

Soluzioni PreIMO 2006 - lavoro di gruppo

Andrea Fogari

18 luglio 2006

1 Teoria dei numeri

Problema 1 Determinare tutte le coppie (a, b) di numeri interi positivi tali che $a > b$ e

$$(a - b)^{ab} = a^b \cdot b^a. \quad (1)$$

Lemma 1 Siano (x, y) due numeri interi primi tra loro, con $x > y$. Allora, se $(x - y) | y$ o $(x - y) | x$, $x - y = 1$.

Infatti, dalla divisibilità si ottiene che $y = k(x - y)$ per qualche k intero. Ma si ha che $x = y + (x - y) = k(x - y) + (x - y) = (k + 1)(x - y)$. Siccome x e y sono primi tra loro e $(x - y)$, positivo, li divide entrambi, si deduce che $x - y = 1$.

Analogamente, $x = k(x - y) \Rightarrow y = (k - 1)(x - y)$.

□

Lemma 2 Per ogni intero positivo x vale:

$$x^{\frac{1}{x}} \leq 2 - \frac{1}{x}$$

Per dimostrarlo useremo la disuguaglianza tra media geometrica e media aritmetica.

$$x^{1/x} = \sqrt[x]{\underbrace{x \cdot \underbrace{1 \cdot 1 \cdot \dots \cdot 1}_{x-1 \text{ volte}}}} \leq \frac{x + \overbrace{1 + \dots + 1}^{x-1 \text{ volte}}}{x} = \frac{x + x - 1}{x} = 2 - \frac{1}{x}. \quad \square$$

Fatto 1: $1 \leq a - b \leq 3$

Dalla (1) si ottiene, elevando tutto a $(\frac{1}{ab})$:

$$(a - b) = a^{\frac{1}{a}} \cdot b^{\frac{1}{b}} \quad (2)$$

Dal lemma 2 sappiamo che:

$$(a - b) = a^{\frac{1}{a}} \cdot b^{\frac{1}{b}} \leq (2 - \frac{1}{a})(2 - \frac{1}{b}) = 4 - \frac{1}{a} - \frac{1}{b} + \frac{1}{ab}$$

Ma b è intero positivo, quindi $ab \geq a$ e $\frac{1}{ab} \leq \frac{1}{a}$. Aggiungendo $\frac{1}{b} + \frac{1}{a} - \frac{1}{ab}$, quantità positiva, alla parte destra dell'ultima disuguaglianza, otteniamo una disuguaglianza stretta ancora valida:

$$(a - b) < 4$$

Poichè $a > b$, $1 \leq a - b \leq 3$.

Sia m il massimo comun divisore tra a e b . Avremo $a = mx$, $b = my$, con x e y primi tra loro e $y < x$. Sostituendo questo nella (1), si ottiene:

$$(mx - my)^{mxy} = (mx)^{my}(my)^{mx}$$

Estraendo la radice m -esima e riordinando:

$$\begin{aligned} m^{mxy}(x - y)^{mxy} &= m^{x+y}x^y y^x \\ m^{mxy-x-y}(x - y)^{mxy} &= x^y y^x \end{aligned} \quad (3)$$

Il massimo comun divisore tra due numeri deve dividere anche la loro differenza. Ma sappiamo che $a - b$ vale 1,2 o 3, quindi anche m vale 1,2 o 3.

Se $m = 1$ l'equazione diventa:

$$(x - y)^{xy} = x^y y^x$$

Dove $x - y, x, y$ sono interi positivi e $xy \geq 2$ perchè $x \neq y$. $(x - y)$ deve dividere sia x sia y , quindi, per il lemma 1, $(x - y) = 1$. Ma $x^y y^x = 1$ implica $x = y = 1$ che è evidentemente contraddittorio. Quindi possiamo escludere il caso $m = 1$.

m divide al massimo un numero tra x e y . Quindi $(x - y)$ deve dividere almeno uno tra x e y . Quindi, per il lemma, $x - y = 1$. Si ottiene:

$$m^{mxy-x-y} = x^y y^x$$

Ma m non può dividere sia x sia y , quindi il minore dei due sarà 1: $y = 1$.

$$m^{x(m-1)-1} = x$$

Restano solo due casi: $m = 2$ e $m = 3$. Dal primo si ottiene:

$$2^{x-1} = x$$

Sappiamo che $x \geq 2$. Il caso $x = 2$ è una soluzione, per $x = 3$ si otterrebbe $4 = 3$, impossibile, e se x cresce di 1, il membro a sinistra raddoppia (aumentando almeno di 4) e quello a destra aumenta di 1. Per induzione, abbiamo verificato che questa è l'unica soluzione.

Se $m = 3$, si ottiene:

$$3^{2x-1} = x$$

Per $x = 2$, $3^{2x-1} = 27 > x$, se x incrementa, il membro a sinistra triplica e quello a destra aumenta di 1. Per induzione, non ci sono soluzioni.

In conclusione, sappiamo che l'unica soluzione è $m = 2, y = 1, x = 2$ che corrisponde a $(a, b) = (4, 2)$. \square

Problema 2 Siano a e b interi positivi tali che $a^n + n$ divide $b^n + n$ per ogni $n \in \mathbb{N}$.

Dimostrare che $a = b$.

Sia p un numero primo maggiore di a e b . Esiste perchè i numeri primi sono infiniti.

Sia k un intero tale che:

$$\begin{cases} k \equiv p & (\text{mod } p-1) \\ k \equiv -a & (\text{mod } p) \end{cases}$$

La sua esistenza è assicurata dal teorema cinese del resto. Infatti p e $p+1$, numeri consecutivi, sono certamente primi tra loro.

Otteniamo che:

$$a^k + k \equiv a + k \equiv a - a \equiv 0 \pmod{p} \quad (4)$$

Infatti $a^k \equiv a \pmod{p}$. Questo si giustifica osservando che k è della forma $c(p-1) + p$, quindi $a^k = a^{c(p-1)+p} = a^p \cdot (a^c)^{p-1} \equiv a^p \equiv a \pmod{p}$. Qui abbiamo applicato il piccolo teorema di Fermat.

Inoltre, $k \equiv -a \pmod{p}$.

Anche $b^k + k \equiv 0 \pmod{p}$. Infatti $b^k + k$, per le ipotesi del problema, è un multiplo di $a^k + k$, il quale è multiplo di p , quindi anche $b^k + k$ è multiplo di p .

$$b^k + k \equiv b - a \pmod{p}$$

Questo si giustifica allo stesso modo di prima, usando il piccolo teorema di Fermat e le congruenze imposte su k . Abbiamo appena dimostrato che $b - a \equiv 0 \pmod{p}$, quindi $b \equiv a \pmod{p}$. Siccome p è un primo maggiore di a e di b , deve essere che $a = b$. Se così non fosse, la differenza tra a e b sarebbe un multiplo di p diverso da 0, quindi almeno uno dovrebbe essere maggiore di p . \square

Problema 3 Determinare tutte le terne di numeri primi (p, q, r) tali che

$$p|q^r + 1 \quad (5)$$

$$q|r^p + 1 \quad (6)$$

$$r|p^q + 1 \quad (7)$$

Lemma 3 Siano p, q due primi dispari. Se $\text{ord}_p q = 2$ allora $p|q+1$ e $2p \leq q+1$.

Da $\text{ord}_p q = 2$ otteniamo $q^2 \equiv 1 \pmod{p}$, quindi $q^2 - 1 \equiv 0 \pmod{p}$ e $(q+1)(q-1) \equiv 0 \pmod{p}$. Per la legge dell'annullamento del prodotto, che vale in \mathbb{Z}_p , uno tra $(q+1)$ e $(q-1)$ deve essere multiplo di p . Se fosse $q-1$ si avrebbe $q \equiv 1 \pmod{p}$, e il suo ordine moltiplicativo rispetto a p sarebbe 1. Quindi $p|q+1$.

Sappiamo che $kp = q+1$ per qualche intero positivo k . Se $k=1$, $q+1$ dovrebbe essere dispari, assurdo. Quindi $k \geq 2$ e $2p \leq q+1$. \square

Lemma 4 Se un intero q divide due interi x e y , allora q divide una qualsiasi combinazione lineare di questi.

Abbiamo $mq = x, nq = y$ con m, n interi. Una combinazione lineare z è della forma $z = jx + ky = j(mq) + k(nq) = q(mj + nk)$, da cui $q|z$. \square

Le condizioni date sono cicliche rispetto alle lettere (p, q, r) , senza perdita di generalità possiamo supporre che p sia il più piccolo primo.

Passo 1: dimostriamo che $p=2$. Supponiamo ora che p, q, r siano tutti dispari.

Dalla (5) otteniamo che:

$$q^r \equiv -1 \pmod{p}$$

$$q^{2r} \equiv 1 \pmod{p}$$

$$\text{ord}_p q | 2r$$

$$\text{ord}_p q | p-1 \quad (\text{perchè l'ordine moltiplicativo modulo } m \text{ divide } \Phi(m))$$

L'ordine di q rispetto a p può essere $1, 2, r$ o $2r$. Poichè è minore o uguale a $p-1$ e $p \leq r$, le possibilità r e $2r$ vanno escluse. Inoltre non può essere 1 perchè si avrebbe $q^r \equiv 1 \equiv -1 \pmod{p}$, che vale soltanto se $p=2$, caso che abbiamo escluso.

Concludiamo che $\text{ord}_p q = 2$, per il lemma 3:

$$p|q+1 \quad (8)$$

Allo stesso modo di prima, la (6) implica:

$$\text{ord}_q r | 2p$$

$$\text{ord}_q r | q-1$$

Tra $1, 2, p, 2p$ escludiamo 1 e p perchè l'ordine moltiplicativo deve essere pari se una certa potenza di r è congrua a -1 modulo p (primo dispari). Se $\text{ord}_q r$

fosse $2p$, si avrebbe $2p|q-1$, in contraddizione con la (8) e il lemma 4, infatti p dovrebbe dividere $(q+1)-(q-1)=2$. Concludiamo che $\text{ord}_q r = 2$ e, per il lemma 3:

$$q|r+1 \quad (9)$$

Dalla (7) otteniamo che:

$$\begin{aligned} \text{ord}_r p &| 2q \\ \text{ord}_r p &| r-1 \end{aligned}$$

Abbiamo già visto che l'ordine moltiplicativo deve essere pari, quindi restano solo le possibilità $\text{ord}_r p = 2$ o $\text{ord}_r p = 2q$. Se $\text{ord}_r p = 2q$, si avrebbe $2q|r-1$, in contraddizione con la (9) e il lemma 4. Quindi $\text{ord}_r p = 2$ e:

$$r|p+1 \quad (10)$$

Mostriamo ora che la (8), la (9) e la (10) sono in contraddizione. Infatti, per il lemma 3 esse implicano:

$$\begin{aligned} 2p &\leq q+1 \\ 2q &\leq r+1 \\ 2r &\leq p+1 \end{aligned}$$

E, sommando queste tre disuguaglianze:

$$2(p+q+r) \leq (p+q+r) + 3$$

$$p+q+r \leq 3$$

Che è ovviamente falsa. Assumendo che tutti i primi siano dispari, si ottiene una contraddizione, quindi il più piccolo dei tre deve essere 2.

Passo 2: dimostriamo che l'unica soluzione è $(2, 5, 3)$.

Ora che sappiamo che $p = 2$, riscriviamo le ipotesi del problema in questo modo:

$$2|q^r + 1 \quad (11)$$

$$q|r^2 + 1 \quad (12)$$

$$r|2^q + 1 \quad (13)$$

Dalla (11) otteniamo che q deve essere dispari.

Dalla (13) otteniamo che $\text{ord}_r 2|2q$. Ma è noto che se, per qualche x , $2^x \equiv -1 \pmod{r}$, ed r è primo, l'ordine moltiplicativo di 2 (rispetto a r) è pari. Se l'ordine moltiplicativo fosse $2q$, avremmo:

$$2q|r-1$$

(è noto che l'ordine moltiplicativo rispetto a m divide $\Phi(m)$)

$$q|r^2 + 1$$

$$q|(-1)(r^2 + 1) - (r+1)(r-1) = 2$$

Nell'ultimo passaggio abbiamo usato il lemma 4. Siccome q è primo dispari, questo è contraddittorio e quindi $\text{ord}_r 2 = 2$.

Da questo segue che $2^2 \equiv 1 \pmod{r}$ e $3 \equiv 0 \pmod{r}$, quindi $r = 3$. Sostituendo questo nella (12) otteniamo $q|3^2 + 1 = 10$. Essendo q dispari, $q = 5$.

□

Problema 4 Siano $f(x)$ e $g(x)$ due polinomi a coefficienti interi con massimo comun divisore uguale ad 1. Dimostrare che esistono infiniti primi per cui esiste $n \in \mathbb{N}$ tale che $p \mid f(n)$ ma $p \nmid g(n)$

Lemma 5 Sia $h(x)$ un polinomio di grado $n \geq 1$ a coefficienti interi. Allora esistono infiniti primi p tali che esiste un $m \in \mathbb{N}$ tale che $p \mid h(m)$.

Dimostriamo questo lemma per assurdo, ossia supponiamo che esista un insieme finito di primi p_1, \dots, p_i tali che, per ogni $x \in \mathbb{N}$, $h(x) = \pm p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_i^{\alpha_i}$, per opportuni esponenti interi non negativi $\alpha_1, \dots, \alpha_i$ dipendenti da x .

Scriviamo $h(x)$ nella forma $h(x) = a_n x^n + \dots + a_1 x + a_0$. Il termine noto a_0 deve essere diverso da 0, altrimenti il polinomio sarebbe uguale a $x(a_n x^{n-1} + \dots + a_1)$ ed è chiaro che per ogni primo q si ha $q \mid h(q)$.

Dimostriamo ora che esiste un $k \in \mathbb{N}$ tale che $|h(k \cdot a_0 \cdot p_1 \cdot \dots \cdot p_i)| > 1$. Esiste perchè è noto che un polinomio non può assumere un insieme finito di valori infinite volte, corrispondenti agli infiniti valori che possiamo dare a k .

Indicando ora $x_0 = k \cdot a_0 \cdot p_1 \cdot \dots \cdot p_i$, osserviamo che $h(x_0) = a_0 [(k \cdot p_1 \cdot \dots \cdot p_i)(a_n x_0^{n-1} + \dots + a_2 x_0 + a_1) + 1]$. Il fattore $(k \cdot p_1 \cdot \dots \cdot p_i)(a_n x_0^{n-1} + \dots + a_2 x_0 + a_1) + 1$ non può essere divisibile per nessun primo tra p_1, \dots, p_i , quindi, essendo $|h(x_0)| > 1$, esiste almeno un primo p_{i+1} diverso da p_1, \dots, p_i che divide $h(x_0)$.
□

Per il teorema di Bezout, dal fatto che $f(x)$ e $g(x)$ hanno MCD di grado 0, deduciamo che esistono due polinomi $i(x)$ e $j(x)$ tali che:

$$f(x)i(x) + g(x)j(x) = k \quad \forall x \in \mathbb{Z}$$

Per il lemma precedente, sappiamo che esistono infiniti primi che dividono $f(x)$ per qualche $x \in \mathbb{N}$. Tra questi, scartiamo quelli che dividono k (che sono comunque finiti), ottenendo l'insieme che chiamiamo S .

Per ogni $p \in S$, $p \mid f(x_0)i(x_0)$ per un certo naturale x_0 . Se p dividesse anche $g(x_0)$, si avrebbe che p dovrebbe dividere anche k , ma questo è impossibile in S . Quindi:

$$\forall p \in S, \quad \exists n \in \mathbb{N} : \quad p \mid f(n) \wedge p \nmid g(n)$$

ma S è infinito, quindi la tesi è vera.. □

2 Algebra

Problema 5 Siano a, b, c le lunghezze dei lati di un triangolo, e siano m_a, m_b, m_c le lunghezze delle relative mediane.

Dimostrare che

$$\left(\frac{a}{m_a} + \frac{b}{m_b} + \frac{c}{m_c}\right)^2 \geq 4 \frac{(a+b+c)^2}{a^2+b^2+c^2}.$$

Prima di tutto esplicitiamo la disuguaglianza tra media aritmetica e media di ordine -2 , che useremo più tardi: siano $\frac{1}{x}, \frac{1}{y}, \frac{1}{z}$ tre reali positivi. Allora:

$$\frac{\frac{1}{x} + \frac{1}{y} + \frac{1}{z}}{3} \geq \sqrt{\frac{3}{x^2 + y^2 + z^2}}$$

Moltiplicando per 3 ed elevando alla seconda otteniamo:

$$\left(\frac{1}{x} + \frac{1}{y} + \frac{1}{z}\right)^2 \geq \frac{27}{x^2 + y^2 + z^2} \quad (14)$$

È noto che le mediane di un triangolo sono ordinate in modo inverso rispetto ai lati relativi. Allora le triple $(a, b, c), (\frac{1}{m_a}, \frac{1}{m_b}, \frac{1}{m_c})$ sono ordinate allo stesso modo. Dalla disuguaglianza di Chebyshev otteniamo che:

$$\frac{a}{m_a} + \frac{b}{m_b} + \frac{c}{m_c} \geq \frac{1}{3}(a+b+c) \left(\frac{1}{m_a} + \frac{1}{m_b} + \frac{1}{m_c}\right) \quad (15)$$

Elevando alla seconda la (15) otteniamo:

$$\left(\frac{a}{m_a} + \frac{b}{m_b} + \frac{c}{m_c}\right)^2 \geq \frac{1}{9}(a+b+c)^2 \left(\frac{1}{m_a} + \frac{1}{m_b} + \frac{1}{m_c}\right)^2$$

Usando la (14) con il termine $\left(\frac{1}{m_a}, \frac{1}{m_b}, \frac{1}{m_c}\right)^2$, otteniamo la nuova disuguaglianza:

$$\left(\frac{a}{m_a} + \frac{b}{m_b} + \frac{c}{m_c}\right)^2 \geq \frac{1}{9}(a+b+c)^2 \frac{27}{m_a^2 + m_b^2 + m_c^2}$$

Ma, sostituendo m_a, m_b, m_c con la nota formula $\frac{1}{2}\sqrt{2(b^2+c^2)-a^2}, \dots$ sappiamo che:

$$m_a^2 + m_b^2 + m_c^2 = \frac{1}{4}(2b^2 + 2c^2 - a^2 + 2c^2 + 2a^2 - b^2 + 2a^2 + 2b^2 - c^2) = \frac{3}{4}(a^2 + b^2 + c^2)$$

. Sostituendo questo nell'ultima disuguaglianza ottenuta abbiamo:

$$\begin{aligned} \left(\frac{a}{m_a} + \frac{b}{m_b} + \frac{c}{m_c}\right)^2 &\geq \frac{1}{9}(a+b+c)^2 \frac{27}{\frac{3}{4}(a^2 + b^2 + c^2)} = \\ &= 4 \frac{(a+b+c)^2}{a^2 + b^2 + c^2} \end{aligned}$$

Che è la tesi. \square

Problema 6 Siano x_1, x_2, \dots, x_n numeri reali positivi.

Dimostrare che

$$\frac{1}{1+x_1} + \frac{1}{1+x_1+x_2} + \dots + \frac{1}{1+x_1+\dots+x_n} < \sqrt{\frac{1}{x_1} + \frac{1}{x_2} + \dots + \frac{1}{x_n}}$$

Passo 1

Dimostriamo che vale la disuguaglianza:

$$\frac{x_1}{(1+x_1)^2} + \dots + \frac{x_n}{(1+x_1+\dots+x_n)^2} \leq 1 - \frac{1}{1+x_1+\dots+x_n} \quad (16)$$

Per induzione su n .

Per $n = 1$ è equivalente a:

$$\frac{x}{(1+x)^2} \leq 1 - \frac{1}{1+x}$$

Moltiplicando per $(1+x)^2$:

$$x \leq (1+x)^2 - (1+x) = x^2 + x$$

che è chiaramente vera.

Supponiamo che valga per un certo n , dimostriamo che vale per $n+1$:

$$\frac{x_1}{(1+x_1)^2} + \dots + \frac{x_{n+1}}{(1+x_1+\dots+x_n+x_{n+1})^2} \leq 1 - \frac{1}{1+x_1+\dots+x_n+x_{n+1}}$$

Sottraendo la (16) da quest'ultima, otteniamo la disuguaglianza equivalente:

$$\frac{x_{n+1}}{(1+x_1+\dots+x_n+x_{n+1})^2} \leq \frac{1}{1+x_1+\dots+x_n} - \frac{1}{1+x_1+\dots+x_n+x_{n+1}}$$

Moltiplicando per $1+x_1+\dots+x_n+x_{n+1}$ si ottiene:

$$\begin{aligned} \frac{x_{n+1}}{1+x_1+\dots+x_n+x_{n+1}} &\leq \frac{1+x_1+\dots+x_n+x_{n+1}}{1+x_1+\dots+x_n} - \frac{1+x_1+\dots+x_n+x_{n+1}}{1+x_1+\dots+x_n+x_{n+1}} = \\ &= 1 + \frac{x_{n+1}}{1+x_1+\dots+x_n} - 1 = \frac{x_{n+1}}{1+x_1+\dots+x_n} \end{aligned}$$

E quest'ultima è valida perchè le frazioni hanno lo stesso numeratore, ma quella a destra ha il denominatore minore. \square

Conclusione Applicando la disuguaglianza di Cauchy-Schwarz alle n -uple $(\frac{1}{\sqrt{x_1}}, \frac{1}{\sqrt{x_2}}, \dots, \frac{1}{\sqrt{x_n}})$ e $(\frac{\sqrt{x_1}}{1+x_1}, \frac{\sqrt{x_2}}{1+x_1+x_2}, \dots, \frac{\sqrt{x_n}}{1+x_1+x_2+\dots+x_n})$ otteniamo:

$$\frac{1}{1+x_1} + \frac{1}{1+x_1+x_2} + \dots + \frac{1}{1+x_1+\dots+x_n} \leq \sqrt{\frac{1}{x_1} + \frac{1}{x_2} + \dots + \frac{1}{x_n}} \cdot \sqrt{\frac{x_1}{(1+x_1)^2} + \dots + \frac{x_n}{(1+x_1+\dots+x_n)^2}}$$

Ma per la (16) sappiamo che fattore più a sinistra è strettamente minore di 1.

Quindi:

$$\frac{1}{1+x_1} + \frac{1}{1+x_1+x_2} + \dots + \frac{1}{1+x_1+\dots+x_n} < \sqrt{\frac{1}{x_1} + \frac{1}{x_2} + \dots + \frac{1}{x_n}}$$

\square .

Problema 7 Determinare tutte le quaterne di interi (a, b, m, n) , con $m > n > 1$, per cui il polinomio $x^n + ax + b$ divide il polinomio $x^m + ax + b$.

Chiamiamo $P(x) = x^n + ax + b$ e $Q(x) = x^m + ax + b$.

Fatto 1: $P(x)$ ha per radici complesse solo le radici dell'unità o 0. Tutte le sue radici diverse da 0 hanno molteplicità 1.

Dal fatto che $P(x)|Q(x)$ deduciamo che $P(x)|Q(x) - P(x)$ ovvero che

$$P(x)H(x) = x^m + ax + b - x^n - ax - b = x^n(x^{m-n} - 1)$$

per un polinomio $H(x)$. Tutte le radici di $P(x)$ sono anche radici di $x^n(x^{m-n} - 1)$. Sia λ una radice complessa di $x^n(x^{m-n} - 1)$. Allora $\lambda^n(\lambda^{m-n} - 1) = 0$ e, per la legge dell'annullamento del prodotto, $\lambda^n = 0$ oppure $\lambda^{m-n} = 1$. Il primo caso implica che $\lambda = 0$, il secondo che λ è una radice dell'unità.

Il polinomio $x^{m-n} - 1$ ha per radici tutte e sole le radici $m - n$ -esime dell'unità. Queste sono esattamente $m - n$, quindi ognuna ha molteplicità 1, perchè anche il grado è $m - n$. Tutte le radici dell'unità di $P(x)$ sono radici anche di $x^{m-n} - 1$, quindi sono distinte (hanno molteplicità 1).

Fatto 2: $b \in \{0, 1, -1\}$

Sappiamo che $P(x)$ ha come radici 0 o le radici dell'unità. Se una sua radice è 0, allora $P(x) = x \cdot H(x)$ per un certo $H(x)$ e quindi $b = 0$. Se tutte le sue radici complesse sono radici dell'unità, allora si scompone in $P(x) = (x - \lambda_1)(x - \lambda_2) \cdots (x - \lambda_n)$ dove $\lambda_1, \dots, \lambda_n$ sono le sue radici. Dalle formule di Vietè deduciamo inoltre che $|b| = |\lambda_1 \cdot \lambda_2 \cdots \lambda_n|$. Siccome λ_i sono tutte radici dell'unità, il loro modulo è 1. Inoltre, il prodotto dei moduli è uguale al modulo del prodotto. Quindi il modulo di b è 1. Essendo b intero, le uniche soluzioni sono $+1$ e -1 .

Fatto 3: il coefficiente di $n - 1$ grado e il coefficiente di 1 grado (di $P(x)$) hanno lo stesso valore assoluto.

Scriviamo $P(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = (x - \lambda_1)(x - \lambda_2) \cdots (x - \lambda_n)$. Dalle formule di Vietè deduciamo che $|a_{n-1}| = |\lambda_1 + \lambda_2 + \dots + \lambda_n|$, mentre

$$\begin{aligned} |a_1| &= |\lambda_1\lambda_2 \cdots \lambda_{n-1} + \dots + \lambda_2\lambda_3 \cdots \lambda_n| = \left| \frac{a_0}{\lambda_1} + \frac{a_0}{\lambda_2} + \dots + \frac{a_0}{\lambda_n} \right| = \\ &= |a_0| \cdot \left| \frac{1}{\lambda_1} + \dots + \frac{1}{\lambda_n} \right| = |\overline{\lambda_1} + \dots + \overline{\lambda_n}| = |\overline{\lambda_1 + \dots + \lambda_n}| = |\lambda_1 + \dots + \lambda_n| = |a_{n-1}| \end{aligned}$$

Qui abbiamo usato alcune note proprietà dei numeri complessi sugli inversi, i moduli e i coniugati, sapendo che il modulo di ciascuna radice e di a_0 è 1. Inoltre il modulo di un reale è uguale al suo valore assoluto, quindi il passo è dimostrato. \square

Cominciamo ora a distinguere vari casi:

Caso 1: $a = 0$ e $b = 0$.

Quindi $P(x) = x^n$ e $Q(x) = x^m$. È chiaro che tutte e sole le soluzioni di questo caso sono quelle con $n \leq m$, ma nelle ipotesi c'è anche che $m > n > 1$, quindi tutte e sole le soluzioni di questo caso sono della forma: $(0, 0, m, n)$, con $m > n > 1$.

Caso 2: $a = 0$ e $b = +1$.

Dobbiamo avere che $x^n + 1 | x^m + 1$. Sia $\omega = e^{i\frac{\pi}{n}}$. ω è una radice di $P(x)$, poichè $\omega^n = e^{i\pi} = -1$. Quindi ω deve essere anche una radice di $Q(x)$, cioè: $\omega^m = e^{i\pi\frac{m}{n}} = -1$, che è vero se e soltanto se $\pi\frac{m}{n}$ è un multiplo dispari di π , cioè se e soltanto se $\frac{m}{n} = (2k+1) \Leftrightarrow m = (2k+1)n$, con k un qualsiasi intero non negativo.

Questa condizione, oltre a essere necessaria, è anche sufficiente. È un fatto noto che $x^n + 1^n | (x^n)^{2k+1} + (1^n)^{2k+1}$.

Una famiglia di soluzioni è $(0, +1, (2k+1)n, n)$, k intero positivo, n intero ≥ 2 .

Caso 3: $a = 0$ e $b = -1$. Allo stesso modo di prima: $\omega = e^{i\frac{2\pi}{n}}$ è una radice di $P(x)$, quindi lo è anche di $Q(x)$, quindi $e^{i\frac{2\pi m}{n}} = 1$, se e soltanto se $\frac{m}{n}$ è intero, se e soltanto se $n | m$.

Questa condizione necessaria è anche sufficiente. È un fatto noto che $x^n - 1^n | (x^n)^k - (1^n)^k$.

Una famiglia di soluzioni è $(0, -1, kn, n)$, k intero positivo ≥ 2 , n intero ≥ 2 .

Caso 4: $a \neq 0$ e $b = 0$. $x^n + ax | x^m + ax$, quindi $x(x^{n-1} + a) | x(x^{m-1} + a)$, se e soltanto se $x^{n-1} + a | x^{m-1} + a$. Ma questo ricade nei casi precedenti, con le sostituzioni di variabili: $b \rightarrow a$, $n \rightarrow n-1$ e $m \rightarrow m-1$. A seconda che a sia $+1$ o -1 , facendo dovute sostituzioni, troviamo le famiglie di soluzioni:

$$(1, 0, (2k+1)n + 2k, n), n \geq 2, k \geq 1$$

$$(-1, 0, kn - k + 1, n), n \geq 2, k \geq 1$$

Caso 5: $a \neq 0$, $b \neq 0$.

In questo caso ($b \neq 0$) tutte le radici di $P(x)$ sono radici dell'unità (conseguenza del fatto 1) e hanno molteplicità 1 (conseguenza del fatto 1). Se $n > 2$, allora il coefficiente di grado $n-1$ -esimo di $P(x)$ sarebbe 0, ma per il fatto 3 anche a sarebbe 0, caso che abbiamo già analizzato. Quindi $P(x) = x^2 + ax + b$ ha grado n .

Siano ω_1 e ω_2 le due radici complesse di $P(x)$. Sono coniugate perchè i coefficienti sono reali. Scriviamo $\omega_1 = \cos\theta + i\sin\theta$, $\omega_2 = \cos\theta - i\sin\theta$. Dalle formule di Vietè sappiamo che $-a = \omega_1 + \omega_2 = 2\cos\theta$. Ma a è intero e il valore assoluto di un coseno è minore o uguale a 1. Quindi $|a| = 2$ (questo se e soltanto se $\omega_1 = \pm 1$) oppure $|a| = 1$. b , invece, è uguale a $\omega_1\omega_2 = \cos^2\theta + \sin^2\theta$. b non può essere negativo, quindi è $+1$.

Analizziamo il caso in cui $a = \pm 2$. Allora $P(x) = x^2 \pm 2x + 1 = (x \pm 1)^2$, ma avrebbe una radice con molteplicità 2: abbiamo dimostrato che è impossibile.

Analizziamo il caso in cui $a = 1$. Allora $\cos\theta = \frac{1}{2}$ e $\omega_1 = e^{i\frac{2\pi}{3}}$. Dal fatto che $P(x) | x^{m-n} - 1 = x^{m-2} - 1$ deduciamo che ω_1 deve essere una radice anche di $x^{m-2} - 1$, cioè $\omega_1^{m-2} = e^{i2\pi\frac{m-2}{3}} = 1$, se e soltanto se $6 | m-2$, cioè $m = 2k+2$ per $k \geq 1$. Inoltre, se $6 | m-2$, allora il polinomio $x^{m-2} - 1$ ha come radici tutte le radici seste dell'unità, quindi anche ω_2 .

Se $a = -1$, allora $\cos\theta = -\frac{1}{2}$ e $\omega_1 = e^{i\frac{2\pi}{3}}$. Facendo lo stesso ragionamento di prima, otteniamo che la condizione necessaria e sufficiente perchè $P(x) | Q(x)$ è che $3 | m-2$ o $m = 3k+2$.

In quest'ultimo caso abbiamo ottenuto le due famiglie di soluzioni:

$$(1, 1, 6k+2, 2)$$

$$(-1, 1, 3k+2, 2). \quad \square$$

Problema 8 Determinare tutte le funzioni $f : \mathbb{R} \rightarrow \mathbb{R}$ tali che

$$f(x+y) + f(x)f(y) = f(xy) + 2xy + 1 \quad (17)$$

per ogni coppia di numeri reali x e y .

Tutte e sole le funzioni che riespletano la (17) sono:

1. $f(x) = 2x - 1$
2. $f(x) = -x - 1$
3. $f(x) = x^2 - 1$

Verifichiamo che sono effettivamente soluzioni dell'equazione funzionale.

1. $f(x+y) + f(x)f(y) = 2(x+y) - 1 + (2x-1)(2y-1) = 4xy;$
 $f(xy) + 2xy + 1 = 2xy - 1 + 2xy - 1 = 4xy$
2. $f(x+y) + f(x)f(y) = -(x+y) - 1 + (-x-1)(-y-1) = xy;$
 $f(xy) + 2xy + 1 = -xy - 1 + 2xy + 1 = xy$
3. $f(x+y) + f(x)f(y) = (x+y)^2 - 1 + (x^2-1)(y^2-1) = x^2y^2 + 2xy;$
 $f(xy) + 2xy + 1 = x^2y^2 - 1 + 2xy + 1 = x^2y^2 + 2xy$

Ora dimostreremo che le soluzioni sono solo queste.

Per abbreviare la scrittura, chiamiamo $f(1) = a$ e $f(-1) = b$. Nella dimostrazione useremo diverse formule che si ottengono sostituendo, nella (17), altri valori al posto di x e y . Le elenchiamo e numeriamo qui di seguito:

$$(x, y) \leftarrow (0, t) \implies f(t) + f(0)f(t) = f(0) + 1 \quad (18)$$

$$(x, y) \leftarrow (1, -1) \implies f(0) + ab = b - 1 \quad (19)$$

$$(x, y) \leftarrow (t-1, +1) \implies f(t) + af(t-1) = f(t-1) + 2t - 1 \quad (20)$$

Dalla (18) ricaviamo che $f(t)[f(0) + 1] = f(0) + 1$. Se $f(0) \neq -1$, questo implica $f(t) = 1 \quad \forall t$, ma sostituendo questa funzione nella (17) si vede subito che non è possibile. Quindi $f(0) = -1$.

Dalla (19) ricaviamo che $ab = b$. Se $b \neq 0$, questo implica $a = 1$. Sostituendo nella (20), ricaviamo $f(t) = 2t - 1$, che è effettivamente una soluzione che abbiamo già verificato. D'ora in poi supporremo $b = 0$. Sostituendo $(2, -1)$ al posto di (x, y) nella (17) e semplificando, troviamo $a = f(-2) - 3$. Sostituendo $(-2, 1)$ nella (17) e semplificando, otteniamo $f(-2)a = f(-2) - 3$. Quindi $a = f(-2)a$. Se $a \neq 0$, $f(-2) = 1$ da cui, sostituendo in una delle ultime equazioni, $a = -2$. Quindi ci sono solo due possibilità: $a = -2$ o $a = 0$.

Sempre sostituendo particolari valori nella (17), troviamo:

$$(x, y) \leftarrow (x, -1) \implies f(x-1) = f(-x) - 2x + 1 \quad (21)$$

$$(x, y) \leftarrow (x-1, +1) \implies f(x) = (1-a)f(x-1) + 2x - 1 \quad (22)$$

$$(x, y) \leftarrow (-x, -1) \implies f(-x-1) = f(x) + 2x + 1 \quad (23)$$

$$(x, y) \leftarrow (-x-1, +1) \implies f(-x) = (1-a)f(-x-1) - 2x - 1 \quad (24)$$

Da queste, facendo delle sostituzioni per togliere i termini $f(x-1)$ e $f(-x-1)$, resta il seguente sistema nelle variabili $f(x)$ e $f(-x)$:

$$f(x) = (1-a)(f(-x) - 2x + 1) + 2x - 1$$

$$f(-x) = (1-a)(f(x) + 2x + 1) - 2x - 1$$

Sostituendo il valore $a = -2$ e risolvendo il sistema lineare, si ottiene $f(x) = -x - 1$, che è una soluzione.

D'ora in poi supporremo $a = b = 0$. Sostituendo questi valori nel sistema, riusciamo ad ottenere che $f(x) = f(-x)$, cioè che la funzione f è pari.

Sostituendo $(t, -t)$ nella (17) otteniamo:

$$-1 + f(t)f(-t) = f(-t^2) - 2t^2 + 1$$

$$f(t)^2 = f(t^2) - 2t^2 + 2$$

Sostituendo (t, t) nella (17) otteniamo:

$$f(2t) + f(t)^2 = f(t^2) + 2t^2 + 1$$

$$f(t)^2 = f(t^2) - f(2t) + 2t^2 + 1$$

Da queste ultime due equazioni deduciamo:

$$f(t)^2 = f(t^2) - 2t^2 + 2 = f(t^2) - f(2t) + 2t^2 + 1$$

$$f(2t) = 4t^2 - 1$$

In quest'ultima, ponendo $t' = \frac{1}{2}t$:

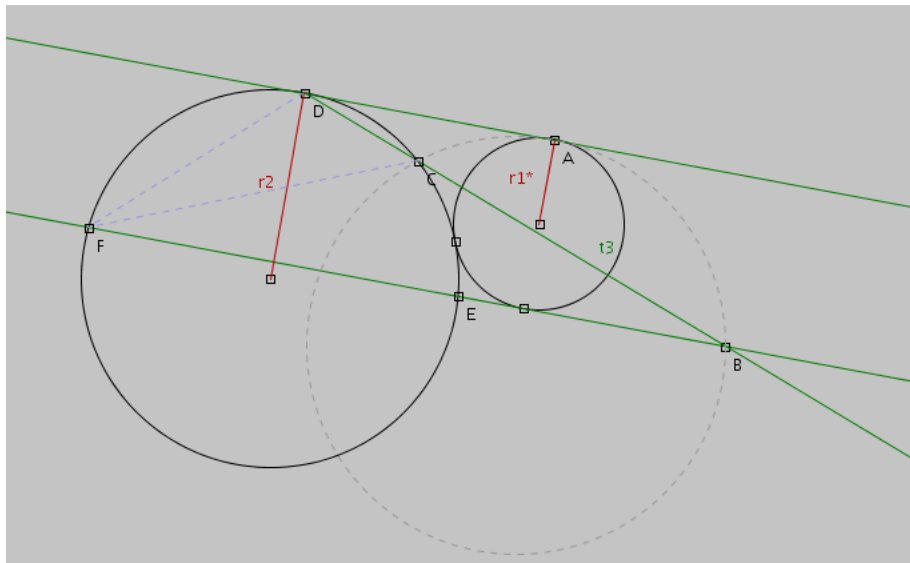
$$f(t') = t'^2 - 1 \quad \forall t' \in \mathbb{R}$$

Che è l'ultima soluzione.

3 Geometria

Problema 9 Due circonferenze Γ_1 e Γ_2 sono tangenti esternamente ed hanno raggi r_1 e r_2 , rispettivamente, con $r_2 > r_1$. La retta t_1 è tangente a Γ_1 e Γ_2 in A e D , rispettivamente. La retta t_2 , parallela a t_1 , è tangente a Γ_1 ed interseca Γ_2 in E ed F . La retta t_3 passa per D ed incontra nuovamente t_2 in B e Γ_2 in C .

Dimostrare che la retta t_1 è tangente alla circonferenza circoscritta ad ABC .



Fatto 1: $DA = DF = DE$. Chiamiamo O_2 e O_1 i centri delle circonferenze Γ_2 e Γ_1 . Sia I l'intersezione tra le rette DO_1 e t_2 . Consideriamo il trapezio rettangolo DAO_1O_2 . Si ha che $DO_2 = r_2$, $AO_1 = r_1$, $O_1O_2 = r_1 + r_2$. Per il teorema di Pitagora, possiamo calcolare $DA^2 = (r_1 + r_2)^2 - (r_2 - r_1)^2 = 4r_1r_2$.

Ora distinguiamo due casi.

Caso 1 : $2r_1 < r_2$, come nella figura. Consideriamo il triangolo rettangolo EIO_2 . $IO_2 = r_2 - 2r_1$, $EO_2 = r_2$, quindi, per il teorema di Pitagora, $EI^2 = r_2^2 - (r_2 - 2r_1)^2 = 4r_1r_2 - 4r_1^2$. Consideriamo il triangolo rettangolo EID . Per il teorema di Pitagora, $ED^2 = EI^2 + DI^2 = 4r_1r_2 - 4r_1^2 + (2r_1)^2 = 4r_1r_2 = AD^2$.

Caso 2 : $2r_1 > r_2$. Applicando il teorema di Pitagora ai triangoli EO_1I ed EID , calcoliamo $ED^2 = ID^2 + IE^2 = ID^2 + (EO_1^2 - IO_1^2) = 2r_1^2 + (r_2^2 - (2r_1 - r_2)^2) = 4r_1r_2 = AD^2$.

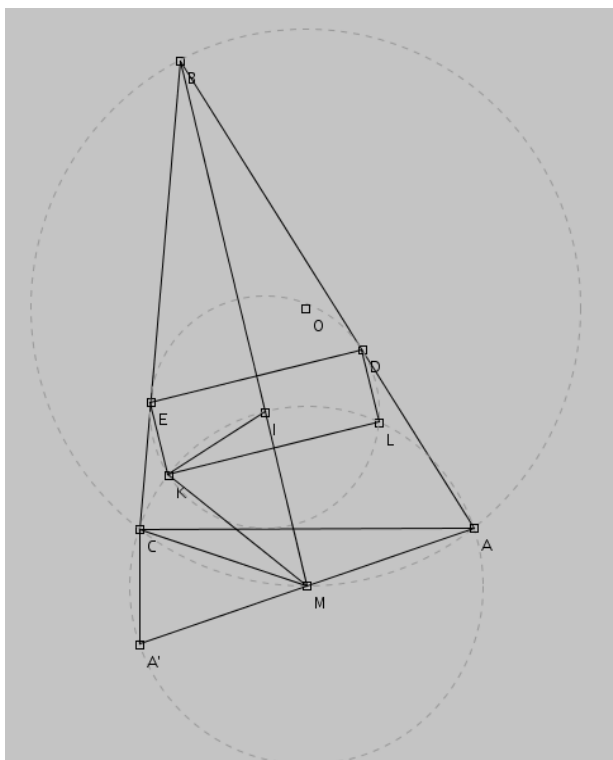
Infine dimostriamo che $DE = DF$ osservando che $E\hat{D}A = E\hat{F}D$ per il teorema degli angoli alla circonferenza e alla tangente, e anche $E\hat{D}A = F\hat{E}D$ considerando DE come retta trasversale alle parallele t_1 e t_2 , quindi il triangolo DEF è isoscele su base EF e $DE = DF$. Concludiamo che $DE = DF = DA$. \square

I triangoli DCF e DBF sono simili. Infatti, oltre all'angolo in comune $F\hat{D}B$, abbiamo che $D\hat{C}F = D\hat{E}F = D\hat{F}E = D\hat{F}B$, per il teorema degli angoli alla circonferenza e per l'osservazione fatta prima.

Da questa similitudine deduciamo che $\frac{DC}{DF} = \frac{DF}{DB}$ o $DF^2 = DC \cdot DB$ o $DA^2 = DC \cdot DB$. Ma $DC \cdot DB$ è la potenza del punto D rispetto alla circonferenza circoscritta ad ABC . Se questo è uguale a DA^2 , per il teorema della secante e della tangente, DA è tangente alla circonferenza circoscritta ad ABC e quindi lo è anche t_1 . \square

Problema 10 In un triangolo ABC si ha che $AB + BC = 3AC$. Sia I l'incentro e siano D ed E i punti in cui la circonferenza inscritta è tangente ai lati AB e BC , rispettivamente. Siano K ed L i simmetrici di D ed E rispetto ad I .

Dimostrare che il quadrilatero $ACKL$ è ciclico.



Indichiamo con α, β, γ la metà degli angoli del triangolo ABC nei vertici, rispettivamente, A, B, C .

Fatto 1: dimostriamo che $BD = AC$. Usiamo il fatto che le due tangenti da un vertice alla circonferenza inscritta sono uguali. Abbiamo che $AB + BC = 2BD + CE + AD$, $AC = CE + AD$. Per le ipotesi del problema, $AB + BC = 3AC$, quindi $2BD + CE + AD = 3CE + 3AD$, quindi $BD = CE + AD = AC$.

Fatto 2: sia M l'intersezione tra la circonferenza circoscritta ad ABC e la semiretta BI . M è il circocentro di IAC .

1. $M\hat{B}A = M\hat{C}A = M\hat{B}C = M\hat{A}C = \beta$, per il teorema degli angoli alla circonferenza (circoscritta ad ABC , in questo caso) e per il fatto che M giace sulla bisettrice di $A\hat{B}C$. Quindi $MC = MA$.
2. $M\hat{I}C = I\hat{C}B + I\hat{B}C = \gamma + \beta$, per il teorema dell'angolo esterno. Inoltre $M\hat{C}I = M\hat{C}A + A\hat{C}I = \beta + \gamma$. Concludiamo che IMC è isoscele su base IC e quindi $IM = CM$.

M è equidistante dai tre punti quindi è il centro della circonferenza circoscritta.

Chiamiamo Γ_1 la circonferenza inscritta ad ABC , di raggio r , e Γ_2 la circonferenza circoscritta a AIC , di centro M e raggio r' .

Fatto 3: sia A' il simmetrico di A rispetto ad M , e quindi diametralmente opposto. Allora il triangolo ACA' è congruente a IDB . Infatti, sono entrambi retti per costruzione. Hanno un lato in comune, $AC = BD$, dimostrato nel fatto 1. Infine hanno un'altro angolo uguale, $\widehat{CAA'}$ e \widehat{DBI} , entrambi uguali a β come già osservato prima.

Ora dimostreremo che i triangoli IMK e CMA' sono congruenti. Dal fatto 3 deduciamo che $CA' = ID = r = IK$. Inoltre $MI = MC = r'$. Resta da dimostrare che l'angolo compreso è uguale.

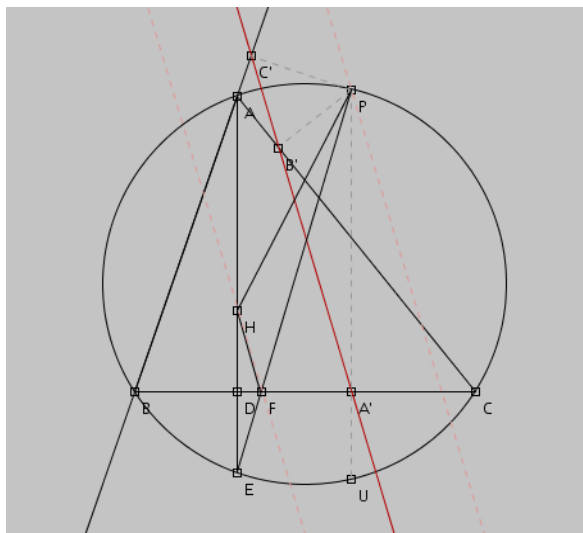
Il quadrilatero $BEID$ è ciclico perchè ha due angoli opposti retti. Quindi $\widehat{DEB} = \widehat{DIB}$, ma quest'ultimo è diametralmente opposto a \widehat{KIM} , quindi $\widehat{KIM} = \widehat{DEB}$.

Il complementare di $\widehat{A'CM}$ è \widehat{MCA} , che a sua volta è uguale a \widehat{CBI} , il cui complementare è \widehat{DEB} . Concludiamo che $\widehat{A'CM} = \widehat{KIM} = 90 - \beta$ e che i triangoli $A'CM$ e KIM sono congruenti.

La conseguenza è che anche KIM è isoscele, quindi $KM = IM = r'$ e K giace sulla circonferenza Γ_2 .

Possiamo fare lo stesso ragionamento con L . Concludiamo che A, C, K, L giacciono sulla stessa circonferenza e quindi che questo quadrilatero è ciclico. \square

Problema 11 Sia ABC un triangolo, H il suo ortocentro, P un punto che sta sulla circonferenza circoscritta. Dimostrare che la linea di Simson ottenuta da P biseca il segmento PH .



Spiegazione della figura: A, B, C sono i vertici del triangolo. A', B', C' sono le proiezioni della linea di Simson sui lati opposti ad A, B, C . D è il piede dell'altezza per A . E è l'intersezione tra l'altezza per A e la circonferenza circoscritta. U è l'intersezione tra la perpendicolare per P al lato BC e la circonferenza circoscritta. F è l'intersezione tra le rette PE e BC .

Fatto 1: $HD = DE$. Lo dimostriamo con la congruenza dei triangoli HDC e EDC . Per costruzione sono entrambi rettangoli ed hanno un lato in comune, inoltre gli angoli \widehat{HCD} e \widehat{DCE} sono uguali. Questo segue dalla catena di congruenze: $\widehat{DCE} = \widehat{BCE} = \widehat{BAE} = 90 - \widehat{DBA} = 90 - (90 - \widehat{HCD}) = \widehat{HCD}$, in cui abbiamo usato il teorema degli angoli alla circonferenza e il fatto che le altezze sono perpendicolari ai lati relativi.

Fatto 2: HDF e EDF sono triangoli congruenti. Infatti hanno i lati (HD, DE) e (DF, DF) rispettivamente congruenti (fatto 1) e l'angolo compreso congruente (è retto).

Fatto 3: HF e la linea di Simson sono parallele. Questo segue dalla catena di uguaglianze:

$$P\widehat{A}C' = P\widehat{B}C' = P\widehat{B}A = P\widehat{E}A = F\widehat{E}D = F\widehat{H}D$$

Nell'ultimo passaggio abbiamo sfruttato, in ordine:

1. la ciclicità del quadrilatero $BA'PC'$, con due angoli retti opposti
2. la collinearità di B, A, C'
3. il teorema sugli angoli alla circonferenza
4. la collinearità di A, D, E e P, F, E
5. la congruenza dei triangoli DFH, DFE

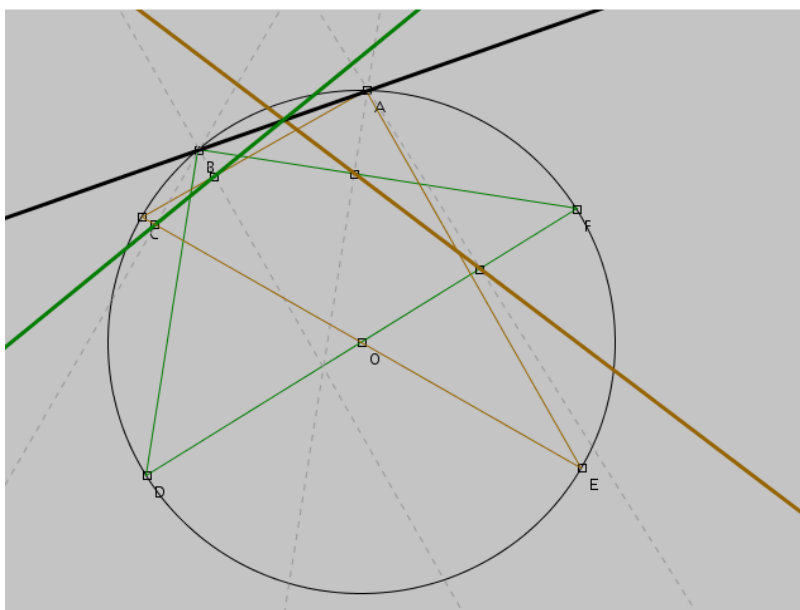
Ora, da $\widehat{DHF} = \widehat{PA'C'}$ deduciamo che anche i loro complementari sono uguali: $\widehat{DFH} = \widehat{DA'C'}$, quindi la retta di Simson e HF formano lo stesso angolo con la retta BC e sono parallele.

Fatto 4: la linea di Simson è la mediana del triangolo $PA'F$. Infatti abbiamo già scoperto che $\widehat{PA'C'}$ e \widehat{PEA} sono angoli congruenti, ma $\widehat{PEA} = \widehat{EPA'}$ per il parallelismo tra AE e PA' , entrambe perpendicolari a BC . Concludiamo che $\widehat{PA'C'} = \widehat{A'PF}$, ma questo è noto come essere necessario e sufficiente perchè AC' sia la mediana di un triangolo rettangolo $FA'P$.

Conclusione: Consideriamo le rette HF e la sua parallela per P . Con il fatto 4 abbiamo dimostrato che sono equidistanti dalla retta di Simson (parallela ad entrambe). Dal teorema di Talete segue direttamente che la retta di Simson biseca anche il segmento PH . \square

Problema 12 Indichiamo con $(X; PQR)$ la linea di Simson del triangolo PQR relativa al punto X .

Sia $ABCDEF$ un esagono i cui vertici giacciono tutti sulla stessa circonferenza. Dimostrare che, se $CDEF$ è un rettangolo, allora le rette $(A; BDF)$, $(B; ACE)$, $(D; ABF)$, $(E; ABC)$ concorrono.



Fatto 1: $(D; ABF) = (E; ABC) = AB$

D ed F sono diametralmente opposti, quindi l'angolo $D\hat{B}F$ è retto e la proiezione di D su BF è B . L'angolo $D\hat{A}F$ è retto, quindi la proiezione di D su AF è A . La retta di Simson del triangolo ABF relativa a D deve quindi passare per A e per B , quindi è proprio la retta AB .

Analogamente si dimostra che $(E; ABC) = AB$ (basta permutare le lettere).

Fatto 2: se M è il punto medio di AB , $M \in (A; BDF)$ e $M \in (B; ACE)$.

Essendo l'angolo $D\hat{B}F$ retto, B è l'ortocentro del triangolo BDF . È noto che la linea di Simson costruita dal punto A sul triangolo BDF biseca il segmento che collega A all'ortocentro di questo triangolo. Quindi $M \in (A; BDF)$.

Allo stesso modo (permutando le lettere) si dimostra che $M \in (B; ACE)$.

Concludiamo che tutte le linee di Simson elencate prima passano per il punto M .

Problema 13 Sia ABC un triangolo. Sia O il centro di una circonferenza che passa per A e C e interseca AB e BC in N e K , rispettivamente; sia M l'intersezione tra le circonferenze circoscritte ad ABC e a BNK , distinta da B .
Dimostrare che OM e MB sono perpendicolari.

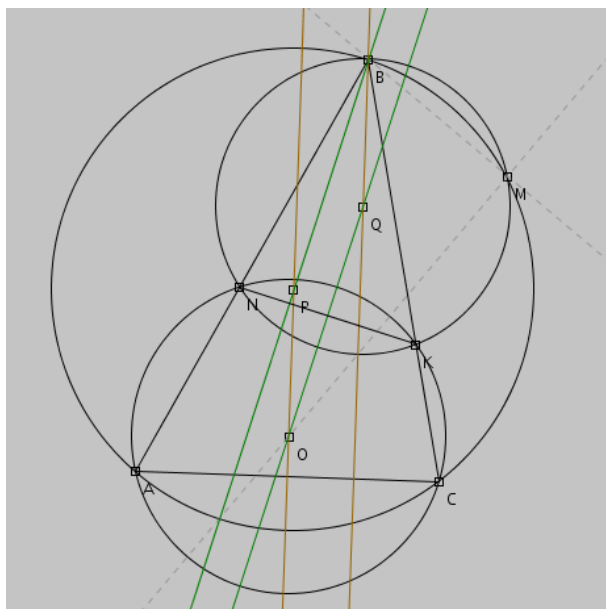


Figura. P è il centro della circonferenza circoscritta ad ABC , Q è il centro della circonferenza circoscritta a BNK .

Fatto 1: $B\hat{N}K = B\hat{C}A, B\hat{K}N = B\hat{A}C$.

Il quadrilatero $ACKN$ è ciclico: quindi ha i lati opposti supplementari; $B\hat{C}A = 180 - A\hat{N}K$. Ma è supplementare di $A\hat{N}K$ anche $B\hat{N}K$, quindi $B\hat{N}K = B\hat{C}A$. Allo stesso modo, il supplementare di $B\hat{A}C$ è $N\hat{K}C$ per la ciclicità del quadrilatero, e il supplementare di $N\hat{K}C$ è $B\hat{K}N$.

Fatto 2: PO e BQ sono rette parallele.

O giace sull'asse di AC ; P giace sull'asse di AC , quindi PO è l'asse di AC ed è perpendicolare ad AC .

$K\hat{Q}B = 2K\hat{N}B$ per il teorema degli angoli al centro e alla circonferenza. Ma KQB è isoscele, quindi $K\hat{B}Q = \frac{180 - K\hat{Q}B}{2} = 90 - K\hat{N}B$. Abbiamo già dimostrato che $K\hat{N}B = B\hat{C}A$, quindi $K\hat{B}Q = 90 - B\hat{C}A$. Sia I l'intersezione tra la retta BQ e la retta AC . Consideriamo il triangolo BIC : ha due lati complementari ($I\hat{B}C = Q\hat{B}C = 90 - B\hat{C}A = 90 - B\hat{C}I$), quindi l'angolo $B\hat{I}C$ è retto e BQ è perpendicolare ad AC .

Sia BQ , sia PO sono perpendicolari ad AC , quindi sono parallele.

Fatto 3: BP è parallela a QO .

QO è l'asse di NK , quindi è perpendicolare a NK .

$A\hat{B}P = 90 - \frac{A\hat{P}B}{2} = 90 - A\hat{C}B = 90 - B\hat{N}K$. Abbiamo usato il fatto che APB è isoscele, il teorema degli angoli al centro e alla circonferenza, il fatto 1.

Sia L l'intersezione tra BP e NK . Il triangolo NLB ha i due angoli \widehat{LNB} e \widehat{LBN} complementari, quindi è retto in L e BP è perpendicolare a NK .

Sia BP , sia QO sono perpendicolari a NK , quindi sono parallele.

Fatto 4: $BQOP$ è un parallelogramma.

È un corollario dei fatti 2 e 3.

Conclusione

Sia D l'intersezione tra le diagonali del parallelogramma $BQOP$ ed E il punto medio di BM . Consideriamo i triangoli BDE e BOM .

1. $BM = 2BE$, per costruzione
2. $BO = 2BD$, perchè le diagonali di un parallelogramma si dividono scambievolmente a metà
3. $\widehat{OBM} = \widehat{DBE}$, perchè i punti $(B; D; O)$ e $(B; E; M)$ sono allineati per costruzione

Da queste considerazioni segue che i triangoli BDE e BOM sono simili e che $\widehat{DEB} = \widehat{OMB}$. Ma la retta perpendicolare a BM in E passa per P e Q (perchè sono centri di circonferenze per le quali BM è una corda), quindi anche per D , quindi $\widehat{DEB} = 90$ e anche $\widehat{OMB} = 90$. Il problema è dimostrato. \square

4 Combinatoria

Problema 14 Sono date n palline numerate da 1 a n , Determinare quanti sono i modi di distribuire queste palline tra 9 persone A, B, \dots, I in modo che A riceva tante palline quante ne ricevono B, C, D, E messe insieme (si intende che 2 distribuzioni sono considerate identiche solo se ognuna delle 9 persone riceve in entrambi i casi le palline con gli stessi numeri).

Passo 1: dimostriamo che il numero di combinazioni è dato dalla formula

$$\sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2k} \binom{2k}{k} 4^k 4^{n-2k} \quad (25)$$

Dividiamo le possibili distribuzioni di palline a seconda del numero k di palline assegnate ad A . k non può essere maggiore di $\lfloor \frac{n}{2} \rfloor$ perchè dobbiamo dare altre k palline a B, C, D, E .

Per ogni scelta di k , dividiamo ulteriormente le combinazioni secondo l'insieme delle palline che saranno distribuite ad $\{A, B, C, D, E\}$. Tutte e sole le scelte possibili sono sottoinsiemi con $2k$ elementi, per il vincolo che A e $\{B, C, D, E\}$ devono ricevere lo stesso numero di palline.

Sia X l'insieme di palline da distribuire a $\{A, B, C, D, E\}$. Dividiamo le combinazioni a seconda dell'insieme X' di palline da distribuire a $\{B, C, D, E\}$, che può essere scelto in $\binom{2k}{k}$ modi. Da ogni scelta deduciamo in modo unico le palline che saranno assegnate ad A (tutte quelle appartenenti a $X \setminus X'$).

Siano p_1, \dots, p_k gli elementi di X' . Possiamo dare p_1 a B, C, D, E , 4 scelte. Possiamo dare p_2 a B, C, D, E , e così via, per un totale di 4^k combinazioni.

Sia Y l'insieme delle palline che non appartengono a X , che quindi saranno assegnate a F, G, H, I . La cardinalità di Y è $n - 2k$, quindi l'assegnazione alle singole persone può essere scelta, come prima, in 2^{n-2k} modi.

Abbiamo usato diversi criteri per suddividere le possibili combinazioni. Due combinazioni sono differenti se, secondo un qualsiasi criterio, danno risultati differenti. Questo giustifica il fatto che, moltiplicando i vari passi fino ad ottenere la (26), la formula non sia nè maggiore nè minore del numero effettivo di combinazioni.

Passo 2: la (26) è equivalente termine di grado 0 nel polinomio:

$$\left(\frac{4}{x} + x + 4\right)^n \quad (26)$$

Sviluppando i coefficienti binomiali nella (26) otteniamo:

$$\sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2k} \binom{2k}{k} 4^k 4^{n-2k} = \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n!}{(2k)!(n-2k)!} \frac{(2k)!}{k!k!} 4^{n-2k+k} = \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n!}{(n-2k)!k!k!} 4^{n-k} \quad (27)$$

Consideriamo lo sviluppo di Newton di (27):

$$\left(\frac{4}{x} + x + 4\right)^n = \sum_{h+i+j=n, h, i, j \geq 0} \frac{n!}{h!i!j!} \left(\frac{4}{x}\right)^h x^i 4^j$$

Osserviamo che nel polinomio (27), otteniamo un monomio di grado 0 se e soltanto se, nel prodotto

$$\underbrace{\left(\frac{4}{x} + x + 4\right)\left(\frac{4}{x} + x + 4\right) \cdots \left(\frac{4}{x} + x + 4\right)}_{n \text{ volte}}$$

si scelgono in ugual numero termini x e termini $\frac{4}{x}$. Chiamiamo k il numero di termini x o $\frac{4}{x}$, sia $f(n)$ il termine noto del polinomio. Applichiamo questo risultato all'ultima formula:

$$f(n) = \sum_{k+k+j=n, k, j \geq 0} \frac{n!}{k!k!j!} \left(\frac{4}{x}\right)^k x^k 4^j$$

Sostituendo $i = n - 2k$ e raccogliendo, otteniamo proprio la (28).

Passo 3: le combinazioni cercate sono $\binom{2n}{n} 4^n$.

Ripartiamo dalla (27), che può essere trasformata in questo modo:

$$\left(\frac{4}{x} + x + 4\right)^n = \frac{1}{x^n} (x^2 + 4x + 4)^n = \frac{1}{x^n} (x + 2)^{2n}$$

. La funzione cercata ora è diventata il coefficiente di grado n del polinomio $(x + 2)^{2n}$, diviso per x^n . Sviluppandolo con Newton, troviamo che il coefficiente di grado n è $\binom{2n}{n} x^n 2^n$. Dividendolo per x^n , otteniamo il risultato, che probabilmente è la forma più chiusa possibile per esprimere $f(n)$. \square

Problema 15 Una gara matematica tra $2n$ studenti viene organizzata secondo il seguente schema. Ogni studente propone un problema; i problemi vengono poi raccolti e distribuiti in modo che ogni partecipante ne riceva uno. La gara si definisce leale se esiste un sottoinsieme di n studenti che hanno ricevuto i problemi proposti dagli altri n .

Dimostrare che il numero di modi di distribuire i problemi ottenendo una gara leale è un quadrato perfetto.

Sia S l'insieme degli studenti ed $f : S \rightarrow S$ la funzione che associa a ciascun studente x lo studente che ha ricevuto l'esercizio proposto da x . Siccome S è una funzione da S in se stesso, f è una permutazione di S .

Passo 1: Ogni permutazione leale f è la composizione di cicli di lunghezza pari.

Siccome f è leale, allora esistono due insiemi $A, B \subseteq S$, con $|A| = |B| = n$, tali che ogni studente di B riceve un problema da uno studente da A . Sia $C \subseteq A$ l'insieme degli studenti di A che mandano il loro problema a uno studente di B . La funzione f , con il dominio ristretto a C ha per codominio B ed è suriettiva, quindi $|C| \geq |B|$. Ma $|B| = |A|$ e $|C| \leq |A|$, essendone un sottoinsieme, quindi $C = A$ e ogni studente di A manda il suo problema ad uno studente di B .

Se uno studente di B mandasse il suo problema a uno studente di B , esisterebbe uno studente di B che riceve il problema da uno studente di B . Ma egli lo riceve già da uno studente di A , quindi questa situazione è impossibile. Concludiamo che ogni studente di B manda il suo problema a uno studente di A .

Indichiamo ora con $f^k(a)$ la composizione di f per k volte.

Per ogni $a \in S$, esiste un intero positivo k tale che $f^k(a) = a$. Infatti, consideriamo la funzione $g : \mathbb{N} - \{0\} \rightarrow S$ $g(k) = f^k(a)$. Negando questa ipotesi, la g sarebbe iniettiva, quindi S avrebbe almeno la cardinalità del numerabile, il che è evidentemente assurdo.

Dimostriamo ora che se $a = f^k(a)$, allora k è pari. Senza perdita di generalità, supponiamo che $a \in A$. Per quanto dimostrato prima, $f^1(a) \in B$. Inoltre, $f^i(a) \in B \implies f^{i+2}(a) \in B$. Abbiamo dimostrato per induzione che $f^x(a) \in B$ per ogni x dispari, ma $f^k(a) = a$ e $a \in A$, quindi $f^k(a) \in A$, quindi k non può essere dispari ed è pari.

È noto che una permutazione si scompone in modo unico come composizione di cicli, ma abbiamo appena dimostrato che ogni ciclo è di lunghezza pari. \square

Passo 2: sia S un insieme finito con $2n$ elementi. Allora il numero di numero di permutazioni che sono prodotto di cicli pari è $[(2n - 1)(2n - 3) \cdots 3 \cdot 1]^2$.

Lo dimostriamo per induzione. Per $n = 1$, c'è un unico ciclo pari perchè deve avere lunghezza 2.

Supponiamo che la formula valga per n , dimostriamola per $n + 1$. Scriviamo $S = \{s_1, s_2, \dots, s_{2n+2}\}$. Dividiamo le permutazioni leali a seconda della persona a cui s_1 consegna il problema. Questa può essere scelta in $2n + 1$ modi, poichè l'unica limitazione è che sia diversa da s_1 .

Dividiamo ulteriormente le permutazioni leali a seconda di $f(f(s_1))$, che è può essere scelto ancora in $2n + 1$ modi, poichè deve essere diverso da $f(s_1)$, ma potrebbe essere proprio s_1 , chiudendo il ciclo (pari).

Consideriamo l'insieme $S' = S - s_1 - f(s_1)$. Distinguiamo due casi per definire una funzione $f' : S' \rightarrow S'$:

Caso 1 : $f(f(s_1)) = s_1$. f' allora è la restrizione di f al dominio S' .

altrimenti : $s_i \neq f^{-1}(s_1) \implies f'(s_i) = f(s_i)$; $s_i = f^{-1}(s_1) \implies f'(s_i) = f(f(s_1))$

In entrambi i casi abbiamo definito una permutazione, con dominio S' e codominio S' , ancora leale. $|S'| = 2n$, quindi, per l'ipotesi induttiva, questa può essere scelta in $[(2n-1)(2n-3) \cdots 3 \cdot 1]^2$ modi. Moltiplicando per $(2n+1)^2$, che sono i modi di scegliere $f(s_1)$ e $f(f(s_1))$, confermiamo la validità della formula anche per $2n+2$. Questa formula mostra esplicitamente che il suo valore è sempre un quadrato perfetto. \square

Problema 16 *In una casa vi sono varie stanze. Ogni stanza contiene almeno 3 lampadine. Il numero totale di lampadine è pari. Ogni lampadina condivide un interruttore con una ed una sola delle altre: mediante tale interruttore è possibile cambiare contemporaneamente lo stato acceso/spento di entrambe le lampadine.*

Dimostrare che, a partire da qualunque configurazione iniziale (nella quale non è detto che 2 lampadine con lo stesso interruttore siano entrambe accese od entrambe spente) è possibile agire sugli interruttori in modo che alla fine ci sia, in ogni stanza, almeno una lampadina accesa ed almeno una lampadina spenta.

Sia S l'insieme delle stanze.

Passo 1: semplificazione del problema.

Definiamo una relazione fra le stanze. Due stanze (a, b) si dicono collegate se e soltanto se si verifica uno dei seguenti casi:

1. $a = b$
2. due lampadine, una in a e una in b , condividono l'interruttore.
3. esiste una stanza c tale che a è collegata a c e c è collegata a b .

Questa relazione è di equivalenza. Infatti soddisfa le proprietà:

riflessiva : se $a = b$, allora a è collegata a b per il primo caso nella definizione di "collegate".

simmetrica : se a è collegata a b , esiste un interruttore che collega una lampadina di a a una lampadina di b . Lo stesso interruttore collega la stessa lampadina di b alla stessa lampadina di a .

transitiva : se a è collegata a c e c è collegata a b , allora, per il terzo caso nella definizione di "collegate", a è collegata a b .

Consideriamo l'insieme quoziente di S rispetto alla relazione "collegate". Se dimostriamo esiste un algoritmo per raggiungere l'obiettivo (ossia ottenere in almeno una stanza almeno una lampadina accesa e una spenta) per ogni insieme di stanze collegate, allora potremmo applicarlo ad ogni classe di equivalenza di S rispetto alla relazione "collegate". Basterà dimostrare questo. Quindi d'ora in poi supporremo che ogni coppia di stanze sia collegata.

Passo 2: discesa infinita.

Definiamo "buone" le stanze con almeno una lampadina accesa e una spenta, "cattive" le altre. Supponiamo che esista un algoritmo che permetta di trasformare una stanza cattiva in una buona ogni volta che esiste una stanza cattiva. Allora il problema è risolto.

Se così non fosse: consideriamo la successione di interi positivi indicanti la cardinalità dell'insieme delle stanze cattive all' n -esima applicazione dell'algoritmo. Sarebbe strettamente decrescente (ogni volta cala di 1 perchè non raggiungiamo mai lo 0), ma per il principio della discesa infinita questa non può esistere.

Quindi, ora basterà dimostrare che non esiste una configurazione di stanze collegate, con almeno una stanza cattiva, in cui non possiamo togliere una stanza cattiva.

Passo 3 Sia s_1 una stanza cattiva. Se è l'unica, basta premere un interruttore e due lampadine cambieranno di stato, e s_1 sarà buona, ma noi abbiamo supposto che sia impossibile far decrescere il numero di lampadine.

Quindi s_1 ha una lampadina che condivide l'interruttore con la lampadina di una stanza s_2 . Premendo questo interruttore, s_1 diventa buona, quindi s_2 diventa cattiva. Continuiamo con questo algoritmo: dalla n -esima stanza, che è appena diventata cattiva (mentre da 1 a $n - 1$ sono buone), scegliamo un'altra stanza con cui condivide un interruttore e premiamo questo interruttore. Così, l'ultima stanza deve diventare cattiva e tutte le precedenti restano buone.

Prima o poi troveremo un interruttore che collega a una stanza già visitata, altrimenti visiteremo un numero infinito di stanze, il che non è possibile. Premendo questo interruttore, entrambe le stanze che collega diventeranno buone. Infatti, una stanza è cattiva, quindi cambiando di stato una lampadina diventa buona. L'altra stanza è buona, ma è già stata visitata: ha almeno tre lampadine, di cui una e una sola lampadina ha uno stato (diciamo accesa) e le altre sono spente. Ma noi siamo arrivati a questa stanza da un'altra via (o non sarebbe la prima stanza in cui ritorniamo ...), quindi cambiando questo interruttore abbiamo due e solo due lampadine accese. Assurdo, perchè abbiamo supposto che in questo stato non sia possibile far scendere il numero di lampadine cattive.

□

Problema 17 *Ad una gara matematica partecipano 10 studenti. Ogni studente riceve 4 problemi da risolvere. Comunque si scelgano 2 studenti, questi hanno al più un problema in comune.*

Determinare il minimo numero di problemi necessario.

Passo 1: dimostriamo che è necessario che il numero di problemi sia maggiore o uguale a 13.

Supponiamo che bastino n ($n \leq 12$) problemi. Se nessun problema è assegnato a più di 3 studenti, allora il numero di soluzioni (per soluzione intendiamo una coppia (*studente, problema*)) sarebbe minore o uguale a $3n \leq 36$. Ma le soluzioni sono esattamente $10 \cdot 4 = 40$, quindi ciò non è possibile. Quindi esiste un problema risolto da 4 studenti.

Siano A, B, C, D questi quattro studenti. A risolve 4 problemi. B ne deve risolvere almeno 3 diversi da quelli di A (infatti ne ha già 1 in comune con A). C ne deve risolvere almeno 3 diversi da quelli di A e di B (infatti ne ha già 1 in comune con A e con B). Allo stesso modo D deve risolvere almeno 3 problemi diversi da quelli di A, B, C messi insieme. Sommando, abbiamo 13 problemi. Assurdo.

Passo 2: sono sufficienti 13 problemi. Siano $A, B, C, D, E, F, G, H, I, L$ i 10 studenti. Numeriamo i 13 problemi da 1 a 13. La seguente tabella da una distribuzione dei problemi che rispetta le condizioni.

A	B	C	D	E	F	G	H	I	L
1	4	7	1	4	7	1	4	7	1
2	5	8	8	2	5	5	8	2	4
3	6	9	6	9	3	9	3	6	7
12	12	12	11	11	11	13	13	13	10