PROMYS 2025 - PROBLEMI DI SELEZIONE

RAVASIO LUCA

20 marzo 2025

Indice

Preambolo

Nel problema 3 e nel problema 8, talvolta uso la notazione (a, b) e $[a, b]$ per indicare il massimo comun divisore e il minimo comune multiplo, analogamente a quanto fatto in [1] e [2]. Tuttavia talvolta nell'esercizio 8 uso la notazione (x, y) per indicare un punto in $\mathbb{R}^2$.

Nel problema 1 per indicare una super-casella talvolta uso $\{a, b, c, d\}$, dove a, b, c e d sono le caselle di cui essa è composta. Inoltre, sempre nel problema 1, talvolta uso $\{x \in [a : b], y \in [c : d]\}$ per indicare un rettangolo nel piano $\mathbb{N}^2$ di cui due lati sono collineari a $x = a$ e $x = b$ e gli altri due a $y = c$ e $y = d$.

Problema 1

Soluzione: 386.

Per risolvere questo problema, la prima cosa che ho fatto è stata generare a mano molti casi piccoli. Ecco di seguito una sottogriglia 16x16 della griglia del problema - da qui in poi chiamata *Griglia Magica* -

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
14	15	12	13	10	11	8	9	6	7	4	5	2	3	0	1
13	12	15	14	9	8	11	10	5	4	7	6	1	0	3	2
12	13	14	15	8	9	10	11	4	5	6	7	0	1	2	3
11	10	9	8	15	14	13	12	3	2	1	0	7	6	5	4
10	11	8	9	14	15	12	13	2	3	0	1	6	7	4	5
9	8	11	10	13	12	15	14	1	0	3	2	5	4	7	6
8	9	10	11	12	13	14	15	0	1	2	3	4	5	6	7
7	6	5	4	3	2	1	0	15	14	13	12	11	10	9	8
6	7	4	5	2	3	0	1	14	15	12	13	10	11	8	9

```
5 4 7 6 1 0 3 2 13 12 15 14 9 8 11 10
4 5 6 7 0 1 2 3 12 13 14 15 8 9 10 11
3 2 1 0 7 6 5 4 11 10 9 8 15 14 13 12
2 3 0 1 6 7 4 5 10 11 8 9 14 15 12 13
1 0 3 2 5 4 7 6 9 8 11 10 13 12 15 14
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
```

La prima cosa che ho notato è stata che nella riga 1 ci sono gli elementi della riga 0 invertiti di posizione presi a blocchi di 2: (0 1 → 1 0), (2 3 → 3 2), ... Nella riga 2 invece ci sono gli elementi della riga 1 invertiti di posizione presi a blocchi di 4: (1 0 3 2 → 2 3 0 1), (5 4 7 6 → 6 7 4 5), ... Nella riga 3 invece ci sono gli elementi della riga 2 invertiti di posizione presi di nuovo a blocchi di 2, come nel blocco colorato di verde. In generale, la dimensione dei blocchi di cui vengono invertite le posizioni degli elementi nel passare dall' iesima riga alla i+1esima è (partendo da i=0): 2, 4, 2, 8, 2, 4, 2, 16, 2, 4, 2, 8, 2, 4, 2, 32, ... Questa lista da qui in poi sarà chiamata *Lista Magica*. Vedendo una sequenza del genere non ho potuto fare a meno di pensare alla funzione che genera la dimensione dei blocchi del Fenwick Tree. Infatti più in generale notai che la dimensione dei blocchi era $g(i) = 2(i \ \& -i)$ (Esattamente la funzione del Fenwick Tree con indexing one-based moltiplicata per due, & rappresenta il bitwise and). Già questo basterebbe a scrivere uno script per risolvere il problema. Se infatti si generano i primi 2^k elementi della prima riga (0, 1, 2, 3, 4, 5, ...) e si invertono i blocchi della dimensione data dalla funzione $g(i)$ generando riga per riga, è possibile generare tutte le righe della sotto-griglia fino alla $2^k - 1$esima. Basta infatti fare attenzione a generare la sotto-griglia di dimensioni $2^k \times 2^k$ per non aver nessun problema con i numeri al di fuori di questa sotto-grigia(le dimensioni di tutti i blocchi che vengono invertiti dividono 2^k, non c'è interazione con i numeri al di fuori della sotto-griglia). Con il seguente script sono in grado di generare una qualsiasi sotto-griglia di dimensione $n = 2^k$ in un tempo $O(n^2)$, calcolabile quindi dalla maggior parte dei computer in un tempo molto modesto data la piccola dimensione dell'input $(1607, 1989 < 2048)$. Tuttavia questo approccio è decisamente impraticabile con carta e penna.

```cpp
// ALGORITMO 1
#include <bits/stdc++.h>
#define ll long long
using namespace std;

int main(){
  ll N;
  cin >> N;
  ios_base::sync_with_stdio(false);
  cin.tie(NULL);

  vector<vector<ll>> V(N, vector<ll>(N));

  for(int j=0; j<N; j++){
    V[0][j] = j;
  }

  for(int i=1; i<N; i++){
    ll k = 2*(i& (-i));
    for(int j=0; j<N; j++){
      V[i][j] = V[i-1][j - j%k + k - (j%k)-1];
    }
  }

  for(int i=N-1; i>= 0; i--){
    for(int j=0; j<N; j++){
      cout << V[i][j] << "\t\t";
    }
    cout << "\n";
  }

}
```

E' quindi necessario trovare un'altra soluzione più semplice da calcolare. Ho generato una sottogriglia della Griglia Magica di moderate dimensioni e l'ho studiata con matlab. A questo punto ho scoperto un paio di cose sorprendenti. La prima cosa che ho notato (anche se di scarsa utilità) è che il plot 3d della sottogriglia genera un frattale simile al tetraedro di Sierpiński. La seconda, che invece ho notato osservando la heatmap della sottogriglia, è che c'è un bel po' di simmetria. Nello specifico tutti i quadrati di coordinate:

$$\{x \in [2^a : 2^a+2^k-1], y \in [2^b : 2^b+2^k-1]\} \iff \{x \in [2^a+2^k : 2^a+2^{k+1}-1], y \in [2^b+2^k : 2^b+2^{k+1}-1]\} \quad (1.1)$$

$$\{x \in [2^a : 2^a+2^k-1], y \in [2^b+2^k : 2^b+2^{k+1}-1]\} \iff \{x \in [2^a+2^k : 2^a+2^{k+1}-1], y \in [2^b : 2^b+2^k-1]\} \quad (1.2)$$

Con $a, b > k$ sono quadrati identici. Ciò è coerente con l'osservazione precedente relativa alla Lista Magica e la funzione g(i).

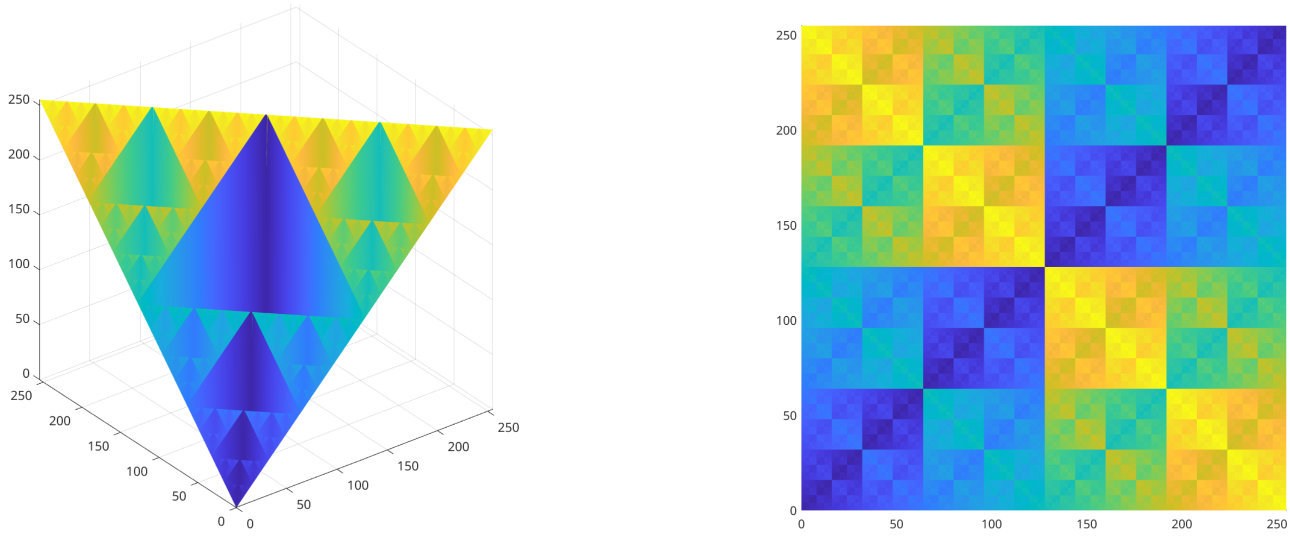


Figura 1.1: Un plot 3d della sottogriglia della Griglia magica e una sua heatmap

Questo ci basta a creare un algoritmo molto più veloce che ci permette di calcolare una singola cella della Griglia Magica in $O(\log \max(i, j))$ dove i, j sono le coordinate in righe-colonne della cella in considerazione:

```
% ALGORITMO 2
function calcola(i, j)
    size = 2048;
    while(j ~= 0)
        if (mod(i, size) >= size/2 && mod(j, size) >= size/2)
            i = i - size/2;
            j = j - size/2;
        elseif (mod(j, size) >= size/2)
            i = i + size/2;
            j = j - size/2;
        end
        size = size /2;
    end

    disp(i);
end
```

Poichè $\log_2(2048) = 11$ e $1989, 1607 < 2048$ possiamo calcolare il valore di quella cella effettuando esattamente 11 divisioni con resto e 22 somme/sottrazioni, qualcosa di decisamente fattibile a mano. In effetti dopo un po' si ottiene come soluzione 386.

Ora dobbiamo dimostrare le proprietà fino ad ora usate.

Teorema 1.1 (Teorema della riga 0)**.** *Nella Griglia Magica, il numero contenuto nella casella (0, n), in cui le coordinate rappresentano la riga e la colonna, è n*

Dimostrazione. La tesi segue immediatamente per n = 0. Per tutti gli altri numeri segue per induzione: se sappiamo che in (0,0) si trova 0, in (0, 1) si trova 1, ... (0, n) si trova n, allora il numero più piccolo che possiamo mettere in (0, n+1) è n+1. ∎

Teorema 1.2 (Teorema della riga 1)**.** *Nella Griglia Magica, il numero contenuto nella casella (1, 2n) è 2n+1, quello contenuto nella casella (1, 2n+1) è 2n.*

Dimostrazione. La tesi segue immediatamente per n = 0: in (1, 0) non possiamo mettere 0 perchè si trova nella casella sottostante, quindi mettiamo 1, mentre in (1, 1) possiamo mettere 0 perchè sia nella casella a sinistra che in quella sottostante c'è un 1. Per tutti gli altri valori di n segue per induzione. Infatti supponiamo che l'ipotesi induttiva valga per tutti i numeri da 0 a n. Segue che tutti i numeri da 0 a 2n+1 sono già stati inseriti nella riga 1. (Vistochè è vera per 0 allora sono stati inseriti 1, 0; vistochè è vera per 1 sono stati inseriti 3, 2; ...; vistochè è vera per n sono stati inseriti 2n+1, 2n). Perciò nella casella 2n+2 possiamo inserire tutti i numeri superiori a 2n+1 (gli altri sono già presenti a sinistra). Tuttavia, a causa del Teorema della riga 0 non possiamo inserire 2n+2, poichè si trova nella casella sottostante (0, 2n+2). Perciò il valore minimo è 2n+3. Anche nella casella 2n+3 non possiamo mettere tutti i numeri inferiori o uguali a 2n+1 (si trovano a sinistra), ma poichè il numero sottostante è 2n+3 allora possiamo inserire 2n+2. □

Lemma 1.3 (Lemma della Super-casella)**.** *Nella Griglia Magica, è possibile accorpare tutti gli elementi di coordinate (0, 2n), (0, 2n+1), (1, 2n), (1, 2n+1) in un'unica Super-casella contenente contemporaneamente 2n e 2n+1 senza influenzare il resto della Griglia Magica.*

Dimostrazione. Il lemma segue dalla definizione della Griglia magica. Infatti se, per il Teorema della riga 0 e il Teorema della riga 1 so che nelle caselle (0, 2n) e (1, 2n+1) ho 2n allora nessun 2n potrà d'ora in avanti comparire nelle colonne 2n e 2n+1 o nelle righe 0 e 1. Lo stesso discorso vale per (0, 2n+1) e (1, 2n) e 2n+1. Ciò implica che possiamo "accorpare" le quattro caselle immaginandoci di scriverci dentro sia uno 2n che un 2n+1. □

Lemma 1.4 (Lemma della Super-riga 0)**.** *Tutte le Super-caselle {(0, 2n), (0, 2n+1), (1, 2n), (1, 2n+1)}* $\forall n \in \mathbb{N}$ *vanno a formare una Super-riga ordinata.*

Dimostrazione. Per il Lemma della Super-casella ogni Super-casella {(0, 2n), (0, 2n+1), (1, 2n), (1, 2n+1)} contiene sia 2n che 2n+1. Si dica che una Super-casella contenente (a, b) è più piccola di una contenente (c, d) se e solo se $\max(a, b) < \min(c, d)$. Dal Lemma della Super-casella segue che l'ordine con cui si trovano le Super-caselle che si trovano sulle righe 0 e 1 è coerente con un ordinamento così definito. Infatti una Super-casella si trova prima di un'altra se e solo se $n_1 < n_2$, poichè le rispettive caselle si troveranno a $\{(0, 2n_1), (0, 2n_1 + 1), (1, 2n_1), (1, 2n_1 + 1)\}$ e $\{(0, 2n_2), (0, 2n_2 + 1), (1, 2n_2), (1, 2n_2 + 1)\}$. Inoltre una super-casella è più piccola di un'altra se e solo se $\max(2n_1, 2n_1 + 1) < \min(2n_2, 2n_2 + 1) \iff 2n_1 + 1 < 2n_2$ e vistochè $n_1, n_2 \in \mathbb{N}$ è equivalente a dire $n_1 < n_2$. Perciò una Super-casella sulle righe 0,1 si trova prima di un'altra se e solo se è più piccola. Da ciò segue che tutte le Super-caselle delle righe 0, 1 vanno a formare una Super-riga ordinata. □

Teorema 1.5 (Teorema della Super-riga 1)**.** *Tutte le Super-caselle* $\{(2, 4n), (2, 4n + 1), (3, 4n), (3, 4n + 1)\} = \{(0, 4n + 2), (0, 4n + 3), (1, 4n + 2), (1, 4n + 3)\} \forall n \in \mathbb{N}$ *e* $\{(2, 4n + 2), (2, 4n + 3), (3, 4n + 2), (3, 4n + 3)\} = \{(0, 4n), (0, 4n + 1), (1, 4n), (1, 4n + 1)\} \forall n \in \mathbb{N}$. *In altre parole, esiste una versione adattata alle super-caselle del Teorema della riga 1*

3	2	1	0	7	6	5	4	11	10	9	8	15	14	13	12
2	3	0	1	6	7	4	5	10	11	8	9	14	15	12	13
1	0	3	2	5	4	7	6	9	8	11	10	13	12	15	14
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Dimostrazione. Dimostreremo la tesi per induzione. Come caso base possiamo verificare manualmente che la tesi vale per i casi base colorati in verde e blu nella sottogriglia soprastante. Ora dimostriamo che se sono state messe nelle righe 2, 3 le prime n Super-caselle (ossia quelle contenenti i numeri (0,1), (2,3), ... (2n, 2n+1)) allora seguiranno in quest'ordine la n+2esima e la n+1esima. Per l'ipotesi induttiva e il Lemma della Super-casella i numeri fino a 2n+1 sono già stati messi nelle Super-caselle a sinistra. Tuttavia non è possibile usare nemmeno i numeri 2n+2 e 2n+3 nelle colonne 2n+2 e 2n+3 perchè per il Teorema della riga 0 e il Teorema della riga 1 essi sono già presenti in entrambe le colonne. Questo ci obbliga ad inserire i numeri 2n+4 e 2n+5. Nello specifico metteremo nella riga 2 a sinistra 2n+4 e a destra 2n+5; nella riga 3 a sinistra 2n+5 e a destra 2n+4, formando così una nuova super-casella. Nelle colonne 2n+4, 2n+5 invece possiamo inserire i numeri 2n+2 e 2n+3, poichè questi non sono presenti nè nelle caselle a sinistra ne nelle caselle sottostanti. Nello specifico metteremmo nella riga 2 2n+2 e 2n+3, per minimizzare il valore delle caselle, mentre nella riga 3 2n+3, 2n+2 a causa degli elementi nella riga 2. Il teorema è dunque dimostrato. □

Ora, è chiaro che possiamo formare Super-caselle di Super-caselle(infatti anche le Super-caselle sono un insieme numerabile e ordinato con un elemento minimo, quello colorato in blu nella sottogriglia soprastante, perciò si comportano come i numeri naturali). In questo modo posso ricostruire le righe 4, 5, 6, 7. Se poi creo Super-caselle di Super-caselle di Super-caselle posso arrivare fino alla riga 15. In questo modo posso procedere indefinitivamente per ottenere la struttura di tutta la griglia.

Definiamo ora una casella della Griglia Magica come una Super-casella di grado 0. Definiamo ora una Super-casella costituita di caselle della griglia magica come di grado 1. Definiamo una Super-casella di Super-caselle di caselle come di grado 2 e così via.

Definiamo ora la cardinalità di una casella della Griglia Magica come 1. La cardinalità di una Super-casella sarà invece 4 moltiplicato per la cardinalità degli elementi di cui è composta. Da ciò consegue che la cardinalità di una Super-casella è pari al numero di caselle che contiene. Si può facilmente dimostrare induttivamente che la cardinalità di una casella è pari 4 elevato al suo grado. Poichè tutte le Super-caselle hanno forma quadrata consegue che la lunghezza del loro lato è la radice quadrata della cardinalità, ossia 2 elevato al loro grado.

Usando questo fatto e il Teorema della riga 0, il Teorema della riga 1, il Lemma della Super-riga 0, il Teorema della Super-riga 1 (e tutti i teoremi simili relativi alle Super-caselle di Super-caselle di ...) possiamo dimostrare le equazioni (1.1) e (1.2). Tuttavia, per dimostrare la correttezza dell'algoritmo 2 e che converge ci basta dimostrarne un'implicazione più semplice. In particolare, basta dimostrare che se $a_{i,j}$ è la casella contenuta nella riga i e nella colonna j:

$$a_{i,j} = a_{i-2^k,j-2^k} \Longleftarrow \left((i \mod 2^{k+1}) \geq 2^k \wedge (j \mod 2^{k+1}) \geq 2^k\right)$$

$$a_{i,j} = a_{i-2^k,j+2^k} \Longleftarrow \left((i \mod 2^{k+1}) \geq 2^k \wedge (j \mod 2^{k+1}) < 2^k\right)$$

Dimostrazione. Sia C la Super-casella appartenente alla Super-riga 0 di grado k+1 contenente $a_{i,j}$. Per il *Lemma della Super-riga 0* e il *Teorema della Super-riga 1* C è formata da 4 Super-caselle di grado k. Ora, sempre per quei due teoremi, la super-casella di grado k che contiene $a_{i,j}$ è uguale alla super-casella di grado k appartenente a C in diagonale rispetto ad essa, da qui, considerando che il lato di ogni Super-casella è 2^k, seguono le 2 identità.

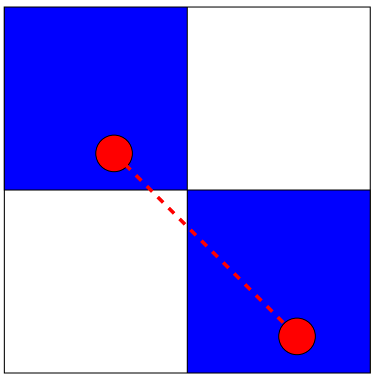


Figura 1.2: Se i due quadrati in blu sono uguali, anche i due punti in rosso sono uguali.

□

Dimostriamo ora che l'algoritmo converge.

Dimostrazione. Sia K il grado della più piccola Super-casella appartenente alla Super-riga 0 di grado K contenente (1989, 1607). Ora, se applichiamo queste due uguaglianze per ogni k da K+1 a 0, siamo sicuri di ottenere l'eguaglianza $a_{i,j} = a_{0,j'}$. Infatti in ogni step viene mantenuta la proprietà $i < 2^{k-1}$(presente all'inizio per la definizione di K): se nel passare da k+1 a k questa proprietà venisse meno, allora sapremmo che $2^{k-1} \leq i < 2^k$, ma in questo caso l'algoritmo avrebbe sottratto ad i 2^{k-1} applicando una delle due uguaglianze, otteniamo dunque un assurdo. Perciò dopo l'ultimo passaggio otteniamo sicuramente $a_{i,j} = a_{0,j'}$. Ora, per il *Teorema della riga 0*, $a_{0,j'} = j'$ questo dimostra la convergenza dell'algoritmo. □

NB. *Sarebbe stato possibile fare una terza implementazione in $O(n)$ che sfrutta la funzione $g(i)$. Tuttavia sarebbe stato necessario dimostrare la $g(i)$ e la complessità computazionale è peggiore rispetto all'algoritmo 2 che è in $O(\log n)$*

NB. *Forse è possibile trovare una soluzione alternativa che faccia uso del tetraedro di Sierpiński e di qualche altra formula geometrica, ma una soluzione è sufficiente. Infatti anche se non ho ricavato una formula chiusa ho comunque trovato un algoritmo il cui risultato è altrettanto facile da calcolare. Supponiamo infatti che esista una soluzione alternativa che fornisce una formula chiusa. Molto probabilmente questa soluzione non sarà polinomiale ma conterrà un'esponenziale. Perciò, anche usando l'algoritmo di esponenziazione veloce, la complessità computazionale rimane $O(\log n)$.*

Problema 2

Chiamiamo step un salto della lepre seguito da un salto della pulce. Possiamo numerare gli step da 1 ad infinito. Vistochè salta prima la lepre e poi la pulce, se la pulce raggiungesse mai la lepre, ciò dovrebbe avvenire alla fine di uno step, perchè il salto della lepre sicuramente aumenta la distanza tra la lepre e la pulce. Definiamo come $f(x)$ la distanza della pulce dal palo dopo x step. Definiamo invece come $g(x)$ la distanza della lepre dal palo dopo x step. Chiaramente se $\frac{f(x)}{g(x)} \geq 1$ ha soluzioni reali positive la pulce raggiunge la lepre.

Dopo il primo step $f(1) = 1\,cm$ mentre $g(1) = 1\,km$. Cerchiamo di capire cosa avviene al secondo. Prima di tutto salta la lepre di 1 km, per cui $g(2) = g(1) + 1\,km$. Tuttavia ciò fa dilatare di un fattore $2\times$ l'elastico. In seguito la pulce fa un salto di 1 cm. Per cui $f(2) = 2f(1) + 1\,cm$. In generale potremmo dire che $g(x) = x\ km$, mentre

$$f(1) = 1cm$$
$$f(x) = f(x-1)\frac{x}{x-1} + 1\,cm$$

Tuttavia questo è molto difficile da calcolare.

Potremmo invece considerare la frazione dell'elastico che la pulce "guadagna" dopo ogni step. Infatti dopo il primo step guadagna $\frac{1\,cm}{1\,km}$. Dopo il secondo step la pulce ha fatto ancora un salto di 1 cm, ma l'elastico è raddoppiato di lunghezza, pertanto "guadagna" $\frac{1\,cm}{2\,km}$. Dopo il terzo $\frac{1\,cm}{3\,km}$ e così via. Pertanto dobbiamo scoprire se la seguente serie diverge, o per lo meno se converge ad un valore superiore ad 1. Noi tuttavia cercheremo di dimostrare che la serie diverge.

$$\frac{1\,cm}{1\,km} + \frac{1\,cm}{2\,km} + \frac{1\,cm}{3\,km} + \frac{1\,cm}{4\,km} + \frac{1\,cm}{5\,km} + \frac{1\,cm}{6\,km} + ...$$

Cominciamo a togliere un fattore 10^{-5} dall'espressione, tanto i fattori non trasformano una serie divergente in una convergente o vice-versa. Otteniamo:

$$\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + ...$$

Che è nota come serie armonica. Ho già visto una dimostrazione della divergenza di questa serie nel 2024 in uno stage di selezione alle olimpiadi internazionali di informatica.

Si elimina $\frac{1}{1}$: un addendo finito non può influenzare la convergenza o divergenza di una serie. Si ottiene:

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \frac{1}{9} + \frac{1}{10} + \frac{1}{11} + \frac{1}{12} + \frac{1}{13} + \frac{1}{14} + \frac{1}{15} + \frac{1}{16} + ... \tag{2.1}$$

Ora, si divide la somma in blocchi di lunghezza 1, 2, 4, 8,... seguendo le potenze di due. Dimostriamo ora che il blocco numero i non può contenere nessun addendo più piccolo di $\frac{1}{2^i}$. Per far ciò dimostriamo che l'ultimo addendo non è più piccolo di $\frac{1}{2^i}$: visto che la serie (2.1) ha addendi in ordine strettamente decrescente, se un elemento qualunque della serie è più piccolo di $\frac{1}{2^i}$ lo è anche l'ultimo elemento della serie. Per capire in che posizione della serie si trovi l'ultimo elemento di un certo blocco sommiamo la dimensione di tutti i blocchi prima di quel blocco e la dimensione del blocco stesso. Per come è stata definita la dimensione dei blocchi, si ottiene $1 + 2 + 4 + 8 + .. + 2^i = 2^{i+1} - 1$ per un'identità nota. In questa serie tutti gli addendi sono esattamente $\frac{1}{p+1}$ dove p è la posizione dell'addendo cominciando a contare da 1. Perciò, visto che conosciamo la posizione dell'ultimo addendo di un certo blocco, possiamo ottenerne il valore: $\frac{1}{2^i-1+1} = \frac{1}{2^i} \geq \frac{1}{2^i}$. Perciò è dimostrato che nell'iesimo blocco non c'è nessun addendo più piccolo di $\frac{1}{2^i}$. Possiamo perciò impostare la disequazione:

$$\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8}+\frac{1}{9}+\frac{1}{10}+\frac{1}{11}+\frac{1}{12}+\frac{1}{13}+\frac{1}{14}+\frac{1}{15}+\frac{1}{16}+\dots \tag{2.2}$$

$$\geq \frac{1}{2}+\frac{1}{4}+\frac{1}{4}+\frac{1}{8}+\frac{1}{8}+\frac{1}{8}+\frac{1}{8}+\frac{1}{16}+\frac{1}{16}+\frac{1}{16}+\frac{1}{16}+\frac{1}{16}+\frac{1}{16}+\frac{1}{16}+\frac{1}{16}+\dots \tag{2.3}$$

Dove abbiamo sfruttato il fatto che ogni addendo di ogni blocco numero i è più grande di $\frac{1}{2^i}$. Ora, ogni blocco numero i della seconda sequenza contiene 2^{i-1} elementi tutti uguali tra loro di valore $\frac{1}{2^i}$. Perciò il valore di tutti gli addendi di ogni blocco sommati tra loro è $2^{i-1} \cdot \frac{1}{2^i} = \frac{1}{2}$. Poiché la serie contiene infiniti blocchi diverge. Inoltre, poiché la serie 2.3 è minore della serie 2.1 segue che anche la serie 2.1 diverge. Poiché diverge, siamo sicuri che la pulce prima o poi raggiungerà la lepre. Ciò avverrà in un tempo molto lungo(la somma dei primi n termini della serie 2.3 è proporzionale ad un logaritmo) ma finito.

Problema 3

Queste sono le regole secondo le quali viene definito S:

(i) $\frac{1}{1} \in S$

(ii) $\frac{a}{b} \in S \implies \frac{b}{2a} \in S \qquad$ se $(a,b) = 1$

(iii) $\frac{a}{b} \in S \wedge \frac{c}{d} \in S \implies \frac{a+c}{b+d} \in S \qquad$ se $(a,b) = 1e(c,d) = 1$

La mia prima idea per risolvere questo problema era stata di vedere quali numeri riuscivo a generare usando solo la prima e la seconda regola. Tuttavia, mi sono subito accorto che la regola (ii) è involutoria.

Lemma 3.1. *La regola (ii) è involutoria.*

Dimostrazione. Secondo (ii) $\frac{a}{b} \in S \implies \frac{b}{2a} \in S$, ma anche $\frac{b}{2a} \in S \implies \frac{2a}{2b} = \frac{a}{b} \in S$ □

NB. *Il lemma 3.1 implica che tutti i numeri appartenenti ad S si dividono in coppie e che ogni numero appartiene ad una e una sola coppia. Inizialmente pensavo che avrei costruito la mia dimostrazione su questo.*

Perciò usando solo le prime due regole si può ottenere soltanto $\frac{1}{1}$ e $\frac{1}{2}$. Appare dunque ovvio che per procedere bisogna applicare la (iii) ad $\frac{1}{1}$ e $\frac{1}{2}$, ottenendo dunque $\frac{2}{3}$. A questo punto possiamo più in generale dimostrare la seguente proposizione:

Teorema 3.2. $\frac{n}{n+1} \in S \quad \forall n \in \mathbb{N}_+$

Dimostrazione. La tesi è stata già provata per i casi base per $n = 1$ e $n = 2$. Per tutti gli altri valori può essere provata per induzione. Supponiamo di aver già dimostrato la tesi per tutti i naturali positivi fino ad n e dimostriamola per $n+1$. Basta applicare la (iii) a $\frac{n}{n+1}$ e $\frac{1}{1}$ per ottenere $\frac{n+1}{n+2} \in S$ □

Da ciò segue il anche:

Teorema 3.3. $\frac{n}{n+2} \in S \quad \forall n \in \mathbb{N} \mid n \geq 2$

Dimostrazione. La tesi segue dal fatto che $\frac{n-1}{n} \in S$ per il teorema 3.2. Applicando la (iii) con $\frac{1}{2}$ e$\frac{n-1}{n}$ si ottiene $\frac{n}{n+2}$ □

Da cui, per esempio, $\frac{3}{5} \in S$.

Considerando che si possono fare versioni del teorema 3.3 utilizzando $\frac{3}{5}$ al posto di $\frac{1}{2}$ viene il sospetto che S sia molto denso tra $\frac{1}{2}$ e $\frac{1}{1}$. Inoltre si può anche dimostrare che tutti gli elementi di S sono compresi tra $\frac{1}{2}$ e $\frac{1}{1}$.

Teorema 3.4. $s \in S \implies \frac{1}{2} \leq s \leq \frac{1}{2}$

Dimostrazione. Per dimostrare la tesi, mostreremo come prima di tutto la (ii) non generi nessun numero esterno all'intervallo $\left[\frac{1}{2}; \frac{1}{1}\right]$ partendo da numeri interni all'intervallo $\left[\frac{1}{2}; \frac{1}{1}\right]$ e poi come la (iii) faccia altrettanto. Siccome $\frac{1}{1}$, il nostro numero "generatore", è interno all'intervallo, allora la rispetteranno anche tutti gli altri elementi di S.

1. $\frac{1}{2} \leq \frac{b}{2a} \leq 1 \iff a \leq b \leq 2a$ poichè $a \neq 0$. $a \leq b \iff \frac{a}{b} \leq 1$, mentre $b \leq 2a \iff \frac{1}{2} \leq \frac{a}{b}$ poichè $b \neq 0$. Ciò implica che la regola (ii) non "crea" numeri fuori dall'intervallo $\left[\frac{1}{2}; \frac{1}{1}\right]$
2. $\frac{1}{2} \leq \frac{a+c}{b+d} \leq 1 \iff \frac{1}{2}(b+d) \leq a+c \leq b+d$. L'ultima catena di diseguaglianze è vera perchè $\frac{a}{b}, \frac{c}{d} \in \left[\frac{1}{2}; \frac{1}{1}\right]$ implica che $\frac{1}{2}b \leq a$, $\frac{1}{2}d \leq c$ e anche che $a \leq b$, $c \leq d$, come mostrato nella prima parte. Perciò anche la regola (iii) non "crea" numeri fuori dall'intervallo.

Ciò dimostra la tesi. □

Viene ora da chiedersi se S coincida con $\left[\frac{1}{2}; \frac{1}{1}\right]$ in $\mathbb{Q}$ o se ne sia solo un sottoinsieme. Cominciamo a dimostrare il seguente lemma:

Lemma 3.5. *Siano $a, b \in \mathbb{N}_+$ tali che $\frac{1}{2} \leq \frac{a-1}{b-2} \leq 1$, $(a-1, b-2)$[1] $= 1$, $a < b$.* $\frac{a-1}{b-2} \in S \implies \frac{a}{b} \in S$

Dimostrazione. La dimostrazione segue banalmente dall'applicazione della regola (iii) ad $\frac{a-1}{b-2}$ e $\frac{1}{2}$ □

Questo lemma è molto utile, perché afferma che se $\frac{a}{b} \notin S \implies \frac{a-1}{b-2} \notin S$. Ciò potrebbe potenzialmente creare una catena di implicazioni che potrebbe essere utile in una dimostrazione per assurdo. Tuttavia sarebbe bello avere una tesi più forte. Ecco dunque i tre seguenti teoremi. Per chiarezza d'esposizione dimostrerò prima i teoremi e poi mostrerò come sono arrivato alla soluzione.

Teorema 3.6. $(2n+1, n+1) = 1 \quad \forall n \in \mathbb{N}$

Dimostrazione. L'MCD divide qualsiasi combinazione lineare. $d \mid 2(n+1) - (2n+1) = 1$ Perciò l'MCD è 1. □

Teorema 3.7. *Siano $a, b \in \mathbb{N}_+$ tali che $\frac{1}{2} \leq \frac{a}{b} \leq 1$, $(a, b) = 1$, $a < b$. Siamo sicuri che $\frac{b-a}{2b-2a-1}$ è ridotta ai minimi termini. Inoltre $\frac{b-a}{2b-2a-1} \in S \implies \frac{a}{b} \in S$*

Dimostrazione. Che $\frac{b-a}{2b-2a-1}$ sia ridotta ai minimi termini segue dal fatto che:

$$\frac{b-a}{2b-2a-1} = \frac{(b-a-1)+1}{2(b-a-1)+1} = \frac{n+1}{2n+1}$$

che è ridotta ai minimi termini per il teorema 3.6.

Consideriamo ora la frazione $\frac{2a-b}{2a-b+1}$. Essa appartiene ad S per il teorema 3.2. Inoltre è ridotta ai minimi termini perchè due numeri consecutivi sono sempre coprimi. Se $\frac{b-a}{2b-2a-1}$ appartiene ad S, allora possiamo applicare la (iii) tra le 2 frazioni.

$$\frac{(2a-b)+(b-a)}{(2a-b+1)+(2b-2a-1)} = \frac{a}{b}$$

da cui la tesi.

□

Possiamo dimostrare quindi il seguente teorema:

Teorema 3.8. $\frac{a}{b} \in \mathbb{Q}, \quad \frac{1}{2} \leq \frac{a}{b} \leq 1 = 1 \implies \frac{a}{b} \in S$

Dimostrazione. Useremo una dimostrazione per assurdo. Supponiamo che un numero $\frac{a}{b}$ come quello descritto nella tesi non sia membro di S. Se $\frac{a}{b}$ non fosse ridotto ai minimi termini possiamo ridurlo ai minimi termini e ottenere un numero uguale. Perciò possiamo supporre che $(a, b) = 1$. Per il teorema 3.7 $\frac{b-a}{2b-2a-1} \in S \implies \frac{a}{b} \in S$. Perciò $\frac{b-a}{2b-2a-1} \notin S$. Tuttavia possiamo continuare ad applicare il teorema 3.7 a $\frac{b-a}{2b-2a-1}$ ottenendo che $\frac{b-a-1}{2b-2a-3}$ non appartiene ad S. In questo modo possiamo creare una lunga serie di implicazioni. Siamo sicuri che la serie di implicazioni non è infinita perché la differenza tra denominatore e numeratore, inizialmente positiva per le ipotesi del teorema, diminuisce di 1 ad ogni passaggio: $b-a > 2b-2a-1-(b-a) = b-a-1$ (potremmo fissare la differenza tra numeratore e denominatore come monovariante e dimostrare che è strettamente decrescente). Perciò prima o poi otterremo che la differenza tra denominatore e numeratore è zero, ma a quel punto significa che siamo arrivati a dire che $\frac{1}{1} \notin S$, un assurdo. Non ci dobbiamo preoccupare del rischio di ottenere prima o poi una frazione che non sia ridotta ai minimi termini perchè il teorema 3.7 garantisce che lo è. La tesi è dunque dimostrata. □

[1] con (a, b) intendo il massimo comune divisore di a e b

Perciò S include tutti e soli i numeri razionali tra $\frac{1}{2}$ e 1 estremi inclusi.

Come sono arrivato a questa soluzione. Il teorema 3.7 potrebbe sembrare un po' frutto di una proprietà fortuitamente notata. Non è così. Infatti inizialmente volevo applicare il lemma 3.5 per ottenere un teorema 3.8 più semplice, tuttavia mi sono scontrato contro il fatto che (iii) necessita di frazioni ridotte ai minimi termini. Infatti non sempre se $(a, b) = 1$ anche $(a - 1, b - 2) = 1$. Perciò mi sono concentrato sul cercare di ottenere a partire da una frazione $\frac{a}{b}$ ridotta ai minimi termini un'altra sempre ridotta ai minimi termini. Mi sono accorto che se $\frac{a-1}{b-2}$ non era ridotta ai minimi termini solitamente $\frac{a-2}{b-3}$ lo era o per lo meno lo era $\frac{a-3}{b-4}$. In generale, c'era sempre un k tale che $\frac{a-k}{b-k-1}$ è una frazione ridotta ai minimi termini. Il che è grandioso vistochè avevo già dimostrato il teorema 3.2, che garantisce che $\frac{k}{k+1} \in S\ \forall k \in \mathbb{N}_+$ (anche se quando l'avevo dimostrato ero convinto che sarebbe stato inutile, come il teorema 3.3 e il lemma 3.1) - posso infatti applicare (iii) a $\frac{a-k}{a-k-1}$ e $\frac{k}{k+1}$. A quel punto dovevo solo assicurarmi che $\frac{a-k}{a-k-1}$ fosse irriducibile. A questo ho sfruttato il fatto noto che $\frac{n+1}{2n+1}$ è irriducibile e ho impostato il seguente sistema:

$$\begin{cases} a - k = n + 1 \\ b - k - 1 = 2n + 1 \end{cases}$$

Da cui si ricava:

$$\begin{cases} k = 2a - b \\ n = b - a - 1 \end{cases}$$

Da cui ho impostato il teorema 3.7

NB. *Forse è possibile usare questa definizione di S come prova che esiste una funzione biunivoca tra i naturali e i razionali, dimostrando che* $|\mathbb{Q}| = \aleph_0$

Problema 4

Questo è un triviale problema di combinatoria. E' ragionevole supporre che le 10 persone siamo distinguibili tra loro, siccome non sono gemelli, così come i 3 comitati, siccome probabilmente fanno cose diverse. Infatti se prendo Pippo dal Comitato Per La Sicurezza Sul Lavoro e lo metto nel Comitato Per La Sostenibilità e prendo Gigi dal Comitato Per La Sostenibilità e lo sposto nel Comitato Per La Sicurezza Sul Lavoro ottengo una combinazione diversa. Per risolvere il problema basta applicare il principio di inclusione-esclusione. Cominciamo infatti ignorando la condizione che non ci sia nessun comitato con 0 membri. Ognuno ha sette scelte: essere nel comitato A, nel comitato B, nel comitato C, A e B, B e C, A e C oppure nessun comitato. Perciò otteniamo 7^{10} possibilità (ho fatto qui l'assunzione che fosse anche possibile non fare parte di nessun comitato). Abbiamo però così contato anche tutte le configurazioni in cui qualche comitato non ha nessun membro. Sottraiamo dunque tutte le configurazioni in cui c'è almeno un comitato senza nessun membro. Possiamo scegliere in 3 modi quale comitato lasciare senza membri. Le 10 persone avranno quindi 4 scelte: far parte di un comitato, far parte dell'altro, far parte di entrambi o non far parte di nessun comitato. Perciò ci sono $3 \cdot 4^{10}$ configurazioni. Tuttavia in questo modo abbiamo sottratto due volte il numero di configurazioni in cui ci sono almeno due comitati senza membri, ri-aggiungiamole. Possiamo scegliere in tre modi i comitati da "vietare". Ogni persona potrà scegliere quindi se far parte del comitato rimanente o di nessun comitato. Ci sono perciò $3 \cdot 2^{10}$ possibilità. Dobbiamo ora solamente escludere il caso in cui nessuno fa parte di nessun comitato. Si ottiene perciò:

$$7^{10} - 3 \cdot 4^{10} + 3 \cdot 2^{10} - 1 = 279332592$$

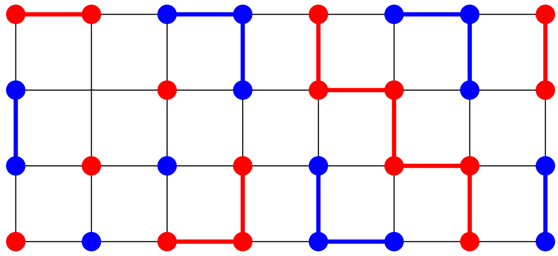
Se invece non fosse possibile scegliere di non far parte di nessun comitato, il calcolo rimane simile.

$$6^{10} - 3^{11} + 3 = 60289032$$

Possiamo essere abbastanza sicuri che i entrambi risultati siano giusti poichè sono divisibili per 6. Infatti, se inizialmente avessimo diviso le 10 persone in 3 gruppi senza assegnare ciascun gruppo ad un comitato, poi avremmo avuto $3! = 6$ modi per assegnare ogni gruppo ad un comitato.

Problema 5

Creando a mano alcune griglie 2×4 ci si rende immediatamente conto che il numero di archi blu e rossi è lo stesso. L'ipotesi sembra essere confermata dalla seguente griglia 4×8.



Ipotesi (Ipotesi della griglia)**.** *In una qualsiasi griglia $2m \times 2n$ i cui vertici sono colorati di rosso o blu in modo che la quantità di vertici rossi e blu in ogni riga e in ogni colonna sia la stessa, la quantità di archi che connettono tra loro due vertici rossi adiacenti (orizzontalmente o verticalmente) è uguale alla quantità di archi che connettono tra loro vertici blu (orizzontalmente o verticalmente).*[2]

Nello specifico, è triviale dimostrare che l' Ipotesi della griglia è vera nel caso in cui $m = 1$, come dimostrato di seguito.

Teorema 5.1. *L'Ipotesi della griglia è vera per $m = 1$;*

Dimostrazione. In ogni colonna se un punto è rosso l'altro è blu. Perciò ci sono due tipi di colonne. Si consideri ogni colonna della griglia, partendo dalla seconda a sinistra e procedendo man mano verso destra. Se una certa colonna è dello stesso tipo della colonna precedente, allora si forma un arco rosso e uno blu. Altrimenti non si forma nessun arco. La tesi è dunque dimostrata. □

Ora, osservando questa dimostrazione, ho trovato un modo per generalizzarla usando il principio dei cassetti.

Teorema 5.2. *In una qualsiasi griglia $2m \times 2n$, i cui vertici sono colorati di rosso o blu in modo che la quantità di vertici rossi e blu in ogni riga e in ogni colonna sia la stessa, la quantità di archi orizzontali che connettono tra loro due vertici rossi adiacenti è uguale alla quantità di archi orizzontali che connettono tra loro vertici blu adiacenti.*

Dimostrazione. Partiamo considerando la prima riga della seconda colonna.

Supponiamo che il vertice della prima riga della seconda colonna sia diverso da quello della prima riga della prima colonna. Senza perdita di generalità (se non fosse così basterebbe scambiare i nomi) supponiamo che quello della prima riga della prima colonna sia rosso, mentre quello della prima riga della seconda colonna sia blu. Nel resto della prima colonna ci sono perciò m-1 vertici rossi (dove m è il numero di righe), mentre nel resto della seconda colonna ci sono m vertici rossi. Perciò ci sarà almeno un vertice rosso costretto a stare di fianco ad un vertice blu. Ora, cancellando momentaneamente tutti e quattro i vertici (i due vertici rosso e blu della prima riga e i due vertici blu e rosso appena trovati) la differenza tra il numero di archi rossi orizzontali e archi blu orizzontali tra le due colonne non cambia. Di più: viene mantenuta la proprietà delle due colonne di avere lo stesso numero di vertici rossi e blu.

Supponiamo ora invece che il vertice della prima riga della prima sia uguale al vertice della prima riga della prima colonna. Senza perdita di generalità affermiamo che sono entrambi rossi. Nel resto della prima riga rimarrebbero m-1 vertici rossi, mentre nella seconda rimarrebbero m vertici blu. E' perciò necessario che almeno un vertice blu della seconda colonna sia di fianco ad un vertice blu della prima colonna. Cancellando i quattro vertici fin qui trovati (i due vertici rossi della prima riga e i due vertici blu appena trovati) la differenza tra il numero di archi rossi orizzontali tra le prime due colonne e il numero di archi blu orizzontali tra le prime due colonne non cambia. Di più: viene mantenuta la proprietà delle due colonne di avere lo stesso numero di vertici rossi e blu.

Possiamo continuare ad applicare i due processi appena descritti qualsiasi sia la prima riga delle due colonne. Ad ogni passo eliminiamo due righe e manteniamo invariata la differenza di archi orizzontali blu e rossi tra le due colonne. Arriveremo in fine ad avere 0 righe. La differenza tra archi blu e rossi orizzontali tra le due colonne è quindi 0. Poichè la differenza tra archi blu e rossi orizzontali tra le due colonne non è variata dall'inizio del processo, otterremo che anche all'inizio c'erano lo stesso numero di archi rossi e blu orizzontali tra le due colonne.

Ripetendo questo processo per ogni coppia di colonne adiacenti si dimostra che il numero di archi orizzontali rossi e blu è lo stesso. □

[2] ho qui deciso di usare la notazione $2n$ per dire che $2n$ è pari. Ovviamente, a differenza dello statement del problema, n e m sono un qualsiasi naturale positivo

Ora che abbiamo dimostrato il teorema 5.2, basta scambiare le righe e le colonne della griglia (ruotandola per esempio di 90 gradi) per ottenere il seguente corollario:

Corollario 5.2.1. *In una qualsiasi griglia $2m \times 2n$, i cui vertici sono colorati di rosso o blu in modo che la quantità di vertici rossi e blu in ogni riga e in ogni colonna sia la stessa, la quantità di archi verticali che connettono tra loro due vertici rossi adiacenti è uguale alla quantità di archi verticali che connettono tra loro vertici blu adiacenti.*

Ora che sappiamo che il numero di archi rossi orizzontali è uguale al numero di archi blu orizzontali e che il numero di archi rossi verticali è uguale al numero di archi blu verticali segue che il numero di archi rossi è uguale al numero di archi blu. Segue quindi:

Corollario 5.2.2. *In una qualsiasi griglia $2m \times 2n$, i cui vertici sono colorati di rosso o blu in modo che la quantità di vertici rossi e blu in ogni riga e in ogni colonna sia la stessa, la quantità di archi che connettono tra loro due vertici rossi adiacenti (orizzontalmente o verticalmente) è uguale alla quantità di archi che connettono tra loro vertici blu (orizzontalmente o verticalmente).*

L'ipotesi della griglia è dunque dimostrata.

Problema 6

E' molto facile ricondurre questo problema ad un problema di combinatoria. Consideriamo l'espressione:

$$(x+y+z)^n$$

Essa può essere espansa nella forma:

$$\dots \underbrace{(x+y+z)(x+y+z)(x+y+z)}_{n \text{ volte}} \dots$$

Ora, è chiaro che ogni termine nella forma $x^i y^j z^k$ è stato ottenuto "scegliendo" tra gli n fattori $(x+y+z)$ disponibili i da cui prendere x, j da cui prendere y, k da cui prendere z. Per il teorema delle combinazioni semplici dunque il coefficiente α di un certo termine $x^i y^j z^k$ è:

$$\alpha = \binom{n}{i}\binom{n-i}{j}\binom{n-i-j}{k} = \binom{n}{i}\binom{n-i}{j}\binom{k}{k} = \frac{n!}{i!(n-i)!}\frac{(n-i)!}{j!(n-i-j)!} = \frac{n!}{i!j!k!} \tag{6.1}$$

Questo risultato è simile al binomio di Newton. Ora, visto che n è fissato, il problema si riconduce a calcolare tutte le scelte di i, j, k per cui

$$2 \nmid \frac{n!}{i!j!k!} \tag{6.2}$$

Vistochè ci interessa solo la divisibilità per 2 possiamo semplificare la 6.2:

$$\nu_2(n!) = \nu_2(i!\,j!\,k!)$$

Dove $\nu_2(x)$ è la valutazione 2-adica di x. E' possibile tuttavia sfruttare il fatto noto che $\nu_p(xy) = \nu_p(x) + \nu_p(y)$ per semplificare ulteriormente la 6.2:

$$\nu_2(n!) = \nu_2(i!) + \nu_2(j!) + \nu_2(k!) \tag{6.3}$$

E' dunque possibile applicare il teorema di Legendre (per la sua dimostrazione rimando a [1, p. 118]).

$$\frac{n - S_2(n)}{2-1} = \frac{i - S_2(i)}{2-1} + \frac{j - S_2(j)}{2-1} + \frac{k - S_2(k)}{2-1}$$

Dove $S_2(n)$ è la somma delle cifre di n scritte in binario. Semplificando e sfruttando il fatto che $n = i + j + k$ si ricava:

$$S_2(n) = S_2(i) + S_2(j) + S_2(k) \tag{6.4}$$

Ed è equivalente alla eq. (6.3). Possiamo ora dimostrare il seguente teorema.

Teorema 6.1. *In un polinomio $(x+y+z)^n$ il numero di termini con coefficienti dispari è $3^{S_2(n)}$*

Dimostrazione. La tesi è implicata dal fatto che ogni cifra 1 della rappresentazione binaria di n ha tre scelte: stare in i, stare in j, stare in k. Dovremo dunque dimostrare questo fatto.

Prima di tutto dimostriamo che $S_2(a) \leq S_2(b)+S_2(c)$ dove $a=b+c$. Se supponiamo che sommando in binario b e c non sia necessario fare nessun riporto, segue banalmente $S_2(a)=S_2(b)+S_2(c)$. Se invece fosse necessario fare qualche riporto si potrebbe sommare in un unico numero tutte le cifre che possono essere sommate senza riporto (che chiamiamo b') e poi sommare tra loro le cifre che possono essere sommate solo facendo riporto(che chiamiamo c'). In questo modo si otterrebbero due numeri, la cui $S_2(b')+S_2(c') < S_2(b)+S_2(c)$ a causa del riporto. Se ora è possibile sommare questi senza riporto lo si faccia, altrimenti si continui a ripetere quest'operazione finché non è possibile sommare i due numeri senza riporto. Questo inevitabilmente succederà, in quanto $S_2(b')+S_2(c')$ è una monovariante(cala sempre e deve rimanere superiore o uguale a 1 se $a \geq 0$). Perciò rimane provato che $S_2(a) \leq S_2(b)+S_2(c)$. Da ciò consegue anche che basta che ci sia un solo riporto (senza perdita di generalità supponiamo che ci sia tra i+j e k)e $S_2(n) < S_2(i+j)+S_2(k) \leq S_2(i)+S_2(j)+S_2(k)$.

Perciò è necessario che non ci sia nessun riporto perchè si verifichi la eq. (6.4). Ciò significa che ogni 1 nella rappresentazione binaria di n proviene da i, j o k. La tesi è dunque provata. □

Come sono arrivato a questa soluzione. Inizialmente non volevo usare il teorema di Legendre. Volevo infatti sfruttare l'espansione della valutazione 2-adica di un fattoriale:

$$\begin{aligned}\nu_2(n!) &= \nu_2(1)+\nu_2(2)+\nu_2(3)+\nu_2(4)+\nu_2(5)+...+\nu_2(n)\\ &= 0+1+0+2+0+1+0+3+0+1+...+\nu_2(n)\end{aligned}$$

Chiaramente se vogliamo evitare che $\nu_2(n!) > \nu_2(i!)+\nu_2(j!)+\nu_2(k!)$ è necessario che l'espansione della valutazione 2-adica di $n!$ sia spezzata in un blocco da $2^{\lfloor \log_2 n \rfloor}$. (Se non ci fosse nessuno tra i, j, k lungo almeno $2^{\lfloor \log_2 n \rfloor}$ non c'è nessuno di loro la cui espansione della valutazione 2-adica del fattoriale contiene $\lfloor \log_2 n \rfloor$. Perciò bisogna "dividere" n in un blocco da $2^{\lfloor \log_2 n \rfloor}$, poi in un blocco da $2^{\lfloor \log_2 m \rfloor}$, dove $m = n - 2^{\lfloor \log_2 n \rfloor}$, poi in un blocco da $2^{\lfloor \log_2 o \rfloor}$, dove $o = m - 2^{\lfloor \log_2 m \rfloor}$ e così via. Sia dunque x il numero di blocchi in cui in cui ho spezzato n. Chiaramente ogni blocco può stare in i, j, k. Inoltre, vistochè ogni blocco rappresenta una cifra nella rappresentazione binaria di n, si ottiene $3^{S_2(n)}$. Anche questo metodo dovrebbe funzionare, solo che è molto difficile dimostrarlo in maniera rigorosa (inizialmente l'avevo pensato addirittura senza valutazione 2-adica, solo quando ho tentato di formalizzarlo l'ho introdotta). Perciò, vedendo la valutazione p-adica di un fattoriale e la somma delle cifre di un numero in base p, ho pensato al teorema di Legendre per provare in maniera più semplice e rigorosa questo teorema.

NB. *Mi sono reso conto a posteriori che è possibile provare la eq.* (6.1) *usando anche il binomio di Newton. Nello specifico basta dire che $(x+(y+z))^n$. Il coefficiente del termine che contiene x^i è per il binomio di Newton $\binom{n}{i}$. Espandiamo ora la scrittura di $(y+z)^{n-i}$. Il coefficiente del termine che ha y^j è $\binom{n-i}{j}$. Basta dunque moltiplicare i due binomiali per ottenere la eq.* (6.1)

Problema 7

7.1 Soluzione principale

Sia T un triangolo equilatero con un vertice A in $(0,0)$ e un vertice B in $(l,0)$, con $l \in \mathbb{Z}_+$. Per delle note relazioni goniometriche ($\angle BAC = \frac{\pi}{3}$), C sta in $(\frac{l}{2}, \frac{\sqrt{3}}{2}l)$. Segue chiaramente che se l è dispari è impossibile che C sia vicino almeno $\frac{1}{10}$ ad un punto a coordinate intere del piano cartesiano. Sia dunque $l = 2x$, $x \in Z_+$. Segue che le coordinate dei vertici del triangolo sono $(0,0)$, $(2x,0)$, $(x, x\sqrt{3})$. E' impossibile che $x\sqrt{3}$ sia intero, ma possiamo approssimarlo quanto più possibile ad uno. Ora, sappiamo che:

$$\sqrt{3} \approx 1.7320508075688772935274463415058723669428052538103806280558069794519330169088000037$$

Infatti è possibile calcolare $\sqrt{3}$ con una precisione arbitraria usando il seguente script Python:

```python
from mpmath import mp, sqrt

mp.dps = 100 # O qualunque numero di cifre significative si intenda generare.
print(sqrt(3))
```

Perciò se $x = 10^{76}$ la coordinata delle ordinate di C, che è l'unica a non essere intera, sarà:

$$C_y \approx 17320508075688772935274463415058723669428052538103806280558069794519330169088.00037$$

Distante perciò meno di $\frac{1}{1000}$ dal punto a coordinate intere più vicino, soddisfando pienamente entrambe le richieste del problema.

7.2 Soluzione alternativa

Se questa soluzione potrebbe sembrare un pochino fuori dai limiti numerici ne ho accidentalmente trovata un'altra distante meno di $\frac{1}{100}$. Nello specifico ho accidentalmente trovato $(0,0), (41,41), (41\frac{1-\sqrt{3}}{2}, 41\frac{1+\sqrt{3}}{2})$.

$$41\frac{1-\sqrt{3}}{2} \approx -15.007 \qquad 41\frac{1+\sqrt{3}}{2} \approx 56.007$$

Si può verificare che le coordinate del terzo punto di questo triangolo corrispondono a quelle scritte risolvendo il seguente sistema:

$$\begin{cases} x^2 + y^2 = 2 \cdot 41^2 \\ (x-41)^2 + (y-41)^2 = 2 \cdot 41^2 \end{cases} \tag{7.1}$$

Tutto è cominciato dalla banale considerazione che $\frac{n \cdot \frac{\sqrt{3}}{2} + k}{d}$, dove $d \mid [n \cdot \frac{\sqrt{3}}{2}] + k$, si approssima ad un intero molto meglio di $n \cdot \frac{\sqrt{3}}{2}$. Ho quindi scoperto che i triangoli equilateri con un vertice in $(0,0)$ e (k,k) hanno il terzo vertice in un punto di coordinate x proporzionali a $\frac{1-\sqrt{3}}{2}$ e y proporzionali a $\frac{1+\sqrt{3}}{2}$. Perciò ho cercato e trovato 41.

NB. *Nello statement del problema non era richiesto di generalizzare per ogni* $\frac{1}{10^n}$*, ma volendo credo che sia possibile sfruttare la rappresentazione di* $\sqrt{3}$ *come frazione continua periodica per dimostrare che nella rappresentazione decimale di* $\sqrt{3}$ *ci sono gruppi di 0 consecutivi arbitrariamente lunghi. Volendo si potrebbe argomentare anche che a causa della sua struttura priva di ordine è improbabile che* $\sqrt{3}$ *non contenga sequenze arbitrariamente lunghe di zeri.*

Problema 8

Risolviamo direttamente il caso $n \times n$ per essere più diretti.

8.1 Qual è il numero massimo di lettere distinte che una linea può attraversare?

E' facile vedere come la griglia in questione possa essere schematizzata come un piano $\mathbb{N}^2$. Ogni lettera può infatti essere considerata come un punto a coordinate intere (la **A** in basso a sinistra sarebbe $(0,0)$). Ciò porta a sospettare che avremo a che fare con equazioni diofantee o il teorema di Pick. Ogni linea del tipo descritto nel problema può essere associata un'equazione nella forma $y = kx$, vistochè passa per **A** che è l'origine. Cerchiamo di dedurre la pendenza di questa retta. Il problema ci dice che essa passa per almeno un altra lettera in grassetto. Sia questa di coordinate (a,b), con $0 \leq a, b < n$. Segue che la pendenza della retta è $\frac{b}{a}$. Abbiamo perciò un'espressione nella forma:

$$xb - ya = 0 \tag{8.1}$$

Possiamo supporre che a e b siano coprimi fra loro. Se non lo fossero l'equazione sarebbe nella forma $x(a,b)b' - y(a,b)a' = 0$, dove $a = (a,b)a'$ e $b = (a,b)b'$. Potremmo dividere per (a,b) ottenendo $xb' - ya' = 0$; segue che la retta in questione passa anche per la lettera maiuscola che si trova in (a', b'). Inoltre per come sono stati definiti a' e b' sono coprimi. Perciò se $(a,b) \neq 1$ possiamo usare usare a' e b' al loro posto.

Dell'espressione $xb - ya = 0$ ci interessano soltanto i punti a coordinate intere (corrispondenti a delle lettere della griglia). Perciò siamo davanti ad un'equazione diofantea lineare. Questa equazione diofantea lineare ha come soluzione particolare $(0,0)$. Perciò possiamo applicare il seguente teorema:

Teorema 8.1. *Sia* $ax + by = c$ *una equazione diofantea tale che* $d = (a,b)$ *sia un divisore di* c*. Detta* $(\bar{x}, \bar{y})$ *una soluzione particolare dell'equazione, tutte e sole le infinite soluzioni sono date dalle coppie* (x,y) *con*

$$x = \bar{x} + k \cdot \frac{b}{d} \qquad y = \bar{y} - k \cdot \frac{a}{d}$$

Questo fatto ben noto è dimostrato in [1, p. 89].

Dunque possiamo esprimere tutte le soluzioni a coordinate intere della eq. (8.1) come:

$$x = k \cdot (-a) \qquad y = -k \cdot b$$

Sostituendo k con il suo opposto l'espressione si semplifica ulteriormente:

$$x = k \cdot a \qquad y = k \cdot b \tag{8.2}$$

E' necessario inoltre imporre che $k \in \mathbb{N}$ poiché le soluzioni negative sono fuori dalla griglia. Segue da quanto detto che tutte le lettere per cui passa la linea descritta nel problema hanno coordinate (ka, kb)[3]. Vogliamo capire quante lettere diverse appartengano a questa retta. Consideriamo per un attimo solo le coordinate delle ascisse delle varie lettere. Esse saranno nella forma $0, a, 2a, 3a, 4a, ...,$. Richiamiamo ora il seguente fatto ben noto dimostrato in [2, p. 16]:

Teorema 8.2. *Siano n ed m due interi positivi coprimi. Allora l'insieme*

$$S = \{0, m, 2m, 3m, 4m, ..., (n-1)m\}$$

costituisce un sistema completo di residui modulo n.

Vistochè $\left(\frac{a}{(n,a)}, n\right) = 1$ ciò significa che:

$$k\frac{a}{(n,a)} \equiv 0 \pmod{n} \qquad \text{per } k = 0, n, 2n, 3n, ...$$

Facendo qualche trasformazione algebrica:

$$\frac{k}{(n,a)}a \equiv k'a \equiv 0 \pmod{n} \qquad \text{per } k' = 0, \frac{n}{(n,a)}, \frac{2n}{(n,a)}, \frac{3n}{(n,a)}, ...$$

Ciò significa che il periodo secondo il quale si ripetono le coordinate delle ascisse delle soluzioni intere dell' eq. (8.2) modulo n divide $\frac{n}{(n,a)}$. Applichiamo ora il teorema 8.2 a a e $\frac{n}{(n,a)}$:

$$ka \equiv 0 \pmod{\frac{n}{(n,a)}} \qquad \text{per } k = 0, \frac{n}{(n,a)}, \frac{2n}{(n,a)}, \frac{3n}{(n,a)}, ...$$

segue che il periodo secondo il quale si ripetono le coordinate delle ascisse delle soluzioni intere dell' eq. (8.2) modulo n è multiplo di $\frac{n}{(n,a)}$, poichè non c'è nessuno zero "in mezzo".

Perciò segue che il periodo secondo il quale si ripetono le coordinate delle ascisse delle soluzioni intere dell' eq. (8.2) modulo n è esattamente $\frac{n}{(n,a)}$. Si può fare un discorso simile per le ordinate e dire che il periodo delle coordinate delle ordinate modulo n è esattamente $\frac{n}{(n,b)}$. Da ciò segue che che il periodo complessivo secondo il quale si ripetono le coordinate x e y dei punti a coordinate intere della rettà è:

$$\left[\frac{n}{(n,a)}, \frac{n}{(n,b)}\right] \tag{8.3}$$

Cerchiamo ora di provare il seguente teorema:

Teorema 8.3. $[kx, ky] = k[x, y]$*, dove le parentesi quadre indicano il minimo comune multiplo di due numeri.*

[3]E' un vettore! Avevo pensato di usare l'algebra lineare per risolvere questo problema, ma ha deciso che avrei complicato solo le cose

Dimostrazione. Come dimostrato in [1, p. 55] è noto che:

$$(x, y)[x, y] = xy \tag{8.4}$$

Inoltre come dimostrato in [1, p. 56] è noto che:

$$(kx, ky) = k(x, y)$$

Possiamo sfruttare questi due fatti per dire:

$$(kx, ky)[kx, ky] = k^2xy \iff (x, y)[kx, ky] = kxy$$

Applicando nuovamente la eq. (8.4) si ricava:

$$[kx, ky] = \frac{kxy}{(x, y)} = k[x, y]$$

da cui la tesi. □

Adoperiamo alcune semplificazioni alla eq. (8.3):

$$\left[\frac{n}{(n,a)}, \frac{n}{(n,b)}\right] = n\left[\frac{1}{(n,a)}, \frac{1}{(n,b)}\right] \cdot \frac{(n,a)(n,b)}{(n,a)(n,b)} = n \cdot \frac{[(n,a),(n,b)]}{(n,a)(n,b)}$$

Siccome $(a, b) = 1$:

$$\frac{[(n,a),(n,b)]}{(n,a)(n,b)} = 1$$

Infatti tutti i primi comuni sia ad a che a n sicuramente non sono comuni sia a b che ad n e vice-versa. Perciò $((n, a), (n, b)) = 1$. Per la eq. (8.4) ciò implica che $[(n, a), (n, b)] = (n, a)(n, b)$. Il risultato finale è che perciò il periodo delle coordinate delle soluzioni della diofantea 8.1 modulo n è lungo n. Perciò ogni retta interseca esattamente n lettere diverse.

Come sono arrivato a questa soluzione. Inizialmente l'idea che avevo avuto per la dimostrazione era piuttosto diversa. Infatti fino alla eq. (8.1) era tutto triviale, ma per trovare la lunghezza del periodo delle lettere volevo spostarmi nel piano dei naturali gaussiani $\mathbb{N}[i]$. Poi volevo estendere il concetto di congruenza modulare ai naturali gaussiani. A questo punto speravo di riuscire a dimostrare in maniera non troppo complessa qualcosa di simile al teorema 8.2 che funzionasse anche per gli interi gaussiani. Il problema è che il teorema andava modificato parecchio (la condizione di coprimalità in $\mathbb{N}[i]$ è piuttosto rara) e non potevo più sfruttare la dimostrazione in [2]. Alla fine sono riuscito a trovare il modo di far funzionare il tutto, ma ho dovuto dimostrare una quantità tale di teoremi che hanno reso i naturali gaussiani e le loro proprietà superflue, per cui ne ho fatto a meno. Ho quindi usato i teoremi che avevo trovato senza applicarli agli interi gaussiani.

8.2 Quanti insiemi distinti di lettere potete ottenere tracciando linee in questa griglia?

Chiaramente ad ogni pendenza diversa corrisponde un insieme di lettere. Cercheremo in seguito di capire se ci siano pendenze le cui rette attraversano lo stesso insieme di lettere.

Un quadrato 2×2 sarà chiaramente in grado di formare 3 rette (una orizzontale, una verticale, una diagonale). Un quadrato di lato n invece sarà in grado di formare sicuramente tutte le rette che forma un quadrato di lato $n-1$ più tutte quelle la cui pendenza sia $\frac{x}{n-1}$ o $\frac{n-1}{y}$. Queste frazioni devono essere però già ridotte ai minimi termini. Ciò significa che $(x, n-1) = 1$ o $(y, n-1) = 1$. Perciò, usando la funzione φ di Eulero:

$$\begin{aligned} P_2 &= 3 \\ P_n &= P_{n-1} + 2\varphi(n-1) \end{aligned}$$

Trasformando il tutto con una sommatoria, si ricava:

$$P_n = 3 + 2\sum_{i=3}^{n} \varphi(i-1)$$

Facendo ora alcune semplificazioni e sfruttando il fatto che $\varphi(1) = 1$:

$$P_n = 3 + 2\sum_{i=2}^{n-1} \varphi(i) = 1 + 2\sum_{i=1}^{n-1} \varphi(i) \tag{8.5}$$

Da cui possiamo generare la sequenza:

$$1, 3, 5, 9, 13, 21, 25, 37, 45, 57, ...$$

Ciò significa che per un quadrato 3×3 le possibili pendenze delle rette sono 5, per una quadrato 9×9 le possibili pendenze sono 57, per un quadrato 81×81 sono 4041, per un quadrato 6×6 sono 25. Se non ci fossero pendenze le cui rette attraversano lo stesso insieme di lettere queste sarebbero le soluzioni, ma purtroppo non è così. Infatti possiamo vedere che nel caso 3×3 ci sono due rette che passano per $\{A, H, F\}$ e $\{A, F, H\}$. In generale questo succede molto spesso, come mostrato nella tabella 8.1 per il caso 4×4.

O	P	Q	R	O	P	Q	R	O	P	Q	R	O	P	Q	R
I	L	M	N	I	L	M	N	I	L	M	N	I	L	M	N
E	F	G	H	E	F	G	H	E	F	G	H	E	F	G	H
A	B	C	D	**A**	B	C	D	A	B	C	D	A	B	C	D
O	P	Q	R	O	P	Q	R	O	P	Q	R	O	P	Q	R
I	L	M	N	I	L	M	N	I	L	M	N	I	L	M	N
E	F	G	**H**	E	F	G	H	E	F	G	H	E	F	G	H
A	B	C	D	A	B	C	D	A	B	C	D	A	B	C	D
O	P	Q	R	O	P	Q	R	O	P	Q	R	O	P	Q	R
I	L	**M**	N	I	L	M	N	I	L	M	N	I	L	M	N
E	F	G	H	E	F	G	H	E	F	G	H	E	F	G	H
A	B	C	D	A	B	C	D	A	B	C	D	**A**	B	C	D
O	**P**	Q	R	O	P	Q	R	O	**P**	Q	R	O	P	Q	R
I	L	M	N	I	L	**M**	N	I	L	M	N	I	L	M	N
E	F	G	**H**	E	F	G	H	E	F	G	H	E	F	G	H
A	B	C	D	A	B	C	D	A	B	C	D	A	B	C	D

Tabella 8.1: Due lettere diverse intersecano le stesso insieme di lettere

Quindi dobbiamo cercare di capire quante siano le rette di questo tipo. Si può notare facilmente che in tutte le griglie le rette di pendenza $\frac{1}{n-1}$ e $\frac{n-1}{1}$ hanno lo stesso insieme di lettere (per tutti gli $n > 2$, altrimenti le rette non sono distinte). Dimostriamo questo fatto:

Teorema 8.4. *Le rette di pendenza $\frac{1}{n-1}$ e $\frac{n-1}{1}$ intersecano tutte lo stesso insieme di lettere indipendentemente da n.*

Dimostrazione. Ciò equivale a dire:

$$(k(n-1), k) \equiv (k', k'(n-1)) \pmod{n} \iff$$

$$\begin{cases} k(n-1) \equiv k' \pmod{n} \\ k \equiv k'(n-1) \pmod{n} \end{cases} \iff$$

$$k \equiv -k' \pmod{n} \qquad \forall n \in \mathbb{N}$$

Ciò dimostra la tesi, perchè afferma che ogni lettera contenuta in una linea è contenuta anche nell'altra nell'altra in una posizione congrua a $-k'$. □

Inizialmente mi ero convinto che fossero solo queste le rette di questo tipo. Speravo di ottenere:

$$C_n = 2\sum_{i=1}^{n-1} \varphi(i)$$

Poi ho provato a scrivere uno script per confermare la mia teoria, vistochè non riuscivo a trovare un modo per provarla, ed ho scoperto che in realtà sono molte di più. Lo script è il seguente:

```
#include <bits/stdc++.h>

using namespace std;

int main(){
  int dimensione_griglia;
  cin >> dimensione_griglia;
  vector<vector<int>> GRIGLIA(dimensione_griglia, vector<int>(dimensione_griglia));

  for(int i=0; i<dimensione_griglia; i++){
    for(int j=0; j<dimensione_griglia; j++){
      GRIGLIA[i][j] = i*dimensione_griglia+j;
    }
  }

  for(int i=dimensione_griglia-1; i>=0; i--){
    for(int j=0; j<dimensione_griglia; j++){
      cout << GRIGLIA[i][j] << "\t";
    }
    cout << endl;
  }

  cout << endl << "---------------" << endl << endl;

  map<set<int>,vector<pair<int, int>>> MAPPA = {};
  set<int> sequenza ={};

  for(int i=1; i<dimensione_griglia; i++){
    for(int j=1; j<dimensione_griglia; j++){
      if(!( gcd(i, j) == 1)) continue;
      pair<int, int> pos = {0, 0};
      sequenza.clear();

      do{
        pos.first += i; pos.second += j;
        pos.first %= dimensione_griglia; pos.second %= dimensione_griglia;
        sequenza.insert(GRIGLIA[pos.first][pos.second]);

      }while(pos.first != 0 or pos.second != 0);

      MAPPA[sequenza].push_back({i, j});
    }
  }

  int sum = 0;

  for(auto i: MAPPA){
    if(i.second.size() == 1) continue;
    for(auto e: i.first) cout << e << " ";
    cout << ": ";
    for(auto e: i.second) cout << "(" << e.first << ", " << e.second << "), ";
    cout << endl;

    sum += i.second.size()-1;
  }
  cout << "BISOGNA RIMUOVERNE: " << sum << endl;

}
```

Sostanzialmente non fa altro che simulare tutte le varie rette e contare quelle che intersecano lo stesso numero di lettere. Per $n = 4$ l'output è:

```
12  13  14  15
8   9   10  11
4   5   6   7
0   1   2   3

--------------

0 2 9 11 : (2, 1), (2, 3),
0 6 8 14 : (1, 2), (3, 2),
0 7 10 13 : (1, 3), (3, 1),
BISOGNA RIMUOVERNE: 3
```

Per $n = 5$ l'output è:

```
20  21  22  23  24
15  16  17  18  19
10  11  12  13  14
5   6   7   8   9
0   1   2   3   4

--------------

0 6 12 18 24 : (1, 1),
0 7 14 16 23 : (1, 2), (3, 1), (4, 3),
0 8 11 19 22 : (1, 3), (2, 1), (3, 4),
0 9 13 17 21 : (1, 4), (2, 3), (3, 2), (4, 1),
BISOGNA RIMUOVERNE: 7
```

Eseguendo lo script per n da 1 a 12 si ottiene la seguente sequenza:

$$0, 0, 1, 3, 7, 9, 17, 25, 33, 39, 53, 61... \tag{8.6}$$

Che però non ricorda nulla di noto. Non è nemmeno presente su OEIS.

Certo, possiamo usare lo script per calcolare il numero di rette che hanno la stessa sequenza di lettere per i valori $3, 9, 6$ e sottrarre alla eq. (8.5) quei valori(risolvendo il problema per $n = 3, 9, 6$), tuttavia usando questo approccio è impossibile generalizzare, a meno di voler utilizzare lo script per ogni valore di n.

Poi però ho notato che su OEIS esisteva un match per la sequenza:

$$1, 3, 4, 6, 6, 12, 8, 12, 12, 18, 12, 24, 14, 24, 24, 24, 18, ... \tag{8.7}$$

ottenuta sottraendo alla sequenza 8.5 i valori della sequenza 8.6. Nello specifico, la sequenza corrisponde con la funzione psi di Dedekind:

$$\psi(n) = n \cdot \prod_{\substack{p|n \\ \text{p è primo}}} \left(1 + \frac{1}{p}\right)$$

Vale la pena notare che questa definizione ricorda in qualche modo una definizione della funzione φ di Eulero:

$$\varphi(n) = n \cdot \prod_{\substack{p|n \\ \text{p è primo}}} \left(1 - \frac{1}{p}\right)$$

Se però non dimostro che la funzione $\bar{f}$ che associa al lato del quadrato n il numero massimo di insiemi di lettere formabili con rette come quelle descritte nel problema è proprio la funzione psi di Dedekind, tutto il lavoro fin qui svolto è inutile. Possiamo però sfruttare una definizione alternativa della funzione di Dedekind, molto simile a quella di φ, documentata in [3]. Nello specifico:

$$\psi(ab) = \psi(a)\psi(b) \qquad \text{se } (a,b) = 1 \qquad \text{in altre parole, la funzione è moltiplicativa} \tag{8.8}$$

$$\psi(p^k) = (p+1)p^{k-1} \qquad \text{dove p è primo} \tag{8.9}$$

Se dimostriamo che anche $\bar{f}$ ha queste proprietà, dimostriamo che $\bar{f}$ è proprio la funzione di Dedekind. Cominciamo a dimostrare il seguente teorema:

Teorema 8.5. *Se $n = p$ (dove p è un primo) e due rette passano entrambe per una stessa lettera diversa da $\boldsymbol{A}$, allora l'insieme di lettere che attraversano è lo stesso.*

Dimostrazione. Sia $\frac{b}{a}$ è la pendenza della prima retta e $\frac{d}{c}$ è la pendenza della seconda. I punti a coordinate interi delle due rette per l' eq. (8.2) sono nella forma (ka, kb) e $(k'c, k'd)$. Perciò se una certa lettera compare in entrambe le rette si ha:

$$\begin{cases} ka \equiv k'c \pmod p \\ kb \equiv k'd \pmod p \end{cases}$$

Ora, da qui possiamo impostare la seguente moltiplicando i membri opposti delle due congruenze, poichè $a \equiv b \pmod n \implies ac \equiv bc \pmod n$:

$$ka \cdot k'd \equiv kb \cdot k'c \pmod p$$

Sfruttando il fatto che quando si lavora modulo p tutti i numeri diversi da 0 hanno un inverso modulare, vistochè $k, k' \neq 0$ (altrimenti sarebbe la lettera **A**!)

$$ad \equiv bc \pmod p$$

Sfruttando ancora gli inversi modulari e il fatto che $a \equiv b \pmod n \implies ac \equiv bc \pmod n$:

$$ac^{-1}j \equiv bd^{-1}j \pmod p$$

Definiamo ora la variabile Λ:

$$k' + ac^{-1}j \equiv k' + bd^{-1}j \equiv \Lambda \pmod p$$

Moltiplichiamo Λ per c e d.

$$\begin{cases} ck' + ja \equiv c\Lambda \pmod p \\ dk' + jb \equiv d\Lambda \pmod p \end{cases}$$

Ma noi sappiamo che $ck' \equiv_p ak$ e che $dk' \equiv_p bk$. Da ciò si ricava:

$$\begin{cases} a(k+j) \equiv c\Lambda \pmod p \\ b(k+j) \equiv d\Lambda \pmod p \end{cases}$$

Ciò significa, che tutte le altre lettere della prima retta sono presenti anche nella seconda retta! Poichè le due rette hanno lo stesso numero di elementi, la tesi è dimostrata!

□

Come sono arrivato a questa soluzione. Dopo aver facilmente trovato:

$$\begin{cases} ka \equiv k'c \pmod p \\ kb \equiv k'd \pmod p \end{cases}$$

ho sommato a entrambi i membri a e b:

$$\begin{cases} ka + a \equiv k'c + a & \pmod p \\ kb + b \equiv k'd + b & \pmod p \end{cases}$$

Da cui dovevo mostrare che $k'c + a$ e $k'd + b$ appartenevano alla seconda retta. In altre parole(aleph e beth sono qui usate come normali variabili):

$$\begin{cases} ck' + a \equiv c \cdot \aleph & \pmod p \\ dk' + b \equiv d \cdot \beth & \pmod p \end{cases}$$

Ossia che $\aleph = \beth$. Ho ottenuto quindi:

$$\begin{cases} k' + ac^{-1} \equiv \aleph & \pmod p \\ k' + bd^{-1} \equiv \beth & \pmod p \end{cases}$$

Nel frattempo avevo trovato che $ad \equiv bc \pmod p$. Alla fine ho riordinato un po' tutto e ottenuto la dimostrazione finale.

Ora è triviale dimostrare il seguente:

Teorema 8.6. $\bar{f}(p) = p + 1$ *dove p è primo*

Dimostrazione. La griglia di maiuscole è costituita da p^2 lettere. Eliminiamo la **A** e consideriamo le altre $n^2 - 1$ lettere. Chiamiamo gruppo l'insieme di lettere esclusa la **A** che vengono attraversate da una stessa retta. Per il teorema 8.5 ogni lettera appartiene ad un solo gruppo. Vistochè tra la **A** e una certa lettera esiste sempre una retta ogni lettera diversa dalla **A** fa parte di un gruppo. Possiamo perciò sfruttare il fatto che ogni gruppo è composto da $p - 1$ lettere perchè ogni retta è composta da p lettere (vedere sezione 8.1) tra le quali c'è la **A** per calcolare il numero totale di gruppi:

$$\frac{p^2 - 1}{p - 1} = p + 1$$

Ora, poichè ad ogni gruppo corrisponde un insieme di lettere, la tesi è dimostrata. □

Questo dimostra che per $\bar{f}$ vale la 8.9 se $k = 1$. Per tutti gli altri valori di k pensavo di dimostrarlo per induzione, ma alla fine invece sono riuscito a generalizzare le dimostrazioni precedenti.

Teorema 8.7. *Se $n = p^i$ e due rette attraversano entrambe una certa lettera diversa da **A** di cui entrambe le coordinate non sono multiple di p, allora l'insieme di lettere che attraversano è lo stesso.*

Dimostrazione. Siano (ka, kb), $(k'c, k'd)$ le coordinate dei punti in cui le due rette passano per la lettera in questione. Se entrambe le coordinate della lettera non sono multiple di p, possiamo impostare la seguente grazie alle leggi di Morgan e al fatto che se un primo divide un prodotto divide almeno uno dei due fattori:

$$\begin{aligned}
&(p \nmid ka \wedge p \nmid kb) \wedge (p \nmid k'c \wedge p \nmid k'd) = 1 && \iff \\
&(\neg(p \mid ka) \wedge \neg(p \mid kb)) \wedge (\neg(p \mid k'c) \wedge \neg(p \mid k'd)) = 1 && \iff \\
&\neg(p \mid ka \vee p \mid kb) \wedge \neg(p \mid k'c \vee p \mid k'd) = 1 && \iff \\
&(p \mid ka \vee p \mid kb) \vee (p \mid k'c \vee p \mid k'd) = 0 && \iff \\
&p \nmid a \wedge p \nmid b \wedge p \nmid c \wedge p \nmid d \wedge p \nmid k \wedge p \nmid k' = 1
\end{aligned}$$

Da ciò segue che a, b, c, d, k, k' sono coprimi con p^i, dunque hanno inverso modulare modulo p^i. Ora, in maniera simile a quanto fatto per il teorema 8.5 possiamo impostare la seguente:

$$\begin{cases} ka \equiv k'c & \pmod{p^i} \\ kb \equiv k'd & \pmod{p^i} \end{cases}$$

Da cui, vistochè tutti i numeri coprimi con p^i hanno un inverso modulare modulo p^i:

$$\begin{cases} k \equiv k'ca^{-1} & \pmod{p^i} \\ k \equiv k'db^{-1} & \pmod{p^i} \end{cases}$$

Eguagliando $k \equiv k$, sfruttando il fatto che anche k' ha inverso modulare e il fatto che $a \equiv b \pmod{n} \implies ac \equiv bc \pmod{n}$:

$$ca^{-1}j \equiv db^{-1}j \qquad \pmod{p^i}$$

$$\Lambda \equiv k + ca^{-1}j \equiv k + db^{-1}j \qquad \pmod{p^i}$$

Da cui, seguendo una procedura analoga alla precedente:

$$\begin{cases} \Lambda a \equiv ka + cj \equiv c(k' + j) & \pmod{p^i} \\ \Lambda b = kb + dj \equiv d(k' + j) & \pmod{p^i} \end{cases}$$

Ciò significa che tutte le lettere della seconda retta sono contenute anche nella prima retta. □

Teorema 8.8. *Se $n = p^i$ e due rette attraversano entrambe in punti diversi una certa lettera di cui una e solo una coordinata è multipla di p, allora l'insieme di lettere che attraversano è lo stesso.*

Dimostrazione. Se solo una coordinata è multipla di p (senza perdita di generalità affermiamo che sia quella delle ascisse) allora la posizione della lettera è nella forma (ap^jk, bk). Perciò tutti i punti a coordinate intere della retta hanno le ascisse multiple di p^j. Perciò possiamo immaginare di "comprimere" orizzontalmente la griglia, lasciando solo le colonne con le ascisse multiple di p^j. A questo punto otteniamo p^j sotto-griglie di lato p^{i-j} appoggiate una sopra l'altra (si considerino solo le lettere maiuscole).

$$\begin{array}{cccc c cc} \mathrm{O} & \mathrm{P} & \mathrm{Q} & \mathrm{R} & & \mathrm{O} & \mathrm{Q} \\ \mathrm{I} & \mathrm{L} & \mathrm{M} & \mathrm{N} & \implies & \mathrm{I} & \mathrm{M} \\ \mathrm{E} & \mathrm{F} & \mathrm{G} & \mathrm{H} & \implies & \mathrm{E} & \mathrm{G} \\ \mathrm{A} & \mathrm{B} & \mathrm{C} & \mathrm{D} & & \mathrm{A} & \mathrm{C} \end{array}$$

Tabella 8.2: Esempio. Abbiamo lasciato solo le colonne multiple di 2.

Ora che il punto (ap^jk, bk) è diventato il punto (ak, bk) con $(a, b) = 1$ e $(ab, p) = 1$, possiamo facilmente dimostrare che tutte le p^j sotto-griglie sono uguali, ossia che ogni retta le attraversa negli stessi punti. Questo perchè:

$$\begin{cases} ka & \mod p^{i-j} \\ kb & \mod p^i \end{cases}$$

è l'espressione del variare delle lettere sulla retta all'interno della griglia rettangolare che abbiamo appena creato. Restringendo il campo ad una sola sotto griglia si ottiene:

$$\begin{cases} ka & \mod p^{i-j} \\ kb & \mod p^{i-j} \end{cases}$$

Quindi tutte le sotto-griglie di lato p^{i-j} sono uguali. Perciò, se le due rette hanno in comune una qualsiasi lettera in queste p^j sotto-griglie, ne hanno una in comune anche nella sotto-griglia in basso a sinistra. Allora possiamo "fingere" di essere nel caso del teorema 8.7, poichè abbiamo (ak, bk) con $(a, b) = 1$ e $(ab, p^{i-j}) = 1$. La considerazione finale del teorema 8.7 infatti era che:

$$\begin{cases} \Lambda a \equiv ka + cs \equiv c(k' + s) & \pmod{p^{i-j}} \\ \Lambda b = kb + ds \equiv d(k' + s) & \pmod{p^{i-j}} \end{cases}$$

(ho cambiato i nomi delle variabili) ma se mettiamo una sopra l'altra j griglie uguali di lato p^{i-j} (ossia se otteniamo la configurazione descritta), la formula diventa:

$$\begin{cases} \Lambda a \equiv ka + cs \equiv c(k' + s) & \pmod{p^{i-j}} \\ \Lambda b = kb + ds \equiv d(k' + s) & \pmod{p^i} \end{cases}$$

Ossia quanto volevamo dimostrare. □

Dai due teoremi appena dimostrati si ottiene il seguente lemma:

Lemma 8.9. *Se $n = p^i$ e due rette attraversano entrambe in punti diversi una certa lettera di cui almeno una coordinata non è multipla di p, allora l'insieme di lettere che attraversano è lo stesso.*

Ricavare il seguente teorema è ora triviale.

Teorema 8.10. $\bar{f}(p) = (p+1)p^{k-1}$ *dove p è primo*

Dimostrazione. Nella griglia ci sono p^{2k} caselle. Di queste p^{2k-2} hanno entrambe le coordinate divisibili da p. Ogni linea contiene p^k lettere, di cui p^{k-1} hanno entrambe le coordinate divisibili per p (infatti se $(a, b) = 1$ questo accade solo se $p \mid k$ nell'espressione (ak, bk)). Da ciò segue:

$$\frac{p^{2k} - p^{2k-2}}{p^k - p^{k-1}} = \frac{p^{2k-2}(p^2 - 1)}{p^{k-1}(p-1)} = p^{k-1}(p+1)$$

□

Abbiamo perciò dimostrato che per $\bar{f}$ vale la regola 8.9. Perciò $\bar{f}$ coincide con ψ per tutti gli interi nella forma p^k con p primo. Rimane da dimostrare la 8.8 per essere certi che $\bar{f} = \psi$. Dimostriamo dunque il seguente teorema:

Teorema 8.11. $\bar{f}(p_1^i\, p_2^j\, p_3^k\, p_4^l ...) = \bar{f}(p_1^i)\, \bar{f}(p_2^j)\, \bar{f}(p_3^k)\, \bar{f}(p_4^l)$

Dimostrazione. Supponiamo che i punti a coordinate intere di una certa retta siano nella forma (ak, bk). Possiamo supporre che $(a, b) = 1$ per quanto già detto dopo l'equazione 8.1. Inoltre, se $(a, p_i^i p_2^j p_3^k ...) \neq 1$ o $(b, p_i^i p_2^j p_3^k ...) \neq 1$ possiamo utilizzare una procedura simile a quella del teorema 8.8 per ricondurci ad un caso in cui a e b sono coprimi con i lati della griglia. Ora potremmo immaginare che la griglia di lettere maiuscole abbia un lato da p_1^i invece che $p_1^i\, p_2^j\, p_3^k\, p_4^l ...$. Chiaramente ogni p_1^i punti a coordinate intere ce ne sarà uno nella forma $(ap_1^i k', bp_1^i k')$. Per la definizione di $\bar{f}$ sappiamo che per andare da $(0, 0)$ ad un qualsiasi punto nella forma (ap_1^i, bp_1^i) possiamo scegliere $\bar{f}(p_1^i)$ diversi insiemi di lettere (l'insieme di lettere che otterremo nello specifico dipende dalla scelta di a e b e quindi dal punto finale (ap_1^i, bp_1^i)). Ora immaginiamo di dividere la griglia in $p_2^{2j}\, p_3^{2k}\, p_4^{2l} ...$ sotto-griglie $p_1^i \times p_1^i$ e condensare le sotto-griglie $p_1^i \times p_1^i$ in delle mega-lettere, rendendo il lato del quadrato di mega-lettere maiuscole di $p_2^j p_3^k p_4^l ...$ mega-lettere. Se consideriamo questa griglia, essa potrà formare $\bar{f}(p_2^j p_3^k p_4^l ...)$ insiemi di mega-lettere diverse. Per ottenere gli insiemi di lettere diverse ottenibili dalla griglia originale, dobbiamo moltiplicare questo numero per gli insiemi di lettere formabili dalle sotto griglie $p_1^i \times p_1^i$, ossia $\bar{f}(p_1^i)$. Infatti possiamo andare dalla mega-lettera (ak, bk) alla mega-lettera $(ak + a, bk + b)$ in $\bar{f}(p^i)$ modi diversi(p^i movimenti a destra di b e in alto di a formano un unico movimento di $(p^i a, p^i b)$, ossia un movimento di (a, b) nella griglia formata dalle mega-lettere!). Perciò il numero totale di insiemi di lettere formabili nella griglia originale è $\bar{f}(p_1^i)\bar{f}(p_2^j p_3 k p_4^l ...)$. Proseguendo in questo modo per $\bar{f}(p_2^j\, p_3^k\, p_4^l)$ si ottiene la tesi. □

Ciò è equivalente alla 8.8. Dunque abbiamo dimostrato che gli insiemi distiniti di lettere che una retta come quella descritta nello statement del problema sono proporzionali alla funzione psi di Dedekind del lato del quadrato di lettere in grassetto.

Riferimenti bibliografici

[1] Salvatore Damantino. *Teoria dei numeri.* Umath, 2018.

[2] Emanuele Campeotto Salvatore Damantino. *Aritmetica modulare.* Umath, 2020.

[3] Wikipedia. *Dedekind psi function.* 2025. URL: https://en.wikipedia.org/wiki/Dedekind_psi_function.