$. Poiché, per ogni coppia (x, y) di interi distinti si ha:

$$(x-y) \mid (q(x) - q(y)),$$

a divide $q(n+aPx)$. Sia allora:

$$r(x) = \frac{1}{a}\, q(n+aPx) \in \mathbb{Z}[x].$$

Notiamo che per ogni intero m si ha $r(m) \equiv 1 \pmod P$: poiché $r(x)$ è non costante, esiste un intero u per cui $r(u) \neq 1$. Poiché nessuno dei p_j può dividere $r(u)$, esiste almeno un altro primo che divide uno degli interi nell'immagine di q, contro l'ipotesi. □

[5] Si noti che, se q è un primo dispari che divide a^p+1 ma non divide $a+1$, $a^p \equiv -1 \pmod q$ comporta che l'ordine di a modulo q sia esattamente pari a $2p$ e dunque p divida $q-1$.

Teorema 3.47. *Per ogni intero $m > 1$, esistono infiniti primi della forma $km + 1$.*

Dimostrazione. Sia $\Phi_m(x)$ l'm-esimo polinomio ciclotomico:

$$\Phi_m(x) = \prod_{\substack{1 \le j < m \\ (j,m)=1}} \left(x - \exp\left(\frac{2\pi i j}{m}\right)\right).$$

Notiamo che si ha:

$$x^m - 1 = \Phi_m(x) \cdot \prod_{\substack{d<m \\ d|m}} \Phi_d(x).$$

Se p è un primo dispari che non divide m, e si verifica $p \mid \Phi_m(a)$, allora $p|(a^m - 1)$ e dunque $\gcd(a, p) = 1$. In tale eventualità, inoltre, l'ordine di a modulo p è precisamente m: se fosse $p|(a^d - 1)$ per un qualche d divisore proprio di m, il polinomio $x^m - 1$ ammetterebbe a come radice doppia in $\mathbb{F}_p$, si avrebbe dunque $p|(m\, a^{m-1})$ contro l'ipotesi $p \nmid m$. Poiché, in virtù del Teorema di Lagrange, l'ordine di a divide $p - 1$, vale l'implicazione:

$$p \text{ dispari}, \quad p \nmid m, \quad p \mid \Phi_m(a) \quad \Longrightarrow \quad p \equiv 1 \pmod{m}.$$

In virtù del lemma precedente, nelle fattorizzazioni di

$$\Phi_m(1),\ \Phi_m(2),\ \Phi_m(3),\ \ldots$$

figurano infiniti primi, e solo un numero finito di questi possono pari o dividere m:
tutti gli altri sono necessariamente congrui a 1 modulo m. □

Teorema 3.48 (Bauer)**.** *Sia $m \ge 3$ un numero intero e*

$$f(x) = \sum_{k=0}^{n} a_k\, x^{n-k}$$

un polinomio a coefficienti interi, che cambia di segno in almeno un punto dell'asse reale. Esistono allora infiniti primi della forma $p \not\equiv 1 \pmod{m}$ che dividono $f(x)$ per un qualche valore di x.

Dimostrazione. Supponiamo preliminarmente, senza perdita di generalità, che si abbia $a_0 > 0$. In virtù della continuità di f esistono due numeri interi t e T, con $t \neq 0$ e $T > 0$, per cui $f(t/T) < 0$: si ha allora che il polinomio a coefficienti interi

$$g(x) \doteqdot T^n f\left(\frac{x}{T}\right) = \sum_{k=0}^{n} a_k\, T^k\, x^{n-k}$$

è negativo nel punto $x = t$. Poniamo:

$$h(x) \doteqdot -\frac{g\,(t - g(t)\,x)}{g(t)} = -1 + x\,\frac{g'(t)}{1!} - g(t)\,x^2\,\frac{g''(t)}{2!} + \ldots + (-1)^{n-1}(g(t))^{n-1} a_0\, x^n.$$

Quest'ultimo è un polinomio a coefficienti interi con coefficiente del monomio di grado n positivo: segue che $h(x)$ è positivo per ogni valore di x sufficientemente grande. Poiché $h(km) \equiv -1 \pmod{m}$, tra i divisori primi di $h(km)$ dev'essercene almeno uno $\not\equiv 1 \pmod{m}$. Supponiamo che i primi di questa forma che dividono almeno un elemento nell'immagine di h siano in quantità finita, e denotiamo con P il loro

prodotto. $h(kmP)$ risulta congruo a -1 sia modulo m che modulo P, esiste perciò almeno un altro primo $\not\equiv 1 \pmod m$ che divide un elemento nell'immagine di h. Ciò prova che l'immagine di h è divisa da infiniti primi della forma $\not\equiv 1 \pmod m$: poiché solo un numero finito di questi possono risultare divisori di $g(t)$ o T, il Teorema è provato. □

Teorema 3.49. *Per ogni intero $n > 1$, esistono infiniti primi della forma $kn - 1$.*

Dimostrazione. Per ogni numero naturale n definiamo due polinomi $U_n(x)$ e $V_n(x)$ attraverso l'equazione:

$$(x+i)^n = U_n(x) + i\,V_n(x).$$

In questo modo si ha:

$$U_n(x) = \frac{(x+i)^n + (x-i)^n}{2}, \qquad \frac{(x+i)^n - (x-i)^n}{2i};$$

inoltre, se ν risulta un divisore positivo di n, si ha che $V_\nu(x)$ divide $V_n(x)$. Posto infatti $n = \mu\nu$, risulta:

$$U_n(x) + i\,V_n(x) = ((x+i)^\nu)^\mu = (U_\nu(x) + i\,V_\nu(x))^\mu,$$

da cui segue:

$$V_n(x) = V_\nu(x) \cdot \left(\binom{\mu}{1} (U_\nu(x))^{\mu-1} - \binom{\mu}{3} (U_\nu(x))^{\mu-3} (V_\nu(x))^2 + \dots \right).$$

Notiamo ora che, se x è un qualunque numero intero, un primo $q \equiv -1 \pmod 4$ non può dividere simultaneamente sia $U_m(x)$ che $V_m(x)$, altrimenti si troverebbe a dividere:

$$U_m(x)^2 + V_m(x)^2 = (x^2+1)^m,$$

mentre x^2+1 non ammette divisori primi della forma $4k-1$. Addizionalmente, se supponiamo che q non divida n, q non può dividere simultaneamente sia $V_\nu(x)$ che $\frac{V_n(x)}{V_\nu(x)}$: in virtù delle considerazioni sinora esposte, ciò segue dal fatto che

$$\frac{V_n(x)}{V_\nu(x)} \equiv \mu\,(U_\nu(x))^{\mu-1} \pmod{V_\nu(x)}.$$

Per ogni valore intero di x, q divide $V_{q+1}(x)$, in quanto:

$$V_{q+1}(x) = \binom{q+1}{1} x^q - \binom{q+1}{3} x^{q-2} + \dots - \binom{q+1}{q} x \equiv (q+1)(x^q - x) \equiv 0 \pmod q.$$

Se, per un qualche valore di x, q divide $V_n(x)$ ma non divide alcun $V_\nu(x)$, con ν che varia nell'insieme dei divisori propri di n, allora $q \equiv -1 \pmod n$. Poniamo, in tali ipotesi, $G = \gcd(n, q+1)$ - in virtù del Lemma di Bézout esistono due numeri naturali A e B per cui si ha:

$$A(q+1) - Bn = G;$$

vale inoltre l'identità:

$$U_G(x)V_{Bn}(x) + V_G(x)U_{Bn}(x) = V_{A(q+1)}(x).$$

Poiché q divide $V_{q+1}(x)$ e $V_{q+1}(x)$ divide $V_{A(q+1)}(x)$, q divide il membro destro dell'ultima identità. Analogamente, poiché per ipotesi q divide $V_n(x)$, q divide $V_{Bn}(x)$ - ne consegue che q divide $V_G(x)U_{Bn}(x)$. Tuttavia q non può dividere $U_{Bn}(x)$, perché divide già $V_{Bn}(x)$. Segue che q divide $V_G(x)$. G è però un

divisore di n, e per le ipotesi fatte non può che essere un divisore improprio: $G = n$,
ossia $q \equiv -1 \pmod{n}$.
Le radici di $V_n(x)$ sono della forma $\cot \frac{k\pi}{n}$ con $k \in [1, n-1]$; detto $\Phi_n(x)$ il polinomio minimo su $\mathbb{Q}$ di $\cot \frac{\pi}{n}$, questo ha $\varphi(n)$ radici reali in $\cot \frac{\pi a}{n}$, ove $a \in [1, n-1], (a, n) = 1$; $W_n(x) \doteqdot n \cdot \Phi_n(x)$ è inoltre un polinomio a coefficienti interi. Per qualunque ν divisore proprio di n si ha:

$$W_n(x) \mid \left(n \cdot \frac{V_n(x)}{V_\nu(x)} \right),$$

per cui se q è un primo congruo a -1 modulo 4 che non divide n ma divide $W_n(x)$, q divide $V_n(x)$ ma non divide alcun $V_\nu(x)$, per cui $q \equiv -1 \pmod{n}$. D'altro canto, in virtù del Teorema di Bauer (con $m = 4$) esistono infiniti primi $q \equiv -1 \pmod 4$ che dividono $W_n(x)$ per un qualche x: tutti questi, eccetto una quantità finita (costituita da coloro che dividono n) sono primi della forma $kn - 1$. □

Vale inoltre un risultato molto più generale, la cui dimostrazione, tuttavia, esula dalle finalità di questo testo:

Teorema 3.50 (Dirichlet)**.** *Esistono infiniti numeri primi in ogni progressione aritmetica della forma $a + b\mathbb{Z}$ con a e b coprimi.*

3.12 Residui quadratici

Dato un gruppo moltiplicativo e abeliano G, $g \in G$ si dice *residuo quadratico* se appartiene all'immagine dell'applicazione $f : G \to G$ definita da

$$f(g) = g \cdot g.$$

Tale applicazione è un *automorfismo* di G, ossia una mappa da G in G compatibile con l'operazione di gruppo:

$$f(g \cdot h) = f(g) \cdot f(h),$$

da cui segue che l'insieme dei residui quadratici è un sottogruppo di G:

$$Q \doteqdot \operatorname{Im} f \leq G.$$

Nel caso di gruppi di ordine dispari, Q coincide con G, in quanto:

$$o(g) = n \longrightarrow n | o(G), n \equiv 1 \pmod 2 \longrightarrow \left(g^{\frac{n+1}{2}} \right)^2 = g^n \cdot g = g \longrightarrow \forall g \in G, g \in \operatorname{Im} f.$$

Incidentalmente, ciè prova anche che in un gruppo di ordine pari ogni elemento di ordine dispari appartiene a Q. Nel caso di gruppi ciclici di ordine pari, preso un qualunque generatore g si ha

$$Q = < g^2 >,$$

in quanto ogni elemento di $< g^2 >$ appartiene all'immagine di f, $o(< g^2 >) = \frac{o(G)}{2}$, e se Q contenesse elementi distinti da quelli di $< g^2 >$, in quanto sottogruppo di G, dovrebbere coincidere con G, dunque contenere anche g, il che è assurdo, dato che il massimo ordine di un elemento di $< g^2 >$ è pari a $\frac{o(G)}{2}$.
Tale fenomeno ha una conseguenza importante:

$$g, h \in (G \setminus Q) \longrightarrow g \cdot h \in Q,$$

nelle ipotesi, infatti, g e h risultano "potenze dispari" di un generatore, ragion per cui il loro prodotto è una "potenza pari", ossia un elemento di Q. A questo punto abbiamo un criterio potente per verificare l'appartenenza di una classe $[a]$ al sottogruppo dei residui quadratici in $\mathbb{Z}/_{p\mathbb{Z}}{}^*$, per p primo dispari:

$$[a] \in Q \iff a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Preso infatti un generatore g, se $[a] \in Q$ è della forma $[g^{2k}]$, e dunque $a^{\frac{p-1}{2}} \equiv g^{k(p-1)} \equiv 1^k \pmod{p}$; in caso contrario si ha

$$a^{\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}} \equiv -1 \pmod{p},$$

in quanto il termine centrale è distinto dalla classe $[1]$, poichè $[g^k] = [1]$ implica $(p-1)|k$, mentre il suo quadrato è esattamente la classe $[1]$. Da tale criterio segue un celebre fatto:

Lemma 3.51. *$[-1]$ è un residuo quadratico in $\mathbb{Z}/_{p\mathbb{Z}}{}^*$ se e solo se $p \equiv 1 \pmod 4$: in tal caso il Teorema di Wilson garantisce che si abbia*

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1 \pmod{p}.$$

Risultati analoghi si hanno per le classi $[2]$ e $[-3]$:

Lemma 3.52. *$[2]$ è un residuo quadratico in $\mathbb{Z}/_{p\mathbb{Z}}{}^*$ se e solo se $p \equiv \pm 1 \pmod 8$.*

Dimostrazione.

$$2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv 2 \cdot 4 \cdot \ldots \cdot p-1 \equiv (-1)^{\frac{p^2-1}{8}} \left(\frac{p-1}{2}\right)!.$$

□

Lemma 3.53. *$[-3]$ è un residuo quadratico in $\mathbb{Z}/_{p\mathbb{Z}}{}^*$ se e solo se $p \equiv 1 \pmod 3$.*

Dimostrazione. Se $p \equiv 1 \pmod 3$, in $\mathbb{Z}/_{p\mathbb{Z}}{}^*$ esiste, per il Teorema di Cauchy, un elemento di ordine 3, che denominiamo ω. Si ha

$$\omega^2 + \omega + 1 \equiv 0 \pmod{p},$$

in quando $[\omega] \neq [1]$ e $[\omega^3] = [1]$. Consideriamo allora $\omega - \omega^2$:

$$\left(\omega - \omega^2\right)^2 \equiv \omega^2 - 2\omega^3 + \omega^4 \equiv (\omega^2 + \omega + 1) - 3 \equiv -3 \pmod{p}.$$

Viceversa, supponiamo che in $\mathbb{Z}/_{p\mathbb{Z}}{}^*$, per $p \equiv 2 \pmod 3$, esista una classe $[q]$ che realizzi $[q^2] = [-3]$. Si ha:

$$\left[\frac{-1+q}{2}\right] \neq [1] \qquad \left(\frac{-1+q}{2}\right)^3 \equiv \frac{q^3 + 3q + 8}{8} \equiv 1 \pmod{p},$$

da cui l'esistenza di un elemento di ordine 3, assurda poichè 3 non è un divisore dell'ordine del gruppo. □

Per la determinazione della radice quadrata di un residuo quadratico in $\mathbb{Z}/_{p\mathbb{Z}}{}^*$ è possibile adoperare un algoritmo di *crivello*: se $[a]$ è residuo quadratico (ossia realizza $a^{\frac{p-1}{2}} \equiv 1 \pmod p$) esiste un numero naturale $b < p/2$ per cui vale $b^2 \equiv a \pmod p$, ovvero

$$b^2 = k \cdot p + a.$$

In tali ipotesi si ha $1 \leq k < p/4$, e la determinazione di k comporta la determinazione di b: chiediamoci dunque quale sia un metodo efficiente per identificare l'unico quadrato nella sequenza

$$m_j = j \cdot p + a, \qquad 1 \leq j < p/4.$$

Prendiamo a titolo di esempio il caso $p = 101, a = 5$. Se m_j è un quadrato, in particolare realizza:

$$m_j \not\equiv 2, 3, 5, 6, 7 \pmod 8,$$

che è come dire:

$$101 \cdot j \not\equiv -3, -2, 0, 1, 2 \pmod 8,$$

condizione a sua volta equivalente (previa moltiplicazione per l'inverso di [101] in $\mathbb{Z}/_{8\mathbb{Z}}{}^*$) a:

$$j \not\equiv 0, 1, 2, 5, 6 \pmod 8.$$

Segue:

$$k \in \{3, 4, 7, 11, 12, 15, 19, 20, 23\}.$$

Inoltre:

$$m_k = b^2 \longrightarrow k \not\equiv 0 \pmod 3,$$

dunque

$$k \in \{4, 7, 11, 19, 20, 23\}.$$

Ed ancora:

$$m_k = b^2 \longrightarrow k \not\equiv 2, 3 \pmod 5,$$

$$k \in \{4, 11, 19, 20\},$$

$$m_k = b^2 \longrightarrow k \not\equiv 0, 4, 5 \pmod 7,$$

$$k \in \{20\},$$

per cui una radice quadrata della classe [5] in $\mathbb{Z}/_{101\mathbb{Z}}{}^*$ è

$$[\sqrt{101 \cdot 20 + 5}] = [45]$$

e l'altra è la classe opposta, $[-45] = [56]$.
Certamente, se abbiamo necessità di generare tutti i $\frac{p-1}{2}$ residui quadratici in $\mathbb{Z}/_{p\mathbb{Z}}{}^*$,
è sufficiente ricordare che:

$$Q = \left\{ [1^2], [2^2], \ldots, \left[\left(\frac{p-1}{2} \right)^2 \right] \right\},$$

in quanto:

$$a \neq b,\ p|(a^2 - b^2) \longrightarrow [a] = [b] \text{ o } [a] = [-b]$$

e il membro destro non può essere soddisfatto da due distinti elementi interi dell'intervallo $\left(0, \frac{p}{2}\right)$.
A questo punto il Teorema cinese del resto rientra prepotentemente nella discussione, comunicandoci, ad esempio, che:

- poichè i residui quadratici sono un sottogruppo, $[-6]$ è un residuo quadratico in $\mathbb{Z}/_{p\mathbb{Z}}{}^*$ se e solo se $p \equiv 1, 5, 7, 11 \pmod{24}$;
- se $n = a^2 + 6b^2$ è un intero libero da quadrati, ogni divisore primo di n è della forma $24k + 1$, $24k + 5, 24k + 7$ o $24k + 11$;
- se $\gcd(m, n) = 1$, la classe $[a]$ è un residuo quadratico in $\mathbb{Z}/_{mn\mathbb{Z}}{}^*$ se e solo se lo è sia in $\mathbb{Z}/_{n\mathbb{Z}}{}^*$ che in $\mathbb{Z}/_{m\mathbb{Z}}{}^*$.

Abbiamo a questo punto tutti gli strumenti necessari alla risoluzione di equazioni della forma

$$ax^2 + bx + c \equiv 0 \pmod{m}$$

meno che uno: un algoritmo per l'estrazione della radice quadrata in un gruppo moltiplicativo ciclico. Esistono due approcci, che pur avendo la medesima efficienza sono concettualmente molto diversi: il primo, dovuto a Cipolla e Lehmer, sfrutta le proprietè dell'automorfismo di Frobenius in campi finiti, riconducendo il problema a quello del calcolo di una potenza di una matrice; il secondo, dovuto a Daniel Shanks, è fondato sulle seguenti osservazioni:

- Se $p-1 = 2^k \cdot q$ con q dispari, per ogni b che non sia un residuo quadratico in $\mathbb{Z}/_{p\mathbb{Z}}{}^*$, b^q risulta una radice primitiva 2^k-esima dell'unità;
- Per ogni residuo quadratico a, a meno di moltiplicare per un'opportuna radice 2^k-esima dell'unità, si ha che $a^{\frac{q+1}{2}}$ è radice quadrata di a.

Per i dettagli consigliamo nuovamente di consultare la bibliografia.
Introducendo ora il *simbolo di Legendre*:

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{se} \quad [a] \text{ è residuo quadratico in } \mathbb{Z}/_{p\mathbb{Z}}{}^* \\ 0 & \text{se} \quad p|a \\ -1 & \text{se} \quad [a] \text{ non è residuo quadratico in } \mathbb{Z}/_{p\mathbb{Z}}{}^* \end{cases}$$

possiamo facilmente verificare che valgono le seguenti proprietè:

- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$;
- $\left(\frac{a+kp}{p}\right) = \left(\frac{a}{p}\right)$;
- Se $p \nmid q$, $\left(\frac{q^2}{p}\right) = 1$,

e formulare il *Teorema di Reciprocità Quadratica*:

Teorema 3.54 (Gauss)**.** *Se p e q sono primi dispari,*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Stupefacente risultato, la cui dimostrazione esula certamente dallo scopo di queste dispense: nuovamente, rimandiamo alla bibliografia. Tornando, per modo di dire, con i piedi per terra, chiediamoci cosa si possa dire, più in generale, della mappa

$$f : G \to G, \qquad f(x) = x^q,$$

se q è un primo dispari e G è un gruppo moltiplicativo abeliano. Come prima, f risulta un automorfismo di G, dunque

$$\operatorname{Im} f \leq G,$$

inoltre

$$o(g) = qk \;\longrightarrow\; o(g^q) = k, \qquad q \nmid o(g) \;\longrightarrow\; o(g^q) = o(g),$$

$$q \nmid o(g) \;\longrightarrow\; \exists\, h \in < g >:\; g = h^q \;\longrightarrow\; g \in \operatorname{Im} f,$$

Si ha conseguentemente che, nei gruppi ciclici, l'ordine di Im f è esattamente pari a $\frac{o(G)}{q}$ oppure a $o(G)$ a seconda che $q|o(G)$ o $q \nmid o(G)$, rispettivamente. Nel caso in cui q divida $o(G)$ si ha inoltre:

$$g \in \operatorname{Im} f \iff g^{\frac{o(G)}{q}} = e,$$

in quanto, preso un generatore g, l'elemento $g^{\frac{o(G)}{q}}$ risulta radice primitiva q-esima dell'unità.

Esercizio 3.55. *Sia $p > 7$ un numero primo. Si provi che in $\mathbb{Z}/_{p\mathbb{Z}}{}^*$ esistono almeno due residui quadratici consecutivi, una volta provato che almeno una classe di resto tra $\{[2], [5], [10]\}$ è un quadrato.*

3.13 Gruppi di permutazioni

Se $\sigma : A \to A$ è una mappa biettiva su un insieme finito, è detta *permutazione*. Le permutazioni su un insieme di cardinalità n formano un gruppo (in generale non abeliano) rispetto alla composizione, usualmente denominato *gruppo simmetrico* su n elementi, in simboli S_n, di ordine $n!$. Sussistono due differenti notazioni per le permutazioni:

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix},$$

$$\sigma = (a_1\ a_2\ \dots\ a_k),$$

dove con la seconda si intende che σ agisce su $\{a_1, a_2, \dots, a_k\}$ in modo ciclico (*è una permutazione ciclica*, o, più semplicemente, un *ciclo*):

$$\sigma(a_1) = a_2,\ \sigma(a_2) = a_3, \dots\ \sigma(a_k) = a_1,$$

lasciando fissi gli elementi di $\{1, 2, \dots, n\} \setminus \{a_1, a_2, \dots, a_k\}$.
L'insieme dei punti fissi di una permutazione si denota con

$$\operatorname{Fix}(\sigma) = \{i : \sigma(i) = i\},$$

e due permutazioni σ_1, σ_2 si dicono *disgiunte* se

$$(\{1, 2, \dots, n\} \setminus \operatorname{Fix}(\sigma_1)) \cap (\{1, 2, \dots, n\} \setminus \operatorname{Fix}(\sigma_2)) = \emptyset.$$

Una permutazione di ordine 2, ossia un 2-ciclo, è detta *trasposizione*. Sussistono i seguenti fatti:

- permutazioni disgiunte commutano;
- ogni permutazione è prodotto di cicli disgiunti;
- ogni m-ciclo è prodotto di $(m-1)$ trasposizioni;
- l'ordine di un m-ciclo è m;

è dunque particolarmente semplice calcolare l'ordine di una permutazione; presa, ad esempio, $\sigma \in S_7$ della forma:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 1 & 6 & 2 & 3 & 7 & 5 \end{pmatrix},$$

si ha:

$$\sigma = (1\ 4\ 2)(3\ 6\ 7\ 5), \qquad o(\sigma) = \frac{3 \cdot 4}{\gcd(3,4)} = 12.$$

Inoltre, se una permutazione σ realizza:

$$\sigma = \tau_1 \cdot \tau_2 \cdot \ldots \cdot \tau_j = \rho_1 \cdot \rho_2 \cdot \ldots \cdot \rho_k$$

con τ_x e ρ_y trasposizioni, allora $j - k$ è pari. Se infatti definiamo la *segnatura* (o *segno*) di una generica permutazione σ attraverso

$$s(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{|\sigma(i) - \sigma(j)|} = \pm 1$$

l'applicazione segno risulta un *omomorfismo*, ossia una mappa che realizza $s(\sigma_1 \cdot \sigma_2) = s(\sigma_1) \cdot s(\sigma_2)$: di conseguenza, il nucleo di tale applicazione

$$\ker s = \{\sigma \in S_n : s(\sigma) = 1\}$$

risulta un sottogruppo di S_n di ordine $\frac{n!}{2}$, detto gruppo *alterno* su n elementi, in simboli A_n.
Si noti che A_n, in generale, non coincide con l'insieme dei quadrati in S_n, per ragioni legate alle decomposizione di una permutazione in cicli disgiunti:

Lemma 3.56. *Se $\sigma = (1\ 2)(3\ 4\ 5\ 6) \in A_6$, non vi è alcun elemento ρ di A_6 per cui si abbia $\sigma = \rho^2$. Infatti il quadrato di un $2k$-ciclo è il prodotto di due k-cicli disgiunti, mentre il quadrato di un ciclo di ordine dispari è un ciclo del medesimo ordine: se fosse $\rho^2 = \sigma$ nella decomposizione in cicli di ρ dovrebbe far capolino un 8-ciclo, assurdo.*

Lemma 3.57. *Se $\sigma_1 = (1\ 4\ 2\ 5\ 3\ 6), \sigma_2 = (1\ 5\ 2\ 6\ 3\ 4), \sigma_3 = (1\ 6\ 2\ 4\ 3\ 5)$ si ha:*

$$\sigma_1^2 = \sigma_2^2 = \sigma_3^2 = (1\ 2\ 3)(4\ 5\ 6).$$

Lemma 3.58. *Se $\sigma \in A_n$ ed L_m è il numero di m-cicli che compaiono nella decomposizione di σ,*

$$\exists \rho \in S_n : \ \sigma = \rho^2 \quad \leftrightarrow \quad \forall k, \ \ L_{2k} \equiv 0 \pmod 2.$$

Se ora chiamiamo *isomorfismo* un omomorfismo iniettivo tra due gruppi finiti di pari cardinalità, abbiamo:

Teorema 3.59 (Cayley)**.** *Ogni gruppo finito G è isomorfo ad un sottogruppo di $S_{o(G)}$.*

Dimostrazione. E' sufficiente associare ad ogni $g \in G$ la permutazione σ_g definita attraverso $\sigma_g(h) = h \cdot g$; si ha:

$$\sigma_g \cdot \sigma_h = \sigma_{h \cdot g} \qquad (\sigma_g)^{-1} = \sigma_{g^{-1}}.$$

□

Teorema 3.60. *A_n è l'unico sottogruppo di indice 2 di S_n.*

Dimostrazione. Qualunque sottogruppo $H < G$ di indice 2 è tale per cui $\sigma_1, \sigma_2 \in G \setminus H$ comporta $\sigma_1 \cdot \sigma_2 \in H$. In particolare ogni sottogruppo di indice 2 di S_n contiene tutti i quadrati, dunque contiene tutti i 3-cicli, ma i 3-cicli generano A_n. □

3.14 Addendum: il Teorema di Wolstenholme

$$\binom{mp}{p} \equiv m \pmod{p^3}.$$

Consideriamo le possibili scelte di p oggetti tra mp oggetti disposti in m scatole, dove ogni scatola contiene p oggetti, e l'azione di gruppo che corrisponde ad uno shift ciclico degli elementi in una certa scatola. Vi saranno m scelte per cui tutti gli elementi appartengono ad una singola scatola, e $\binom{p}{2}\left(\binom{2p}{p}-2\right)$ scelte per cui gli elementi appartengono esattamente a due scatole. Le restanti possibilitè, per cui gli oggetti appartengono a $k \geq 3$ scatole, per effetto dell'azione di gruppo forniscono un contributo complessivo che è certamente un multiplo di p^3. Segue:

$$\binom{mp}{p} = m + \binom{p}{2}\left(\binom{2p}{p}-2\right) + kp^3 = m + \binom{p}{2}\sum_{k=1}^{p-1}\binom{p}{k}^2 + kp^3 = m + Kp^3.$$

Parte seconda:

$$H_{p-1} \equiv 1 \pmod{p^2}.$$

Esercizio 3.61 (IMO shortlist 2011)**.** *Sia p un numero primo dispari. Per ogni intero a, si ponga:*

$$S_a = \frac{a}{1} + \frac{a^2}{2} + \ldots + \frac{a^{p-1}}{p-1}.$$

Nell'ipotesi in cui m ed n sono due numeri interi tali per cui:

$$S_4 + S_3 - 3S_2 = \frac{m}{n},$$

si dimostri che p divide m.

3.15 Il campo dei numeri complessi

Sia $i \notin \mathbb{R}$ una radice quadrata di -1. Lo spazio vettoriale

$$\mathbb{R}[i] = \left\{a + b\,i : (a,b) \in \mathbb{R}^2\right\}$$

è detto *campo dei numeri complessi* e usualmente denotato con $\mathbb{C}$. Valgono i seguenti fatti:

- $(a+b\,i)(c+d\,i) = (ac-bd) + (ac+bd)\,i$;
- $\frac{1}{a+b\,i} = \frac{1}{a^2+b^2}\,(a-b\,i)$.

Se $z = a + b\,i$, la *parte reale* di z è $\Re(z) = a$, la *parte immaginaria* è $\Im(z) = b$.
Il *coniugio* è un automorfismo dello spazio vettoriale:

$$\bar{z} = \Re(z) - i \cdot \Im(z),$$

mentre il *modulo* è la distanza del punto $(a,b) \in \mathbb{R}^2$ dall'origine:

$$|z| = \sqrt{a^2+b^2} = z \cdot \bar{z}.$$

Estendendo il dominio dell'usuale funzione esponenziale al campo dei numeri complessi, attraverso [6]

$$e^z = \sum_{j=0}^{+\infty} \frac{z^j}{j!},$$

si ha che per ogni numero reale θ vale *l'identità di De Moivre*:

$$e^{i\theta} = \cos(\theta) + i\,\sin(\theta);$$

l'*argomento* di $z \neq 0$, in simboli $\arg z$, è l'unico numero reale θ nell'intervallo $[0, 2\pi)$ per cui si ha:

$$z = |z|e^{i\theta}.$$

Si noti che per $z, w \in \mathbb{C} \setminus \{0\}$ si verifica:

$$|z \cdot w| = |z| \cdot |w|, \qquad \arg(z \cdot w) = \arg(z) + \arg(w) \pmod{2\pi}.$$

Si ha inoltre:

$$\cos(\theta) = \frac{e^{i\theta} + e^{-i\theta}}{2}, \qquad \sin\theta = \frac{e^{i\theta} - e^{-i\theta}}{2i}.$$

3.16 Polinomi

Dato un anello $\mathbb{A}$, commutativo e con identità, l'anello dei polinomi a coefficienti in $\mathbb{A}$, in simboli $\mathbb{A}[x]$, è costituito dagli elementi

$$p(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n, \quad a_i \in \mathbb{A}.$$

Poiché $\mathbb{Z}$ è un anello euclideo, la funzione *grado* rende $\mathbb{Z}[x]$ un anello euclideo: tra i polinomi a coefficienti interi è dunque possibile implementare un algoritmo coerente di divisione con resto. Se ora ξ è *radice* di $p(x)$, ossia realizza $p(\xi) = 0$, si ha

$$(x - \xi) \mid p(x),$$

(il viceversa è banale) e ξ è detta radice *di molteplicità* k se

$$(x - \xi)^k \mid p(x), \quad (x - \xi)^{k+1} \nmid p(x).$$

Un risultato centrale è dovuto a Gauss[7]:

Teorema 3.62 (fondamentale dell'Algebra)**.** *Ogni polinomio a coefficienti reali o complessi di grado k ammette esattamente k radici in $\mathbb{C}$, contate con molteplicità.*

Altri risultati importanti sono:

Lemma 3.63. *Ogni polinomio di grado dispari a coefficienti reali ammette almeno una radice reale.*

Lemma 3.64. *Se $p(x) = a_0x^n + \ldots + a_n$ è un polinomio a coefficienti interi con una radice razionale $\xi = \pm\frac{a}{b}$, allora $a|a_n$ e $b|a_0$.*

Lemma 3.65. *Se $\xi \in \mathbb{C} \setminus \mathbb{R}$ è radice di $p(x) \in \mathbb{R}[x]$, allora lo è anche $\bar{\xi}$.*

[6] Notiamo come il parametro dell'esponenziale così definito possa vivere in spazi molto diversi: se z è un numero reale, troviamo una funzione analitica intera; se z è un numero complesso, troviamo una funzione olomorfa e intera; se z è una matrice, troviamo l'esponenziale di matrice, che fornisce le soluzioni dei sistemi dinamici linearizzati; se z è un generico operatore differenziale con spettro limitato, troviamo il flusso integrale.

[7] Ne omettiamo la dimostrazione, di carattere prettamente analitico. I curiosi sono liberi di indagare sul concetto di *indice di avvolgimento* di una curva e sul *principio di Rouché*.

Lemma 3.66. *Ogni polinomio a coefficienti interi coprimo con la sua derivata è privo di radici multiple (ossia con molteplicità maggiore di uno).*

Dimostrazione. Se ξ è radice di molteplicità $k \geq 2$ di $p(x)$, allora $(x-\xi)^k$ divide $p(x)$, ossia:

$$p(x) = (x-\xi)^k q(x),$$

da cui:

$$p'(x) = (x-\xi)^{k-1}\left((x-\xi)q'(x) + k\,q(x)\right),$$

dunque ξ è radice di molteplicità $k-1$ di $p'(x)$. □

Analizziamo ora le relazioni che intercorrono tra radici e coefficienti. Utilizziamo la notazione

$$[x^k]\,p(x)$$

per denotare il coefficiente del termine x^k nel polinomio $p(x)$; diciamo che un polinomio è *monico* se $[x^{\partial p}]\,p(x) = 1$. Si ha:

Teorema 3.67 (Viète)**.** *Se $p(x) \in \mathbb{C}[x]$ è monico di grado n, con radici $\xi_1, \ldots, \xi_n \in \mathbb{C}$ (eventualmente coincidenti), allora*

$$[x^{n-j}]\,p(x) = (-1)^j \sum_{1 \leq i_1 < \ldots < i_j \leq n} \prod_{h=1}^{j} \xi_{i_j}$$

Dimostrazione. E' sufficiente considerare il coefficiente di x^{n-j} in $p(x) = \prod_{j=1}^{n}(x-\xi_j)$. □

E' ora naturale discutere di *funzioni simmetriche*: una funzione $f : \mathbb{K}^n \to \mathbb{K}$ è detta *simmetrica* se

$$\forall \sigma \in S_n,\ f(x_1, x_2, \ldots, x_n) = f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}).$$

Alla categoria appartengono le funzioni simmetriche elementari di n variabili:

$$e_1(x_1,\ldots,x_n) = x_1 + \ldots + x_n, \qquad e_2(x_1,\ldots,x_n) = x_1x_2 + x_1x_3 + \ldots + x_1x_n + x_2x_3 + \ldots + x_{n-1}x_n,$$

$$e_k(x_1,\ldots,x_n) = \sum_{1 \leq i_1 < \ldots < i_k \leq n} x_{i_1} \cdot \ldots \cdot x_{i_k}$$

e le somme di potenze:

$$p_k(x_1,\ldots,x_n) = \sum_{j=1}^{n} x_j^k.$$

Le une sono legate alle altre attraverso il seguente

Teorema 3.68 (formule di Newton-Girard)**.**

$$k \cdot e_k = \sum_{j=1}^{k} (-1)^{j-1} e_{k-j}\, p_1.$$

Dimostrazione. Si consideri il polinomio $p(t)$, di grado n, avente termine noto 1 e radici $\frac{1}{x_1}, \ldots, \frac{1}{x_n}$. Per il teorema di Viète si ha:

$$p(t) = \prod_{j=1}^{n}(1 - x_j\,t) = \sum_{k=0}^{n}(-1)^k\, e_k\, t^k,$$

alché, derivando il membro centrale e il membro destro rispetto a t, quindi moltiplicando per t:

$$\sum_{k=0}^{n}(-1)^k\, k e_k\, t^k = -\left(\sum_{j=1}^{n} \frac{x_j\,t}{1 - x_j\,t}\right) \cdot \prod_{j=1}^{n}(1 - x_j\,t).$$

Espandendo ora il fattore sinistro del membro destro in serie di potenze otteniamo:

$$\sum_{k=0}^{n}(-1)^k\, k e_k\, t^k = \left(\sum_{j=1}^{\infty} p_j\, t^j\right)\cdot\left(\sum_{l=0}^{n}(-1)^{l-1}\, e_l\, t^l\right),$$

e la tesi segue dal raffronto del coefficiente di x^k nei due termini. □

Abbiamo dunque modo di esprimere le funzioni simmetriche elementari in termini delle somme di potenze e viceversa, il tutto indipendentemente dal numero di variabili in gioco. Un'altra funzione simmetrica notevole è il *discriminante* di un polinomio: sia $p(z) \in \mathbb{C}[z]$ un polinomio con radici $\xi_1, \ldots, \xi_{\partial p} \in \mathbb{C}$ (eventualmente ripetute se presenti con molteplicità maggiore di uno). La quantità[8]

$$\Delta p = \prod_{1\le i<j\le \partial p}(\xi_i - \xi_j)^2 = (-1)^{\binom{\partial p}{2}}\prod_{j=1}^{\partial p} p'(\xi_i)$$

è un polinomio simmetrico nelle variabili $\xi_1, \ldots, \xi_{\partial p}$, dunque può essere espresso in termini dei coefficienti di p, in quanto:

Lemma 3.69. *Ogni polinomio simmetrico può essere espressa attraverso somme e prodotti di funzioni simmetriche elementari.*

Dimostrazione. E' sufficiente provare la tesi per polinomi omogenei, ossia somme di monomi di pari grado, quindi procedere per induzione sul grado delle variabili nei monomi. □

Inoltre, è evidente che il discriminante è invariante per traslazioni: se $q(x) = p(x+\tau)$, allora $\Delta p = \Delta q$.

Discutiamo ora di numeri *algebrici*. Un numero $z \in \mathbb{C}$ è detto algebrico su $\mathbb{Q}$ se esiste un polinomio monico $p \in \mathbb{Q}[x]$ per cui si abbia $p(z) = 0$, o, equivalentemente, se esiste un polinomio (non necessariamente monico) $q(x) \in \mathbb{Z}[x]$ per cui si abbia $q(z) = 0$. Se z è algebrico su $\mathbb{Q}$, esiste un unico elemento monico di $\mathbb{Q}[x]$ di minimo grado che annulla z: se infatti vi fossero due distinti polinomi monici p_1, p_2 di grado n (minimo) per cui $p_1(z) = 0 = p_2(z)$, z risulterebbe radice di $p_1 - p_2$, di grado strettamente inferiore a n, contravvenendo l'ipotesi di minimalità. Tale elemento è detto *polinomio minimo* di z su $\mathbb{Q}$: le sue radici sono dette *radici coniugate* di z, il suo grado è il *grado algebrico* di z su $\mathbb{Q}$. Ogni polinomio minimo su $\mathbb{Q}$ di grado n è *irriducibile*, ossia non può essere espresso come prodotto di due elementi di $\mathbb{Q}[x]$ di grado inferiore ad n; inoltre è privo di radici multiple.
Esistono diversi criteri per certificare l'irriducibilità di un polinomio su $\mathbb{Q}$:

Lemma 3.70 (Eisenstein)**.** *Se $q(x) \in \mathbb{Z}[x]$ è un polinomio monico di grado n, ed esiste un numero primo p per cui si abbia:*

$$\forall m \in [1, n-1] \quad p \,|\, [x^m]q(x), \qquad p^2 \nmid q(0),$$

allora $q(x)$ è irriducibile su $\mathbb{Q}$.

Lemma 3.71. *Se $q(x)$ è irriducibile su $\mathbb{K} \supseteq \mathbb{Z}$, lo è anche $q(x+m)$ per ogni intero m.*

Lemma 3.72. *Se nell'immagine di $\mathbb{Z}$ attraverso $q(x) \in \mathbb{Z}[x]$ vi sono più di $2\cdot\partial q$ numeri primi, $q(x)$ è irriducibile su $\mathbb{Q}$.*

Lemma 3.73. *Se $q(x)$ è irriducibile su $\mathbb{F}_p$ lo è anche su $\mathbb{Q}$.*

[8] La seconda uguaglianza segue dal fatto che, posto $n = \partial p$,

$$p(x) = \prod_{j=1}^{n}(x-\xi_j) \quad \longrightarrow \quad p'(\xi_i) = \prod_{j\neq i}(x-\xi_j).$$

Lemma 3.74 (Stickelberger)**.** *Se $q(x) \in \mathbb{F}_p[x]$ è privo di radici multiple, condizione necessaria affinché $q(x)$ sia irriducibile su $\mathbb{F}_p$ è che si abbia $\left(\frac{\Delta q}{p}\right) = (-1)^{1+\partial q}$.*

E' inoltre importante ricordare che:

Lemma 3.75. *Per ogni numero naturale $n \geq 2$, il polinomio minimo su $\mathbb{Q}$ di $z = e^{\frac{2\pi i}{n}}$ (n-esimo polinomio ciclotomico) ha grado $\varphi(n)$; inoltre ogni numero della forma z^m con $\gcd(m,n) = 1$ è radice coniugata di z.*

Lemma 3.76. *Per ogni numero naturale n e per ogni coppia (α, β) di numeri algebrici su $\mathbb{Q}$ non nulli,*

$$\alpha^{\frac{1}{n}}, \quad \alpha^n, \quad \alpha \cdot \beta, \quad \frac{\alpha}{\beta}, \quad \alpha + n\,\beta$$

sono numeri algebrici su $\mathbb{Q}$.

Dimostrazione. Supponiamo che α e β abbiano gradi algebrici u e v, e polinomi minimi

$$p_\alpha(x) = x^u - a(x), \qquad p_\beta(x) = x^v - b(x).$$

Sia ora $\mathbb{V}$ lo spazio vettoriale generato dai monomi $\alpha^t\,\beta^s$ con $0 \leq t < u$, $0 \leq s < v$: tale spazio ha dimensione limitata da $u \cdot v$. Ne consegue che, comunque presi $uv + 1$ elementi di $\mathbb{V}$, ne esiste una combinazione lineare nulla. In particolare $\alpha + \beta$ risulta radice di un polinomio a coefficienti in $\mathbb{Q}$ di grado limitato da $u \cdot v$ (prendiamo $1, (\alpha+\beta), (\alpha+\beta)^2, \ldots, (\alpha+\beta)^{uv}$ come elementi di $\mathbb{V}$), e lo stesso vale per $\alpha \cdot \beta$. Per quanto riguarda α^n, si riproduca lo stesso ragionamento sullo spazio vettoriale generato da $1, \alpha, \alpha^2, \ldots, \alpha^{u-1}$. Si noti inoltre che $\frac{1}{\beta}$ è radice del polinomio

$$x^v\, p_\beta\left(\frac{1}{x}\right) \in \mathbb{Q}[x],$$

$\alpha^{\frac{1}{n}}$ è radice del polinomio

$$p_\alpha(x^n) \in \mathbb{Q}[x],$$

$n \cdot \beta$ è radice del polinomio

$$p_\beta\left(\frac{x}{n}\right) \in \mathbb{Q}[x].$$

A questo punto i polinomi minimi delle quantità citate nel lemma vanno identificati tra i fattori irriducibili dei polinomi così costruiti. Si ricordi tuttavia che, se u è coprimo con v, il grado algebrico di $\alpha + \beta$ su $\mathbb{Q}$ è esattamente pari al prodotto $u \cdot v$, il che garantisce l'automatica irriducibilità del polinomio costruito attraverso $\mathbb{V}$. □

Parliamo ora di problemi di problemi di *interpolazione*: ci chiediamo, ad esempio, come determinare un polinomio a coefficienti interi $p(x)$ che realizzi

$$\begin{cases} p(1) &= 13 \\ p(2) &= 27 \\ p(3) &= 40. \end{cases}$$

Per l'euclidicità di $\mathbb{Z}[x]$ abbiamo:

$$(x-1) \,|\, p(x) - 13, \qquad (x-2) \,|\, p(x) - 27, \qquad (x-3) \,|\, p(x) - 40.$$

Condizione necessaria e sufficiente per soddisfare la prima condizione è che si abbia:

$$p(x) = (x-1)p_1(x) + 13,$$

alché la seconda e la terza condizione mutano in:

$$p_1(2) = 14, \qquad 2 \cdot p_1(3) = 27,$$

dunque non vi sono soluzioni in $\mathbb{Z}[x]$, in quanto p_1, polinomio a coefficienti interi, non può valere $\frac{27}{2}$ nel punto 3. Proseguiamo tuttavia nella determinazione delle soluzioni in $\mathbb{Q}[x]$:

$$p_1(x) = (x-2)p_2(x) + 14, \qquad p_2(3) = -\frac{1}{2},$$

$$p_2(x) = (x-3)q(x) - \frac{1}{2}.$$

Abbiamo che tutte le soluzioni in $\mathbb{Q}[x]$ sono della forma:

$$p(x) = 13 + (x-1)\left(14 + (x-2)\left(-\frac{1}{2} + (x-3)q(x)\right)\right),$$

in corrispondenza con le soluzioni $q(x)$ del sistema

$$\begin{cases} q(0) &= 0 \\ q(1) &= 14 \\ q(2) &= 27. \end{cases}$$

attraverso la relazione $q(x) + 13 = p(x+1)$. Saremmo potuto pervenire più rapidamente alla soluzione attraverso una semplice considerazione: se

$$\begin{cases} n_1(x) &= \frac{1}{2}(x-2)(x-3) \\ n_2(x) &= -(x-1)(x-3) \\ n_3(x) &= \frac{1}{2}(x-1)(x-2) \end{cases}$$

si ha che, per $m \in [1,3]$, $n_i(m) = \delta_{im}$, dunque tutte e sole le soluzioni in $\mathbb{Q}[x]$ del sistema iniziale sono della forma:

$$(13n_1(x) + 27n_2(x) + 40n_3(x)) + (x-1)(x-2)(x-3)q(x).$$

Il metodo esposto è sostanzialmente un'equivalente polinomiale del teorema cinese del resto e prende il nome di *interpolazione di Newton-Lagrange*. Vediamo ora un'interessante applicazione di questa tecnica al calcolo del determinante delle matrici di Vandermonde, ricordando preliminarmente un risultato di algebra lineare.

Lemma 3.77 (Cramer)**.** *Se $A \in \mathrm{GL}_n(\mathbb{K})$, la soluzione del sistema lineare*

$$A\,x = (v_1, \ldots, v_n)^T = v \neq 0$$

è data, per ogni $i \in [1,n]$, da

$$x_i = \frac{\det A^{(i)}}{\det A},$$

dove $A^{(i)}$ è la matrice ottenuta da A sostituendo la i-esima colonna con il vettore v.

Dimostrazione. Sia $\{e_1, \ldots, e_n\}$ la base canonica di $\mathbb{F}^n$ e siano f ed f_i le applicazioni lineari associate ad A ed $A^{(i)}$, rispettivamente. Si ha:

$$\begin{cases} f_i : e_i \to v = f\,x, \\ f_i : e_k \to f\,e_k \qquad \forall k \neq i, \end{cases}$$

dunque:

$$\begin{cases} f^{-1}\,f_i : e_i \to x, \\ f^{-1}\,f_i : e_k \to e_k \qquad \forall k \neq i. \end{cases}$$

La matrice associata, nella base canonica, all'applicazione $f^{-1}\,f_i$ ha perciò elementi non nulli unicamente sulla diagonale e sulla i-esima colonna; in particolare si verifica $\det(f^{-1}\,f_i) = x_i$. D'altro canto, per il teorema di Binet si ha $\det(f^{-1}\,f_i) = \frac{\det f_i}{\det f}$, da cui la tesi. □

Sia ora $V(x_0, \ldots, x_k)$ la matrice di Vandermonde $(k+1) \times (k+1)$ per cui si ha $V_{i,j} = x_i^j$ con $i, j \in [0, k]$. V è naturalmente associata ad un problema di interpolazione: supponendo infatti di voler determinare i coefficienti $d^T = (d_0, \ldots, d_k)$ del polinomio $q(x) = d_0 + d_1\, x + \ldots + d_k x^k$ sotto le ipotesi

$$q(x_0) = 1, \quad q(x_i) = 0 \quad \forall i \in [1, k],$$

detta $\{e_0, \ldots, e_k\}$ la base canonica di $\mathbb{F}^{k+1}$, ci troviamo di fronte alla risoluzione del sistema lineare:

$$Vd = e_0.$$

Se gli x_i sono tutti distinti, certamente $V \in \mathrm{GL}_{k+1}(\mathbb{K})$, in quanto una soluzione al problema è data da

$$q(x) = \frac{\prod_{i=1}^{k}(x_i - x)}{\prod_{i=1}^{k}(x_i - x_0)},$$

e, in particolare, vale:

$$d_0 = \frac{\prod_{i=1}^{k} x_i}{\prod_{i=1}^{k}(x_i - x_0)}.$$

In virtù del lemma precedente abbiamo però:

$$d_0 = \frac{\det V(x_1, \ldots, x_n)}{\det V(x_0, \ldots, x_n)} \prod_{i=1}^{k} x_i,$$

dunque:

$$\forall n, \quad \frac{\det V(x_0, \ldots, x_n)}{\det V(x_1, \ldots, x_n)} = \prod_{i=1}^{k}(x_i - x_0)$$

e, per induzione su n,

Teorema 3.78.

$$\det V(x_0, \ldots, x_k) = \prod_{k \geq i > j \geq 0} (x_i - x_j) = \pm\sqrt{\Delta\left(\prod_{i=0}^{k}(x - x_i)\right)}.$$

È particolarmente interessante interpretare "a rovescio" l'ultima identità: supponiamo che $p \in \mathbb{Q}[x]$ sia un polinomio coprimo con la sua derivata. In tali ipotesi, p ammette ∂p radici complesse distinte $(\zeta_1, \ldots, \zeta_{\partial p})$, e si ha:

$$\Delta p = \det\left(V^T(\zeta_1, \ldots, \zeta_{\partial p}) \cdot V(\zeta_1, \ldots, \zeta_{\partial p})\right);$$

la matrice che figura nel membro destro, che denotiamo con P, è una matrice simmetrica e invertibile, i cui elementi sono somme di potenze[9] delle radici di p:

$$P \in \mathrm{GL}_{\partial p}(\mathbb{Q}), \qquad \forall i, j \in [0, \partial p - 1],\ P_{i,j} = p_{i+j}(\zeta_1, \ldots, \zeta_{\partial p}).$$

Il Teorema (3.78) permette perciò di esplicitare la dipendenza che sussiste tra il discriminante e le funzioni simmetriche elementari delle radici, e, conseguentemente, la dipendenza che sussiste tra il discriminante di un polinomio e l'insieme dei suoi coefficienti.

3.17 Coefficienti binomiali e successioni per ricorrenza

Il coefficiente binomiale $\binom{n}{k}$ è dato dal numero di possibili scelte di k elementi tra n:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!};$$

[9] Convenzionalmente, assumiamo $p_0(\zeta_1, \ldots, \zeta_{\partial p}) = \partial p$.

per $m \leq 0,\ n < 0$ o $n > m$ si pone, convenzionalmente:

$$\binom{m}{n} = 0.$$

Valgono le seguenti proprietà:

1. $\binom{n}{k} = \binom{n}{n-k}$;
2. $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$;
3. $(a+b)^n = \sum_{j=0}^{n} \binom{n}{j} a^j\, b^{n-j}$;
4. $\sum_{j=0}^{n} \binom{n}{j} = 2^n$;
5. $\sum_{j=0}^{n} \binom{n}{j}(-1)^j = 0$;
6. $\sum_{j=k}^{N} \binom{j}{k} = \binom{N+1}{k+1}$.

Inoltre:

Lemma 3.79 (Chu-Vandermonde)**.**

$$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}.$$

Dimostrazione.

$$\sum_{k=0}^{n} \binom{n}{k}\binom{n}{n-k} = [x^n]\left(\sum_{k=0}^{n}\binom{n}{k}x^k\right)^2 = [x^n](1+x)^{2n} = \binom{2n}{n}.$$

□

Digerita questa cospicua mole di risultati, ci chiediamo cosa si possa dire della somma delle k-esime potenze dei primi N numeri naturali positivi, ossia di:

$$p_k(N) \doteqdot \sum_{n=1}^{N} n^k.$$

Leggende narrano che Gauss da giovane fosse uno scolaro particolarmente molesto, tanto che il suo insegnante, per tenerlo buono, gli assegnò un giorno il compito di calcolare la somma dei numeri naturali da 1 a 100, reputando ciò piuttosto tedioso e certamente non alla portata di un bambino. Il piccolo Gauss, dopo appena qualche attimo di macchinazione, esclamò con fierezza: "5050!", lasciando di stucco il suo insegnante, che aveva impiegato tempi ben maggiori per portare a termine il medesimo compito. Quest'ultimo, sopraffatto dall'ammirazione, o forse solo dall'invidia, pretese che il suo alunno palesasse l'artificio diabolico usato per rispondere con tale prontezza. Il piccolo Gauss, senza scomporsi, articolò: "$100+1 = 99+2 = 98+3$, così via per 50 volte, è semplice", quindi riprese a far cagnara.

Il caso $k = 1$ è dunque anteriore al Risorgimento. Per non sfigurare al cospetto di Gauss, consideriamo dapprima il caso $k = 2$. Poiché $n^2 = 2\binom{n}{2} + \binom{n}{1}$,

$$\sum_{n=1}^{N} n^2 = 2\sum_{n=1}^{N}\binom{n}{2} + \sum_{n=1}^{N}\binom{n}{1} = 2\binom{N+1}{3} + \binom{N+1}{2} = \frac{N(N+1)(2N+1)}{6},$$

fatto probabilmente farraginoso da articolare a parole ma sicuramente conciso e di grande effetto. Analogamente, per $k = 3$:

$$\sum_{n=1}^{N} n^3 = 6\sum_{n=1}^{N}\binom{n+1}{3} + \sum_{n=1}^{N}\binom{n}{1} = 6\binom{N+2}{4} + \binom{N+1}{2} = \frac{N^2(N+1)^2}{4} = \left(\sum_{n=1}^{N} n\right)^2.$$

Possiamo dunque asserire che, in generale, $p_k(N)$ è un polinomio in N, a coefficienti razionali[10], di grado $k+1$: i suoi coefficienti possono essere dunque dedotti per interpolazione, anche in virtù del fatto che[11]:

$$p_k(N+1) - p_k(N) = (N+1)^k,$$

in stile gaussiano. Un artificio analogo permette di esplicitare le somme della forma

$$B_k(n) = \sum_{j=0}^{n} \binom{n}{j} j^k.$$

Nel caso $k=2$, ad esempio, si ha:

$$B_2(n) = 2\sum_{j=0}^{n}\binom{n}{j}\binom{j}{2} + \sum_{j=0}^{n}\binom{n}{j}\binom{j}{1} = 2\binom{n}{2}\sum_{j=0}^{n}\binom{n-2}{j-2} + \binom{n}{1}\sum_{j=0}^{n}\binom{n-1}{j-1} = 2^{n-2}\left(n^2+n\right);$$

mentre nel caso $k=3$ si ha:

$$B_3(n) = 6\sum_{j=0}^{n}\binom{n}{j}\binom{j}{3}+6\sum_{j=0}^{n}\binom{n}{j}\binom{j}{2}+\sum_{j=0}^{n}\binom{n}{j}\binom{j}{1} = 6\binom{n}{3}2^{n-3}+6\binom{n}{2}2^{n-2}+\binom{n}{1}2^{n-1} = 2^{n-3}(n^3+3n^2).$$

Più in generale, poniamo:

$$f_k(x) = \sum_{j=0}^{n}\binom{n}{j} j^k\, x^j, \qquad f(x) = f_0(x) = (1+x)^n$$

e consideriamo l'operatore differenziale (xD) che agisce come:

$$(xD)f = x\cdot\frac{df}{dx}.$$

Si ha $(xD)\,x^k = k\cdot x^k$, da cui:

Teorema 3.80.

$$B_k(n) = (xD)^k\,(1+x)^n\big|_{x=1} = \left.\frac{d^k}{dt^k}(1+e^t)^n\right|_{t=0}.$$

Chiamando ora δ l'operatore (di *differenza in avanti*)

$$\delta : p(x) \longrightarrow p(x) - p(x+1),$$

abbiamo che:

- $p\in\mathbb{Z}[x] \longrightarrow \delta p\in\mathbb{Z}[x]$;
- $\delta(pq) - p\cdot(\delta q) - q\cdot(\delta p) + (\delta p)\cdot(\delta q) = 0$;[12]
- $\partial(\delta p) = \partial p - 1$;
- $[x^{\partial p-1}](\delta p) = -\partial p\cdot[x^{\partial p}](p)$;

[10] *Accortezza, prego:* p_k ha coefficienti razionali, ma sugli interi assume unicamente valori interi.

[11] Suggeriamo al lettore di provare che $[N^{k+1}]\,p_k(N) = \frac{1}{k+1}$ in quanto:

$$\left|\sum_{n=1}^{N} n^k - \int_0^N x^k\,dx\right| = O(N^k).$$

[12] Ricordiamo che un operatore differenziale D è una *derivazione* se soddisfa:

$$D(f\cdot g) = (D\,f)\cdot g + f\cdot(D\,g),$$

dunque δ non è una derivazione, ma solo a causa del piccolo contributo $(\delta f)(\delta g)$.

- $\delta^{\partial p} p = (-1)^{\partial p} \cdot (\partial p)! \cdot [x^{\partial p}](p)$.

E' ora possibile fornire una risposta ben motivata a tutti i quiz di intelligenza che chiedono: *"Qual è il prossimo numero nella sequenza?"*. Supponiamo di avere una sequenza di 5 numeri interi, ad esempio $(10, 11, 17, 23, 71)$, e supponiamo che questi siano i valori assunti in $(0, 1, 2, 3, 4)$ da un certo polinomio $q(x)$, di grado 4, a coefficienti razionali: è semplice determinare $q(5)$. Infatti δq assume i valori

$$(-1, -6, -6, -48) \text{ su } (0, 1, 2, 3),$$

$\delta^2 q$ assume i valori

$$(5, 0, 42) \text{ su } (0, 1, 2),$$

$\delta^3 q$ assume i valori

$$(5, -42) \text{ su } (0, 1),$$

dunque $(\delta^4 q)(0) = 47$. Ma se q ha grado 4, $\delta^4 q$ è costante, alché, procedendo a ritroso, $\delta^3 q$ assume i valori

$$(5, -42, -89) \text{ su } (0, 1, 2),$$

$\delta^2 q$ assume i valori

$$(5, 0, 42, 131) \text{ su } (0, 1, 2, 3),$$

δq assume i valori

$$(-1, -6, -6, -48, -179) \text{ su } (0, 1, 2, 3, 4),$$

q assume i valori

$$(10, 11, 17, 23, 71, 250) \text{ su } (0, 1, 2, 3, 4, 5),$$

dunque $q(5) = 250$ è una risposta perfettamente plausibile per il nostro test di intelligenza. Il metodo esposto per la ricostruzione del valore di un certo polinomio in un punto è detto *metodo delle differenze finite*. Passiamo ora a dibattere di *successioni (definite) per ricorrenza*, in particolare di successioni *autonome* e *ricorrenti lineari*:

$$a_n = b_1 \cdot a_{n-1} + b_2 \cdot a_{n-2} + \ldots + b_k \cdot a_{n-k},$$

cui la successione di Fibonacci è esempio prototipico:

$$\begin{cases} F_0 &= 0 \\ F_1 &= 1 \\ F_n &= F_{n-1} + F_{n-2}. \end{cases}$$

Per tali successioni $\{a_n\}_{n\in\mathbb{N}}$ il polinomio

$$p(x) = x^k - b_1 x^{k-1} - b_2 x_{k-2} - \ldots ... - b_k$$

è detto *polinomio caratteristico*. Successioni di numeri razionali aventi il medesimo polinomio caratteristico $p(x)$ costituiscono uno spazio vettoriale su $\mathbb{Q}$ di dimensione ∂p; nell'ipotesi che $p(x)$ sia irriducibile su $\mathbb{Q}$, con radici distinte $\xi_1, \ldots, \xi_k$, le successioni

$$\{\xi_1^n\}_{n\in\mathbb{N}}, \quad \ldots, \quad \{\xi_k^n\}_{n\in\mathbb{N}}$$

sono linearmente indipendenti con polinomio caratteristico $p(x)$, dunque $\forall n \in \mathbb{N}$ si ha:

$$a_n = c_1\xi_1^n + c_2\xi_2^n + \ldots + c_k\xi_1^k, \quad c_i \in \mathbb{Q}[\xi_1].$$

Nel caso della successione di Fibonacci il polinomio caratteristico è il polinomio minimo su $\mathbb{Q}$ della sezione aurea ($\varphi = \frac{1+\sqrt{5}}{2}$, con radice coniugata $\bar{\varphi} = \frac{1-\sqrt{5}}{2} = 1 - \varphi = -\frac{1}{\varphi}$), dunque:

$$F_n = c_1\varphi^n + c_2(1-\varphi)^n, \quad F_0 = c_1 + c_2 = 0, \quad F_1 = c_1\varphi + c_2(1-\varphi) = 1$$

e si ha il seguente

Lemma 3.81 (Binet)**.**

$$F_n = \frac{1}{\sqrt{5}}\left(\varphi^n - (1-\varphi)^n\right).$$

Presa invece la successione di Lucas:

$$\begin{cases} L_0 &= 2 \\ L_1 &= 1 \\ L_n &= L_{n-1} + L_{n-2}. \end{cases}$$

si ha:

$$L_n = \varphi^n + (1-\varphi)^n,$$

inoltre L_n è combinazione lineare di F_n ed F_{n+1}, così come F_n è combinazione lineare di L_n ed L_{n+1}:

$$\begin{cases} L_n &= -F_n + 2\,F_{n+1} &= F_{n-1} + F_{n+1} \\ F_n &= \frac{1}{5}\left(-L_n + 2\,L_{n+1}\right) &= \frac{1}{5}\left(L_{n-1} + L_{n+1}\right) \end{cases}$$

Per le formule di Binet si ha inoltre:

$$\begin{cases} L_{2k} &= L_k^2 - 2\,(-1)^k & \\ L_{2k+1} &= L_k L_{k+1} - (-1)^k &= L_{k+1}^2 - L_k^2 \\ F_{2k} &= F_k L_k &= F_k(2\,F_{k+1} - F_k) \\ F_{2k+1} &= F_{k+1}^2 + F_k^2 & \end{cases}$$

Un'altra importante identità, facilmente dimostrabile per induzione su k, è la seguente:

$$F_m = F_k\,F_{m-k+1} + F_{k-1}\,F_{m-k}. \tag{3.2}$$

Con la scelta dei parametri $m = 2n-1, k = n$ si ottiene

$$F_{2n-1} = F_n^2 + F_{n-1}^2,$$

mentre con la scelta dei parametri $m = 2n-1, k = n-1$ si ottiene

$$F_{2n-1} = F_{n-1}F_{n+1} + F_{n-2}F_n.$$

Raffrontando le due identità prodotte possiamo scrivere:

$$(F_n^2 - F_{n-1}F_{n+1}) + (F_{n-1}^2 - F_{n-2}F_n) = 0,$$

fatto che garantisce, per induzione, la validità dell'uguaglianza:

$$F_n^2 - F_{n-1}F_{n+1} = (-1)^{n+1}.$$

In modo del tutto analogo, la scelta dei parametri $m = 2n-1, k = n-r$ porta a concludere:

$$F_n^2 - F_{n-r}F_{n+r} = (-1)^{n+r}\,F_r^2,$$

$$F_n^4 - F_{n-2}F_{n-1}F_{n+1}F_{n+2} = 1.$$

Ulteriore conseguenza dell'identità (3.2) è la seguente:

$$\gcd(F_m, F_k) = \gcd(F_{k-1}\cdot F_{m-k}, F_k) = \gcd(F_{m-k}, F_k) = F_{\gcd(m,k)}.$$

Dal binomio di Newton e dall'identità di Binet si ha:

$$F_n = 2^{1-n}\sum_{k=0}^{\lfloor\frac{n-1}{2}\rfloor}\binom{n}{2k+1}\cdot 5^k,$$

$$F_{2n} = \sum_{k=0}^{n} \binom{n}{k} \cdot F_k,$$

mentre è semplice provare, unicamente per induzione, l'identità[13]:

$$F_{n+1} = \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n-k}{k}.$$

La successione di Fibonacci, solo in quanto autonoma e a termini interi, è periodica modulo m per ogni numero naturale $m \geq 2$; in particolare, detto $\pi(m)$ il periodo della successione di Fibonacci modulo m, si ha:

- $\frac{\log m}{\log \varphi} < \pi(m) \leq m^2 - 1$;
- $k \,|\, \pi(F_k)$;
- se p è un primo congruo a 2 o 3 modulo 5, $\pi(p) \,|\, 2(p+1)$;
- se p è un primo congruo a 1 o 4 modulo 5, $\pi(p) \,|\, p-1$;
- se p è un primo congruo a 1 o 9 modulo 20, $\pi(p) \,|\, \frac{p-1}{2}$;
- se, al solito, $\nu_p(m) = \max\{h \in \mathbb{N} : p^h | m\}$, vale $\nu_5(F_k) = \nu_5(k)$, in quanto:

$$F_{5k} = 5F_k \left(25F_k^4 + 25(-1)^k F_k^2 + 1\right);$$

- dal punto precedente, segue $\pi(5^k) = 4 \cdot 5^k$.

SEQUENZE DI BEATTY, TEOREMA DI ZECKENDORFF E CODIFICA DI FIBONACCI.

Si noti inoltre che la successione $\left\{\frac{F_{n+1}}{F_n}\right\}_{n=1}^{\infty}$ converge linearmente verso φ, in quanto:

- il fatto che $\left|\frac{F_{n+1}}{F_n} - \frac{F_{n+2}}{F_{n+1}}\right| = \frac{1}{F_n F_{n+1}} < \frac{5}{\varphi^{2n+1}-1}$ garantisce che $\left\{\frac{F_{n+1}}{F_n}\right\}_{n=1}^{\infty}$ sia una successione di Cauchy, dunque ammetta limite $L \in \mathbb{R}$;
- posto $L = \lim_{n\to+\infty} \frac{F_{n+1}}{F_n}$, si ha $L \geq 1$ e $L = 1 + \frac{1}{L}$, dunque $L = \varphi$;
- $|F_{n+1} - \varphi F_n| = \frac{1}{\sqrt{5}} \left|\bar{\varphi}^{n-1} + \bar{\varphi}^{n+1}\right| \leq \frac{2}{\sqrt{5}\,\varphi^n}$ garantisce che, $\forall \varepsilon > 0$, si abbia definitivamente $\left|\frac{F_{n+1}}{F_n} - \varphi\right| \leq \frac{2}{5\,F_n^2 - (1+\varepsilon)}$.

Più semplicemente si consideri che, con la notazione propria delle frazioni continue, si ha:

$$\frac{F_{n+1}}{F_n} = [(1,)^n].$$

In generale, sussiste un legame molto stretto tra successioni per ricorrenza autonome e lineari, problemi di Cauchy per equazioni differenziali ordinarie a coefficienti costanti, orbite nel gruppo moltiplicativo $\mathrm{GL}_k(\mathbb{Q})$. Si considerino, ad esempio, le identità:

$$\begin{pmatrix} F_{n+2} \\ F_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix}, \quad \begin{pmatrix} L_{n+2} \\ L_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} L_{n+1} \\ L_n \end{pmatrix},$$

dove figura la matrice compagna (*companion*, o *matrice di Frobenius*) del polinomio $x^2 - x - 1$, polinomio caratteristico della ricorrenza. Tale matrice è diagonalizzabile in quanto ha autovalori distinti (il suo polinomio caratteristico è un elemento irriducibile di $\mathbb{Q}[x]$). Abbiamo poi che la traccia di una matrice

[13] *Suggerimento:* ambo i membri soddisfano la medesima equazione di ricorrenza.

(ossia la somma degli elementi che figurano sulla diagonale) è invariante per cambiamenti di base, ed è dunque pari alla somma degli autovalori. Da queste semplici considerazioni seguono facilmente le identità:

$$L_k = \mathrm{Tr}\left(\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^k\right), \qquad \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^k = \begin{pmatrix} F_{k+1} & F_k \\ F_k & F_{k-1} \end{pmatrix}.$$

$p|F_p, p|F_{p-1} op|F_{p+1}$ a seconda che si abbia $p = 5, p \equiv \pm 1 \pmod{10}, p \equiv \pm 3 \pmod{10}$. Usando $(F_n, F_m) = F_{(n,m)}$ si ha che se un primo $q > 5$ divide F_p allora $q > p$: ciò fornisce un'inusuale dimostrazione dell'infinità dei primi. (MOHANTY)

Esercizio 3.82. (☠) *Si dimostri che per ogni numero naturale $n \geq 2$ si ha:*

$$\sum_{0 \leq i \leq k \leq n} \frac{(-1)^i}{i!} \cdot \frac{(n-k-1)^2}{(n-k)!} = 1.$$

Dimostrazione. Proviamo preliminarmente il seguente lemma:

Lemma 3.83. *Per ogni coppia di numeri naturali c e d, si ha:*

$$\sum_{a=0}^{c} \binom{c}{a}\binom{a}{d}(-1)^a = (-1)^c \cdot \delta(c,d).$$

La somma che figura nel membro sinistro è infatti la valutazione in 1 del polinomio $p(x)$ che si ottiene applicando d volte l'operatore di differenza in avanti al polinomio $(1-x)^c$. Se $d < c$, $p(x)$ ha una radice in $x = 1$, per cui la valutazione è nulla. Se $d > c$, $p(x)$ è identicamente nullo. Non resta allora che analizzare il caso $c = d$, per cui il lemma segue facilmente. Possiamo in alternativa utilizzare la derivata in luogo dell'operatore di differenza in avanti, ottenendo, ugualmente:

$$\sum_{a=0}^{c} \binom{c}{a}\binom{a}{d}(-1)^a = \frac{1}{d!}\frac{d^d}{dx^d}(1-x)^c\Big|_{x=1} = (-1)^d \cdot \delta(c,d).$$

Operiamo allora una reindicizzazione della somma che vogliamo calcolare:

$$\sum_{0 \leq i \leq k \leq n} \frac{(-1)^i}{i!} \cdot \frac{(n-k-1)^2}{(n-k)!} = \sum_{\substack{a,b \in [0,n] \\ 0 \leq a+b \leq n}} \frac{(-1)^a (b-1)^2}{a!\, b!}.$$

Reindicizzando nuovamente su $a + b$, otteniamo:

$$\sum_{\substack{a,b \in [0,n] \\ 0 \leq a+b \leq n}} \frac{(-1)^a (b-1)^2}{a!\, b!} = \sum_{c=0}^{n} \frac{1}{c!} \sum_{a=0}^{c} \binom{c}{a} (-1)^a (c-1-a)^2.$$

Espandiamo ora il quadrato presente nell'ultima somma e sfruttiamo il fatto che $a^2 = 2\binom{a}{2} + \binom{a}{1}$ per metterci nella condizioni di applicare il lemma menzionato:

$$\begin{aligned} \sum_{c=0}^{n} \frac{1}{c!} \sum_{a=0}^{c} \binom{c}{a} (-1)^a (c-1-a)^2 &= \sum_{c=0}^{n} \frac{(c-1)^2}{c!} \sum_{a=0}^{c} \binom{c}{a} (-1)^a \\ &+ \sum_{c=0}^{n} \frac{2c-1}{c!} \sum_{a=0}^{c} \binom{c}{a}\binom{a}{1} (-1)^a a \\ &+ \sum_{c=0}^{n} \frac{2}{c!} \sum_{a=0}^{c} \binom{c}{a}\binom{a}{2} (-1)^a. \end{aligned}$$

Il contributo della prima somma che figura nel membro destro è pari a 1 (contribuisce solo $c = 0$), il contributo della seconda è pari a -1 (contribuisce solo $c = 1$) e il contributo della terza è pari a 1 (contribuisce solo $c = 2$): il Teorema è provato. □

3.18 Disuguaglianze

Una funzione $f : D \subseteq \mathbb{R}^n \to \mathbb{R}$ è detta *convessa* se

$$\forall \lambda \in [0,1],\, \forall x, y \in D, \quad f(\lambda x + (1-\lambda)y) \leq \lambda\, f(x) + (1-\lambda)\, f(y),$$

o, equivalentemente,

$$\forall \lambda_1, \ldots, \lambda_n,\ \lambda_i \in [0,1],\ \sum_{j=1}^{n} \lambda_j = 1 \ \text{ si ha } \ f\left(\sum_{j=1}^{n} \lambda_j\, x_j\right) \leq \sum_{j=1}^{n} \lambda_j\, f(x_j),$$

Una funzione è detta *concava* se è l'opposto di una funzione convessa.
Condizioni sufficienti affinché una funzione $f : \mathbb{R} \to \mathbb{R}$ risulti convessa sull'intervallo $[a, b]$ sono:

- $f \in C^0([a,b]),\ \forall (c,d) \in [a,b]^2,\ f\left(\frac{c+d}{2}\right) \leq \frac{f(c)+f(d)}{2}$ (continuità e convessità per punti medi);
- $f \in C^1([a,b]), f'(x)$ è una funzione debolmente crescente su $[a, b]$;
- $f \in C^2([a,b]), f'' \geq 0$.

In tali ipotesi f soddisfa la *disuguaglianza di Jensen*[14]:

$$\forall (c_1, \ldots, c_k) \in [a,b]^k,\ \forall (\lambda_1, \ldots, \lambda_k) \in [0,1]^k \cap \left\{ \sum_{j=1}^{k} \lambda_j = 1 \right\},\ f\left(\sum_{j=1}^{k} \lambda_j\, c_j\right) \leq \sum_{j=1}^{k} \lambda_j\, f(c_j),$$

inoltre il suo sopragrafico è convesso e giace al di sopra di ogni retta tangente; se dunque $f \in C^1([a,b])$ si ha:

$$\forall (x,y) \in [a,b]^2, f(x) \geq f'(y)(x-y) + f(y),$$

mentre per le rette secanti si ha:

$$\forall (c,d) \in [a,b]^2 : a \leq c < d \leq b, \begin{cases} \forall y \in [c,d], & f(y) \leq \dfrac{f(d)-f(c)}{d-c}\, y + \dfrac{d\, f(c) - c\, f(d)}{d-c}, \\ \forall y \in [a,b] \setminus [c,d], & f(y) > \dfrac{f(d)-f(c)}{d-c}\, y + \dfrac{d\, f(c) - c\, f(d)}{d-c}. \end{cases}$$

Supponiamo ora che $f : D \subseteq \mathbb{R}^n \to \mathbb{R}$ sia una funzione convessa e D sia un dominio semplicemente connesso. I risultati che seguono, pur semplici nella loro formulazione e dimostrazione, sono centrali nella teoria delle funzioni convesse:

- f è una funzione continua sulla parte interna di D; la cardinalità dei punti della parte interna di D per cui f non è differenziabile è al più numerabile;
- se f ammette massimo, lo assume sulla frontiera del dominio D.

Siano ora $(a_1, \ldots, a_k)$ e $(b_1, \ldots, b_k)$ due sequenze di numeri reali non negativi con le seguenti proprietà:

- $\forall i < j,\ a_i \geq a_j$ e $b_i \geq b_j$ (ordinate debolmente descrescenti);

[14] L'uguaglianza può verificarsi solo nel caso in cui i vari c_i coincidano.

- $\forall i \in [1,k],\ A_i \doteqdot \sum_{j=1}^{i} a_j \geq \sum_{j=1}^{i} b_j \doteqdot B_i$ (la prima sequenza maggiora la seconda);
- $\sum_{j=1}^{k}(a_j - b_j) = 0$ (medesima somma).

La *disuguaglianza di Karamata*, anche nota come *disuguaglianza di Hardy-Littlewood*, asserisce che in tali ipotesi una qualunque funzione reale convessa realizza:

$$\sum_{i=1}^{k} f(a_i) \geq \sum_{i=1}^{k} f(b_i).$$

Dimostrazione. Se f è convessa, la funzione

$$\delta_f(a,b) = \frac{f(b) - f(a)}{b - a}$$

è simmetrica nei suoi argomenti e crescente al crescere del secondo argomento.
Se nelle ipotesi del teorema poniamo dunque

$$c_i = \delta_f(a_i, b_i),$$

abbiamo:

$$\sum_{i=1}^{k}(f(a_i) - f(b_i)) = \sum_{i=1}^{k} c_i(a_i - b_i) = \sum_{i=1}^{k} c_i(A_i - A_{i-1} - B_i + B_{i-1}) = \sum_{i=1}^{k-1}(c_i - c_{i+1})(A_i - B_i),$$

ma

$$c_i = \delta_f(a_i, b_i) \geq \delta_f(b_i, a_{i+1}) \geq \delta_f(a_{i+1}, b_{i+1}) = c_{i+1}$$

e la tesi è provata. □

Se ora le sequenze $(a_1, \ldots, a_k)$ e $(b_1, \ldots, b_k)$ soddisfano le ipotesi del teorema di Karamata, per ogni funzione convessa f e per ogni sequenza di numeri reali non negativi $\{\lambda_i\}_{i=1}^{k}$ tale per cui la somma $\sum_{i=1}^{k} \lambda_i(a_i - b_i)$ sia nulla, si ha:

Teorema 3.84 (Weighted Karamata)**.**

$$\sum_{j=1}^{k} \lambda_j\, f(a_j) \geq \sum_{j=1}^{k} \lambda_j\, f(b_j).$$

Dimostrazione. E' sufficiente provare il risultato nel caso $\lambda_i \in \mathbb{N}$, quindi nel caso $\lambda_i \in \mathbb{Q}$, quindi concludere per continuità. □

Siano ora $\{a_i\}_{i=1}^{k}$ e $\{b_i\}_{i=1}^{k}$ due sequenze di numeri reali. Il polinomio di secondo grado

$$p(x) = \sum_{j=1}^{k}(a_j\, x + b_j)^2,$$

in quanto somma di quadrati, assume valori non negativi per ogni $x \in \mathbb{R}$. L'importante risultato:

Teorema 3.85 (Cauchy-Schwarz)**.**

$$\left(\sum_{j=1}^{k} a_j\, b_j\right)^2 \leq \left(\sum_{j=1}^{k} a_j^2\right) \cdot \left(\sum_{j=1}^{k} b_j^2\right)$$

segue dunque dalla constatazione che $p(x)$ ha discriminante non positivo; l'uguaglianza ha luogo unicamente nel caso in cui esista una costante $\lambda \in \mathbb{R}$ tale da realizzare:

$$\forall j \in [1,k], \;\; a_j = \lambda\, b_j.$$

A partire da una disuguaglianza banale, è in realtà possibile ottenere la disuguaglianza di Cauchy-Schwarz per *amplificazione* (o *interpolazione*). Siano $v, w \in \mathbb{R}^n \setminus \{0\}$. Allora:

$$\|v - w\| \geq 0,$$

da cui, per l'identità di polarizzazione (anche nota come *Teorema del coseno* o *Teorema di Carnot*):

$$< v, w > \;\leq\; \frac{1}{2}(\|v\|^2 + \|w\|^2).$$

Il membro sinistro è un prodotto scalare, in particolare una forma bilineare: segue che rimpiazzando v con λv e w con $\frac{1}{\lambda}\, w$ il suo valore non muta. Possiamo perciò asserire:

$$\forall v, w \in \mathbb{R}^n \setminus \{0\}, \;\; \forall \lambda > 0, \qquad < v, w > \;\leq\; \frac{1}{2}(\lambda^2 \|v\|^2 + \frac{1}{\lambda^2}\, \|w\|^2).$$

Operiamo ora la seguente accortezza: scegliamo λ^2 in modo da minimizzare il membro destro. Poiché

$$\min_{\substack{x,y \geq 0 \\ xy = k}} (x + y) = 2\sqrt{k},$$

(volendo, per AM-GM) la migliore scelta per λ^2 risulta essere $\frac{\|w\|}{\|v\|}$, e da tale scelta segue:

$$< v, w > \;\leq \|v\| \|w\|,$$

che è la disuguaglianza di Cauchy-Schwarz in forma vettoriale. Addizionalmente, notiamo che lo scarto tra il quadrato del membro destro e il quadrato del membro sinistro può essere precisamente quantificato:

Teorema 3.86 (Sharpened Cauchy-Schwarz Inequality)**.**

$$\left(\sum_{j=1}^{n} a_j^2\right) \cdot \left(\sum_{j=1}^{n} b_j^2\right) - \left(\sum_{j=1}^{n} a_j b_j\right)^2 = \sum_{1 \leq i < j \leq n} (a_i b_j - a_j b_i)^2 \;\; \geq 0.$$

Dimostrazione. È sufficiente raffrontare i monomi di grado 4 che figurano nel termine sinistro con quelli che figurano nel termine centrale. □

Siano ora $\{a_i\}_{i=1}^k$ e $\{b_i\}_{i=1}^k$ due sequenze debolmente crescenti di numeri reali non negativi. Si ha:

Teorema 3.87 (Disuguaglianza di riarrangiamento)**.**

$$\forall \sigma \in S_k, \quad \sum_{j=1}^{k} a_j b_j \geq \sum_{j=1}^{k} a_j b_{\sigma(j)} \geq \sum_{j=1}^{k} a_j b_{k+1-j}.$$

Dimostrazione. Supponiamo che per $\sigma_1, \sigma_2 \in S_k$ si abbia

$$\sigma_1 = (n_1\, n_2)\, \sigma_2,$$

con $n_1 < n_2$ e $\sigma_1^{-1}(n_1) < \sigma_2^{-1}(n_2)$.
In tal caso diciamo che σ_1 può essere ottenuta da σ_2 attraverso una *inversione*, e vale:

$$\sum_{j=1}^{k} (a_j\, b_{\sigma_2(j)} - a_j\, b_{\sigma_1(j)}) = (a_{\sigma_1^{-1}(n_1)} b_{n_2} + a_{\sigma_1^{-1}(n_2)} b_{n_1}) - (a_{\sigma_1^{-1}(n_1)} b_{n_1} + a_{\sigma_1^{-1}(n_2)} b_{n_2}),$$

$$\sum_{j=1}^{k}(a_j\, b_{\sigma_2(j)} - a_j\, b_{\sigma_1(j)}) = (b_{n_2} - b_{n_1})(a_{\sigma_1^{-1}(n_1)} - a_{\sigma_1^{-1}(n_2)}) \leq 0, \tag{3.3}$$

ed avremmo ottenuto la disuguaglianza opposta nel caso in cui fosse valsa $\sigma_1^{-1}(n_1) > \sigma_2^{-1}(n_2)$.
Posto dunque:

$$S(\sigma) = \sum_{j=1}^{k} a_j b_{\sigma(j)},$$

abbiamo:

$$\text{sign}(S(\sigma) - S((n_1\, n_2)\,\sigma) = \text{sign}(\sigma^{-1}(n_2) - \sigma^{-1}(n_1)),$$

tuttavia ogni permutazione di S_k può essere scritta come prodotto di al più $k-1$ trasposizioni:

$$\sigma = (1\,\eta_1)(2\,\eta_2)\ldots(k-1\,\eta_{k-1}),$$

con il vincolo addizionale $\eta_i \geq i$ (assumiamo che $(i\,i)$ rappresenti la permutazione identica e), segue:

$$\forall \sigma \in S_k : \sigma \neq e,\ \ S(\sigma) \leq S(e).$$

Se ora $\{a_i\}_{i=1}^k$ e $\{c_i\}_{i=1}^k$ sono due sequenze di numeri reali non negativi, l'una crescente e l'altra decrescente, possiamo ricalcare le nostre orme semplicemente cambiando di segno la (3.3) e ottenere:

$$\sum_{j=1}^{k} a_i\, c_i \leq \sum_{j=1}^{k} a_i\, c_{\sigma_i}.$$

La dimostrazione è perciò conclusa prendendo $c_i = b_{k+1-i}$.
Notiamo che la chiusura transitiva della relazione antisimmetrica

$$\sigma_1 < \sigma_2 \quad \Longleftrightarrow \quad \sigma_1 \text{ può essere ottenuta da } \sigma_2 \text{ tramite un'inversione}$$

munisce il gruppo S_k di un ordinamento parziale; in tale contesto, si può asserire con certezza

$$S(\sigma_i) \geq S(\sigma_j) \qquad \text{oppure} \qquad S(\sigma_i) \leq S(\sigma_j)$$

solo se σ_i e σ_j sono in relazione, ossia appartengono ad una stessa catena. Incondizionatamente, la permutazione identica maggiora ogni altro elemento di S_k e la permutazione $\sigma(i) = k+1-i$ è maggiorata da ogni altro elemento di S_k. □

Sommando ora le k disuguaglianze di riarrangiamento date dalle potenze del k-ciclo $\sigma = (1, 2, \ldots, k)$ in S_k abbiamo[15]:

Teorema 3.88 (Chebyshev)**.** *Se $\{a_i\}_{i=1}^k$ e $\{b_i\}_{i=1}^k$ sono due sequenze non decrescenti di numeri reali non negativi,*

$$k \cdot \sum_{j=1}^{k} a_k b_k \geq \left(\sum_{j=1}^{k} a_k\right) \cdot \left(\sum_{j=1}^{k} b_k\right).$$

La disuguaglianza cambia verso se le due sequenze sono ordinate in modo opposto, l'uguaglianza ha luogo se e solo se tutti gli elementi di una o dell'altra sequenze coincidono.

Presi ora k numeri reali non negativi $x_1, \ldots, x_k$ ed una sequenza di numeri reali non negativi $a_1, \ldots, a_k$, denotiamo con $T[a_1, \ldots, a_k]$ la quantità:

$$T[a_1, \ldots, a_k] = \sum_{\sigma \in S_k} x_{\sigma(1)}^{a_1} x_{\sigma(2)}^{a_2} \cdot \ldots \cdot x_{\sigma(k)}^{a_1} \doteqdot \sum_{sym} \prod_{j=1}^{k} x_j^{a_j}.$$

Vale il seguente:

[15] Incidentalmente, notiamo come la disuguaglianza di Chebyshev proceda in direzione opposta a quella della disuguaglianza di Cauchy-Schwarz.

Teorema 3.89 (Schur)**.**

$$\forall a, b \in \mathbb{R}^+, \quad T[a+2b, 0, 0] + T[a, b, b] \geq 2 \cdot T[a+b, b, 0].$$

Dimostrazione. E' sufficiente verificare che per ogni terna di numeri reali non negativi (x, y, z) si ha:

$$x^a(x^b - y^b)(x^b - z^b) + y^a(y^b - z^b)(y^b - x^b) + z^a(z^b - x^b)(z^b - y^b) \geq 0.$$

Senza perdere di generalità possiamo assumere che valga $x \geq y \geq z$, alché il terzo addendo risulta non negativo ed è sufficiente provare:

$$x^a(x^b - z^b) - y^a(y^b - z^b) \geq 0,$$

ossia:

$$x^{a+b} - y^{a+b} - z^b(x^a - y^a) \geq 0.$$

Ciò è semplice, in quanto:

$$x^{a+b} - y^{a+b} - z^b(x^a - y^a) \geq x^{a+b} - y^{a+b} - y^b(x^a - y^a) = x^a(x^b - y^b) \geq 0.$$

□

Inoltre, se $\{a_i\}_{i=1}^k$ e $\{b_i\}_{i=1}^k$ sono due sequenze che soddisfano le ipotesi della disuguaglianza di Karamata, vale il seguente risultato, anche noto come *disuguaglianza di riarrangiamento generalizzata* o *disuguaglianza di bunching*:

Teorema 3.90 (Muirhead)**.**

$$T[a_1, \ldots, a_k] \geq T[b_1, \ldots, b_k].$$

L'uguaglianza si verifica unicamente nei casi in cui coincidano tutte le variabili x_i, o coincidano le sequenze $\{a_i\}_{i=1}^k$ e $\{b_i\}_{i=1}^k$.

Dimostrazione. Si consideri che per ogni sequenza $\{a_i\}_{i=1}^k$, per ogni coppia di numeri naturali (n_1, n_2) che realizza $1 \leq n_1 < n_2 \leq k$ e per ogni $\rho \in \left[0, \frac{a_{n_1} - a_{n_2}}{2}\right]$, la sequenza

$$\{b_i\}_{i=1}^k \doteqdot (a_1, a_2, \ldots, a_{n_1 - 1}, a_{n_1} - \rho, a_{n_1+1}, \ldots, a_{n_2-1}, a_{n_2} + \rho, \ldots, a_k) \tag{3.4}$$

è maggiorata dalla sequenza $\{a_i\}_{i=1}^k$; in particolare:

$$\sum_{sym} \prod_{j=1}^{k} x_j^{a_j} \geq \sum_{sym} \prod_{j=1}^{k} x_j^{b_j}, \tag{3.5}$$

in quanto vale:

$$\sum_{sym} \left(x_{n_1}^{a_{n_1}} x_{n_2}^{a_{n_2}} + x_{n_1}^{a_{n_2}} x_{n_2}^{a_{n_1}}\right) \geq \sum_{sym} \left(x_{n_1}^{a_{n_1} - \rho} x_{n_2}^{a_{n_2} + \rho} + x_{n_1}^{a_{n_2} + \rho} x_{n_2}^{a_{n_1} - \rho}\right),$$

a sua volta implicata da:

$$\left(x_{n_1}^{a_{n_1} - a_{n_2} - \rho} - x_{n_2}^{a_{n_1} - a_{n_2} - \rho}\right) \cdot \left(x_{n_1}^{\rho} - x_{n_2}^{\rho}\right) \geq 0.$$

D'altro canto, se $\{a_i\}_{i=1}^k$ maggiora $\{c_i\}_{i=1}^k$, è possibile mandare la prima sequenza nella seconda con una successione di trasformazioni del tipo esposto in (3.4), e la tesi è provata. □

Teorema 3.91 (Disuguaglianza delle medie). *Se $m_1 > m_2$,*

$$\left(\frac{1}{k}\sum_{j=1}^{k} x_j^{m_1}\right)^{\frac{1}{m_1}} \geq \left(\frac{1}{k}\sum_{j=1}^{k} x_j^{m_2}\right)^{\frac{1}{m_2}},$$

dove l'uguaglianza è verificata nel solo caso in cui tutti gli x_i coincidano.

Dimostrazione. Studiamo dapprima il caso $m_1 > m_2 > 0$. Ponendo $y_j = x_j^{\frac{1}{m_2}}$ abbiamo che è sufficiente provare:

$$\forall t > 1, \quad \left(\frac{1}{k}\sum_{j=1}^{k} y_j^t\right)^{\frac{1}{t}} \geq \frac{1}{k}\sum_{j=1}^{k} y_j,$$

dove, per omogeneità, non è restrittivo supporre $\sum_{j=1}^{k} x_j = k$.
Posto dunque $z_i = y_i - 1$, è sufficiente provare:

$$\sum_{j=1}^{k} (1+z_j)^t \geq k.$$

Tuttavia per $t > 1$ la funzione $f(x) = (1+x)^t$ risulta convessa sull'intervallo $[-1, +\infty)$: il suo grafico giace dunque al di sopra del grafico di una qualunque tangente. In particolare, presa la tangente nell'origine, si ha:

$$(1+x)^t \geq 1 + t\,x,$$

nota anche come *disuguaglianza di Bernoulli*. L'applicazione di tale risultato permette di asserire:

$$\sum_{j=1}^{k} (1+z_j)^t \geq k + t\sum_{j=1}^{k} z_j = k,$$

come desiderato. Il caso $0 < m_1 < m_2$ può essere ricondotto al caso appena analizzato attraverso la sostituzione $y_i = \frac{1}{x_i}$; in ultima istanza si ha, per $r > 0$:

$$\left(\sum_{j=1} x_j^{-r}\right)^{-\frac{1}{r}} \leq \sqrt[k]{x_1 \cdot \ldots \cdot x_k} \leq \left(\sum_{j=1} x_j^{r}\right)^{\frac{1}{r}}$$

attraverso la sostituzione $x_i = y_i^r$ nelle disuguaglianze geometrico-armonica e aritmo-geometrica. □

Teorema 3.92 (Disuguaglianza di Newton). *Se $(x_1, \ldots, x_n)$ è una n-upla di numeri reali positivi e*

$$d_k \doteqdot \binom{n}{k}^{-1} [t^{n-k}] \prod_{j=1}^{n} (t + x_j),$$

allora $\forall k \in [1, n-1]$ si ha:

$$d_{k-1} d_{k+1} \leq d_k^2.$$

Dimostrazione. Preso il polinomio omogeneo bivariato

$$p(x, y) = \prod_{j=1}^{n} (x + y\,x_j),$$

i valori del rapporto $\frac{x}{y}$ per cui p si annulla sono tutti reali positivi, e tale proprietà, per il teorema di Rolle, si conserva per derivazione. Segue, in particolare, che il polinomio omogeneo bivariato

$$q_k(x, y) \doteqdot \frac{\partial^{n-2} p}{(\partial y)^{k-1} (\partial x)^{n-k-1}} = n! \left(d_{k-1}\frac{x^2}{2} + d_k\,x\,y + d_{k+1}\frac{y^2}{2}\right)$$

ha discriminante non negativo, da cui la tesi. □

Teorema 3.93 (Disuguaglianza di MacLaurin)**.** *Nelle ipotesi del precedente teorema si ha:*

$$\sqrt[k]{d_k} \geq \sqrt[k+1]{d_{k+1}}.$$

Dimostrazione. Posto $d_0 = 1$, per la disuguaglianza di Newton si ha

$$(d_0\, d_2) \cdot (d_1\, d_3)^2 \cdot (d_2\, d_4)^3 \cdot \ldots \cdot (d_{k-1}\, d_{k+1})^k \leq d_1^2 \cdot d_2^4 \cdot d_3^6 \cdot \ldots \cdot d_k^{2k},$$

da cui:

$$d_{k+1}^k \leq d_k^{k+1},$$

equivalente alla tesi. □

Teorema 3.94 (Beatty)**.** *Sia r un numero irrazionale maggiore di 1 ed s il numero irrazionale che realizza $\frac{1}{r} + \frac{1}{s} = 1$. In tali ipotesi, ogni numero intero positivo o è della forma $\lfloor nr \rfloor$ o è della forma $\lfloor ns \rfloor$ per un qualche $n \in \mathbb{N}_0$.*

Dimostrazione. Supponiamo che esistano tre interi a, b, c tali per cui $a = \lfloor br \rfloor = \lfloor cs \rfloor$. Abbiamo allora:

$$br < a < br + 1, \qquad cs < a < cs + 1,$$

dove le disuguaglianze sono strette in virtù dell'irrazionalità di r ed s. Segue:

$$b + c < \frac{a}{r} + \frac{a}{s} = a < b + c + 1,$$

ma ciò è impossibile, in quanto l'intero a non può giacere strettamente tra due interi consecutivi. Viceversa, supponiamo che un certo intero a non possa essere espresso né nella forma $\lfloor br \rfloor$, per un qualche $b \in \mathbb{Z}$, né nella forma $\lfloor cs \rfloor$, per un qualche $c \in \mathbb{Z}$. Siano allora $b_0 = \lceil \frac{a}{r} \rceil$ e $c_0 = \lceil \frac{a}{s} \rceil$. Valgono:

$$\frac{a}{r} < b_0 < \frac{a}{r} + 1, \qquad \frac{a}{s} < c_0 < \frac{a}{s} + 1,$$

da cui segue:

$$a < (b_0 + c_0) < a + 2,$$

che comporta $(b_0 + c_0) = a + 1$. Si ha $b_0 r > a$, e supposto $a \neq \lfloor b_0 r \rfloor$, $b_0 r > a + 1$.
Analogamente, si ha $c_0 s > a$, e supposto $a \neq \lfloor c_0 s \rfloor$, $c_0 s > a + 1$. Ma allora:

$$(b_0 + c_0) > \frac{a}{r} + \frac{1}{r} + \frac{a}{s} + \frac{1}{s} = a + 1,$$

assurdo in virtù di quanto provato in precedenza. □

In alternativa, si consideri l'insieme ordinato $U = r\mathbb{N}_0 \cup s\mathbb{N}_0$. Dato $m \in \mathbb{N}_0$, definiamo U_m come:

$$U_m = U \cap (0, m).$$

U_m contiene $\lfloor \frac{m}{r} \rfloor$ elementi di $r\mathbb{N}_0$ e $\lfloor \frac{m}{s} \rfloor$ elementi di $s\mathbb{N}_0$. Per provare il Teorema è sufficiente provare che $U_{m+1} \setminus U_m$ non è mai vuoto, fatto che è conseguenza della disuguaglianza:

$$\left(\left\lfloor \frac{m+1}{r} \right\rfloor - \left\lfloor \frac{m}{r} \right\rfloor \right) + \left(\left\lfloor \frac{m+1}{s} \right\rfloor - \left\lfloor \frac{m}{s} \right\rfloor \right) > 0.$$

La supposizione che ambedue gli addendi (interi non negativi) nel membro sinistro siano nulli conduce infatti a:

$$\left\{ \frac{m}{r} \right\} > 1 - \frac{1}{r}, \qquad \left\{ \frac{m}{s} \right\} > 1 - \frac{1}{s},$$

da cui segue:

$$\left\{\frac{m}{r}\right\} + \left\{\frac{m}{s}\right\} > 1.$$

Tuttavia $\frac{m}{r} + \frac{m}{s} = m \in \mathbb{N}_0$, per cui il membro sinistro è esattamente pari ad 1.
Questo approccio ammette una immediata generalizzazione:

Teorema 3.95. *Se $r_1, \ldots, r_k$ sono k numeri irrazionali positivi la cui somma dei reciproci è uguale ad 1, e tali per cui gli insiemi $r_1\mathbb{N}_0, \ldots r_k\mathbb{N}_0$ sono tutti disgiunti, ogni numero naturale positivo n può essere espresso nella forma $\lfloor mr_j \rfloor$ per un qualche $m \in \mathbb{N}_0$ e per un unico $j \in [1, k]$.*

Esercizio 3.96. *Si provi che, se $p, q \in \mathbb{R}^+$ sono tali per cui ogni numero intero positivo può essere espresso o come $\lfloor pn \rfloor$, per un qualche $n \in \mathbb{Z}$, o come $\lfloor qm \rfloor$, per un qualche $m \in \mathbb{Z}$, allora $p, q \notin \mathbb{Q}$ e $\frac{1}{p} + \frac{1}{q} = 1$.*

Teorema 3.97 (Zeckendorf)**.** *Ogni numero naturale positivo può essere espresso in modo unico come somma di numeri di Fibonacci con indici non consecutivi.*

Dimostrazione. Per ogni $n > 0$, esiste certamente un $m \geq 2$ tale per cui $n \in [F_m, F_{m+1})$, in quanto la sequenza dei numeri di Fibonacci è strettamente crescente dal secondo termine in poi. In tali ipotesi, allora, $(n - F_m) \in [0, F_{m-1})$, per cui l'indice del più grande numero di Fibonacci $\leq (n - F_m)$ è al più pari a $(m - 2)$: ciò prova che, sottraendo ripetutamente da n il più grande numero di Fibonacci $\leq n$, in al più $\frac{m}{2}$ passi otteniamo 0, dunque una rappresentazione di n come somma di numeri di Fibonacci con indici non consecutivi:

$$\begin{array}{llll} n = 1234, & m = 16, & F_m = 987, & n - F_m = 247; \\ n = 247, & m = 13, & F_m = 233, & n - F_m = 14; \\ n = 14, & m = 7, & F_m = 13, & n - F_m = 1; \\ n = 1, & m = 2, & F_m = 1, & n - F_m = 0. \end{array}$$

$$1234 = F_{16} + F_{13} + F_7 + F_2.$$

□

La rappresentazione (di Zeckendorf) così calcolata è inoltre unica. Se, infatti,

$$n = \sum_{m \in M_n} F_m, \qquad M_n \subset \mathbb{N} \setminus \{0, 1\}, \qquad M_n \cap (M_n - 1) = 0,$$

detto A_n il massimo dell'insieme M_n si ha $n \in [F_{A_n}, F_{A_n+1})$. E' sufficiente procedere per induzione: se $A_n = 2$ oppure $A_n = 3$, la tesi è banalmente verificata. Se $A_n \geq 4$, allora $\max(M_n \setminus \{A_n\}) \leq A_n - 2$, per cui:

$$\sum_{m \in M_n} F_m = F_{A_n} + \sum_{m \in M_n \setminus \{A_n\}} F_m < F_{A_n} + F_{A_n - 1} = F_{A_n + 1}.$$

In virtù di quest'ultimo risultato esiste allora una corrispondenza biunivoca tra i numeri naturali positivi e i numeri naturali positivi nella cui rappresentazione binaria non figurano "1" consecutivi: poiché è ben

definita la mappa $n \to M_n$, lo è pure la mappa

$$\varphi_Z : n \longrightarrow \sum_{m \in M_n} 2^{m-2}.$$

che denominiamo *codifica di Fibonacci* di n. Se ora B_n è l'unico sottoinsieme di $\mathbb{N}$ per cui:

$$n = \sum_{m \in B_n} 2^m,$$

la mappa:

$$\varphi_B : n \longrightarrow \sum_{m \in B_n} F_{m+2}$$

è l'inversa di φ_Z,

Esercizio 3.98. (☠). *Per ogni numero naturale $n \geq 12$ si ha:*

$$n^{\frac{11}{9}} < \varphi_Z(n) < n^{\frac{13}{9}}.$$

Esercizio 3.99. *Per ogni numero naturale $k > 2$, si consideri la sequenza:*

$$G_0 = 1,\ G_1 = 2^1,\ \ldots\ ,\ G_{k-1} = 2^{k-1}, \qquad G_m = G_{m-1} + \ldots + G_{m-k},$$

e si provi che ogni numero naturale $n > 1$ può essere espresso in un modo unico come somma di elementi distinti della sequenza, in modo tale che non figurino mai k addendi con indici consecutivi.

Teorema 3.100 (Lekkerkerker)**.** *La decomposizione di Zeckendorf di un intero x nell'intervallo $[F_n, F_{n+1})$ presenta mediamente $\frac{n}{\varphi^2+1}$ addendi.*

Dimostrazione. Consideriamo che $\varphi_Z(x)$ ha $n-1$ bit, e calcoliamo quanti interi nell'intervallo dato hanno una decomposizione di Zeckendorf che consta di $k+1$ addendi. Il problema è equivalente a contare quante stringhe binarie distinte possiamo ottenere inserendo k cifre "1" nelle intercapedini tra $n-k$ cifre "0" consecutive: chiaramente, $\binom{n-k-1}{k}$. Il numero medio di addendi è dunque dato da:

$$\frac{1}{F_{n-1}} \sum_{k=0}^{n} (k+1) \binom{n-k-1}{k},$$

e il Teorema segue dal fatto che:

$$\sum_{k=0}^{n} \binom{n-k-1}{k} = F_{n-1}.$$

□

Teorema 3.101 (Ostrowski)**.** *Sia $\alpha \in (0,1)$ un numero irrazionale associato alla frazione continua $[0; a_1, a_2, \ldots]$, con convergenti $\frac{p_n}{q_n} = [0; a_1, \ldots, a_n]$. Ogni numero intero positivo N può essere rappresentato in modo unico come:*

$$N = \sum_{k=1}^{m} b_k\, q_{k-1},$$

dove:

$$\begin{cases} 0 \leq b_1 \leq a_1 - 1, & \\ 0 \leq b_k \leq a_k & \text{per} \quad k \geq 2, \\ b_k = 0 & \text{se} \quad b_{k+1} = a_{k+1}. \end{cases}$$

Teorema 3.102 (D'Aurizio)**.** *Preso $\varphi = \frac{1+\sqrt{5}}{2}$, un numero naturale positivo è della forma $\lfloor \varphi \cdot j \rfloor$ per un qualche $j \in \mathbb{N}_0$ oppure della forma $\lfloor \varphi^2 \cdot k \rfloor$ per un qualche $k \in \mathbb{N}_0$ a seconda che $\nu_2(\varphi_Z(n))$ sia pari oppure dispari, rispettivamente.*

Dimostrazione. Notiamo preliminarmente che, in virtù del Teorema di Beatty, ogni numero naturale positivo o è della forma $\lfloor \varphi \cdot j \rfloor$ o è della forma $\lfloor \varphi^2 \cdot k \rfloor$, poiché $\frac{1}{\varphi} + \frac{1}{\varphi^2} = 1$. Proviamo che ogni F_{2k}, con $k > 0$, è della prima forma:

$$\varphi F_{2k-1} - F_{2k} = \frac{1}{\varphi^{2k-1}} \in (0,1) \quad \Longrightarrow \quad F_{2k} = \lfloor \varphi \cdot F_{2k-1} \rfloor.$$

Analogamente, ogni F_{2k+1}, con $k > 0$, è della seconda forma:

$$\varphi^2 F_{2k-1} - F_{2k+1} = \frac{1}{\varphi^{2k-1}} \in (0,1) \quad \Longrightarrow \quad F_{2k+1} = \lfloor \varphi^2 \cdot F_{2k-1} \rfloor.$$

Abbiamo inoltre, per ogni intero $k > 0$:

$$F_{2k+2} - \varphi^2 F_{2k} = \frac{1}{\varphi^{2k}}, \qquad F_{2k+1} - \varphi F_{2k} = \frac{1}{\varphi^{2k}}.$$

Supponiamo che $\nu_2(\varphi_Z(n))$ sia pari. In virtù del Teorema di Zeckendorf abbiamo:

$$n = F_{2k} + \sum_{m \in M} F_m,$$

dove $k > 0$ e gli elementi di M sono $\geq (2k+2)$ e non consecutivi. Vale allora:

$$0 = \frac{1}{\varphi} - \sum_{k=1}^{+\infty} \frac{1}{\varphi^{2k}} < \varphi \cdot \left(F_{2k-1} + \sum_{m \in M} F_{m-1} \right) - n < \sum_{k=0}^{+\infty} \frac{1}{\varphi^{2k+1}} = 1,$$

per cui n è della prima forma:

$$n = \left\lfloor \varphi \cdot \left(F_{2k-1} + \sum_{m \in M} F_{m-1} \right) \right\rfloor.$$

Analogamente, se $\nu_2(\varphi_Z(n))$ è dispari, si ha:

$$n = F_{2k+1} + \sum_{m \in M} F_m,$$

dove $k > 0$ e gli elementi di M sono $\geq (2k+3)$ e non consecutivi. Vale allora:

$$n = \left\lfloor \varphi^2 \cdot \left(F_{2k-1} + \sum_{m \in M} F_{m-2} \right) \right\rfloor.$$

□

SEGUONO ORA UN PO' DI FATTI SU FIBONACCI.

$$\binom{p-1}{n} \equiv (-1)^n \pmod{p},$$

$$2^{p-2}F_{p-1} = \binom{p-1}{1} + \binom{p-1}{3}5 + \ldots + \binom{p-1}{p-2}5^{\frac{p-3}{2}},$$

$$2^{p-1}F_{p-1} \equiv -\left(1 + 5 + \ldots + 5^{\frac{p-3}{2}}\right) \equiv \frac{1 - 5^{\frac{p-1}{2}}}{4} \pmod{p},$$

$$2^p F_{p+1} \equiv (p+1)\left(1 + 5^{\frac{p-1}{2}}\right).$$

Conseguenza: se $\left(\frac{5}{p}\right) = +1$ allora $F_{p-1} \equiv 0 \pmod{p}$ e $F_p \equiv 1 \pmod{p}$, per cui il periodo modulo p della successione di Fibonacci divide $p-1$. Se $\left(\frac{5}{p}\right) = -1$ allora $F_{p+1} \equiv 0 \pmod{p}$ e $F_p \equiv -1 \pmod{p}$, per cui il periodo modulo p della successione di Fibonacci divide $2(p+1)$.
FATTO: se una progressione aritmetica contiene un numero di Fibonacci, allora ne contiene infiniti. Possiamo infatti supporre che la progressione sia della forma $F_k + m\mathbb{Z}$, e dal fatto che la successione di Fibonacci è periodica modulo m dedurre che $\exists\, j > k : F_j \equiv F_k \pmod{m}$.
FATTO: se una progressione aritmetica è della forma $a + 5^k\mathbb{Z}$ essa contiene infiniti numeri di Fibonacci, in quanto $\{F_n\}_{n\in\mathbb{N}}$ rappresenta tutte le possibili classi di resto (mod 5^k) (divertente da provare per induzione su k).
FATTO: dato un primo $p \equiv \pm 1 \pmod{5}$, il periodo della successione di Fibonacci (mod p) ha lunghezza $p-1$, e in esso figura per due volte la classe di resto 1. Detto dunque E_p il numero di classi di resto non rappresentate dalla successione di Fibonacci (mod p), si ha $E_p \geq 2$.
FATTO: un numero n appartiene alla successione di Fibonacci se e solo se $5m^2 \pm 4$ è un quadrato, ragion per cui:

$$E_p \geq \frac{1}{4}\sum_{k=0}^{p-1}\left(1 - \left(\frac{5k^2-4}{p}\right)\right)\left(1 - \left(\frac{5k^2+4}{p}\right)\right),$$

in quanto il membro destro conta le classi (mod p) per cui né $(5k^2-4)$ né $(5k^2+4)$ risultano residui quadratici (mod p). Poiché 5 è residuo quadratico modulo p, il membro destro nell'ultima disuguaglianza risulta pari a:

$$\frac{1}{4}\sum_{k=0}^{p-1}\left(1 - \left(\frac{k-1}{p}\right)\right)\left(1 + \left(\frac{k}{p}\right)\right)\left(1 - \left(\frac{k+1}{p}\right)\right) = \frac{1}{4}\left(p + 1 - \sum_{k=0}^{p-1}\left(\frac{k^3-k}{p}\right)\right),$$

Se $p \equiv -1 \pmod{4}$, per quanto noto sul numero di punti della curva ellittica $y^2 = x^3 - x$ su $\mathbb{F}_p$,
si ha $\sum_{k=0}^{p-1}\left(\frac{k^3-k}{p}\right) = 0$, da cui:

$$E_p \geq \frac{p+1}{4},$$

e questo risultato può essere provato anche per via elementare (vedi discorso sulle 3-AP in $\mathbb{F}_p$ e sulle soluzioni di $x^2 + y^2 \equiv 2 \pmod{p}$). Nel caso in cui $p \equiv 1 \pmod{4}$ il Teorema di Hasse (che nel caso specifico della curva ellittica $y^2 = x^3 - x$ può essere dimostrato facendo unicamente ricorso ali teoremi di reciprocità quadratica e biquadratica e alle somme di Jacobi, cfr. Ireland & Rosen pg. 307) garantisce che si abbia:

$$E_p > \left(\frac{\sqrt{p}-1}{2}\right)^2.$$

INTRODURRE TEORIA DEI DISCRIMINANTI - vedi relazione TFA

Esercizio 3.103. *Si determini il minimo di*

$$\frac{a+b+c}{\sqrt[3]{abc}}$$

quando a, b, c sono tre numeri reali positivi soggetti al vincolo:

$$a^2+b^2+c^2 = \frac{27}{11}(ab+ac+bc).$$

Dimostrazione. Per omogeneità non è restrittivo supporre che si abbia $a+b+c=1$. Va allora massimizzata la quantità $P=abc$ sotto il vincolo che a, b, c siano tre radici positive del polinomio:

$$p(x) = x^3 - x^2 + \frac{11}{49}x - P,$$

in quanto $a^2+b^2+c^2 = (a+b+c)^2 - 2(ab+ac+bc)$, dunque $ab+ac+bc = \frac{11}{49}$. Poiché $p(x)$ è una funzione crescente su $\mathbb{R}^-$ e $p(0)<0$, le radici reali di $p(x)$ sono tutte positive; queste sono una oppure tre a seconda del valore del discriminante di $p(x)$, che dipende unicamente da P. Il minimo ricercato si avrà allora in corrispondenza di un valore di P per cui il discriminante di $p(x)$ si annulla. Si ha:

$$\Delta(p(x)) = \Delta(p(x+1/3)) = \Delta\left(x^3 - \frac{16}{147}x + \frac{1}{1323} - P\right) = -\frac{3176523P^2 - 4802P - 605}{117649},$$

ragion per cui il discriminante di $p(x)$ si annulla in corrispondenza di $P = -\frac{121}{9261}$ e di $P = \frac{5}{343}$.
Abbiamo allora che il minimo cercato risulta pari a:

$$\frac{7}{\sqrt[3]{5}}$$

e si realizza in corrispondenza dei valori di a, b, c che risultano radici del polinomio:

$$p(x) = x^3 - x^2 + \frac{11}{49}x - \frac{5}{343} = \left(x - \frac{1}{7}\right)^2\left(x - \frac{5}{7}\right).$$

□