

Soluzioni di qualche problema dalla gara nazionale iraniana

Andrea Fogari

15 gennaio 2007

Soluzione di alcuni problemi dalla gara nazionale delle olimpiadi della matematica iraniane del 2006.

1 Algebra

Problema 1.1. Siano x_1, x_2, \dots, x_s reali positivi tali che $x_1 x_2 \cdots x_s = 1$.

Dimostrare che, per ogni $m \geq n > 0$:

$$x_1^m + x_2^m + \dots + x_s^m \geq x_1^n + x_2^n + \dots + x_s^n$$

Dimostrazione. Poniamo $d = m - n$. Siccome la disuguaglianza è simmetrica, possiamo assumere $x_1 \geq x_2 \geq \dots \geq x_s$. Questo implica che:

$$x_1^n \geq x_2^n \geq \dots \geq x_s^n$$

$$x_1^d \geq x_2^d \geq \dots \geq x_s^d$$

Quindi, applicando la disuguaglianza di Chebyshev a queste s -uple ordinate allo stesso modo, e poi AM-GM, otteniamo:

$$\begin{aligned} & \frac{x_1^m + x_2^m + \dots + x_s^m}{s} = \\ & \frac{x_1^d \cdot x_1^n + x_2^d \cdot x_2^n + \dots + x_s^d \cdot x_s^n}{s} \\ & \geq \frac{x_1^d + x_2^d + \dots + x_s^d}{s} \cdot \frac{x_1^n + x_2^n + \dots + x_s^n}{s} \\ & \geq \sqrt[s]{x_1^d \cdot x_2^d \cdots x_s^d} \cdot \frac{x_1^n + x_2^n + \dots + x_s^n}{s} \\ & = 1 \cdot \frac{x_1^n + x_2^n + \dots + x_s^n}{s} \end{aligned}$$

□

Problema 1.2. $P(x)$ è un polinomio a coefficienti reali tale che per ogni $x \geq 0$, $P(x) \geq 0$. Dimostrare che esistono due polinomi a coefficienti reali $A(x), B(x)$ tali che $P(x) = A(x)^2 + xB(x)^2$.

Dimostrazione. Sia S l'insieme dei polinomi che possono essere scritti nella forma $A(x)^2 + xB(x)^2$, T l'insieme dei polinomi F tali che $x \geq 0 \Rightarrow F(x) \geq 0$. Vogliamo dimostrare che $S = T$. Chiaramente, se un elemento appartiene ad S , appartiene anche ad T , perchè il quadrato di un polinomio è sempre non negativo.

Il prodotto di due elementi di S è ancora un elemento di S :

$$\begin{aligned} (A^2 + xB^2)(C^2 + xD^2) &= A^2C^2 + xA^2D^2 + xB^2C^2 + x^2B^2D^2 \\ &= A^2C^2 + xA^2D^2 + xB^2C^2 + x^2B^2D^2 + (2xA^2B^2C^2D^2 - 2xA^2B^2C^2D^2) \\ &= (A^2C^2 + 2xA^2B^2C^2D^2 + x^2B^2D^2) + (xA^2D^2 - 2xA^2B^2C^2D^2 + xB^2C^2) \\ &= (AC + BD)^2 + x(AD - BC)^2 \end{aligned}$$

Inoltre, se $P(x) = A(x)^2 + xB(x)^2$ con $k \geq 0$ allora $kP(x) = (\sqrt{k}A(x))^2 + x(\sqrt{k}B(x))^2$. Quindi, essendo il coefficiente direttivo di P positivo (altrimenti per $x \rightarrow +\infty, P(x) \rightarrow -\infty$), possiamo supporre P monico.

Per il teorema fondamentale dell'algebra, $P(x)$ si scompone come prodotto di polinomi a coefficienti reali di grado 1 o 2. Dimostriamo che ogni fattore è un elemento di T . Per assurdo, tra tutti i polinomi a coefficienti reali che dividono P i cui fattori non appartengono a T , scegliamo uno Q di grado massimo. Se Q non ha radici reali positive, allora ogni suo fattore non ne ha, ma un polinomio (monico) senza radici reali positive è sempre non negativo per $x \geq 0$, quindi appartiene a T , impossibile per come è stato scelto Q . Se Q ha una radice positiva λ di molteplicità maggiore di 2, allora $(x - \lambda)^2$ è un fattore di Q che appartiene a T , impossibile. Quindi Q ha una radice positiva λ di molteplicità 1, cioè $Q(\lambda) = 0$ ma $Q'(\lambda) \neq 0$, quindi in un intorno di λ si avrà $Q(x_0) < 0$ con $x_0 > 0$. P è ottenuto moltiplicando Q per fattori che sono non negativi sui reali positivi, quindi in un intorno di λ si avrà $P(x) < 0$.

Resta da verificare solo che ogni polinomio monico di primo o secondo grado che appartiene a T , appartiene a S .

- il polinomio è di primo grado, allora deve essere della forma $x + a$ con a non negativo. Allora $x + a = (\sqrt{a})^2 + x(1^2)$.
- il polinomio $R(x) = x^2 + bx + c$ è di secondo grado. Consideriamo il polinomio $K(x) = (b - x)^2 - 4c$. Siccome $K(0) \leq 0$ perchè il discriminante di R non può essere positivo, K avrà una radice non negativa λ . Allora $R(x) = (x^2 + (b - \lambda)x + c) + x(\sqrt{\lambda})^2$, dove $x^2 + (b - \lambda)x + c$ è il quadrato di un polinomio perchè ha determinante 0.

□

Problema 1.3. P, Q, R sono polinomi non nulli tali che, per ogni $z \in \mathbb{C}$, $P(z)Q(\bar{z}) = R(z)$.

- se P, Q, R sono a coefficienti reali, dimostrare che $Q(x)$ è un polinomio costante
- quest'affermazione vale ancora se P, Q, R sono a coefficienti complessi?

Dimostrazione. Dimostreremo che se P, Q, R sono a coefficienti complessi, $Q(x)$ è un polinomio costante.

Possiamo supporre che P ed R non abbiano radici in comune. Infatti, se hanno una radice λ in comune, esistono polinomi P', R' tali che $P(x) = (x - \lambda)P'(x)$ e $R(x) = (x - \lambda)R'(x)$. Sappiamo che:

$$\forall x \in \mathbb{C} \quad P(x)Q(\bar{x}) = R(x)$$

Sostituendo:

$$\forall x \in \mathbb{C} \quad (x - \lambda)P'(x)Q(\bar{x}) = (x - \lambda)R'(x)$$

Quindi, dividendo per $(x - \lambda)$:

$$\forall x \in \mathbb{C}, x \neq \lambda \quad P'(x)Q(\bar{x}) = R'(x)$$

Ma l'uguaglianza deve valere anche per $x = \lambda$. Infatti $P(x), R(x)$, essendo polinomi, sono funzioni continue, e $Q(\bar{x})$, essendo composizione delle funzioni continue \bar{x} e $Q(x)$, è continua. Le funzioni continue sono chiuse rispetto alla somma e alla moltiplicazione, quindi anche $f(x) = P(x)Q(\bar{x}) - R(x)$ è continua. Questa funzione vale 0 per ogni $x \neq \lambda$. Se $f(\lambda) \neq 0$, questo sarebbe un punto di discontinuità, quindi $f(\lambda) = 0$.

Chiaramente possiamo continuare questo procedimento di "scartare le radici" finchè ce ne sono a disposizione, continuando ad avere l'uguaglianza per ogni x complesso. Quindi possiamo supporre che $P(x)$ ed $R(x)$ non abbiano radici in comune. A questo punto, se z è una radice di P , avremo che $R(z) = P(z)Q(\bar{z}) = 0$, e z sarebbe una radice di R . Quindi P è senza radici, cioè è un polinomio costante, poniamo $P(x) = k$. Chiamiamo $S(x) = \frac{R(x)}{k}$. Allora

$$\forall x \in \mathbb{C} \quad Q(\bar{x}) = S(x)$$

cioè, $Q(\bar{x})$ è una funzione polinomiale, che per comodità identificheremo con il polinomio.

Sia $Q'(x) = \overline{Q(\bar{x})}$. $Q'(x)$ è ancora un polinomio. Infatti, se

$$Q(x) = q_n x^n + q_{n-1} x^{n-1} + \dots + q_1 x + q_0$$

Allora, per le proprietà del coniugato:

$$\begin{aligned} Q'(x) &= \overline{q_n \bar{x}^n + q_{n-1} \bar{x}^{n-1} + \dots + q_1 \bar{x} + q_0} \\ &= \overline{q_n \bar{x}^n} + \overline{q_{n-1} \bar{x}^{n-1}} + \dots + \overline{q_1 \bar{x}} + \overline{q_0} \\ &= \overline{q_n} x^n + \overline{q_{n-1}} x^{n-1} + \dots + \overline{q_1} x + \overline{q_0} \end{aligned}$$

Ora, sia n il grado di $Q(\bar{x})$; si scelgano qualsiasi $n + 1$ reali a_1, \dots, a_{n+1} . Poichè, per il teorema fondamentale dell'algebra, l'equazione $Q(\bar{x}) = a_i$ ha sempre

soluzione per ogni $1 \leq i \leq n + 1$, esiste anche una $n + 1$ -upla di complessi s_1, \dots, s_{n+1} tale che $Q(s_i) = a_i$ per ogni $1 \leq i \leq n + 1$. Inoltre, poichè (per ogni $1 \leq i \leq n + 1$) a_i è un reale, avremo

$$Q(\overline{s_i}) = a_i = \overline{a_i} = \overline{Q(s_i)} = Q'(s_i)$$

Quindi $Q'(x) = Q(\overline{x})$ per $n+1$ valori distinti di x . Poichè $Q(\overline{x})$ e $Q'(x)$, polinomi di grado n , assumono lo stesso valore in $n + 1$ punti distinti, devono essere lo stesso polinomio. Quindi, per ogni $x \in \mathbb{C}$:

$$Q(\overline{x}) = Q'(x)$$

$$Q(\overline{x}) = \overline{Q(x)}$$

$$Q(\overline{x}) \in \mathbb{R}$$

Quindi, essendo la funzione \overline{x} biiettiva, il codominio di Q sono i numeri reali. Questo è possibile solo se Q è di grado 0. Se Q fosse di grado ≥ 1 , scelto un complesso **non reale** ω , il polinomio $Q(x) - \omega$, per il teorema fondamentale dell'algebra, avrebbe almeno una soluzione, ma $Q(x)$ non è mai non reale, assurdo. \square

2 Combinatoria

Problema 2.1. *Sia A un insieme di n elementi. Trovare tutte le antcatene di dimensione massima dell'insieme dei sottoinsiemi di A , ordinato per inclusione.*

Dimostrazione. Caso 1: n è pari. Poniamo per comodità $n = 2k$.

Sia C l'insieme di tutti i sottoinsiemi di A con k elementi. C è un'antcatena perchè due insiemi distinti, uno sottoinsieme dell'altro, non possono avere lo stesso numero di elementi. Dimosteremo che ogni antcatena diversa da C ha meno elementi di C .

Data una generica famiglia di sottoinsiemi X , indichiamo con $f(X)$ il numero di catene massimali che hanno almeno un elemento tra quelli di X .

- non esiste una catena contenente due elementi di X . Altrimenti quei due elementi sarebbero uno sottoinsieme dell'altro, impossibile.
- contiamo quante sono tutte le catene massimali di $P(A)$ (l'insieme dei sottoinsiemi di A). Ogni catena massimale si ottiene partendo da \emptyset e aggiungendo ogni volta un elemento, sempre diverso da quegli aggiunti prima. Quindi è ovvio che le catene massimali sono in corrispondenza biunivoca con le permutazioni di n elementi, che sono $n!$.
- calcoliamo $f(X)$. Ogni supponiamo che un insieme $x \in X$ contenga y elementi. Allora per costruire una catena massimale che contenga x , dobbiamo solo scegliere come ordinare gli y elementi di x , e come ordinare gli $(n - y)$ elementi che non sono contenuti in x . Deduciamo:

$$f(X) = \sum_{x \in X} |x|!(n - |x|)!$$

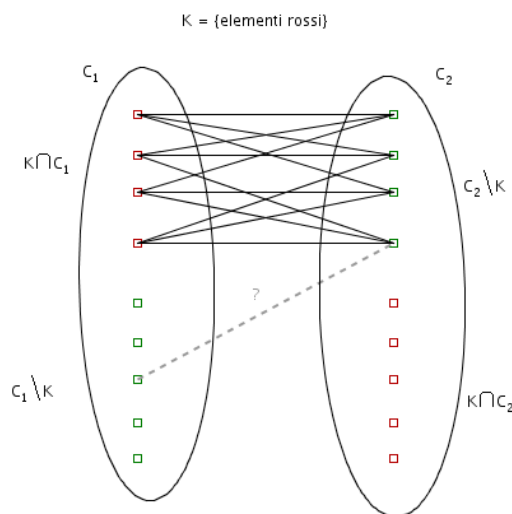
- calcoliamo $f(C)$. Ogni catena massimale avrà almeno un elemento di cardinalità k , quindi $f(C) = n!$.
- supponiamo esista un'antcatena D con $|D| = |C|$. Se D è diversa da C , allora esiste un elemento $d \in D$ tale che $|d| \neq k$. Poichè questo implica che $|d|(n - |d|)! > k!k!$, avremo che $f(D) > f(C) = n!$. Ma è impossibile che un insieme di catene massimali sia più grande dell'insieme di tutte le catene massimali . . .
- l'ultimo argomento ovviamente funziona anche se $|D| > |C|$ o se esistono più elementi di D con più o meno di k elementi.

Caso 2: n è dispari. Poniamo per comodità $n = 2k + 1$.

Sia C_1 l'insieme di tutti i sottoinsiemi di A con k elementi, C_2 l'insieme di tutti i sottoinsiemi di A con $k + 1$ elementi. La dimostrazione del caso 1 implica che non possono esistere antcatene di dimensione massima con un numero di elementi diverso da k o $k + 1$. Ora dimostreremo che ogni antcatena di dimensioni massime con gli elementi che appartengono a $C_1 \cup C_2$, deve essere C_1 o C_2 .

Consideriamo l'insieme $G = C_1 \cup C_2$ e connettiamo due elementi se e soltanto se uno è sottoinsieme dell'altro. Otteniamo un grafo. Vediamo com'è sto grafo.

- G è bipartito. Abbiamo infatti che $G = C_1 \cup C_2$, ma nessun elemento di C_1 è collegato con un altro elemento di C_1 , e lo stesso vale per C_2 .
- G è $k+1$ -regolare. Un insieme di k elementi può essere esteso a uno di $k+1$ aggiungendo uno qualsiasi degli elementi che non gli appartengono. Un insieme di $k+1$ elementi può essere ridotto a uno di k elementi togliendo uno qualsiasi degli elementi che gli appartengono.
- G è connesso. A partire da un qualsiasi elemento x , posso procedere in questo modo: aggiungo un elemento, tolgo un elemento, aggiungo, tolgo, ... fino a raggiungere un qualsiasi elemento y .



Questo ci è utile. Infatti, sia K una catena di dimensioni massime. Allora

$$(K \cap C_1) \cup (C_2 \setminus K), (K \cap C_2) \cup (C_1 \setminus K)$$

sono due componenti sconnesse del grafo. Resta da dimostrare appunto questo. Ciascuno degli elementi di $K \cap C_1$ non è collegato con elementi di C_1 , e neanche con elementi di K , quindi è collegato solo con elementi di $C_2 \setminus K$. Inoltre $|C_1| = |C_2| = |K|$, quindi $|K \cap C_1| = |C_2 \setminus K|$. Il numero di coppie (non ordinate) di elementi connessi, il primo in $K \cap C_1$ e il secondo in $C_2 \setminus K$ è $(k+1) \cdot |K \cap C_1|$ perchè ogni elemento di $C_2 \setminus K$ ha grado $k+1$ ed è collegato solo ad elementi di $C_2 \setminus K$. Poichè anche gli elementi di $C_2 \setminus K$ hanno tutti grado $k+1$, da questo segue che gli elementi di $C_2 \setminus K$ sono collegati solo ad elementi di $K \cap C_1$.

Questo conclude il problema. Infatti, abbiamo diviso il grafo in due componenti sconnesse. Ma il grafo è connesso, quindi uno degli $(K \cap C_1) \cup (C_2 \setminus K), (K \cap C_2) \cup (C_1 \setminus K)$ è vuoto, cioè $K = C_1$ o $K = C_2$.

□

Problema 2.2. La Fondazione Nazionale per la Felicità vuole stimare la felicità della gente del Paese. La Fondazione ha scelto n persone a cui, per un certo periodo, viene chiesto ogni mattina se sono felici o no. Si sa che, confrontando le risposte date in due qualsiasi giorni distinti, esattamente metà delle persone ha cambiato idea. Dimostrare che, dopo k giorni dall'inizio del sondaggio, le persone che fino a quel momento hanno dato tante risposte "sì" quante "no" sono al più

$$n - \frac{n}{k}$$

Lemma 1. Fissato l'intero positivo k , con la condizione che i reali non negativi a, b abbiano somma k , la funzione:

$$f(a, b) = \binom{a}{2} + \binom{b}{2}$$

ha minimo se $a = b$ e massimo se $a = 0$ o $b = 0$.

Dimostrazione. Sviluppando i binomiali e raccogliendo possiamo riscrivere la funzione come:

$$f(a, b) = \frac{1}{2}(a^2 + b^2 - a - b) = \frac{1}{2}(a^2 + b^2 - k)$$

Questa funzione assumerà massimo e minimo negli stessi punti in cui ha massimo e minimo:

$$g(a, b) = a^2 + b^2$$

perchè abbiamo moltiplicato per una costante e aggiunto una costante. Per $AM - GM$:

$$a^2 + b^2 \geq \frac{1}{2}(a + b)^2 = \frac{1}{2}k^2$$

con uguaglianza sse $a = b = \frac{k}{2}$. Inoltre $k^2 = (a + b)^2 \geq a^2 + b^2$ perchè $(a + b)^2 - a^2 - b^2 = 2ab$, intero non negativo. L'uguaglianza la otteniamo se e soltanto $2ab = 0$, quindi $a = 0$ o $b = 0$. \square

Dimostrazione del problema. Conteremo in due modi le terne p, g_1, g_2 tali che p è una persona che ha risposto allo stesso modo nel giorno g_1 e nel giorno g_2 . L'ordine dei giorni non conta. Indichiamo il numero di queste terne con x .

Scelti a caso due giorni, per le ipotesi del problema, esistono esattamente $\frac{n}{2}$ persone che hanno dato una risposta diversa in quei due giorni, quindi esistono esattamente $\frac{n}{2}$ persone che hanno dato la stessa risposta. I modi di scegliere due giorni tra tutti i k trascorsi sono $\binom{k}{2}$, da questo ragionamento otteniamo

$$x = \binom{k}{2} \frac{n}{2} \tag{1}$$

Ora contiamo nel secondo modo. Sia s_i il numero di risposte "sì" che ha dato la i -esima persona nei primi k giorni, ed n_i il numero di risposte "no" che ha dato la i -esima persona nei primi k giorni. Fissata una persona, per trovare tutte le terne p, g_1, g_2 dobbiamo sommare le coppie di giorni in cui ha risposto "sì" e le coppie di giorni in cui ha risposto "no". Questo ragionamento ci dà la formula per x :

$$x = \sum_{i=1}^n \left(\binom{s_i}{2} + \binom{n_i}{2} \right)$$

È chiaro che, per ogni i , $s_i + n_i = k$ perchè le uniche risposte possibili sono sì o no. Supponiamo che esistano più di $n - \frac{n}{k}$ persone per cui $s_i = n_i$ (stiamo negando la tesi del teorema). Possiamo trovare $\lceil n - \frac{n}{k} \rceil$ persone per cui $s_i = n_i$, e quindi il loro addendo nella sommatoria sopra è uguale a $2^{\binom{k}{2}}$. Se k non è dispari, nessuno può aver dato tante risposte sì quante no, ed il problema è ovvio. Per le restanti persone, grazie al lemma 1, possiamo usare la sovrastima $\binom{k}{2}$ (il numero di coppie di giorni in cui una persona ha dato la stessa risposta è massimo se tutte le risposte sono uguali). Con questo ragionamento otteniamo una sovrastima di x :

$$x < \left(n - \frac{n}{k}\right) 2^{\binom{k}{2}} + \frac{n}{k} \binom{k}{2}$$

La disuguaglianza è stretta perchè le persone con $s_i = n_i$ sono più di $n - \frac{n}{k}$, quindi almeno una ha subito la sovrastima. Sviluppiamo ora i binomiali nell'ultima formula:

$$x < n \left(\frac{k-1}{k}\right) 2^{\frac{\binom{k}{2}(\frac{k}{2}-1)}{2}} + \frac{n k(k-1)}{2}$$

Raccogliamo, semplifichiamo:

$$\begin{aligned} x &< n(k-1) \frac{1}{2} \left(\frac{k}{2} - 1\right) + n \frac{k-1}{2} \\ x &< \frac{n}{2} \left((k-1) \left(\frac{k}{2} - 1\right) + (k-1) \right) \\ x &< \frac{n k(k-1)}{2} \\ x &< \frac{n}{2} \binom{k}{2} \end{aligned}$$

Ma, applicando la formula (1), otteniamo la contraddizione:

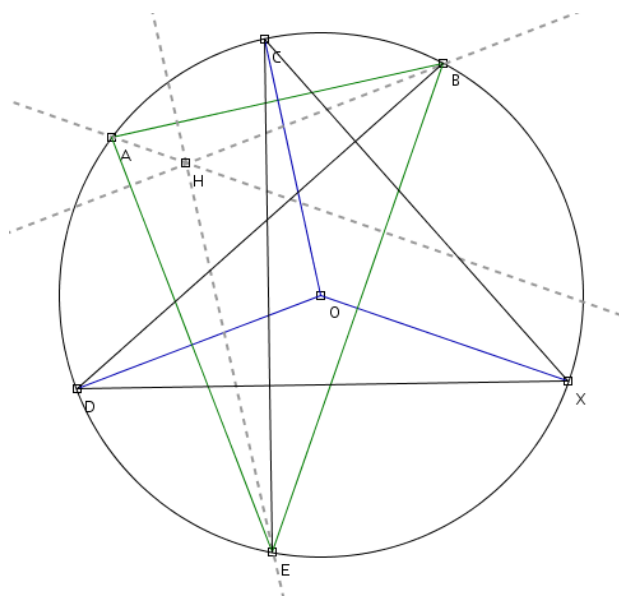
$$x < x$$

□

3 Geometria

Problema 3.1. Sia AB una corda di una circonferenza di centro O . C è il punto medio dell'arco AB . X è un punto sulla circonferenza. D è l'intersezione tra la circonferenza e la perpendicolare da B alla retta CX . E è l'intersezione tra la circonferenza e la perpendicolare da C alla retta DX .

Siano l_1, l_2, l_3 le parallele ad OC, OD, OX per E, B, A . Dimostrare che l_1, l_2, l_3 concorrono. Trovare il luogo dei punti di concorrenza al variare di X sulla circonferenza.



Dimostrazione. Siano F l'intersezione tra CX e BD , G l'intersezione tra DX e CE . Allora il quadrilatero $CDFG$ è ciclico perchè $\angle CFD = \angle CGD = 90$. Quindi X è il punto medio dell'arco BE , perchè $\angle BDG = \angle FDG = \angle FCG = \angle XCE$.

Inoltre, D è il punto medio dell'arco AE , perchè:

$$90 - \angle ABD = \angle CBA + \angle XCB$$

$$90 - \angle DBE = 90 - \angle DXE = \angle XEC = \angle XEB + \angle BEC$$

Ma $\angle CBA + \angle XCB = \angle XEB + \angle BEC$ perchè gli archi AC, CB sono uguali.

Poichè C è il punto medio dell'arco AB , X è il punto medio dell'arco BE e D è il punto medio dell'arco EA , abbiamo che OC, OD, OX sono rispettivamente perpendicolari ad AB, EA, BE , quindi l_1, l_2, l_3 sono le altezze del triangolo ABE ed è noto che concorrono.

Cerchiamo ora i punti di X da cui la costruzione di E perderebbe significato:

- la costruzione della retta CX perde significato sse X coincide con C .
- la perpendicolare da un punto a una retta è sempre ben definita.
- l'ulteriore intersezione tra una secante e la circonferenza è definita anche quando la retta è tangente

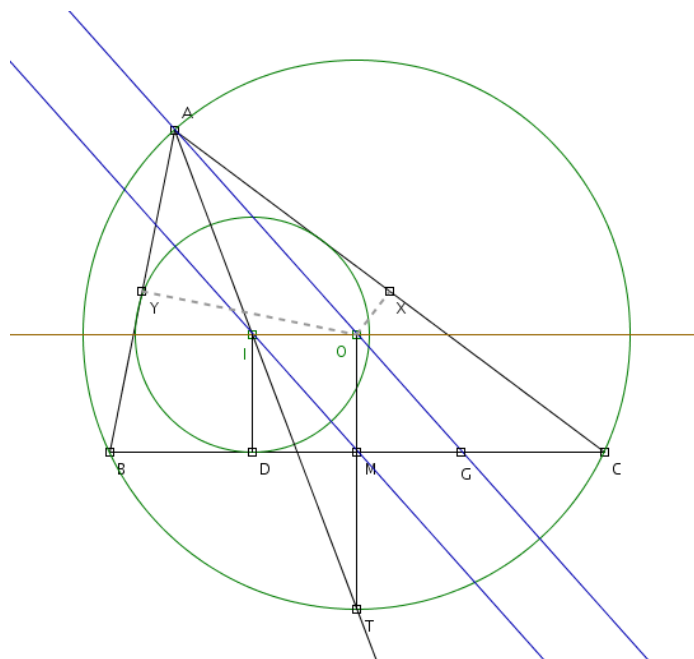
- la costruzione della retta DX perde significato se X coincide con D . Allora la retta BX sarebbe perpendicolare a CX , allora B, C sarebbero diametralmente opposti e quindi B coincide con A . Assurdo.

Ad ogni posizione di E diversa da A, B è possibile far corrispondere una posizione di X da cui la costruzione data nel problema porterebbe alla posizione di E di nostra scelta. Infatti basta scegliere il punto medio dell'arco BE . Inoltre, se E coincide con A o B , la costruzione dell'ortocentro non ha più significato.

Il problema di trovare il luogo dei punti di concorrenza è quindi equivalente a trovare il luogo degli ortocentri di ABE al variare di E sulla circonferenza, ovvero Cesenatico 2006/3 \approx 668, 667.

Lo dimostriamo in questo modo: sia M il punto medio di AB . Al variare di E sulla circonferenza, il baricentro G si ottiene con un'omotetia di centro M e fattore $\frac{1}{3}$. L'ortocentro si trova da G con un'omotetia di centro O e fattore 3. La composizione di due omotetie è un'omotetia. L'immagine della circonferenza è un'altra circonferenza, dello stesso raggio (perchè $\frac{1}{3} \cdot 3 = 1$). L'immagine di O è il simmetrico di O rispetto ad M . Quindi il luogo degli ortocentri è dato da una circonferenza simmetrica alla circonferenza originale rispetto alla retta AB . Bisogna togliere le immagini dei punti A, B che sono date dalle intersezioni delle rette perpendicolari ad AB , passanti per A, B , e la circonferenza immagine. \square

FIXME! (il caso ottusangolo)



Problema 3.2. Sia ABC un triangolo, M il punto medio di BC , I il suo incentro, T il punto medio dell'arco BC non contenente A della circonferenza circoscritta ad ABC . Dimostrare che:

$$\cos \angle ABC + \cos \angle ACB = 1 \Leftrightarrow MI = MT$$

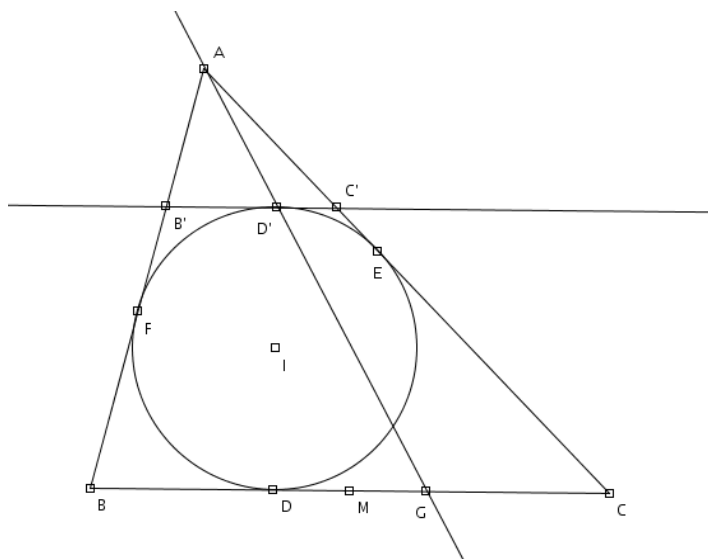
Prima, sistemo le notazioni: indichiamo con O il circocentro di ABC , con a, b, c i lati BC, CA, AB , con α, β, γ gli angoli $\angle CAB, \angle ABC, \angle BCA$, con r il raggio della circonferenza inscritta, con R il raggio della circonferenza circoscritta, con p il semiperimetro, con (ABC) la sua area. Quando saranno necessari nuovi punti, li aggiungeremo.

Per risolvere questo problema ci serviremo di qualche fatto (piu' o meno) noto. Non essendo sicuro che questi siano dati per scontati, mi toccherà prima dimostrarli tutti.

Fatto 1. A, I, T sono allineati.

Dimostrazione. Essendo T il punto medio dell'arco BC non contenente A , gli archi BT e CT sono congruenti. Per il teorema degli angoli alla circonferenza, avremo quindi: $\angle TAB = \angle TAC$, cioè T giace sulla bisettrice dell'angolo $\angle BAC$. Poichè anche I giace su questa bisettrice, questo fatto è dimostrato. \square

Fatto 2. Sia D la proiezione dell'incentro su BC . Sia s la retta IM , s' la parallela ad IM passante per A . Allora s' si ottiene da s con un'omotetia di centro D e fattore 2.



Dimostrazione. Siano E, F le proiezioni di I su CA, AB , D' il simmetrico di D rispetto a I , G l'intersezione delle rette AD' e BC . L'omotetia di centro A che porta D' in G ha fattore k e manda B' in B e C' in C . $B'C'$ è tangente all'incirconfenza perchè parallela a BC e passante per il simmetrico di D rispetto al centro dell'incirconfenza, quindi è la simmetrica di BC rispetto al centro dell'incirconfenza, quindi chiaramente è ancora tangente.

Ora useremo ripetutamente il fatto che le tangenti (pensate come segmenti) tratte da un punto a una circonferenza esterna sono congruenti. Quindi $BD = BF$, $CE = CD$, $AF = AE$, $B'F = B'D'$, $C'E = C'D'$.

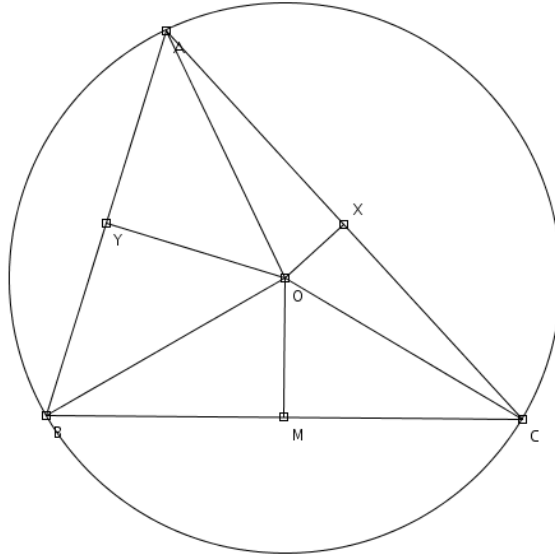
Grazie a queste uguaglianze otteniamo che:

$$\begin{aligned}
 BG - CG &= \frac{1}{k}(B'D' - C'D') = \frac{1}{k}(B'F - C'E) = \\
 &= -\frac{1}{k}(-B'F + C'E) = -\frac{1}{k}((AF - B'F) - (AE - C'E)) = \\
 &= \frac{1}{k}(AC' - AB') = AC - AB = (AE + EC) - (AF + FB) = EC - FB = CD - BD
 \end{aligned}$$

Quindi, $BG + BD = CD + CG$; sottraendo la stessa quantità $BD + DC = BG + GC = BC$ otteniamo $BD - GC = GC - BD$ o finalmente $BD = CG$. Quindi, M che è il punto medio di BC è anche il punto medio di DG .

Concludendo, l'omotetia di centro D e fattore 2 manda M in G , I in D' , quindi la retta IM nella retta $D'G = AD'$. \square

Fatto 3. Siano X, Y i punti medi di CA e BA . Allora $OM + OX + OY = R + r$.



Dimostrazione. MX, XY, YM sono la metà dei segmenti a cui sono paralleli.

Per gli angoli retti (O infatti è l'intersezione degli assi di AB, BC, CA) i quadrilateri $OMCX, OXAY, OYBM$ sono ciclici. Applichiamo ad essi il teorema di Tolomeo:

$$OM \cdot CX + OX \cdot CM = OC \cdot MX$$

$$OX \cdot CY + OY \cdot CX = OA \cdot XY$$

$$OY \cdot CM + OM \cdot CY = OB \cdot YM$$

Cioè, sfruttando una notazione più comoda:

$$OM \cdot \frac{b}{2} + OX \cdot \frac{a}{2} = R \cdot \frac{c}{2}$$

$$OX \cdot \frac{b}{2} + OY \cdot \frac{b}{2} = R \cdot \frac{a}{2}$$

$$OY \cdot \frac{b}{2} + OM \cdot \frac{c}{2} = R \cdot \frac{b}{2}$$

Inoltre, partizionando la superficie di ABC nei triangoli BOC, COA, AOB otteniamo che:

$$OM \cdot \frac{a}{2} + OX \cdot \frac{b}{2} + OY \cdot \frac{c}{2} = (ABC)$$

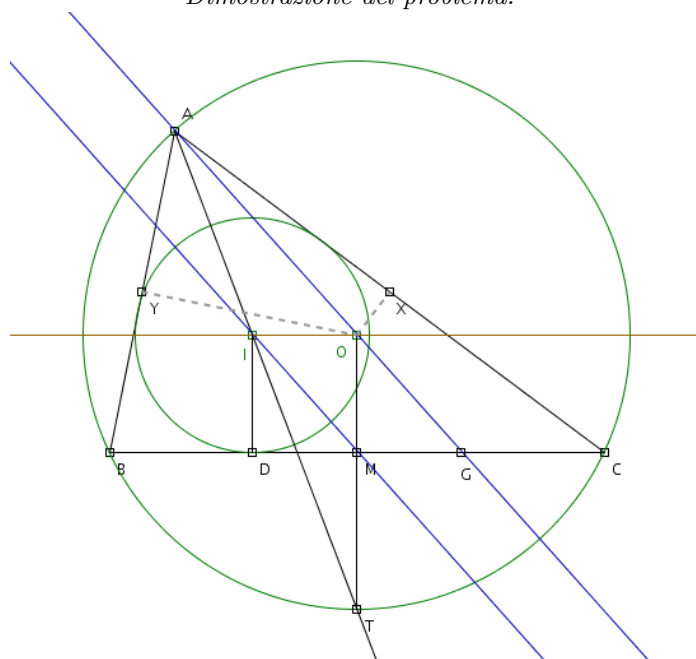
Sommando queste ultime quattro equazioni e raccogliendo, otteniamo:

$$p \cdot (OM + OX + OY) = p \cdot R + (ABC)$$

$$OM + OX + OY = R + \frac{(ABC)}{p} = R + r$$

Come da dimostrare. □

Dimostrazione del problema.



$MI = MT$ se e soltanto se $\angle MIT = \angle MTI$. Poichè O, M, T e A, I, T sono allineati, $\angle MTI = \angle OTA$. Poichè $OT = OA$ (sono raggi), OTA è isoscele, quindi $\angle OTA = \angle OAT$. Quindi, $MI = MT$ se e soltanto se $\angle MIT = \angle OAT$, se e soltanto se IM è parallela ad OA .

Sia G l'intersezione tra AO e BC . Per un fatto che abbiamo dimostrato, $MD = MG$. Inoltre, $\angle IDM = \angle OMG = 90$. $\angle IMD = \angle OGM$ se e soltanto se le rette IM e OG sono parallele. Quindi, i triangoli IDM e OMG sono congruenti (per il criterio angolo-lato-angolo) se e soltanto se IM ed OG sono parallele. Ma i triangoli IDM e OMG sono congruenti se e soltanto se $ID = OM$. Quindi IM e OG sono parallele se e soltanto se $OM = r$.

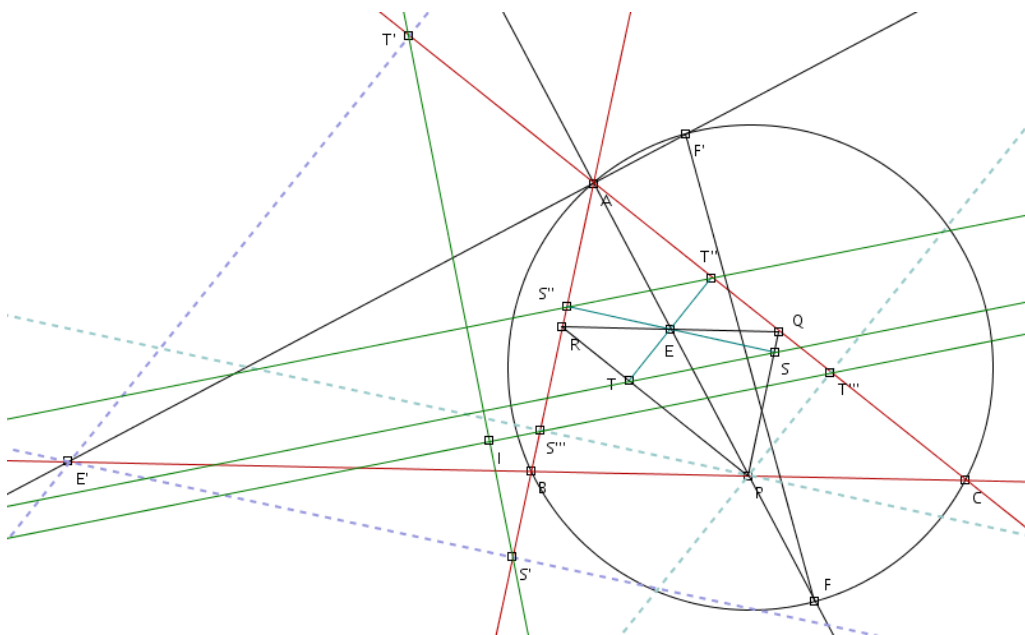
Siano X, Y i punti medi di AC, AB . Per un lemma che abbiamo dimostrato, $OM + OX + OY = R + r$, quindi $OM = r$ se e soltanto se $OX + OY = R$.

$\angle AOX = \frac{1}{2}\angle AOC = \frac{1}{2} \cdot 2 \cdot \angle ABC = \angle ABC = \beta$. Allo stesso modo, $\angle AOY = \gamma$. Il triangolo AOX è rettangolo. Per la definizione di coseno di un angolo come rapporto tra il cateto adiacente e l'ipotenusa, abbiamo $OX = R \cos \beta$ e $OY = R \cos \gamma$. Quindi $OX + OY = R$ se e soltanto se $R \cos \beta + R \cos \gamma = R$, o $\cos \beta + \cos \gamma = 1$.

Così concludiamo la dimostrazione. □

Problema 3.3. Sia ABC un triangolo; P, Q, R i punti medi di BC, CA, AB , E l'intersezione tra AP e QR , F l'intersezione tra AP e il circocentro di ABC , F' il punto diametralmente opposto ad F , E' l'intersezione tra AF' e BC .

Siano S, T le proiezioni di E su PQ, PR . Siano S', T' le proiezioni di E' su AB, BC . Dimostrare che le rette ST e $S'T'$ sono perpendicolari.



Dimostrazione. • $AR = QP = \frac{1}{2}AB$, $AQ = RP = \frac{1}{2}AC$, quindi $ARPQ$ è un parallelogramma perchè ha i lati opposti congruenti. E , l'intersezione delle diagonali, sarà il punto medio di AP .

- Siano S'', T'' le proiezioni di E su AB, AC . E, S, S'' sono allineati perchè le rette AB e PQ sono parallele. Quindi gli angoli $\angle AES'', \angle PES$ sono congruenti essendo opposti al vertice. Inoltre $EA = EP$, già dimostrato. Quindi i triangoli EPS, EAS'' , entrambi retti, sono congruenti. Per lo stesso motivo EPT, EAT'' sono congruenti. L'omotetia di centro E e fattore -1 porta quindi S in S'' e T in T'' . Quindi le rette $ST, S''T''$ sono parallele.
- Siano S''', T''' le proiezioni di P su AB, AC . L'omotetia di centro A e fattore 2 porta E in P , S'' in S''' , T'' in T''' . Quindi le rette S'', T'' e S''', T''' sono parallele. Concludiamo che $ST, S''T''$ sono parallele. La tesi diventa dimostrare che $S'T'$ e $S'''T'''$ sono perpendicolari.

- Sia I l'intersezione tra ST e $S'''T'''$. Usiamo ora gli angoli orientati.

$$\begin{aligned}
\angle IT'T''' + \angle T'T'''I &= \angle S'T'A + \angle AT'''S''' = \\
&= (90 - \angle E'T'S') + (90 - \angle S'''T'''P) = \\
&= \angle S'T'E' + \angle PT'''S''' = \\
&= \angle S'AE' + \angle PAS''' = \\
&= \angle BAE' + \angle PAB = \\
&= \angle PAE' = \angle PAF' = \angle FAF' = 90
\end{aligned}$$

Abbiamo usato il fatto che $E'S'AT'$ e $PT'''AS'''$ sono quadrilateri ciclici, oltre all'allineamento di vari punti, al fatto che alcuni angoli della figura sono retti, e alle proprietà degli angoli orientati.

□

4 Teoria dei Numeri

Problema 4.1. Per ogni $n \in \mathbb{N}^+$, sia $L(n)$ il numero di naturali $1 \leq a \leq n$ tali che $n \mid a^n - 1$. Se p_1, p_2, \dots, p_k sono tutti e soli i primi che dividono n , definiamo $T(n)$ come $(p_1 - 1)(p_2 - 1) \cdots (p_k - 1)$.

a. dimostrare che per ogni n :

$$\phi(n) \mid L(n)T(n)$$

b. dimostrare che, se n e $T(n)$ sono primi tra loro:

$$\phi(n) = L(n)T(n)$$

Faccio notare che la versione originale del problema, come scritta su Mathlinks, nel primo punto chiedeva da dimostrare che $n \mid L(n)T(n)$. Dimostro che questa enunciazione è scorretta. Sia p un primo. Allora $a^p \equiv a \pmod{p}$ per il piccolo teorema di Fermat. Quindi $a^p \equiv 1 \pmod{p}$ se e soltanto se $a \equiv 1 \pmod{p}$, quindi $L(p) = 1$. $T(p) = p - 1$. Il problema chiederebbe da dimostrare che $p \mid p - 1$, che chiaramente è impossibile.

Visto il secondo punto, la più naturale correzione del problema sarebbe sostituire $n \mid L(n)T(n)$ con $\phi(n) \mid L(n)T(n)$, che, come dimostrerò, è vero.

Per il teorema fondamentale dell'aritmetica, possiamo scrivere in modo unico $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. Ora dimostreremo che

$$L(n) = \prod_{1 \leq i \leq k} \gcd(n, p_i^{e_i-1}(p_i - 1)) \quad (2)$$

Sia a un intero tale che

$$a^n \equiv 1 \pmod{n} \quad (3)$$

Chiaramente dovrà essere $\gcd(a, n) = 1$, supponendo questo ci toglieremo un po' di problemi per il futuro. Il fatto che $a^n \equiv 1 \pmod{p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}}$ è equivalente al fatto che siano soddisfatte contemporaneamente tutte le congruenze:

$$a^n \equiv 1 \pmod{p_i^{e_i}} \quad \forall 1 \leq i \leq k \quad (4)$$

La (3) implica chiaramente ciascuna delle (4). Inoltre, se ciascuna delle (4) è soddisfatta, essendo i moduli a due a due relativamente primi, per il teorema cinese del resto a quel sistema di congruenze corrisponde un'unica soluzione modulo n . Se ciascuna delle (4) ha s_i soluzioni, ad ogni scelta di soluzioni corrisponde un'unica soluzione della (3). La cardinalità dell'insieme delle scelte è data da $s_1 s_2 \cdots s_k$. Tutto questo giustifica che, per dimostrare la (2) sarà sufficiente dimostrare che per ogni p_i , l'insieme delle soluzioni (modulo $p_i^{e_i}$, ovviamente) alla relativa (4) ha cardinalità:

$$\gcd(n, \phi(p_i^{e_i})) = \gcd(n, p_i^{e_i-1}(p_i - 1)) \quad (5)$$

Distinguiamo il caso in cui p_i sia 2 o un primo dispari.

- Si ha $\phi(2^e) = 2^{e-1}$. Se a è dispari, allora

$$a^n \equiv a^{2^e p_1^{e_1} \dots p_k^{e_k}} \equiv (a^{2 p_1^{e_1} \dots p_k^{e_k}})^{\phi(2^e)} \equiv 1 \pmod{2^e}$$

- Se p è un primo dispari, allora esiste un generatore modulo p^e , chiamiamolo g . Sarà $a = g^t$ per un certo $1 \leq t \leq \phi(p^e)$. Allora $a^n \equiv 1 \pmod{p^e}$ se e soltanto se $g^{tn} \equiv 1 \pmod{p^e}$ se e soltanto se $\phi(p^e) \mid tn$, se e soltanto se $\frac{\phi(p^e)}{\gcd(\phi(p^e), n)} \mid \frac{n}{\gcd(\phi(p^e), n)} t$. Poichè $\frac{\phi(p^e)}{\gcd(\phi(p^e), n)}$ è coprimo con $\frac{n}{\gcd(\phi(p^e), n)}$, avremo che $\frac{\phi(p^e)}{\gcd(\phi(p^e), n)} \mid t$. I multipli di $\frac{\phi(p^e)}{\gcd(\phi(p^e), n)}$ compresi tra 1 e $\phi(p^e)$ sono

$$\frac{\phi(p^e)}{\gcd(\phi(p^e), n)} = \gcd(\phi(p^e), n)$$

Questi valori di t generano tutti e soli gli a tali che $a^n \equiv 1 \pmod{p^e}$.

Ora che abbiamo dimostrato la nostra formula, passiamo a dimostrare il problema. Abbiamo che

$$p_i^{e_i-1} \mid \gcd(p_1^{e_1} \dots p_i^{e_i} \dots p_k^{e_k}, p_i^{e_i-1}(p_i - 1))$$

Per la proprietà elementare della divisibilità:

$$a \mid b \wedge c \mid d \Rightarrow ab \mid cd$$

Otteniamo che:

$$p_1^{e_1-1} p_2^{e_2-1} \dots p_k^{e_k-1} \mid L(n)$$

E inoltre:

$$\begin{aligned} \phi(n) &= p_1^{e_1-1} p_2^{e_2-1} \dots p_k^{e_k-1} (p_1 - 1) \dots (p_k - 1) = \\ &= p_1^{e_1-1} p_2^{e_2-1} \dots p_k^{e_k-1} T(n) \mid L(n) T(n) \end{aligned}$$

Che dimostra il primo punto. Se inoltre $\gcd(n, T(n)) = 1$ allora $n, p_i^{e_i} (p_i - 1)$ non hanno il fattore $p_i - 1$ in comune, quindi $\gcd(n, \phi(p_i^{e_i})) = p_i^{e_i-1}$, quindi $L(n) = p_1^{e_1-1} \dots p_k^{e_k-1}$ e chiaramente $L(n)T(n) = \phi(n)$. \square

FIXME! (punto b)

Problema 4.2. Siano a, b, c, t interi positivi. Dimostrare che se c^t ha q fattori primi distinti, allora

$$a^{c^t} - b^{c^t}$$

ha almeno qt fattori primi distinti.

Come al solito, dimostriamo prima qualche lemma. Che a scriverli da soli sono già interessanti!

Lemma 2. Siano a e b interi positivi tali che $\gcd(a, b) = 1$. Allora, per ogni $m, n \in \mathbb{N}^+$:

$$\gcd(a^m - b^m, a^n - b^n) = a^{\gcd(m, n)} - b^{\gcd(m, n)}$$

Dimostrazione. Poniamo $d = \gcd(m, n)$. Per il teorema di Bezout, esistono due interi h, k tali che $hm + kn = d$. Sia x un intero che divide entrambi $a^m - b^m$ e $a^n - b^n$. Avremo che:

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

$$a^n \equiv b^n \pmod{x}$$

Eleviamo entrambi i membri a h nella prima equazione e a k nella seconda. Infatti, essendo entrambi a, b relativamente primi ad x (se non lo fosse uno non lo sarebbe neanche l'altro, ma a e b sono coprimi), le potenze ad esponente negativo sono ben definite.

$$a^{mh} \equiv b^{mh} \pmod{x}$$

$$a^{nk} \equiv b^{nk} \pmod{x}$$

Moltiplicando le ultime due congruenze otteniamo:

$$a^{mh+nk} \equiv b^{mh+nk} \pmod{x}$$

$$a^d \equiv b^d \pmod{x}$$

$$x \mid a^d - b^d$$

Quindi ogni fattore comune tra $a^m - b^m, a^n - b^n$ divide anche $a^d - b^d$. È inoltre noto che, se $d \mid m$ e $d \mid n$:

$$a^d - b^d \mid a^m - b^m, \quad a^d - b^d \mid a^n - b^n$$

Quindi $a^d - b^d$ è il massimo comun divisore tra $a^m - b^m$ e $a^n - b^n$. \square

Lemma 3. Siano a, b interi positivi coprimi, n un intero positivo. Allora, nella scomposizione:

$$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \dots + ab^{n-2} + b^{n-1})$$

ogni fattore in comune tra $(a - b)$ e $(a^{n-1} + a^{n-2}b + \dots + ab^{n-2} + b^{n-1})$ è un divisore di n .

Dimostrazione. Se $d \mid a - b$ allora $a \equiv b \pmod{d}$. Ma quindi:

$$\begin{aligned} & a^{n-1} + a^{n-2}b + \dots + ab^{n-2} + b^{n-1} \equiv \\ & \equiv a^{n-1} + a^{n-1} + \dots + a^{n-1} + a^{n-1} \equiv na^{n-1} \pmod{d} \end{aligned}$$

Essendo a coprimo con d (se a ha un fattore in comune con d , lo ha anche b , e quindi $\gcd(a, b) > 1$), se $d \mid na^{n-1}$ allora $d \mid n$. \square

Lemma 4. *Siano a, b interi positivi coprimi, sia p un primo dispari tale che $p \mid a - b$ ma $p^2 \nmid a - b$. Allora, per ogni $n \in \mathbb{N}$, il massimo k tale che*

$$p^k \mid a^{p^n} - b^{p^n}$$

è $n + 1$.

Dimostrazione. Passo base. Per $n = 0$ abbiamo per ipotesi che $p^1 \parallel a - b$.

Passo induttivo. Abbiamo, per la nota scomposizione,

$$a^{p^n} - b^{p^n} = (a^{p^{n-1}} - b^{p^{n-1}})X \quad (6)$$

Dove

$$X = (a^{(p-1)p^{n-1}} + a^{(p-2)p^{n-1}}b^{p^n} + a^{(p-3)p^{n-1}}b^{2p^{n-1}} + \dots + b^{(p-1)p^{n-1}})$$

Il primo fattore, per ipotesi induttiva, è divisibile per p esattamente n volte. Per dimostrare il lemma basterà quindi dimostrare che il secondo fattore è divisibile per p , ma non per p^2 . Per comodità, facciamo la sostituzione $c = a^{p^{n-1}}$ e $d = b^{p^{n-1}}$. L'ipotesi induttiva ci dice quindi che $p^n \parallel c - d$. Quindi esiste un intero i tale che $d = c + ip^n$, dove i non è multiplo di p . Ora, riscriviamo X in funzione di c e ragioniamo modulo p^2 .

$$c^{p-1} + c^{p-2}(c + ip^n) + c^{p-3}(c + ip^n)^2 + \dots + (c + ip^n)^{p-1} \quad (7)$$

Dimostriamo la semplice congruenza:

$$(c + ip^n)^x \equiv c^x + xip^n \pmod{p^{n+1}}$$

Infatti, nello sviluppo di Newton della somma $(c + ip^n)^x$, già $(ip^n)^2 = i^2p^{2n} \equiv 0 \pmod{p^{n+1}}$ perchè $2n \geq n+1$ essendo $n \geq 1$. A maggior ragione si annullano gli addendi in cui eleviamo ip^n a una potenza maggiore di 2. Inoltre, essendo questa congruenza valida modulo p^{n+1} sarà anche valida modulo p^2 . Ora, applicando questa congruenza, otteniamo che:

$$\begin{aligned} & c^{p-1} + c^{p-2}(c + ip^n) + c^{p-3}(c + ip^n)^2 + \dots + (c + ip^n)^{p-1} \equiv \\ & c^{p-1} + c^{p-2}(c + ip^n) + c^{p-3}(c^2 + 2ip^n) + \dots + (c^{p-1} + (p-1)ip^n) \equiv \\ & pc^{p-1} + ip^n(1 + 2 + \dots + (p-1)) \pmod{p^2} \end{aligned}$$

Il primo addendo, essendo c non divisibile per p , è congruo a p modulo p^2 . Il secondo addendo, per $n \geq 2$ è ovviamente multiplo di p^2 . Se invece $n = 1$, allora abbiamo la somma $1 + 2 + \dots + (p-1)$ che è nota essere un multiplo di p . Qui usiamo il fatto che p è un primo *dispari*!! Quindi in ogni caso il secondo addendo si annulla, e X è congruo a p modulo p^2 , cioè è divisibile esattamente per p . \square

Ora, se volessimo estendere questo lemma anche al caso $p = 2$? Abbiamo usato il fatto che p è un primo dispari solo nell'ultima parte, e solo nel caso in cui $n = 1$. La condizione p dispari è necessaria, ad esempio $2 \parallel 5 - 3$ ma $2^4 \parallel 5^2 - 3^2$. Però questa estensione del lemma per $p = 2$ funziona, la dimostrazione è la stessa:

Siano a, b interi positivi relativamente primi, con $a - b$ pari. Sia k tale che $2^k \parallel a^2 - b^2$. Allora per ogni $n \geq 2$ abbiamo

$$2^{k+n-1} \parallel a^{2^n} - b^{2^n}$$

Dimostrazione del problema; punto a. Possiamo supporre a, b primi tra loro perchè, essendo gli esponenti di a e b uguali, possiamo 'raccogliere' qualsiasi fattore comune. Se c^t ha q fattori primi distinti, allora anche c ha q fattori distinti. Scriviamo quindi $c = p_1^{e_1} p_2^{e_2} \dots p_q^{e_q}$. Indichiamo con F l'insieme dei primi che dividono $a^c - b^c$, e con F_i ($1 \leq i \leq q$) l'insieme di tutti i primi che dividono $a^{p_i^t} - b^{p_i^t}$. Osserviamo che per ogni $1 \leq i \leq q$:

$$a^{p_i^t} - b^{p_i^t} \mid a^{c^t} - b^{c^t}$$

Quindi ogni primo che divide $a^{p_i^t} - b^{p_i^t}$ divide anche $a^{c^t} - b^{c^t}$, cioè:

$$F_1 \cup F_2 \cup \dots \cup F_q \subseteq F$$

Dimostriamo che gli insiemi F_i sono a due a due disgiunti. Infatti, per $p_i \neq p_j$:

$$\gcd(a^{p_i^t} - b^{p_i^t}, a^{p_j^t} - b^{p_j^t}) = 1$$

per il lemma 2. Grazie a questo, abbiamo:

$$|F_1| + |F_2| + \dots + |F_q| = |F_1 \cup F_2 \cup \dots \cup F_q| \leq |F|$$

La nostra tesi è dimostrare che $|F| \geq qt$. Se dimostriamo che per ogni $1 \leq i \leq q$, $|F_i| \geq t$, questo implica la tesi. Quindi riuinciamo il problema in questo modo: *Sia p un primo, a, b interi positivi coprime. Dimostrare che $a^{p^t} - b^{p^t}$ ha almeno t divisori primi distinti.* Lo dimostriamo per induzione.

Passo base: $t = 1$. Allora se $a^p - b^p = \pm 1$, abbiamo due potenze p -esime ($p \geq 2$) consecutive, ma questo è possibile solo se uno tra a e b è 0. Ma a, b sono interi positivi.

Passo induttivo: sia $t \geq 2$. Vogliamo dimostrare che $a^{p^t} - b^{p^t}$ ha un fattore primo non presente in $a^{p^{t-1}} - b^{p^{t-1}}$. Abbiamo la scomposizione:

$$a^{p^t} - b^{p^t} = (a^{p^{t-1}} - b^{p^{t-1}})X = (a^{p^{t-1}} - b^{p^{t-1}})(a^{(p-1)p^{t-1}} + \dots + b^{(p-1)p^{t-1}})$$

Per il lemma 3, se c'è un fattore in comune tra $a^{p^{t-1}} - b^{p^{t-1}}$ e X , questo è un divisore di p , quindi è p . Nella dimostrazione del lemma 4, abbiamo dimostrato che se $p \mid X$ allora $p \parallel X$. Questo, per $t \geq 2$, vale anche se $p = 2$. Quindi: se ogni fattore primo di X è anche un fattore di $a^{p^{t-1}} - b^{p^{t-1}}$, $X = 1$ o $X = p$.

Chiaramente X è più grande. Senza perdita di generalità assumiamo che a sia il massimo tra $\{a, b\}$: avremo $a \geq 2$. (Se $a = 1$ allora $b = 1$ ed $a^k - b^k = 0$ è divisibile per ogni primo, per ogni k). Allora

$$X \geq a^{p^{t-1}(p-1)} \geq 2^{p^{t-1}(p-1)} \geq 2^p > p$$

Quindi X ha un fattore primo che non divide $a^{p^{t-1}} - b^{p^{t-1}}$, e questo conclude l'induzione, che a sua volta conclude il problema. \square

Dimostrazione del problema; punto b. \square

Problema 4.3. a. $P(x), R(x)$ sono polinomi a coefficienti razionali e $P(x)$ non è il polinomio nullo. Dimostrare che esiste un polinomio non nullo a coefficienti razionali $Q(x)$ tale che:

$$P(x) \mid Q(R(x))$$

b. $P(x), R(x)$ sono polinomi a coefficienti interi e $P(x)$ è monico. Dimostrare che esiste un polinomio monico a coefficienti interi $Q(x)$ tale che:

$$P(x) \mid Q(R(x))$$

Ci serviremo di un lemma sui polinomi simmetrici.

Un polinomio in n variabili $P(x_1, \dots, x_n) \in K[x_1, \dots, x_n]$ si dice simmetrico se, per ogni permutazione $\sigma : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ si ha $P(x_1, \dots, x_n) = P(\sigma(x_1), \dots, \sigma(x_n))$.

I polinomi simmetrici (o somme simmetriche) elementari in n variabili sono definiti come:

$$\begin{aligned} \sigma_1 &= x_1 + x_2 + \dots + x_n \\ \sigma_2 &= x_1x_2 + x_1x_3 + \dots + x_{n-1}x_n \\ \sigma_k &= \sum_{A \subseteq \{1, \dots, n\}, |A|=k} \prod_{i \in A} x_i \\ \sigma_n &= x_1x_2 \cdots x_n \end{aligned}$$

Lemma 5. Ogni polinomio simmetrico in n variabili a coefficienti interi è un polinomio a coefficienti interi nelle somme simmetriche elementari con n variabili.

Dimostrazione. (più che altro uno schizzo di dimostrazione. Formalizzarla è molto lungo.) Ad ogni monomio $M = x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$ tale che $e_1 \geq e_2 \geq \dots \geq e_n$ associamo il vettore n -dimensionale $f(M) = (e_1, e_2, \dots, e_n)$. Definiamo infine una funzione che manda vettori di naturali “non crescenti” in vettori di naturali.

$$g(v) = (e_1 - e_2, e_2 - e_3, \dots, e_{n-1} - e_n, e_n)$$

La funzione h manda vettori in polinomi nelle somme simmetriche elementari:

$$h(e_1, e_2, \dots, e_n) = \sigma_1^{e_1} \sigma_2^{e_2} \cdots \sigma_n^{e_n}$$

Ora dimostreremo che ogni monomio M (con gli esponenti ordinati appare un'unica volta nell'espansione di $h(g(f(M)))$) e che ogni ulteriore monomio N dell'espansione di $h(g(f(M)))$, se non è semplicemente M con le variabili permutate, è tale che il vettore $f(M)$ maggiorizza $f(N)$.

Si tratta di ottenere il polinomio $M = x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$ nell'espansione di

$$(x_1 + \dots + x_n)^{e_1 - e_2} (x_1x_2 + x_1x_3 + \dots + x_{n-1}x_n)^{e_2 - e_3} \cdots (x_1x_2 \cdots x_n)^{e_n}$$

In totale ci sono $(e_1 - e_2) + (e_2 - e_3) + \dots + (e_{n-1} - e_n) + e_n = e_1$ fattori, in ciascuno dei quali possiamo ottenere un x_1 al più con esponente 1. Quindi dovremo scegliere un fattore con x_1 in ogni fattore. In particolare, in tutti i fattori $(x_1 + \dots + x_n)$ possiamo scegliere solo x_1 . Ora, togliendo x_1 da tutti i fattori, restano le funzioni simmetriche con $n - 1$ variabili, con esponenti $e_2 - e_3, \dots, e_n$.

Ripetendo lo stesso ragionamento per scegliere x_2 , e poi x_3, \dots si dimostra per induzione che la scelta è unica. Scusate l'informalità.

Sia $N, f(N) = (k_1, k_2, \dots, k_m)$ un monomio che esce dallo sviluppo di $h(g(f(M)))$. Poichè ogni fattore è omogeneo, avremo $k_1 + \dots + k_n = e_1 + \dots + e_n$. Inoltre, per ogni $1 \leq i \leq n$, $k_1 + \dots + k_i \leq e_1 + \dots + e_i$. Infatti, ogni fattore σ_1 aumenta il grado di 1. Ogni fattore di grado σ_2 aumenta il grado di 2. Si va avanti fino a σ_i , che aumenta il grado di i . Da $\sigma_i + 1$ a σ_n il grado del monomio formato dalle i variabili con esponente più alto aumenta al massimo di i per ogni fattore. Quindi

$$\begin{aligned} k_1 + \dots + k_i & \\ & \leq 1(e_1 - e_2) + 2(e_2 - e_3) + 3(e_3 - e_4) + \dots + \\ & \quad + i(e_i - e_{i+1}) + i(e_{i+1} - e_{i+2}) + \dots + i(e_n) \\ & = e_1 + e_2 + \dots + e_i \end{aligned}$$

Ora, abbiamo dimostrato che una somma simmetrica di monomi con coefficiente 1 e vettore di esponenti v è ottenibile se è ottenibile se è ottenibile ogni somma simmetrica di monomi con vettore di esponenti che è maggiorato da v . La dimostrazione che ogni somma simmetrica di monomi con coefficiente 1 è ottenibile segue dal principio di ϵ -induzione applicato ai vettori che abbiamo considerato, con l'ordinamento parziale di maggiorazione. L'estremo inferiore di quest'ordine, nell'insieme da noi considerato, cioè i vettori di naturali aventi una somma fissata ad n , è proprio il vettore $(1, 1, 1, \dots, 1)$ che corrisponde ad una somma simmetrica elementare, che è certo ottenibile. Quindi anche il "passo base" dell'induzione è dimostrato.

Essendo il polinomio da noi considerato a coefficienti interi, basterà sommare ogni somma simmetrica di monomi con coefficiente 1 (che abbiamo dimostrato ottenibile in funzione delle somme simmetriche elementari) moltiplicata per un opportuno coefficiente intero. \square

Dimostrazione del problema. Sia A l'insieme di tutte le radici complesse di P . Con $m(\lambda)$ indichiamo la molteplicità della radice λ .

$$Q(x) = \prod_{\lambda \in A} (x - R(\lambda))^{m(\lambda)}$$

Dimostriamo che Q è il polinomio cercato.

Prima verifichiamo che $P(x) \mid Q(R(x))$. Basta dimostrare che ogni radice di $P(x)$ è una radice di $Q(R(x))$ con la stessa molteplicità. Se $P(\lambda) = 0$ e λ ha molteplicità n , allora $(x - R(\lambda))^n \mid Q(x)$ (per come è stato definito Q), quindi $(R(x) - R(\lambda))^n \mid Q(x)$, ma λ è una radice di $R(x) - R(\lambda)$.

Ora dimostriamo che Q ha i coefficienti razionali. Ogni coefficiente di Q è evidentemente ottenuto con un polinomio simmetrico a coefficienti interi nelle variabili $R(\lambda_1), \dots, R(\lambda_n)$. Essendo R a coefficienti razionali, ogni coefficiente di A è un polinomio simmetrico a coefficienti razionali in $\lambda_1, \dots, \lambda_n$. Questo polinomio, grazie al nostro lemma, è un polinomio a coefficienti razionali nelle somme simmetriche elementari di $\lambda_1, \dots, \lambda_n$. Ma le somme simmetriche elementari di $\lambda_1, \dots, \lambda_n$ sono esattamente ciascuno dei coefficienti di P , divisi per il coefficiente direttivo. Quindi ciascuno dei coefficienti di Q è un polinomio a coefficienti razionali nei coefficienti di P , e quindi tutti i coefficienti di Q sono razionali.

Se R è a coefficienti interi, P è a coefficienti interi, e il coefficiente direttivo di P è 1, lo stesso ragionamento ci porta a dire che i coefficienti di Q sono interi. Inoltre Q , per come è definito, è monico. Questo conclude la dimostrazione. \square