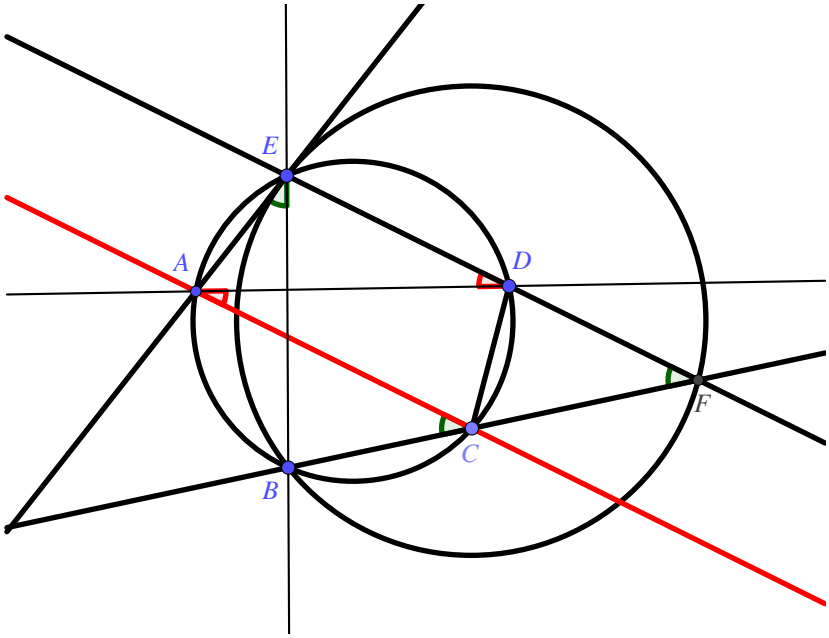
XXXVI Olimpiade Italiana di Matematica

Sedi distrettuali, 25 settembre 2020

1. Su una circonferenza consideriamo nell'ordine cinque punti A, B, C, D, E. Supponiamo che le rette BC e DE si intersechino in un punto F, che F e A siano da parti opposte rispetto alla retta BE, e che la circonferenza circoscritta al triangolo BFE sia tangente (in E) alla retta AE.

   (a) Dimostrare che le rette AC e DE sono parallele.

   (b) Dimostrare che $AE = CD$.



Soluzione

(a) Tracciamo la retta EB. L'angolo $\widehat{AEB}$ nella circonferenza $ABCDE$ sottende l'arco AB ed è quindi uguale all'angolo $\widehat{ACB}$; d'altra parte, lo stesso angolo $\widehat{AEB}$ nella circonferenza circoscritta al triangolo BFE è compreso tra la corda BE e la tangente alla circonferenza nel punto E, quindi è uguale all'angolo $\widehat{EFB}$ che sottende la stessa corda nella stessa circonferenza. Di conseguenza la retta BF forma con le due trasversali AC ed EF angoli corrispondenti uguali, il che implica che le due rette AC ed EF (che è anche DE) sono parallele.

(b) Poiché AC e DE sono parallele, gli angoli $\widehat{CAD}$ e $\widehat{EDA}$, alterni interni formati con la trasversale AD, sono uguali. Ma allora anche le corde che essi sottendono sono uguali, per cui $AE = CD$.

2. Determinare tutte le coppie (a, b) di numeri interi positivi che verificano le seguenti tre condizioni:

   - $b > a$ e $b - a$ è un numero primo,
   - la cifra delle unità di $a + b$ è 3,
   - ab è il quadrato di un numero intero.

Soluzione 1 Sia $a = dx$ e $b = dy$ con $(x, y) = 1$. Allora $p = b - a = d(y - x)$. Ci sono due casi:

(a) $d = p$, ma allora $y - x = 1$ e dunque $ab = p^2x(x + 1)$. Ma allora $x(x + 1) = z^2$, che è assurdo perché $x > 0$.

(b) $d = 1$. Dato che ab è un quadrato e $(a, b) = 1$, allora $a = u^2$ e $b = v^2$. Da qui possiamo concludere in più modi:

a) La cifra delle unità di un quadrato può essere $1, 4, 5, 6, 9$: abbiamo che $u^2 + v^2$ ha cifra delle unità uguale a 3, quindi le cifre delle unità di u^2 e v^2 sono 9 e 4. Quindi $b - a$ ha cifra delle unità uguale a 5, cioè è un multiplo di 5. Allora $p = 5 = u^2 - v^2 = (u - v)(u + v)$, quindi $a = u^2 = 4$, $b = v^2 = 9$.

b) Vale $(v - u)(v + u) = p$, quindi $v - u = 1$, $v + u = p$. Abbiamo quindi $v = \frac{p+1}{2}$ e $u = \frac{p-1}{2}$, cioè $a = \left(\frac{p-1}{2}\right)^2$ e $b = \left(\frac{p+1}{2}\right)^2$.
Osserviamo che $a + b = 2^{-1}(p^2 + 1) \equiv 3 \pmod 5$, quindi $p^2 \equiv 0 \pmod 5$ e quindi $p = 5$. Da qui $a = 4, b = 9$ che soddisfa.

c) $u^2 + v^2 \equiv 3 \pmod 5$, ovvero $u^2 \equiv v^2 \equiv 4 \pmod 5$. Allora:

$$p = b - a = 2v^2 - 3 \equiv 0 \pmod 5$$

cioè $p = 5$, quindi $u = 2$, $v = 3$.

Soluzione 2 Sia $b = a + p$. Allora $a(a + p) = k^2 > 0$. Ma allora calcolando il delta del polinomio $a^2 + ap - k^2 = 0$ si ottiene $p^2 + 4k^2 = \Delta^2$ e dunque

$$p^2 = (\Delta - 2k)(\Delta + 2k).$$

Essendo $k > 0$, si ha che $\Delta = \frac{p^2+1}{2}$. Ma allora

$$a = \frac{-p + \Delta}{2} = \left(\frac{p - 1}{2}\right)^2 \text{ e } b = a + p = \left(\frac{p + 1}{2}\right)^2.$$

A questo punto possiamo concludere come in 1b).

3. Siano $a_1, a_2, \ldots, a_{2020}$ e $b_1, b_2, \ldots, b_{2020}$ dei numeri reali, non necessariamente distinti. Supponiamo che gli interi positivi n per cui l'equazione

$$\left|a_1|x-b_1| + a_2|x-b_2| + \cdots + a_{2020}|x-b_{2020}|\right| = n \tag{1}$$

ha *esattamente due* soluzioni reali siano in numero finito.

Dimostrare che gli interi positivi n per cui l'equazione (1) ha *almeno una* soluzione reale sono in numero finito.

Soluzione Definiamo

$$f(x) = \left|\sum_{i=1}^{2020} a_i|x-b_i|\right|,$$

e

$$A = \sum_{i=1}^{2020} a_i, \qquad B = \sum_{i=1}^{2020} a_i b_i.$$

Osservazione 1 Se x è un reale abbastanza grande (almeno $b_+ = \max\{b_i \ : \ 1 \le i \le 2020\}$), tutte le espressioni $x - b_i$ sono positive, dunque

$$f(x) = |Ax - B|.$$

Osservazione 1' Se x è un reale abbastanza piccolo (al più $b_- = \min\{b_i \ : \ 1 \le i \le 2020\}$), tutte le espressioni $x - b_i$ sono negative, dunque si ha similmente

$$f(x) = |-Ax + B| = |Ax - B|.$$

Osservazione 2 Fissato qualunque reale $M > 0$, abbiamo che $f(x)$ è limitata per $|x| < M$, cioè esiste una costante U tale che $f(x) \le U$ per ogni $|x| < M$; infatti, applicando la disuguaglianza triangolare:

$$f(x) = \left|\sum_{i=1}^{2020} a_i|x-b_i|\right| \le \sum_{i=1}^{2020} |a_i||x-b_i| \le \sum_{i=1}^{2020} |a_i||x| + |a_i||b_i| \le \sum_{i=1}^{2020} |a_i|M + |a_i||b_i|.$$

(Poiché f è una funzione continua, la stessa conclusione segue dal teorema di Weierstrass applicato a f, una volta ristretta al dominio $[-M, M]$.)

Studiamo ora l'equazione $f(x) = n$, distinguendo due casi in funzione della valore di A.

Caso $A = 0$ In questo caso notiamo che non esistono soluzioni se $n > \max\{|B|, U\}$.

Infatti, un'ipotetica soluzione reale x non può soddisfare $x \ge b_+$ oppure $x \le b_-$, perché in questi casi abbiamo già mostrato che $f(x) = |B| < n$. Ma non può nemmeno soddisfare $b_- \le x \le b_+$ perché abbiamo mostrato che $f(x) \le U < n$ (scegliendo M abbastanza grande in modo che $M > b_+$ e $M > -b_-$).

In particolare esiste solo un numero finito di n interi tali che $f(x) = n$ ammette soluzione.

Caso $A \neq 0$ In questo caso mostriamo che, se $n > \max\{f(b_+), f(b_-), U\}$, allora esistono esattamente due soluzioni, una maggiore di b_+ e una minore di b_-.

Anche in questo caso non esistono soluzioni con $b_- \le x \le b_+$, perché, come prima, si avrebbe $f(x) \le U < n$. Allora l'equazione diventa semplicemente

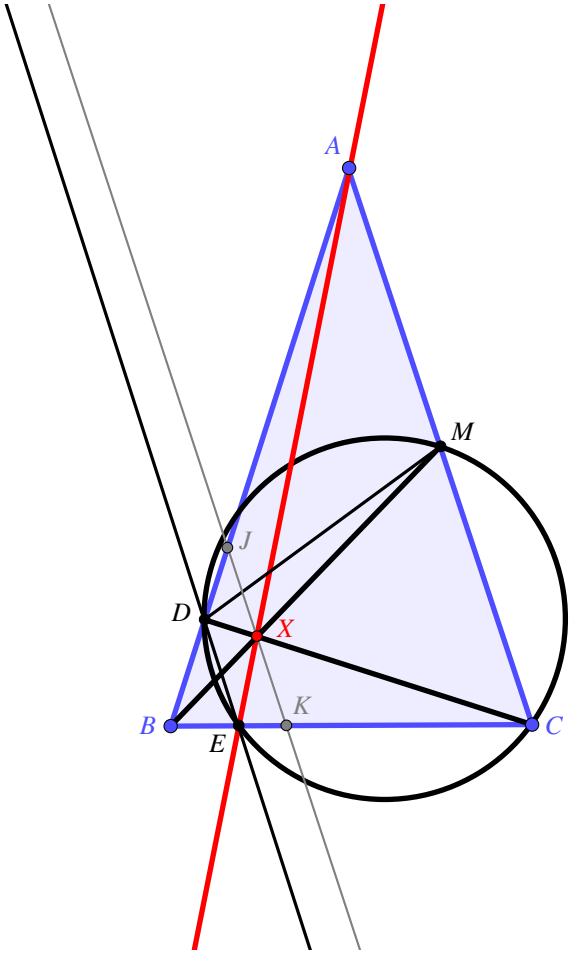
$$n = f(x) = |Ax - B|$$

che ammette come soluzioni $x = \frac{B \pm n}{A}$. Osserviamo che sono entrambe accettabili (cioè appartengono all'insieme $\{x : x < b_-\} \cup \{x : x > b_+\}$). Se $A > 0$, $\frac{B+n}{A} > b_+$ è equivalente a $n > Ab_+ - B$, quindi è garantita da $n > |Ab_+ - B| = f(b_+)$; similmente l'altra soluzione sfrutta $n > f(b_-)$. Il caso $A < 0$ è del tutto analogo.

In particolare, questo caso contraddice l'ipotesi.

4. Sia ABC un triangolo acutangolo con $AB = AC$. Sia D il piede dell'altezza uscente da C, sia M il punto medio di AC, e sia E la seconda intersezione tra il lato BC e la circonferenza circoscritta al triangolo CDM.

   Dimostrare che le rette AE, BM e CD passano per uno stesso punto se e solo se $CE = CM$.



Soluzione 1 Sia X l'intersezione tra BM e CD. Dimostreremo che entrambe le condizioni sono equivalenti al parallelismo di DE e AC.

(a) Dimostriamo che $CM = CE$ se e solo se DE è parallelo a AC. Infatti, l'angolo $\widehat{CDA}$ è retto per ipotesi, quindi D appartiene alla semicirconferenza di centro M e raggio CM, da cui $DM = CM$; ma allora, considerando la circonferenza $CMDE$, $CM = CE$ se e solo se l'angolo $\widehat{MCD}$ e l'angolo $\widehat{EDC}$, sottendendo corde uguali, sono uguali, e quindi se e solo se il segmento ED è parallelo ai segmenti CM e CA perché le loro due rette formano angoli alterni interni uguali con la trasversale CD.

(b) Dimostriamo che A, X, E sono allineati se e solo se DE è parallelo a AC. Infatti, per il teorema di Ceva l'allineamento è equivalente all'uguaglianza $AD \cdot BE \cdot CM = DB \cdot EC \cdot MA$, cioè (poiché $CM = MA$) $AD : DB = EC : BE$, che per il teorema di Talete è equivalente al parallelismo di DE e AC.

(dimostrazione alternativa di questa parte senza usare il teorema di Ceva) Tracciamo la parallela da AC passante per X e chiamiamo rispettivamente J e K le intersezioni di questa rette con AB e BC. Per il teorema di Talete il parallelismo è equivalente a $JX : AM = XK = MC$ (da cui $JX = XK$), al fatto che il triangolo JDX sia simile al triangolo ADC (da cui $DX : XC = JX : AC$) e a $EK : KC = DX : XC$. Inoltre $JX : AC = XK : AC$ (poiché $JX = XK$), cioè $EK : KC = XK : AC$, il che è equivalente a dire che A, X, E sono allineati sempre per il teorema di Talete (esiste un unico punto nel segmento JK per cui vale la proporzione, ed è quello di intersezione tra la retta AE e JK).

Vale la pena di osservare che ambedue le condizioni del testo implicano che il punto E sia interno al segmento BC, perciò nei precedenti calcoli di angoli non si verificano problemi di configurazione.

Altre strade per la prima parte erano anche dimostrare che il quadrilatero $CMDE$ è un trapezio (isoscele), oppure dimostrare che l'angolo $\widehat{BAC}$ è forzato ad avere un'ampiezza di 36°.

Soluzione 2 Denotiamo con Γ la circonferenza circoscritta a CMD, indichiamo con F la seconda intersezione di Γ con AB e indichiamo con 2θ l'angolo $\widehat{BAC}$. A meno di omotetie possiamo supporre $AB = AC = 2$: in questo caso

$$CD = 2\sin(2\theta), \quad AD = 2\cos(2\theta), \quad BC = 4\sin(\theta)$$

e considerando la potenza di A rispetto a Γ

$$AF = \frac{AM \cdot AC}{AD} = \frac{1}{\cos(2\theta)}, \quad BF = 2 - \frac{1}{\cos(2\theta)}.$$

Vale inoltre $BD = BA - AD = 2(1 - \cos(2\theta)) = 4\sin^2(\theta)$ e per la potenza di B rispetto a Γ

$$BE = BF \cdot \frac{BD}{BC} = BF\sin(\theta) = 2\sin(\theta) - \frac{\sin(\theta)}{\cos(2\theta)}.$$

Per differenza tra BC e BE abbiamo

$$EC = 2\sin(\theta) + \frac{\sin(\theta)}{\cos(2\theta)}.$$

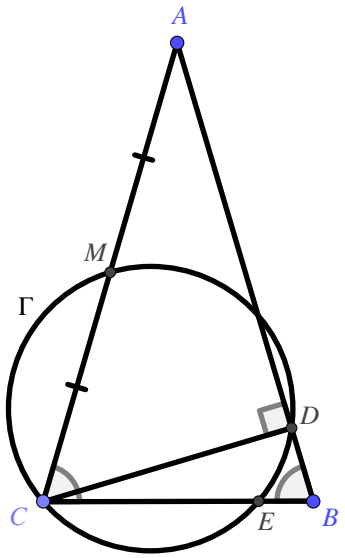
Per il Teorema di Ceva, la concorrenza delle rette AE, BM, CD è equivalente alla condizione $BD \cdot EC = BE \cdot AD$, poiché $AM = MC$. Per quanto esplicitato in precedenza, l'identità $BD \cdot EC = BE \cdot AD$ è a sua volta equivalente a

$$2\cos(2\theta) - 1 = 4\sin^2(\theta) + \frac{2\sin^2(\theta)}{\cos(2\theta)}.$$

Facendo ricorso alle formule di duplicazione abbiamo che vi è concorrenza se e solo se $x = \sin\theta$ soddisfa

$$2(1 - 2x^2) - 1 = 4x^2 + \frac{2x^2}{1 - 2x^2},$$

e dalla fattorizzazione del polinomio di quarto grado risultante si ha $4x^2 = 1 \pm 2x$. L'unica soluzione geometricamente accettabile è $x = \frac{\sqrt{5}-1}{4}$, per cui si ha $EC = 1$. Viceversa, $EC = 1$ comporta che $x = \frac{\sqrt{5}-1}{4}$. Incidentalmente questo rivela anche che si ha concorrenza sono nel caso in cui l'angolo $\widehat{BAC}$ ha un'ampiezza di 36 gradi.



Soluzione 3 Ponendo l'origine in C e, senza perdita di generalità, B sull'asse x con coordinate $B = (4, 0)$, sia M di coordinate $M = (1, a)$, dove $a \geq 2$ dato che il triangolo è acutangolo ed isoscele. Di conseguenza, $A = (2, 2a)$. La retta AB ha equazione

$$\frac{4 - x}{2} = \frac{-y}{-2a} \implies 4a - ax = y.$$

Ponendo $D = (x_D, y_D)$ ed imponendo stia su AB, e scrivendo Pitagora per CDB, abbiamo

$$\begin{cases} 4a - ax_D = y_D \\ CD^2 + DB^2 = CB^2 \end{cases} \implies \begin{cases} a(4 - x_D) = y_D \\ x_D^2 + y_D^2 + (4 - x_D)^2 + y_D^2 = 16 \end{cases}$$

$$\implies \begin{cases} a(4 - x_D) = y_D \\ x_D^2(1 + a^2) - 4x_D(1 + 2a^2) + 16a^2 = 0 \end{cases} \implies \begin{cases} y_D = \frac{4a}{1+a^2} \\ x_D = \frac{4a^2}{1+a^2} \end{cases}$$

quindi abbiamo $D = \frac{4a}{1+a^2}(a, 1)$. Γ è una circonferenza passante per l'origine, dunque la sua equazione è del tipo

$$(x - p)^2 + (y - q)^2 = p^2 + q^2.$$

Imponendo il passaggio per M e D, abbiamo

$$\begin{cases} 1 + a^2 = 2(p + aq) \\ \frac{16a^2(1+a^2)}{(1+a^2)^2} = 8a\frac{ap+q}{1+a^2} \end{cases} \implies \begin{cases} p = \frac{3a^2-1}{2(a^2-1)} \\ q = \frac{a}{2}\frac{3-a^2}{1-a^2} \end{cases}$$

Intersecando Γ con BC, troviamo che $(x_E - p)^2 = p^2 \implies x_E = 2p$, cosicchè $E = (2p, 0)$. Siamo quindi pronti ad analizzare le tesi. Abbiamo che

$$CE = CM \iff x_E^2 = 1 + a^2 \iff (1 - 3a^2)^2 = (1 + a^2)(1 - a^2)^2 \iff a^4 - 10a^2 + 5 = 0$$

dove l'ultima equazione ha una sola soluzione positiva e reale. Dall'altro lato, abbiamo che la concorrenza di AE, CD, BM è equivalente per il teorema di Ceva a

$$CE \cdot BD \cdot AM = EB \cdot FA \cdot MC.$$

Dato che $AM = MC$, abbiamo che

$$CE \cdot BD = EB \cdot FA \iff \frac{3a^2 - 1}{a^2 - 1}\sqrt{\left(4 - \frac{4a^2}{1 + a^2}\right)^2 + \left(\frac{4a}{1 + a^2}\right)^2} = \left(4 - \frac{3a^2 - 1}{a^2 - 1}\right)\sqrt{\left(2 - \frac{4a^2}{1 + a^2}\right)^2 + \left(2a - \frac{4a}{1 + a^2}\right)^2}$$
$$\iff (a^2 - 1)(a^2 - 3) = 2(3a^2 - 1) \iff a^4 - 10a^2 + 5 = 0.$$

5. Sia S l'insieme degli interi maggiori o uguali a 2. Una funzione $f : S \to S$ si dice *primordiale* se verifica le seguenti proprietà:

   - è surgettiva (cioè per ogni $s \in S$ esiste almeno un $n \in S$ tale che $f(n) = s$),
   - è crescente sui primi (cioè se $p_1 < p_2$ sono numeri primi, allora $f(p_1) < f(p_2)$),
   - per ogni $n \in S$, il valore di $f(n)$ è il prodotto di $f(p)$ al variare di p tra tutti i primi che dividono n (quindi, per esempio, $f(360) = f(2^3 \cdot 3^2 \cdot 5) = f(2) \cdot f(3) \cdot f(5)$).

   Determinare il massimo ed il minimo valore possibile per $f(2020)$, al variare di f tra tutte le funzioni primordiali.

   Soluzione 1 Siano $p_1 = 2, p_2 = 3, \ldots$ i numeri primi ordinati in modo crescente.

   Minimo Il minimo valore di $f(2020)$ è 216.

   - *Lower bound* Sia f una generica funzione primordiale. Data la stretta monotonia sui primi vale $f(p_{i+1}) \geq f(p_i) + 1$. Per induzione si mostra che $f(p_n) \geq n + 1$, essendo $f(2) \geq 2$.
     Ma allora $f(2020) = f(2) \cdot f(5) \cdot f(101) \geq 2 \cdot 4 \cdot 27 = 216$ essendo 101 il 26-esimo numero primo.
   - *Costruzione* Definiamo $f_*(p_i) = i+1$ e $f_*(n) = \prod_{p|n} f_*(p)$ dove il prodotto è sui primi distinti. Questa funzione soddisfa banalmente le condizioni 2 e 3. Inoltre per ogni $s \in S$ vale $s = f_*(p_{s-1})$, dunque f_* è suriettiva e perciò primordiale.
     D'altra parte $f_*(2020) = f_*(2) \cdot f_*(5) \cdot f_*(101) = 2 \cdot 4 \cdot 27 = 216$.

   Massimo Il massimo valore di $f(2020)$ è 584.

   - *Upper bound* Sia f una funzione primordiale, $\mathbb{P}$ l'insieme dei numeri primi e $Q = f(\mathbb{P})$.

     Osservazione 1: I numeri primi stanno in Q.
     Infatti, sia q primo; per suriettività dovrà essere $q = f(n)$ per qualche $n \in S$. Dato che $f(n) = \prod_{p|n} f(p)$ sui primi distinti, per fattorizzazione unica dovrà valere $q = f(p)$ (e p era l'unico fattore primo di n).

     Osservazione 2: I quadrati dei numeri primi stanno in Q.
     Sia q un primo; per suriettività vale $q^2 = f(n) = \prod_{p|n} f(p)$. Per unicità della fattorizzazione dovrà valere $f(p) = q^2$, oppure $f(p_1) = f(p_2) = q$ con $p_1 \neq p_2$; quest'ultima è tuttavia impossibile per la condizione di monotonia.

     Osservazione 3: Per ogni primo q vale una tra $q^3 \in Q$ e $q^4 \in Q$. Per suriettività infatti vale $q^4 = f(n) = \prod_{p|n} f(p)$. Questo ci lascia le seguenti possibilità:
     - $f(p_1) = f(p_2) = f(p_3) = f(p_4) = q$
     - $f(p_1) = f(p_2) = q, f(p_3) = q^2$
     - $f(p_1) = q, f(p_2) = q^3$
     - $f(p_1) = q^4$

     Dato che le prime due sono impossibili per la monotonia, resta una delle ultime due.

     Consideriamo ora $U = \{2, 3, 4, 5, 7, 9, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41, 43, 47, 49, 53, 59, 61, 67, 71, 73\}$. Per le prime due osservazioni vale $U \subset Q$, e per la terza vale una tra $U \cup \{8\} \subset Q$ e $U \cup \{16\} \subset Q$.
     Poiché f è crescente, e dato che $f(p_i)$ è l'i-esimo elemento di Q, si ha che $f(p_i)$ è minore o uguale dell'i-esimo elemento di $U \cup \{8/16\}$. In entrambi i casi il 26-esimo elemento dell'unione è 73, dunque $f(101) \leq 73$.
     Inoltre $f(2) \leq 2$ e $f(5) \leq 4$, perciò $f(2020) \leq 2 \cdot 4 \cdot 73 = 584$.
   - *Costruzione* Sia $U = \{2, 3, 4, 5, 7, 9, 11, 13, 16, 17, 19, 23, 25, 29, 31, 37, 41, 43, 47, 49, 53, 59, 61, 67, 71, 73\}$ l'insieme che conosciamo con il 16, con elementi ordinati $u_1, \ldots, u_{26}$.
     Definiamo $f^*(p_i) = u_i$ per $i \leq 26$ e $f^*(p_j) = j - 26 + 73$ per $j > 26$; sia poi $f^*(n) = \prod_{p|n} f^*(p)$.
     Questa f^* soddisfa le condizioni 2 e 3. Inoltre è ovviamente suriettiva per $s \geq 74$.
     D'altra parte con gli elementi di U posso costruire ogni intero ≤ 73, dato che posso scrivere $2, 4, 8, 16, 32, 64$ come prodotti di u_j, e ci sono tutti i primi e i quadrati dei primi ≤ 73. Perciò f^* è suriettiva e quindi primordiale.

Soluzione 2 Facciamo una dimostrazione diversa solo per quanto riguarda il **massimo** di $f(2020)$. Costruiamo una funzione f^* con il seguente algoritmo ricorsivo, di tipo *greedy* (o algoritmo del mangione):

- $f^*(2) = 2$
- $f^*(p_{i+1})$ è il minimo elemento di S che non si riesce ad esprimere come prodotto di alcuni tra $f^*(p_1), \dots, f^*(p_i)$ (ciascuno preso al più una volta).

Analizziamo le proprietà della funzione così definita.

- *Upper bound* Vogliamo dimostrare che se f è primordiale, allora $f(p_i) \leq f^*(p_i)$ per ogni i.
  Supponiamo per assurdo che non sia così e sia i il primo indice per cui $f(p_i) > f^*(p_i)$. Per suriettività vale $f^*(p_i) = f(n)$ per qualche intero $n \in S$.
  Se n avesse un fattore p_j con $j \geq i$, allora varrebbe $f(n) \geq f(p_j) \geq f(p_i) > f^*(p_i)$ che è assurdo. Dunque n ha solo fattori primi $< p_i$, cioè $f(n) = f(p_{a_1}) \cdots f(p_{a_k})$ con $a_i < i$.
  Ma questo è assurdo, perché vorrebbe dire che $f^*(p_i) = f(n)$ si potrebbe scrivere come prodotto di $f(p_{a_j})$, che contrasta la definizione.
  A questo punto è sufficiente svolgere l'algoritmo fino a calcolare $f^*(p_{26}) = 73$ per ottenere che $f(101) \leq 73$, ovvero $f(2020) \leq 584$.
- *Costruzione* Basta mostrare che f^* (estesa opportunamente a tutto S) è crescente e suriettiva.
  Se per assurdo valesse $f^*(p_{i+1}) \leq f^*(p_i)$, starei contraddicendo la minimalità di $f^*(p_i)$; oppure ponendo $f^*(p_{i+1}) = f^*(p_i)$, chiaramente impossibile perché $f^*(p_{i+1})$ per definizione non deve essere esprimibile.
  Sia ora $s \in S$; data la monotonia stretta, trovo che esiste un i per cui $s < f^*(p_i)$. Ma allora posso esprimere s come prodotto di alcuni tra $f^*(p_1), \dots, f^*(p_{i-1})$, cioè f^* è suriettiva.
  Infine, $f^*(2020) = 2 \cdot 4 \cdot 73 = 584$.

Soluzione 3 Facciamo una terza dimostrazione per il **massimo** di $f(2020)$. Sia a_i la successione ordinata dei p^{2^k} con $k \geq 0$ e p primo.

- *Upper bound* Premettiamo un paio di lemmi generali

  Lemma 1: Siano x_i, y_j successioni ordinate, ognuna composta di elementi distinti; supponiamo che esista una permutazione $\sigma : \mathbb{N} \to \mathbb{N}$ tale che $x_i \leq y_{\sigma(i)}$. Allora $x_i \leq y_i$ per ogni i.
  Sia per assurdo $x_k > y_k$ il primo indice per cui la tesi fallisce; osserviamo che allora $y_0, \dots, y_{k-1}, y_k$ possono essere maggioranti solo di $x_0, \dots, x_{k-1}$, ovvero che se $0 \leq i \leq k$, allora $\sigma^{-1}(i) \in \{0, 1, \dots, k-1\}$. Questo però contraddice l'iniettività di σ^{-1}, dunque abbiamo un assurdo.

  Lemma 2: Sia $c_0, c_1, \dots$ una successione ordinata che genera additivamente $\mathbb{N}^+$ (cioè ogni $n > 0$ è somma di alcuni c_i distinti). Allora vale $c_i \leq 2^i$.
  Si dimostra per induzione; $c_0 = 1$, perché è il minimo. Supponiamo sia vero fino ad i e per assurdo $c_{i+1} > 2^{i+1}$; allora 2^{i+1} si deve poter scrivere come somma di alcuni tra $c_0, \dots, c_i$; tuttavia $\sum c_j \leq \sum 2^j = 2^{i+1} - 1$, quindi non riesco a generare 2^{i+1}, assurdo.

  Data una f primordiale, poniamo $f(p_i) = b_i$; poiché f è surgettiva per ipotesi, allora la successione b_i genera moltiplicativamente S, ovvero ogni $m \in S$ si scrive come $m = \prod_{j \in J} b_j$ per un opprtuno insieme di indici J. Inoltre b_i è strettamente crescente.

  Mostriamo ora che se b_i è una qualunque successione che genera moltiplicativamente S, allora vale $b_i \leq a_i$.

  Infatti, per ogni primo p, la successione b_i dovrà contenere p^{c_i} dove $c_0, c_1, \dots$ genera additivamente $\mathbb{N}$; ma allora per il lemma 2 si ha $c_i \leq 2^i$.

  Considerato l'insieme $X = \bigcup_{p \in \mathbb{P}} \{p^{c_j}\}_{j \in \mathbb{N}}$ e i suoi elementi ordinati x_i, grazie al lemma 1 si ha che $x_i \leq a_i$. Concludiamo osservando che $\{b_i\} \supset X$ e dunque $b_i \leq x_i$.

  Pertanto vale sempre $f(p_i) \leq a_i$.
- *Costruzione* Sia $f^*(p_i) = a_i$ e $f(n) = \prod_{p|n} f^*(p)$. Questa soddisfa ovviamente le condizioni 2 e 3.

  D'altra parte è facile verificare che la successione dei p^{2^k} genera davvero tutto S, poiché basta saper generare tutti i p^j e questi si ottengono scrivendo j in base 2.

6. In ogni casella di una tabella 8×8 abita un cavaliere o un furfante. Come da tradizione, i cavalieri dicono sempre la verità, mentre i furfanti mentono sempre. Tutti gli abitanti della tabella affermano che "il numero dei furfanti nella mia colonna è maggiore (strettamente) del numero dei furfanti nella mia riga".

   Determinare quante sono le possibili configurazioni compatibili con questa affermazione.

Soluzione Chiamiamo $r(i)$ e $c(j)$ il numero di furfanti nella riga i e nella colonna j, rispettivamente. Il testo equivale a dire che l'abitante della casella (i, j) è un cavaliere se $c(j) > r(i)$, un furfante altrimenti.

1. Il primo passo, fondamentale, è dimostrare che tutti i numeri $c(j)$ sono uguali fra loro. Procediamo per assurdo: supponiamo che non sia vero e, senza perdita di generalità, che sia $c(j_2) > c(j_1)$ per due certi indici di colonna j_1, j_2. Allora, se una casella (i, j_1) della colonna j_1 è abitata da un cavaliere, abbiamo $c(j_1) > r(i)$, quindi, a fortiori, $c(j_2) > r(i)$; e di conseguenza la casella (i, j_2) della colonna j_2 è anch'essa abitata da un cavaliere. Quindi nella colonna j_2 ci sono almeno tanti cavalieri quanti nella colonna j_1, contraddicendo l'ipotesi $c(j_2) > c(j_1)$, cioè che nella colonna j_2 ci siano invece più furfanti che nella colonna j_1. Perciò tutti i $c(j)$ devono essere uguali.

2. Dimostriamo ora che la tabella è, per così dire, "a strisce": infatti, ovviamente, per tutte le caselle di una fissata riga i il numero $r(i)$ è costante, quindi se l'abitante della casella (i, j) è cavaliere o furfante dipende solo da $c(j)$: però abbiamo appena dimostrato che questi numeri sono tutti uguali, quindi ogni data riga è costituita o da soli cavalieri, o da soli furfanti.

3. Verifichiamo allora quali tra le tabelle "a strisce" sono compatibili con le ipotesi del problema. Si vede facilmente che in realtà lo sono tutte, salvo quella in cui ci sono solo cavalieri: infatti

   - se è presente almeno una riga di furfanti, ogni furfante ha 8 furfanti nella propria riga, e un numero necessariamente ≤ 8 di furfanti nella propria colonna (e quindi quello che dice è falso); viceversa, ogni cavaliere ha 0 furfanti nella propria riga e un numero > 0 di furfanti nella propria colonna (e quindi dice la verità)
   - se invece non ci fosse alcuna riga di furfanti, e quindi gli abitanti fossero tutti cavalieri, tutti avrebbero 0 furfanti sia sulla propria riga, sia sulla propria colonna, e quindi mentirebbero, il che è impossibile.

   Ci sono quindi $2^8 - 1 = 255$ configurazioni compatibili con le condizioni date.