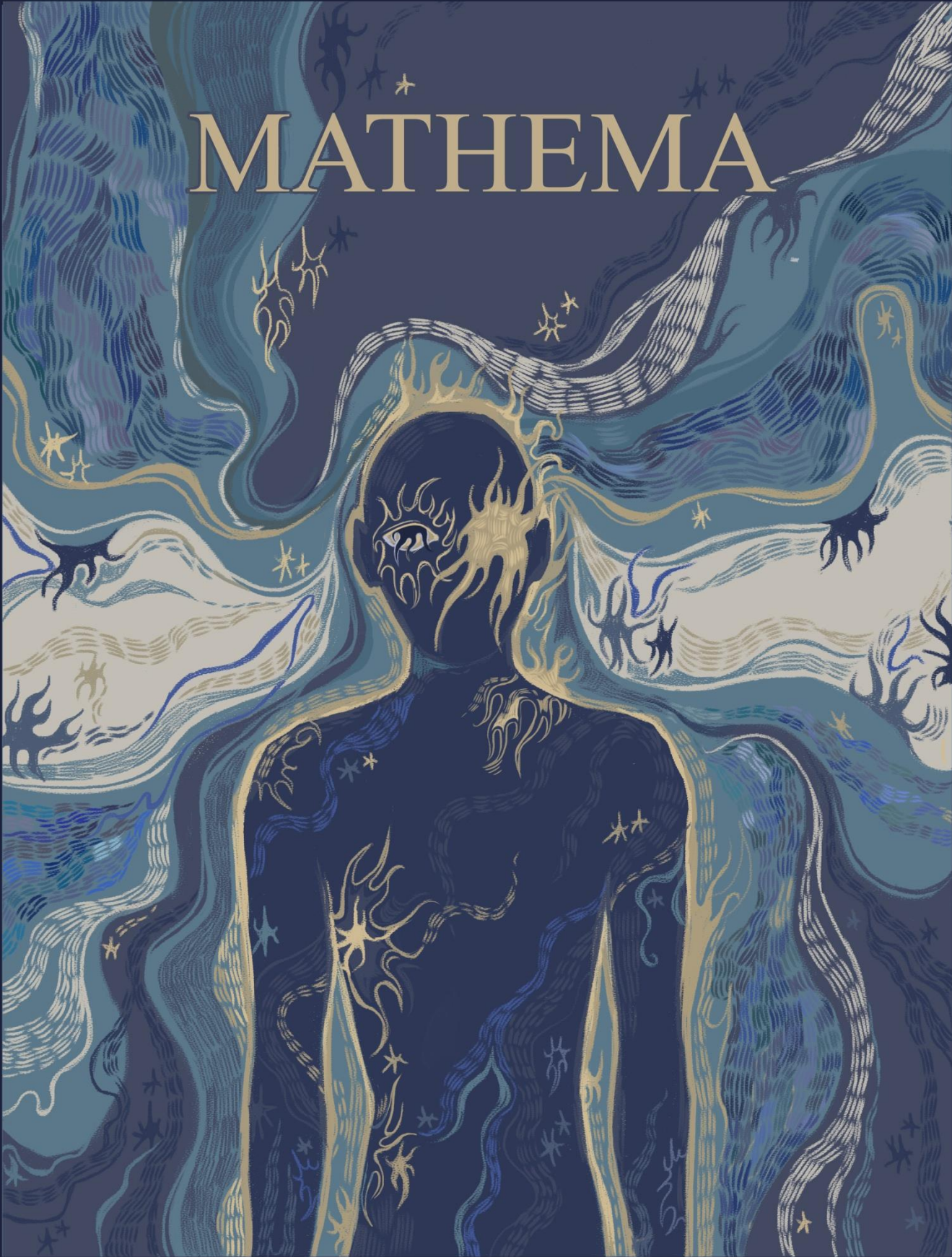


MATHEMA



Elevii clasei IX I-Colegiul Național „Gheorghe Lazăr” Sibiu

Coordonator: prof. Dorca Doriană

MATHÈMA
PARADOXURI MATEMATICE

SIBIU

2022

ISBN 978-973-0-37069-0



PARADOXURI
MATEMATICE

CUPRINS

Paradoxurile lui Zenon	2
Paradoxul plicului	4
Paradoxul spânzuratului	5
Problema lui Monty Hall	6
Paradoxul prieteniei	8
Problema claselor de complexitate P și NP	10
Algoritmul RSA	12
Paradoxul ascensorului	15
Paradoxul bibliotecarului	17
Paradoxul infinitului	18
Paradoxul Hiperjocului	19
Paradoxul Liniei și Zonei Disparute	21
Paradoxul Braess	23
Banda lui Möbius	27
Paradoxul Olbers	28
Paradoxul zilelor de naștere	30
Paradoxul Grand Hotel al lui Hilbert	32
Paradoxul frunzelor de ceai	33
Paradoxul Calului	34
Efectul Mpemba	36
De la pisica lui Schrödinger la multivers	37
Paradoxul lui Russell	40
Probabilitățile în jocul de noroc	41
Riemann și numerele prime	48

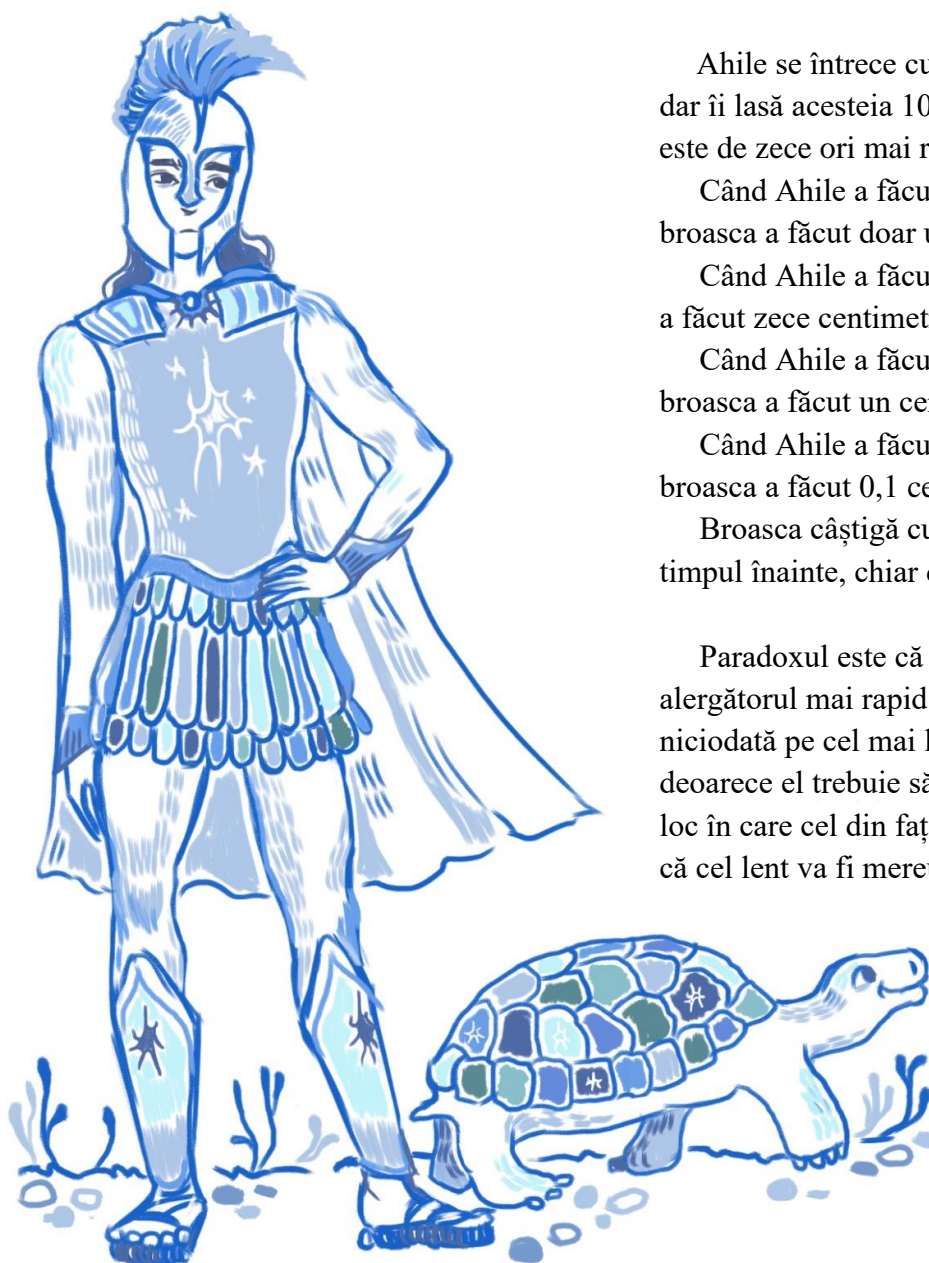
Paradoxurile lui Zenon

Dospinescu Miruna

Paradoxurile lui Zenon susțin doctrina lui Parmenide care enunțează că „toate sunt una” și, în ciuda a ceea ce arată simțurile omului, credința în pluralitate și în schimbare este greșită, mișcarea fiind doar o iluzie.

Aceste paradoxuri sunt unele din primele exemple de folosire a metodei de demonstrație prin reducere la absurd.

Ahile și broasca țestoasă



Ahile se întrece cu o broască țestoasă, dar îi lasă acesteia 10 metri avans. Ahile este de zece ori mai rapid.

Când Ahile a făcut cei zece metri, broasca a făcut doar unul.

Când Ahile a făcut acel metru, broasca a făcut zece centimetri.

Când Ahile a făcut cei zece centimetri, broasca a făcut un centimetru.

Când Ahile a făcut acel centimetru, broasca a făcut 0,1 centimetri.

Broasca câștigă cursa, fiind absolut tot timpul înainte, chiar dacă cu puțin.

Paradoxul este că într-o cursă, alergătorul mai rapid nu-l poate depăși niciodată pe cel mai lent, aflat în fața sa, deoarece el trebuie să ajungă întâi într-un loc în care cel din față fusese deja, astfel că cel lent va fi mereu în față.

Din punct de vedere matematic problema poate fi abordată în mai multe moduri.

O posibilă explicație ar fi să se considere două puncte A și B. Distanța dintre cele două puncte este x . Pentru ca din punctul A să se poată ajunge în punctul B este necesar să se parcurgă mai întâi jumătate din distanța inițială, adică $x/2$. Pentru ca punctul A să ajungă din punctul curent în punctul B este necesar să mai parcurgă jumătate din distanța rămasă, deci o pătrime din distanța totală, sau $x/4$. Și așa mai departe pentru următoarele distanțe ($1/8$, $1/16\dots$). Pentru a obține distanța totală D pe care A o parcurge se însumează toate distanțele și se obține următoarea serie geometrică:

$$D = \frac{x}{2} + \frac{x}{4} + \frac{x}{8} + \frac{x}{16} + \dots = \frac{\frac{x}{2}}{1 - \frac{1}{2}} = x$$

În concluzie, distanța D pe care A o parcurge este într-adevăr egală cu distanța x dintre A și B, ceea ce înseamnă că A ajunge în punctul B.

„**Paradoxul săgeții**” ne spune că o săgeată aflată în mișcare între punctele A și B nu se află la un moment dat nici în punctul A, pentru că a plecat de acolo, nici în punctul B, că n-a ajuns încă acolo. Dacă reduci distanța AB la lungimea săgeții, înseamnă că săgeata este, de fapt, în repaus. Cum concluzia este evident falsă, este vorba de un paradox din domeniul logicii.

Bibliografie:

<https://www.scientia.ro/stiinta-la-minut/110-matematica/1477-paradoxurile-lui-zenon.html>
https://ro.wikipedia.org/wiki/Paradoxurile_lui_Zenon

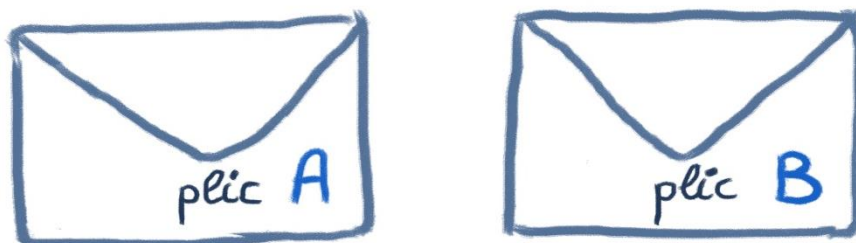
Paradoxul plicului

Bîja Alexandra și Albescu David

Ni se prezintă două plicuri de formă identică, ambele închise și sigilate, astfel încât este imposibil să le vedem conținutul, și trebuie să alegem unul dintre ele. Ni se spune că **fiecare plic are o anumită sumă de bani**, iar suma din unul dintre plicuri (nu ni se spune care dintre ele) este **dublul sumei din celălalt plic** (să presupunem și că banii sunt sub formă de verificați, deci și plicurile sunt aceleași ca greutate și volum)

Deoarece este imposibil să știm câți bani sunt în fiecare dintre plicuri, alegerea noastră pentru unul dintre ele este **aleatorie**. Totuși, imediat după alegerea unuia dintre plicuri, ni se oferă opțiunea de a schimba între ele, adică de a returna plicul pe care l-am ales și de a primi plicul în locul lui celălalt, în care există, desigur, fie **o sumă de bani dublă** decât cea pe care o avem acum, fie **doar jumătate din această sumă**.

Ar trebui să efectuăm schimbul sau rămănem cu alegerea noastră inițială?



a) alegem să nu schimbăm plicurile

Presupunem ca alegem plicul A în valoare de x lei prin urmare în plicul B putem avea suma de $2x$ lei sau suma de $x/2$ lei.

Am câștigat: x lei puteam câștiga: încă o suma de x lei și puteam pierde: $x/2$ lei. Concret dacă în plic se aflau 100 de lei noi am câștigat 100 de lei dar puteam câștiga 200 de lei și pierdeam doar 50 de lei

b) alegem să schimbăm plicurile

Presupunem că alegem plicul A în valoare de x lei și îl schimbăm pentru plicul B care poate avea suma de $2x$ lei sau suma de $x/2$ lei.

Astfel am câștigat 200 de lei fie am pierdut 50 de lei

În concluzie, dacă ar fii să schimbăm plicul am pierde 50 de lei dar am putea câștiga încă 100 plecând de la suma de 100 din plic.

Bibliografie:

<https://www.ynet.co.il/articles/0,7340,L-3460198,00.html>

<https://mikyab.net/ro/posturi/65903>

Paradoxul spânzuratului

Bîja Alexandra și Albescu David

Un judecător îl anunță pe condamnat că va fi spânzurat într-una din zilele lucrătoare din săptămâna următoare, însă execuția îl va lua prin surprindere pe prizonier. Nu va ști ziua în care va fi spânzurat până când un gardian va veni la ușă să și îl ducă la spânzurătoare. Gîndindu-se la ceea ce a spus judecătorul, prizonierul se retrage bucuros în celula sa, fiind sigur că nu va fi spânzurat. Săptămîna următoare, miercuri, gardianul bate la ușă și îl ducă pe prizonier la spânzurătoare. De ce era prizonierul sigur că nu va fi spânzurat?

Acest prizonier nu poate să moară.

Prizonierul s-a gîndit că execuția nu ar putea fi vineri, pentru că, dacă nu a fost spânzurat pînă joi, ar mai fi doar o zi posibilă, prin urmare nu ar mai fi o surpriză pentru el ziua execuției. Din moment ce judecătorul a zis că ziua execuției va fi o surpriză pentru el, este sigur că vineri nu va fi executat. Apoi se gîndește că joi nu poate fi spânzurat pentru că dacă pînă miercuri nu a fost executat iar vineri nu are cum să fie executat, ar mai fi doar o zi posibilă - joi, însă nu ar mai fi o surpriză pentru el.

Pe același considerent elimină și zilele de miercuri, marți și luni, prin urmare se întoarce vesel în celulă, sigur că nu va fi executat.



Bibliografie: www.diseara.ro

Problema lui Monty Hall

Penteleiciuc Maria-Lavinia, Fleacă Anastasia Maria și Orza Anamaria

Problema Monty Hall (sau paradoxul lui Monty Hall) este o faimoasă problemă a teoriei probabilității legată de jocul cu premii "SUA Let's Make a Deal". Își ia numele de la cel al gazdei spectacolului, Maurice Halprin, cunoscut sub pseudonimul de Monty Hall. Problema este cunoscută și sub numele de paradoxul Monty Hall, deoarece soluția poate părea contraintuitivă, dar nu este o adevărată antinomie, deoarece nu generează contradicții logice.

În joc, trei uși închise sunt prezentate concurentului; în spatele uneia este o mașină, în timp ce fiecare dintre celelalte două ascunde o capră. Jucătorul poate alege una dintre cele trei uși, câștigând premiul corespunzător. După ce jucătorul a selectat o ușă, dar nu a deschis-o încă, gazda spectacolului - cel ce știe ce se află în spatele fiecărei uși - deschide una dintre celelalte două, dezvăluind una dintre cele două capre și îi oferă jucătorului șansa de a-și schimba inițiala alegere, trecând la singura ușă rămasă; schimbarea ușii îmbunătățește șansele jucătorului de a câștiga mașina, crescând de la $1/3$ la $2/3$.



Cei mai mulți oameni consideră că opțiunea de a schimba ușa nu contează pentru că probabilitatea de a alege mașina este 50/50. Acest lucru ar fi adevărat dacă gazda ar deschide o ușă la întâmplare, dar nu este cazul; ușa deschisă depinde de opțiunea inițială a participantului, deci nu este o alegere independentă.

Înainte ca gazda să deschidă o ușă probabilitatea ca mașina să fie în spatele oricărei uși este de $1/3$. Dacă mașina este în spatele primei uși, gazda poate deschide fie ușa a doua, fie ușa a treia, deci probabilitatea ca mașina să fie în spatele primei uși și gazda să deschidă ușa a treia este $1/3 * 1/2 = 1/6$. Dacă mașina este în spatele ușii a doua (și participantul a ales prima ușă), gazda trebuie să deschidă ușa a treia, deci probabilitatea ca mașina să fie în spatele celei de-a doua uși și gazda să deschidă ușa a treia este de $1/3 * 1 = 1/3$. Acestea sunt singurele situații în care gazda deschide ușa a treia, deci dacă participantul a ales prima ușă și gazda deschide ușa a treia, este de două ori mai probabil ca mașina să fie în spatele ușii a doua. Esența problemei este că dacă mașina este în spatele ușii a doua, gazda trebuie să deschidă ușa a treia, dar dacă mașina se află în spatele primei uși, gazda poate deschide oricare din celelalte două.

Pentru a înțelege de ce probabilitatea câștigării automobilului crește prin schimbarea opțiunii inițiale, un instrument ajutător este înmulțirea numărului ușilor dintre care se poate alege de la 3 la 100. Inițial gazda oferă posibilitatea alegerii unei singure uși dintr-un total de 100, deci probabilitatea ca premiul cel mare să se afle acolo este una dintr-o sută, adică 1%, iar probabilitatea ca el să nu se afle acolo este de 99%. În următorul pas, gazda, care știe ce e în spatele ușilor, deschide toate celelalte uși necâștigătoare cu excepția uneia dintre ele, rămânând astfel numai 2 uși închise, cea aleasă inițial de concurent și cea lăsată de gazdă în mod conștient de conținutul ei. Deși mai sunt doar 2 uși închise, probabilitatea pentru fiecare dintre ele de a fi cea câștigătoare, în mod evident, nu este egală. Singurul caz în care ușa lăsată de gazdă ar fi necâștigătoare, ar fi acela în care concurentul ar fi nimerit din prima încercare ușa câștigătoare, iar probabilitatea ca acest lucru să se fi întâmplat este de 1%, deci în proporție de 99% sigur ușa câștigătoare este cea lăsată de gazdă.

Aceeași logică se aplică și în cazul variantei cu numărul minim de uși în care jocul este posibil, adică trei, doar că în acest caz numărul redus de uși creează impresia că probabilitatea pentru cele două uși rămase, de a fi câștigătoare, este de 50%, când de fapt este de 33,3% față de 66,6% (sau $1/3$ față de $2/3$).

Vos Savant a comentat spunând că deși anumită confuzie a fost cauzată de faptul că unii cititori nu au realizat că trebuie să presupună că gazda trebuie să dezvăluie întotdeauna o capră, aproape toți numeroșii ei corespondenți au înțeles corect presupunerile problemei, și încă erau convinși inițial că răspunsul acesteia, acela de a schimba ușa, era greșit.

Paradoxul prieteniei

Penteleiciuc Maria-Lavinia, Fleacă Anastasia Maria
și Orza Anamaria

Paradoxul prieteniei este o observație empirică potrivit căreia prietenii tăi au mai mulți prieteni decât tine. Acum, oamenii de știință susțin că este foarte probabil ca prietenii tăi să fie și mai bogați și mai fericiți ca tine.

În 1991, sociologul Scott Feld a realizat o descoperire surprinzătoare în timp ce studia proprietățile rețelelor sociale. Feld a calculat numărul mediu de prieteni pe care îi avea o persoană din rețea și a comparat cifrele cu numărul mediu de prieteni pe care îi aveau, la rândul lor, prietenii lor. În ciuda așteptărilor s-a constatat că cel de-al doilea număr este mai mare mereu decât primul. Sau, cu alte cuvinte, prietenii tăi au mai mulți prieteni decât tine.

Young-Ho Eom de la Universitatea din Toulouse, Franța, și Hang-Hyun Jo de la Universitatea Aalto, Finlanda, au investigat în acest domeniu pentru a descoperi dacă paradoxul prieteniei se poate aplica și în ceea ce privește numărul de prieteni ai prietenilor tăi, fericirea sau bogăția acestora. Ei au ajuns la concluzia că oamenii care au mulți prieteni au o probabilitate mai mare de a fi și prietenii tăi. Atunci când fac asta, ei cresc numărul mediu de prieteni pe care îi au prietenii tăi. De aceea, în medie, prietenii tăi au mai mulți prieteni decât tine. Ei au constatat de asemenea că, în mod probabil, ei sunt mai fericiți și mai bogați decât tine.



Bibliografie:

<https://www.descopera.ro/dnews/11905223-paradoxul-prieteniei-de-ce-prietenii-tai-o-duc-mai-bine-ca-tine>

<https://pariurix.com/casino/despre-cazino/monthly-hall-problema-pe-care-putini-stiu-sa-o-rezolve-corect.html#gref>

https://ro.m.wikipedia.org/wiki/Problema_lui_Monty_Hall

<https://destepti-ro.cdn.ampproject.org/v/s/destepti.ro/probleme-de-matematika-amuzante-paradoxul-lui-monty->

[hall?amp=1&_gsa=1&_js_v=a9&usqp=mq331AQKKAFQArABIICAw%3D%3D#amp_tf=De%20la%20%251%24s&aoh=16590965859422&referrer=https%3A%2F%2Fwww](https://destepti-ro.cdn.ampproject.org/v/s/destepti.ro/probleme-de-matematika-amuzante-paradoxul-lui-monty-hall?amp=1&_gsa=1&_js_v=a9&usqp=mq331AQKKAFQArABIICAw%3D%3D#amp_tf=De%20la%20%251%24s&aoh=16590965859422&referrer=https%3A%2F%2Fwww)

[.google.com&share=https%3A%2F%2Fdestepti.ro%2Fprobleme-de-matematika-amuzante-paradoxul-lui-monty-hall](https://destepti-ro.cdn.ampproject.org/v/s/destepti.ro/probleme-de-matematika-amuzante-paradoxul-lui-monty-hall)

https://koaha.org/wiki/Problema_di_Monty_Hall

<https://www.infoarena.ro/the-monty-hall-problem>

<https://semneletimpului-ro.cdn.ampproject.org/v/s/semneletimpului.ro/social/paradoxul-prieteniei-stiinta-din-spatele->

[popularitatii.html/amp?amp_gsa=1&_js_v=a9&usqp=mq331AQKKAFQArABIICAw%3D%3D#amp_tf=De%20la%20%251%24s&aoh=16590968395230&referrer=https%3A%2F%2Fwww.google.com&share=https%3A%2F%2Fsemneletimpului.ro%2Fsocial%2Fpar](https://semneletimpului-ro.cdn.ampproject.org/v/s/semneletimpului.ro/social/paradoxul-prieteniei-stiinta-din-spatele-popularitatii.html/amp?amp_gsa=1&_js_v=a9&usqp=mq331AQKKAFQArABIICAw%3D%3D#amp_tf=De%20la%20%251%24s&aoh=16590968395230&referrer=https%3A%2F%2Fwww.google.com&share=https%3A%2F%2Fsemneletimpului.ro%2Fsocial%2Fparadoxul-prieteniei-stiinta-din-spatele-popularitatii.html)

[adoxul-prieteniei-stiinta-din-spatele-popularitatii.html](https://semneletimpului-ro.cdn.ampproject.org/v/s/semneletimpului.ro/social/paradoxul-prieteniei-stiinta-din-spatele-popularitatii.html)

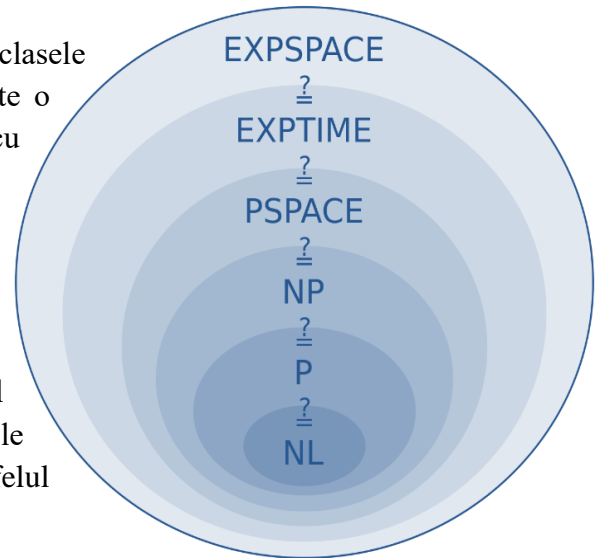
https://ro.frwiki.wiki/wiki/Paradoxe_de_1%27amiti%C3%A9



Problema claselor de complexitate P și NP

Iagăru Dragoș și Dospinescu Tudor

Problema ține strict de informatică teoretică și de clasele de complexitate P și NP. O clasă de complexitate este o mulțime formată din probleme ce pot fi rezolvate cu ajutorul unui algoritm cu complexitate asemănătoare. Complexitatea este măsurată în funcție de resursele necesare pentru funcționarea algoritmului (cele mai importante fiind timpul necesar rezolvării problemei și memoria din calculator utilizată). Studiul relațiilor dintre clasele de complexitate reprezintă un capitol important din informatica teoretică. Până acum, relațiile dintre clasele de complexitate au fost acceptate în felul următor:

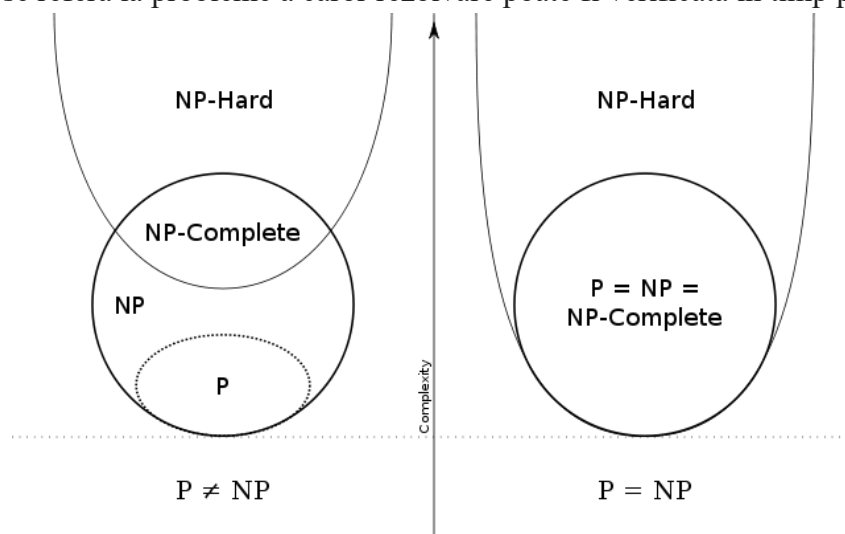


$NL \subseteq P \subseteq NP \subseteq PSPACE \subseteq EXPTIME \subseteq EXPSPACE$.

Această problemă implică clasele **P** și **NP**, întrebarea fiind dacă cele două mulțimi sunt egale.

Clasa P se referă la probleme care se pot rezolva în timp polinomial („repede”). O problemă se poate rezolva în timp polynomial dacă timpul în care algoritmul rulează este mărginit superior (nu depășește) o expresie polinomială. O expresie polinomială este orice expresie care implică variabile, coeficienți și se folosește doar de operațiile de adunare, scădere, înmulțire, împărțire și ridicare la putere. Adică $T(n) = O(n^k)$, $T(n)$ fiind timpul în care a fost rezolvată problema.

Clasa NP se referă la probleme a căror rezolvare poate fi verificată în timp polinomial.



Așadar, întrebarea devine: „Toate probleme care se pot verifica în timp polinomial se pot și rezolva în timp polinomial?”. Problema este una din cele șapte „Probleme ale mileniului” care valorează 1.000.000\$ pentru prima rezolvare corectă.

Principiul rezolvării acestui paradox se bazează pe noțiunea de „**NP-complet**”:

Există o noțiune care include clasa NP denumită „**NP-tari**” cu proprietatea că aceste probleme sunt cel puțin la fel de complexe ca toate problemele din NP. Pe scurt, „**NP-tari**” includ cele mai grele probleme din NP, pe lângă alte probleme și mai grele, dar care tot pot fi verificate în timp polinomial. O problemă „**NP-completă**” este o problemă care este și „**NP-tare**” dar și NP în același timp. Astfel, o rezolvare în timp polinomial la o problemă NP-completă ar duce la rezolvarea în timp polinomial al tuturor problemelor din NP, ceea ce ar dovedi că $\mathcal{P} = \mathcal{NP}$, iar o demonstrație contradictorie ar duce la $\mathcal{P} \neq \mathcal{NP}$.

Posibile consecințe:

De-a lungul timpului, majoritatea cercetătorilor acceptă noțiunea că $\mathcal{P} \neq \mathcal{NP}$. O rezolvare contradictorie a problemei ar avea mari consecințe. $\mathcal{P} = \mathcal{NP}$ ar duce la metode eficiente de rezolvare a tuturor problemelor din NP, având un mare impact asupra domeniilor care au la bază probleme NP-complete, precum criptografia. Găsirea soluțiilor a problemelor NP în timp polinomial ar duce la distrugerea majorității sistemelor de criptare, acestea având nevoie să fie înlocuite. Consecințele demonstrării că $\mathcal{P} \neq \mathcal{NP}$ nu ar fi la fel de mari, având în vedere că aceasta este concluzia așteptată. Totodată, acest rezultat ar duce la un progres în informatica teoretică.

Bibliografie:

- <https://www.britannica.com/science/P-versus-NP-problem>
- <https://www.claymath.org/sites/default/files/pvsnp.pdf>
- https://en.wikipedia.org/wiki/P_versus_NP_problem
- https://en.wikipedia.org/wiki/Complexity_class

Algoritmul RSA

Radu Andra

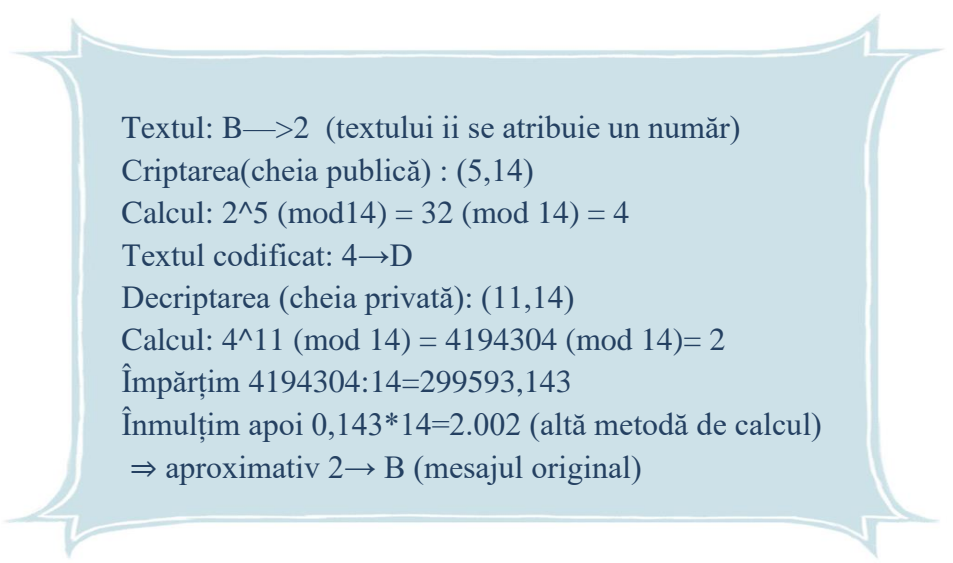
RSA este unul dintre cei mai vechi algoritmi criptografici și primul algoritmul folosit atât pentru criptare, cât și pentru semnătura electronică. Algoritmul a fost dezvoltat în 1977 și publicat în 1978 de Ron Rivest, Adi Shamir și Leonard Adleman la MIT, fiind denumit mai apoi după aceștia.

RSA este un algoritm *asimetric*, adică folosește chei diferite (set de numere întregi) pentru criptare și decriptare. Astfel, pentru a cripta un mesaj se folosește o **cheie publică**, iar pentru decriptarea informației confidențiale o **cheie privată**.

Luând un exemplu pentru a înțelege rolul cheilor, dacă Alice dorește să îi trimită un mesaj lui Bob și nu dorește ca altcineva decât Bob să-l citească, Alice va afla cheia publică a lui Bob și cu aceasta poate cripta mesajul. Deoarece Bob este singurul care are cheia privată (prin urmare capabil să decripteze mesajul criptat cu cheia publică), el va fi și singurul care poate decripta mesajul, nici Alice neputând să decripteze mesajul fiindcă nu deține cheia privată a lui Bob.

De asemenea, prin această metodă de criptare se poate garanta și originea unui mesaj. În cazul exemplului anterior: presupunem că Alice, înainte de a cripta mesajul folosind cheia publică a lui Bob, îl va cripta folosind propria cheie privată și abia ulterior o va recifra folosind cheia publică a lui Bob. Când Bob primește mesajul și îl decriptează folosind cheia sa privată, va primi totuși un mesaj criptat. Acest mesaj dat va avea nevoie apoi de decriptarea cheii publice a lui Alice, asigurându-se astfel că mesajul a fost trimis doar de Alice, singura care are cheia privată cu care a fost criptat mesajul.

Exemplu pentru a înțelege partea matematică din modul de funcționare a criptării și decriptării informației:



Textul: B → 2 (textului îi se atribuie un număr)
Criptarea (cheia publică) : (5, 14)
Calcul: $2^5 \pmod{14} = 32 \pmod{14} = 4$
Textul codificat: 4 → D
Decriptarea (cheia privată): (11, 14)
Calcul: $4^{11} \pmod{14} = 4194304 \pmod{14} = 2$
Împărțim $4194304 : 14 = 299593, 143$
Înmulțim apoi $0,143 * 14 = 2,002$ (altă metodă de calcul)
⇒ aproximativ 2 → B (mesajul original)

Cum am știut ce cheie privată era nevoie pentru cheia publică din exemplu?

RSA se bazează pe complexitatea de calcul ridicată a factorizării prime. Funcționarea sa redusă la un nivel de bază este următoarea:

Se aleg două numere prime aleatoriu, **P** & **Q** suficient de mari pentru a asigura securitatea algoritmului; pt ex: $P=2$ $Q=7$

Calculăm produsul lor $N=P*Q$, denumit *modulo* sau *modul de criptare*; pt ex: $N=2*7=14$

Calculăm *funcția phi/ indicatorul Euler* $\varphi(N) = (P-1)*(Q-1)$ (este valoarea indicatoarei Euler în **N**); pt ex: numărul de numerele prime cu 14, mai mici decât 14 este 6 (1,3,5,9,11,13); $6=1*6=(2-1)*(7-1)$

Alegem un număr natural **E**, prim cu $\varphi(N)$, mai mare decât 1 și mai mic decât $\varphi(N)$, numit *exponent de criptare* sau *exponent privat*; pt ex: $E \in \{2,3,4,5\}$ && $\text{cmmdc}(E, 6)=1 \Rightarrow E=5 \Rightarrow$ avem astfel cheia de criptare

Calculăm numărul **D**, denumit *exponent privat* sau *exponent de decriptare*, astfel încât

$$D * E \pmod{\varphi(N)} = 1;$$

$$\text{pt ex: } 5 * D \pmod{6} = 1 \Rightarrow D \in \{5, 11, 17, \dots\}$$

Putem alege oricare dintre aceste valori, însă în exemplu am ales $D=11$.

Rezultă că avem astfel ambele chei (5,14) și (11,14)


```

file:///D:/Works/git/RSA-csharp/bin/Debug/RSA.EXE
-----
RSA测试
-----
【512私钥 (XML)】:
<RSAKeyValue><Modulus>x1b+X/UFeyaSPUWnbqk8u6oIF6LPQvof9cg9XGy6Zuukc80cvkDNXBFovu
vU58BGiYHDMSFdMS5LEwbPSRA1dw==</Modulus><Exponent>AQAB</Exponent><P>7hYpKf1CFpN6
sSPt19ULN0c7ptHhAB/d03Z0z4/uc98=</P><Q>1laF43G6BXjw8zDdMVx18tWY9jWsSs+ZvQgj3o6LM
Wk=</Q><DP>UG50IZXvWakg/c7haTXJXmnvoP+uP1iEaJ4wAB7js4k=</DP><DQ>kt/UfacX7toSWsOY
P3Td+1puKAfdoCIkWomycrbBIUk=</DQ><InverseQ>aX13qHd+XLAIfdUDtZUFUm1IAT5Ihhe+cCZ/
EifIZ0=</InverseQ><D>gBCrrApvLjaBjUvKnZwspwQ93rGCZo07KzRR96cCuktW2ju9rM1dAMqzyUs
hhBy7NNOo9N2QPRgBvcPjFHFwQ==</D></RSAKeyValue>

【512私钥 (PEM)】:
-----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBAMdW/1/1RRMmkj1Fp26pPLuqCBeiz0L6H/XIPUxsumbrpHPNHL5A
zUwX6L7r1OfARomBwzEhXTEuSxMGz0kQNXcCAwEAAQJBAIAQg6wKby42gY1Lyp2U
rKcEPd6xgmaN0ys0UfenArpLUto7vazJXQDKs81bIYQcuzTtqMjdkD0YA b3KYxRx
UoECIQDuFikp+UIWk3qxI+2X1Us05zum0eEAH907dnTPj+5z3wIhANZWheNkxugU4
8PMw3TGMdfLUmPY1rErPmb0II960izFpAIBQbnQh1e9ZqSD9zuFpNc1eae+g/64/
WIRonjAaHuOziqIhAJLf1X2nF+7aElrDmD903fpabigBxaaiJFqJsnK2wSFJAiBo
Bcjeod35csAh91U03NQUWauGbpkiGF75wJn8Sj8hnQ==
-----END RSA PRIVATE KEY-----

【512公钥 (PEM)】:
-----BEGIN PUBLIC KEY-----
MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAMdW/1/1RRMmkj1Fp26pPLuqCBeiz0L6
H/XIPUxsumbrpHPNHL5AzUwX6L7r1OfARomBwzEhXTEuSxMGz0kQNXcCAwEAAQ==
-----END PUBLIC KEY-----

【加密】:
ZMu9GNLcNgt82fCTmeoqa8LIWtzZTwmLd4dC/AdxtnaWfDhSh7E5HC0e1WU16TfKCLmCqvH5FC23YGmh
93N3sQ==
【解密】:
abc内容123
【签名SHA1】:
J1mu8l0qzqh/9PmTB/2K2FO+SZRMWz39SyiG+dX8QT0vcWn70qXUQZwdn1MP4UXi5ya9jEgfucA1idqi
cXoTCA==

【用PEM新创建的RSA是否和上面的一致】:
XML: True
PKCS1: True
PKCS8: True
【用XML新创建的RSA是否和上面的一致】:

```

În general totuși, deoarece se bazează pe o operație complexă din punct de vedere al timpului de calcul și al resurselor folosite viteza algoritmului RSA este mult mai mică decât a altor algoritmi de criptare, cel mai des fiind astfel folosiți algoritmi simetrici.

Aceasta este o imagine pentru a înțelege cum arată în realitate cheile criptografice:

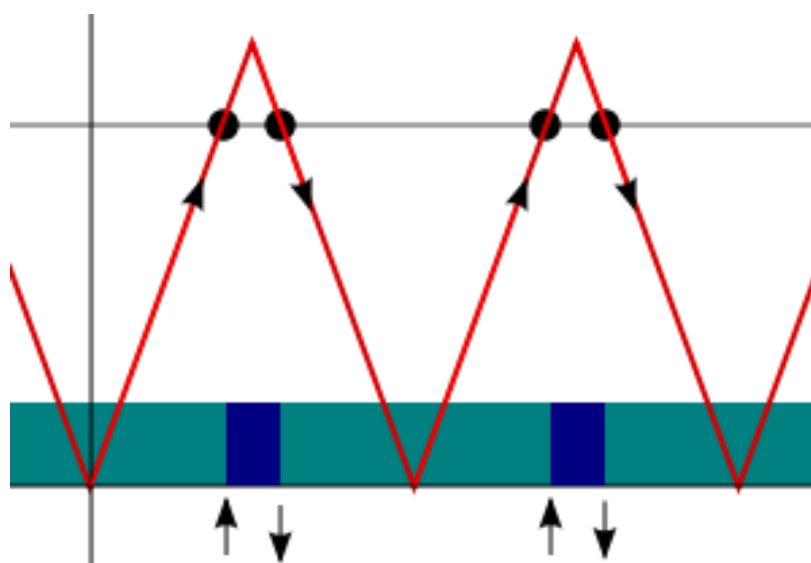
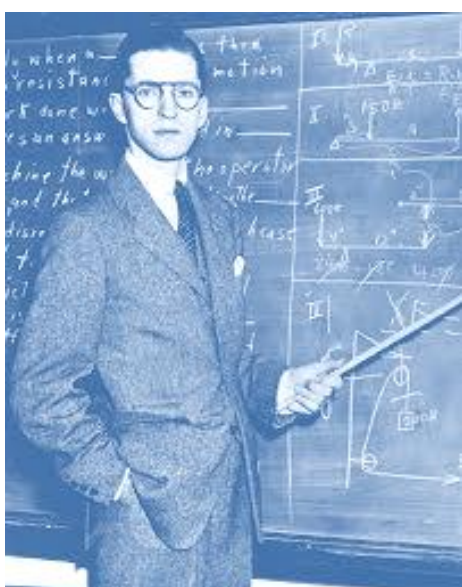
Bibliografie:

- <https://www.geeksforgeeks.org/rsa-algorithm-cryptography/>
- [https://en.wikipedia.org/wiki/RSA_\(cryptosystem\)?wprov=sfti1](https://en.wikipedia.org/wiki/RSA_(cryptosystem)?wprov=sfti1)
- <https://itigic.com/ro/cryptography-symmetric-and-asymmetric-key-algorithms-explained/>
- <https://youtu.be/oOcTVTPUsPQ>
- <https://youtu.be/-0slxSL9B6A>
- https://www.tutorialspoint.com/cryptography_with_python/cryptography_with_python_understanding_rsa_algorithm.htm

Paradoxul ascensorului

Alexandru Alexandrov, Crețu Victor și Junger Ernest

Doi fizicieni pe nume George Gamow și Marvin Stern, aveau birourile în aceeași clădire (unul având birou la primul etaj și celălalt la penultimul etaj). La un moment dat, aceștia au observat ceva ciudat la mișcarea ascensoarelor: Marvin Stern, cel ce avea biroul în vârful clădirii, a observat că ascensorul venea de fiecare dată de jos, iar Gamow a văzut opusul, fiind la primul etaj, a observat ca liftul venea mereu de sus.

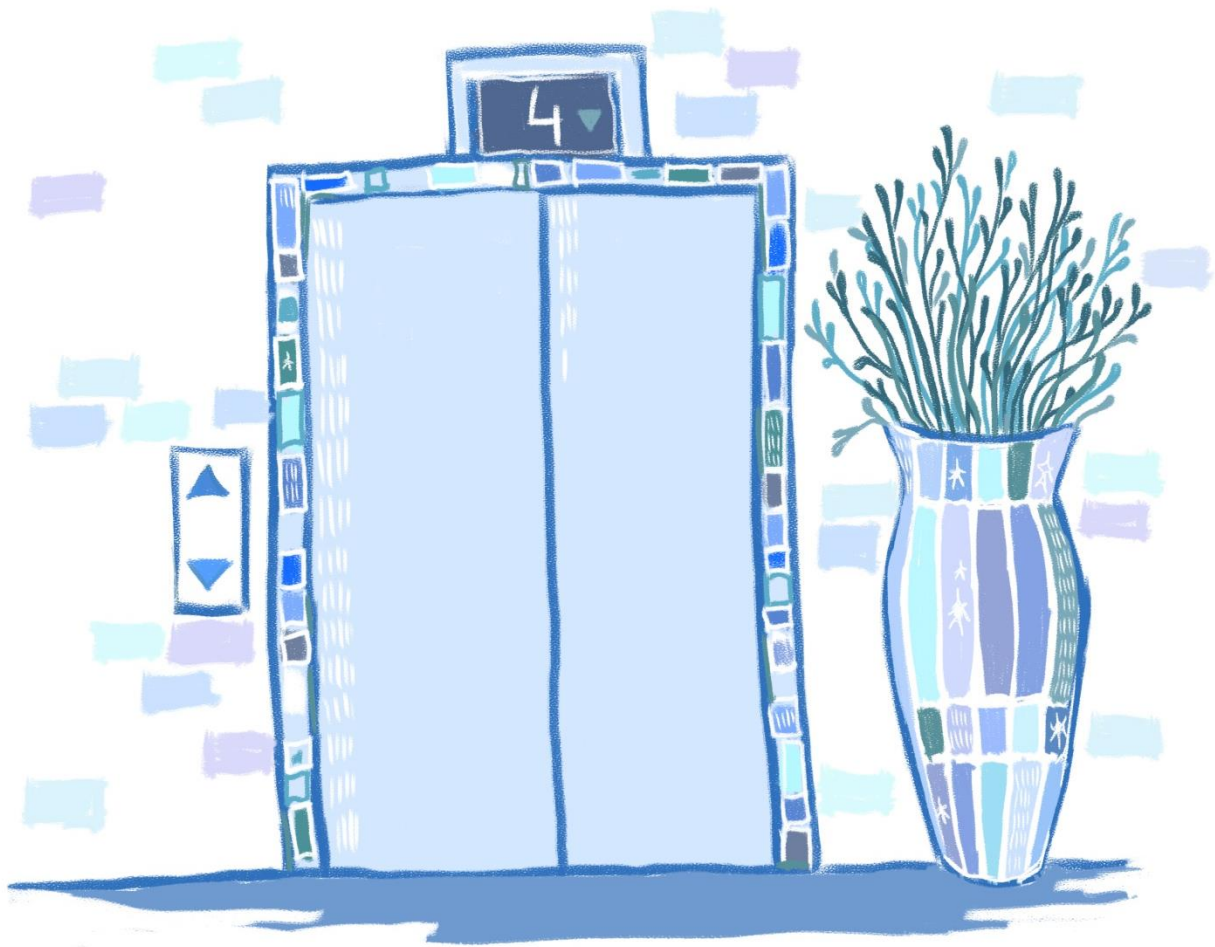


Acea observație a savanților a fost denumită “Paradoxul ascensorului” și este până și astăzi o problemă destul de cunoscută. Acest paradox descrie fenomenul prin care ascensorul pare să meargă într-o singură direcție, ca și acum acesta ar fi fost asamblat la mijlocul clădirii și dezasamblat în vârf sau la subsolul clădirii.

Interesant, în ciuda aparent simplă, această observație a fost dovedită falsă de către Donald Knuth în 1969 printr-un exemplu pe care l-ar înțelege și un preșcolar.

Exemplul dat a fost următorul: “Să presupunem că locuiți la penultimul etaj al unei clădiri cu șapte etaje; apelând liftul de acolo, va veni mai des (aproximativ 5/6 din timp) de jos decât de sus. Acest fenomen este ușor de explicat: liftul este utilizat în mod egal de chiriașii de la diferitele etaje și, prin urmare, petrece mai mult timp pe primele 5 etaje decât pe ultimul.

Într-un hotel mare, întotdeauna cu 7 etaje, dar cu 5 ascensoare în loc de unul, toate cele 5 utilizate într-un mod nediferențiat de oaspeții diferitelor etaje, fenomenul va fi aproape dispărut.



Dacă ați fi la primul etaj atunci cele mai mari șanse ar fi ca ascensorul să vină de sus deoarece sus sunt mai multe nivele decât jos. Același principiu îl putem aplica și unei persoane care așteaptă liftul la etajul 28 sau 29. Însă, dacă ar fi mai mult de un lift în acea clădire tendința scade - deoarece există o șansă mai mare ca o persoană care intenționează să urce în lift are deja un lift la un etaj inferior. Iar, pentru a avea o perspectivă mai simplă, cu un infinit număr de lifturi am avea probabilități egale.

Bibliografie:

https://en.wikipedia.org/wiki/Elevator_paradox
[https://wikicro.icu/wiki/Elevator_paradox_\(physics\)](https://wikicro.icu/wiki/Elevator_paradox_(physics))
https://koaha.org/wiki/Paradosso_dell%27ascensore

Paradoxul bibliotecarului

Apostol Vlad

Paradoxul bibliotecarului este o altă versiune a paradoxului lui Russell, datorată filosofului și matematicianului francez Ferdinand Gonseth.

Managerului unei mari biblioteci i se încredințează sarcina de a produce cataloagele corespunzătoare. Mai întâi cataloghează după titluri, apoi după autori, apoi pe subiecte, apoi după numărul de pagini și așa mai departe. Pe măsură ce cataloagele se înmulțesc, bibliotecarul nostru pregătește catalogul tuturor cataloagelor. În acest moment apare o observație. Majoritatea cataloagelor nu se raportează singure, dar există unele (cum ar fi catalogul tuturor volumelor cu mai puțin de 5000 de pagini, catalogul tuturor cataloagelor etc.) care se raportează singure. Dintr-un exces de zel, bibliotecarul scrupulos decide, în acest moment, să construiască *catalogul tuturor cataloagelor care nu se includ*. A doua zi, după o noapte nedormită petrecută la îndoială dacă acest nou catalog ar trebui sau nu să se includă, bibliotecarul nostru cere să fie eliberat din misiune.

Se poate observa că prima traducere glumă a antinomiei lui Russell, cea a așa-numitului paradox al frizerului, nu dă naștere unui adevărat paradox logic: faptul că relația „bărbierit ...” este definită pentru toți locuitorii al insulei, cu excepția frizerului, nu diferă de faptul că, în număr real, proprietatea „având un număr invers” este valabilă pentru toate, cu excepția zero.

Observă EW Beth: "Dilema [frizerului] nu constituie o dilemă pentru logică. De fapt, ipoteza că una sau cealaltă regulă de drept are consecințe absurde nu este în sine absurdă. Un astfel de eveniment poate ridica probleme serioase de drept [...] dar nu dă naștere la probleme logice". O altă versiune a paradoxului este cea a bibliotecii infinite, în care există și volume scrise niciodată despre lucruri niciodată gândite sau care nu au existat niciodată și care include, și mai paradoxal, și *catalogul tuturor cataloagelor care nu se includ pe ele însele*.

De altfel, se amintește că atât Jorge Luis Borges, cât și Umberto Eco au scris despre paradoxul bibliotecarului. Primul din povestea *Biblioteca lui Babel*, cuprins în volumul *Finzioni*, și cu diverse aluzii în textele de pe *Uqbar*, al doilea citând primul din *De Bibliothec*.



Bibliografie: https://koaha.org/wiki/Paradosso_del_bibliotecario

Paradoxul infinitului

(Georg Cantor)

Iacob Diana și Timofte Ana

Georg Cantor a fost un matematician german. Acesta a creat teoria mulțimilor, care a devenit o teorie fundamentală a matematicii.

Conform teoriei numerelor infinite a lui Cantor, mulțimile de numere naturale, întregi și rationale au aceleași număr de elemente, și anume, o infinitate (alef zero). Acestora li se poate aplica o „corespondență biunivocă”, care demonstrează egalitatea infinitelor dintre mulțimile anterior menționate. Astfel se naște ideea de mulțime numărabilă, adică elementele acesteia au un corespondent în mulțimea numerelor naturale.

Numere întregi		Numere naturale
0	\leftrightarrow	0
-1	\leftrightarrow	1
1	\leftrightarrow	2
-2	\leftrightarrow	3
2	\leftrightarrow	4
...	\leftrightarrow	...
-n	\leftrightarrow	2n-1
n	\leftrightarrow	2n

Mulțimea numerelor întregi este numărabilă deoarece putem număra (cu numere naturale) elementele acesteia. Atât mulțimea numerelor naturale cât și cea a numerelor întregi au o infinitate de elemente.

Întrebarea este, cum ar putea două infinite să fie inegale? Folosind metoda reducerii la absurd și metoda liniei diagonale care s-a născut chiar în timpul acestei demonstrații, Cantor a realizat că mulțimea numerelor reale este mai mare decât infinitul standard al celorlalte mulțimi.

Presupunem că mulțimea numerelor reale este numărabilă, deci, ar trebui ca toate numerele reale de la 0 la 1 să aibă un corespondent în mulțimea numerelor naturale. (metoda reducerii la absurd)

Facem o corespondență biunivocă între numerele naturale și cele reale (absolut toate numerele incluse).

0	0,12345...
1	0,34566...
2	0,82635...
3	0,42410...
4	0,92754...
...	...
∞	∞
0, 25725... (de la 0, 14614... de pe diagonală)	

Acum cream un nou număr real (prin metoda diagonalei) punându-i drept zecimale cifrele de pe diagonală ale numerelor cu o infinitate de zecimale și schimbându-le (putem aduna sau scădea 1 cum am făcut mai sus). Astfel, noul număr va fi diferit de toate cele precedente cu cel puțin o zecimală.

Problema este că a apărut un nou număr real ,tot între 0 și 1, dar diferit de toate cele precedente, deci care nu aparține tabelului. Paradoxal, în tabel au fost însă trecute toate valorile posibile dintre 0 și 1.

Explicația lui Cantor este că numerele reale sunt **non-numărabile**, deci fără corespondent în tabel (nu se stabilește corespondența biunivocă), iar infinitatea lor este mai mare decât infinitatea numerelor naturale.

$$\infty\mathbb{N} < \infty\mathbb{R}$$

Paradoxul Hiperjocului (William Seymour Zwicker)

William Seymour Zwicker este un matematician American, cunoscut pentru studiile realizate în domenii precum Teoria mulțimilor și Teoria alegerii sociale. El este creditat cu inventarea conceptului de Paradox al hiperjocului.

Definiții:

Un joc G este de *lungime finită* dacă satisface următoarele condiții:

- G este un joc cu 2 jucători, în care Jucătorul 1 și Jucătorul 2 alternează rândul. Fiecare jucător cunoaște mișcările celuilalt.
- G nu este un joc de noroc, ci de strategie.
- De fiecare dată când este jucat, G se termină după un număr finit de mișcări.

Exemple de jocuri de lungime finită:

- Șah
- Dame
- X și 0

Hiperjocul

Hiperjocul este un joc de *lungime finită*, care are următoarele reguli:

1. Hiperjocul începe cu jucătorul 1 care alege un joc, G , din mulțimea ce conține toate jocurile finite.
2. Jucătorul 2 începe apoi să joace G , ca prim jucător, cu Jucătorul 1 ca al doilea jucător.
3. Hiperjocul se termină când se termină G .

Teoretic, hiperjocul este un joc de *lungime finită*, deoarece doar adaugă o nouă mișcare la un joc de lungime finită. Dacă hiperjocul are o lungime finită, înseamnă *că și acesta face parte din mulțimea jocurilor de lungime finită*. Însă dacă hiperjocul face parte din această mulțime, înseamnă că Jucătorul 1 poate să aleagă să joace hiperjocul. După aceea, Jucătorul 2, primind rolul primului jucător al hiperjocului, poate la rândul său să aleagă tot hiperjocul. Apoi, Jucătorul 1, devenit din nou primul jucător al hiperjocului, poate să aleagă din nou hiperjocul. *Acest ciclu poate continua la infinit*, însă asta înseamnă că hiperjocul *nu* are de fapt o lungime finită, și atunci nu poate aparține mulțimii jocurilor de lungime finită.

Așa apare un paradox: hiperjocul este și nu este în același timp inclus în mulțimea jocurilor de lungime finită.

Similarități cu paradoxul infinitului al lui Cantor

Observăm cum mulțimea jocurilor finite este o mulțime numărabilă (oricât de multe jocuri finite există, le putem da o etichetă, un indice). Hiperjocul, seamănă cu noul număr creat cu metoda diagonalei în mulțimea numerelor reale – ar trebui să facă parte din mulțimea numărabilă, însă apariția lui stârnește paradoxul. Așadar, putem înțelege Hiperjocul dacă îl clasificăm într-o altă mulțime de jocuri, una non-numărabilă, care conține și acest tip de joc (finit în anumite cazuri, infinit în altele).

Bibliografie

https://ro.m.wikipedia.org/wiki/Georg_Cantor

Mintea noastră cea de toate zilele – Roger Penrose

<https://youtu.be/OxGsU8oIWjY>

<https://youtu.be/OxGsU8oIWjY>

<https://blogs.ams.org/mathgradblog/2021/12/10/the-hypergame-paradox/>

<https://www.youtube.com/watch?v=0rpXDbO-RZ8>

https://en.wikipedia.org/wiki/William_S._Zwicker

Paradoxul Liniei și Zonei Disparute

Țeposu Vlad și Ihora Vlad

Ambele sunt de fapt mai mult iluzii optice ușor explicabile decât paradoxuri, ba mai mult le-am compara cu puzzle-uri deoarece testează cât de prudent ești și cât de rapid poți procesa informația.

Deoarece ambele conțin dispariția unui obiect și primul conține doar linii, în timp ce al doilea constă în forme geometrice cu 2 dimensiuni, considerăm că cel precedent e cel mai simplu așa că o să începem cu el, ca de încălzire.

Linia Dispărută

1. Pornind de la o foaie cu 10 linii paralele desenate pe ea, tăiați foaia pe diagonală (ca în Fig. 1).
2. Mutati foaia din dreapta în jos și mai la stânga așa încât să se alinieze liniile (ca în Fig. 2) și observați că acum aveți doar 9 linii.

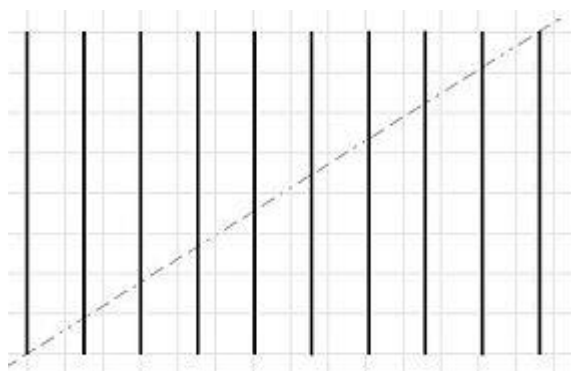


Fig.1

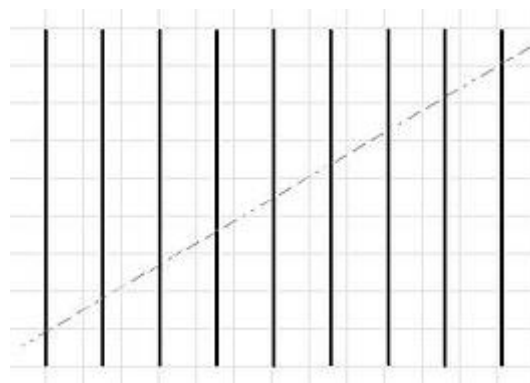


Fig. 2

Explicație:

Explicația este simplă și începe de la faptul că prima și ultima linie nu sunt tăiate, așa că dacă numerotăm fiecare linie de la stânga la dreapta cu numerele de la 1 la 10, putem observa că rearanjând foile, linia 10 cu partea de sus tăiată din linia 9 formează o nouă linie, la fel și partea de jos tăiată din linia 2 cu întreaga linie 1, așa că avem 9 linii mai lungi, iar din moment ce două linii nu au fost tăiate nu avem o părți rămase

Zona dispăruta

1. Desenați pe o foaie, o serie de figuri geometrice, iar apoi tăiați foaia așa încât să aveți o foaie cu fiecare figură (ca în Fig. 3).
2. Rearanjați figurile (ca în Fig. 4), și observați că un pătrat lipsește de și triunghiul pare să aibă aceeași mărime.

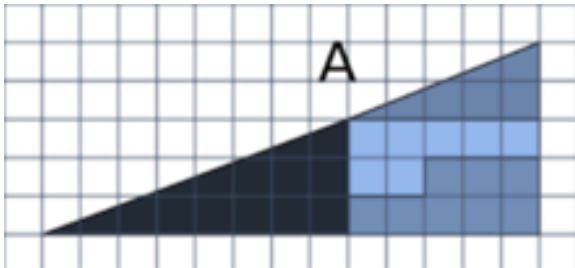


Fig. 3

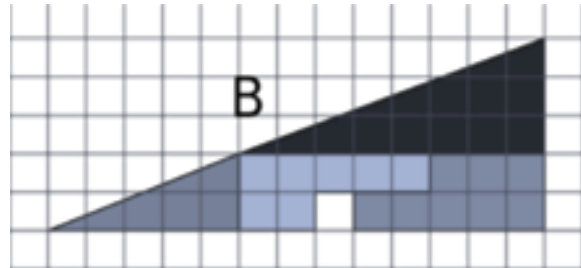


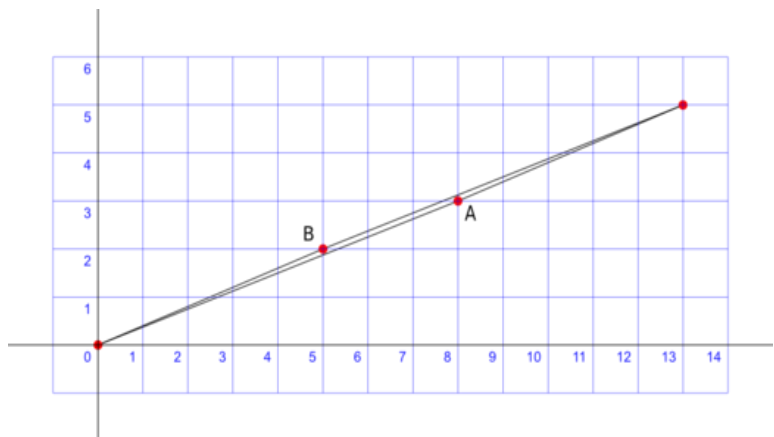
Fig. 4

Explicație:

Cheia înțelegerii acestei iluzii, este faptul că niciun triunghi mare din figuri nu este de fapt un triunghi, deoarece are ipotenuza puțin îndoită, în Fig. 3 în interior, iar în Fig. 4, în exterior, asta este datorită faptului că cele două triunghiuri mici nu au unghiul ascuțit echivalent (putem demonstra ușor prin calculând tangentele: 3:8, respectiv 2:5 și din moment ce tangentele sunt diferite și unghiurile vor fi).

Pătratul care apare este de fapt diferența de arie care provine din “îndoirea” ipotenuzei.

! Încă un mod de a-ți da seama că figurile mari nu sunt de fapt triunghiuri este prin a calcula aria fiecărei figure mici și aria unui triunghi cu catetele de marime 6, respectiv 13. Calculând aria figurilor mici ne dă 32 de pătrățele, iar triunghiul mare ar fi trebuit să aiba 32,5 pătrățele ($\frac{6 \cdot 13}{2} = 32,5$).



Bibliografie

https://koaha.org/wiki/Paradosso_dell%27area_scomparsa

https://en.wikipedia.org/wiki/Missing_square_puzzle

Paradoxul Braess

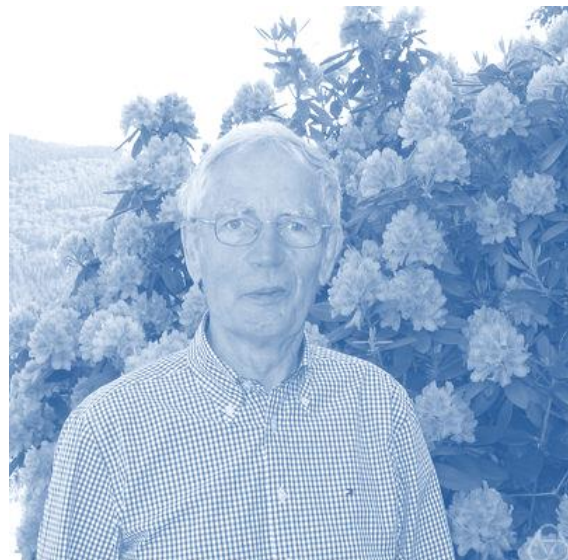
Corabian Andrei

Paradoxul Braess este constatarea că extinderea unei rețele de drumuri cu unul sau mai multe drumuri poate crea mai mult trafic care se deplasează prin aceasta în ansamblu. Matematicianul german Dietrich Braess a descoperit contradicția în 1968.

Rețelele electrice și sistemele biologice pot fi capabile să ofere analogii pentru contradicție. Teoretic, o rețea defectă ar putea fi îmbunătățită prin tăierea unora dintre componentele sale. Uneori, când autostrăzile importante existente sunt închise, s-a demonstrat că fluxul de trafic se îmbunătățește, iar paradoxul a fost folosit pentru a explica acest lucru.

Matematicianul

Dietrich Braess, un matematician de la Universitatea Ruhr, Germania, a observat că fluxul într-o rețea de drumuri ar putea fi împiedicat prin adăugarea unui drum nou, când lucra la modelarea traficului. Ideea lui a fost că, dacă fiecare șofer ia decizia optimă cu privire la ruta care este cea mai rapidă, o scurtătură ar putea fi aleasă prea des pentru ca șoferii să aibă cei mai scurți timpi de călătorie posibil. Mai formal, ideea din spatele descoperirii lui Braess este că echilibrul Nash ar putea să nu echivaleze cu cel mai bun flux global printr-o rețea.



Enunțul Paradoxului:

„Pentru fiecare punct al unei rețele rutiere, fie dat numărul de mașini care pornesc de la acesta și destinația mașinilor. În aceste condiții, se dorește să se estimeze distribuția fluxului de trafic, numai asupra calității drumului, dar și asupra densității fluxului. Dacă fiecare șofer ia calea care îi pare cea mai favorabilă, timpii de rulare rezultați nu trebuie să fie minimi. Mai mult, se indică printr-un exemplu că o extindere a rețelei rutiere poate determina o redistribuire a traficului care are ca rezultat timpi de rulare individuale mai mari.”

Dacă funcțiile de latență sunt liniare, adăugarea unei margini nu poate înrăutăți niciodată timpul total de călătorie la echilibru cu un factor mai mare de $4/3$.

Exemple din realitate

În Seul, Coreea de Sud, traficul în jurul orașului s-a accelerat când o autostradă a fost distrusa ca parte a proiectului de restaurare Cheonggyecheon. În Stuttgart, Germania, după investițiile în rețeaua de drumuri în 1969, situația traficului nu s-a îmbunătățit până când o porțiune de drum nou construit a fost din nou închisă circulației. În 1990, închiderea temporară a străzii 42 din New York pentru Ziua Pământului a redus cantitatea de aglomerație din zonă. În 2008, Youn, Gastner și Jeong au demonstrat rute specifice în Boston, New York și Londra unde acest lucru ar putea avea loc și au indicat drumuri care ar putea fi închise pentru a reduce timpul estimat de călătorie. În 2009, New York a experimentat închiderea Broadway-ului la Times Square. și Herald Square, care a avut ca rezultat îmbunătățirea fluxului de trafic și piețe pietonale permanente.

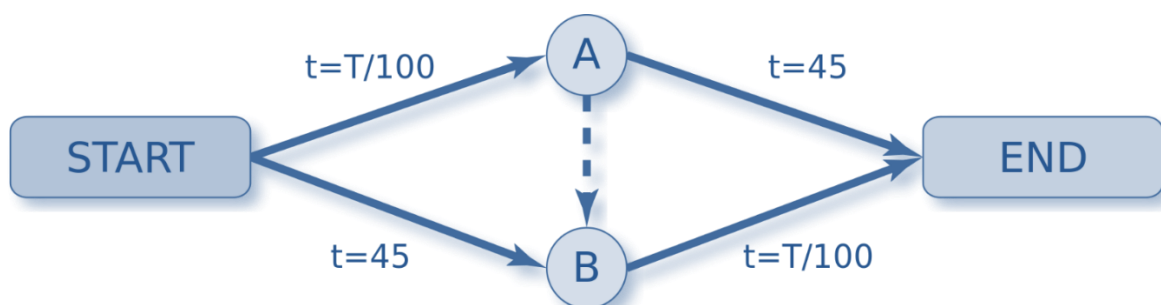
Observatii facute de cercetatori

În 2012, Paul Lacroix, de la institutul de planificare și dezvoltare din Île-de-France, a scris că „În ciuda temerilor inițiale, îndepărtarea drumurilor principale nu provoacă deteriorarea condițiilor de trafic dincolo de ajustările inițiale. Transferurile de trafic sunt limitate. și sub așteptări.

În același an, oamenii de știință de la Institutul Max Planck pentru Dinamică și Auto-Organizare au demonstrat, prin simulare computerizată, potențialul fenomenului de a apărea în rețelele de transport a energiei unde generarea de energie este descentralizată.

Tot în 2012, o echipă internațională de cercetători de la Institut Néel (CNRS, Franța), INP (Franța), IEMN (CNRS, Franța) și UCL (Belgia) a publicat în Physical Review Letters, o lucrare care arată că paradoxul lui Braess poate apărea în sisteme de electroni mezoscopici. În special, ei au arătat că adăugarea unei căi pentru electroni într-o rețea nanoscopică a redus în mod paradoxal conductanța acesteia. Acest lucru a fost demonstrat atât prin simulări, cât și prin experimente la temperatură scăzută, folosind SMG (un proces de scanare pentru probe microscopice)

Explicația Matematică



Avem un punct de start S și un punct destinație D, cu 4000 de șoferi care vor să ajungă din S în D, fără un drum direct între cele două .

Acestea sunt legate între ele de 4 drumuri, traseul de sus fiind notat cu a și cel de jos cu b .

2 dintre acestea nu au o capacitate mare de trafic, așa că timpul de călătorie depinde de numărul de șoferi de pe drum, notat cu T .

Celelalte două au capacități mari de trafic, deci timpul până la destinație nu depinde de câți șoferi circulă pe drum, iar acestea sunt parcurse în 45 minute.

Inițial, drumul pe care șoferii aleg să calatorească nu contează, deoarece în ambele cazuri vor trece pe un drum care depinde de trafic și unul care nu depinde.

Deci, dacă unul dintre drumuri este mai liber decât celalt, șoferii îl vor alege pe acela, până când drumul pe care îl foloseau înainte va rămâne mai liber și apoi îl vor alege pe acela.

Timpul de călătorie (în acest caz) este:

$$\frac{a}{100} + 45 = \frac{b}{100} + 45 = 65 \text{ minute}$$

(deoarece sunt 4000 de șoferi $\Rightarrow a + b = 4000 \Rightarrow$ timpul de călătorie)

În concluzie, în această situație, se creează un echilibru deoarece șoferii nu câștigă schimbând drumul.

Însă, dacă adăugăm un drum care să lege punctele A și B , care are o capacitate de trafic mare și aproximăm că timpul de parcurgere pentru acesta este de 0 minute (în realitate nu există un drum care să fie parcurs instant dar această aproximare ne va simplifica calculele, fără a schimba semnificativ rezultatul final, atunci strategia șoferilor se schimbă.

Când drumul este inaugurat dar niciun șofer nu circulă încă pe el, șoferii realizează că este mai eficient să mergă pe prima porțiune din a , iar apoi pe a doua porțiune din b , deoarece în acest fel timpul de călătorie devine:

$$\frac{2000}{100} + \frac{2000}{100} = 40 \text{ min}$$

(jumătate din șoferi merg pe drumul a și cealaltă jumătate pe drumul pe b , deci 2000 de șoferi pe fiecare drum)

Deoarece șoferii au realizat că durează mai puțin dacă parcurg doar porțiunile a_1 și b_2 , mai mulți șoferi încep să facă același lucru până când 2500 din cei 4000 ajung să urmeze această rută, moment în care porțiunile a_1 și b_2 sunt tot mai circulante, deci timpul de călătorie crește și ajunge la:

$$\frac{2500}{100} + \frac{4000}{100} = 65 \text{ min}$$

2000 de șoferi urmează ruta aceasta, iar ceilalți 1500 urmează ruta b => pe porțiunea b2
 circulă toți cei 4000 de șoferi, deci timpul de călătorie crește drastic, până când timpul total
 ajunge la 65 de minute, deci la fel de eficiente ca traseele inițiale a și b.

(Traseul b1 – b2 este și mai ineficient deoarece durează $45 + 45 = 90$ min)

De asemenea, șoferii care urmau traseul b au ajuns să necesite 85 de minute pentru
 călătoria de 65, deoarece acum toți cei 4000 șoferi circulă pe porțiunea b2, care aduce timpul
 de călătorie la:

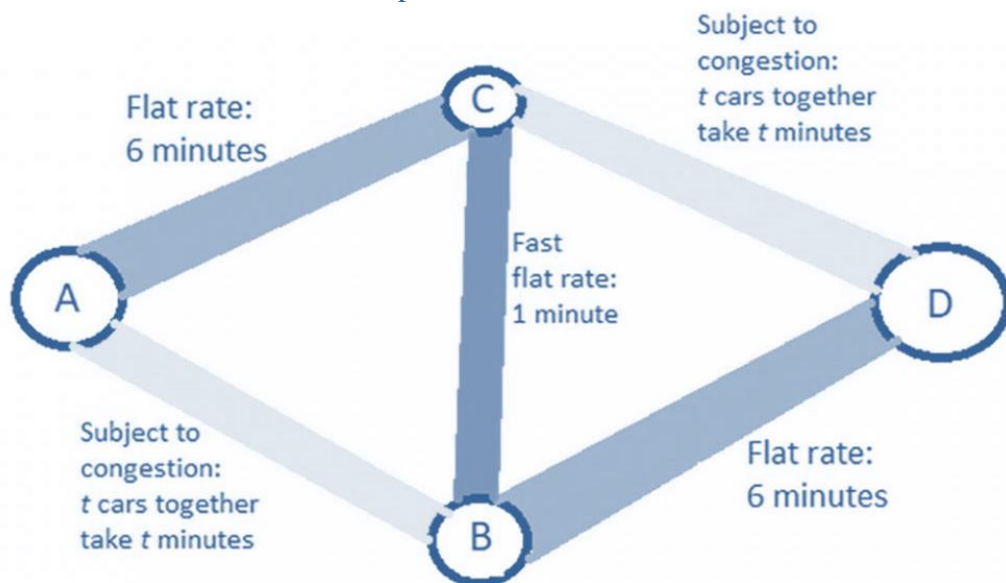
$$45 + \frac{4000}{100} = 85 \text{ min}$$

Așa că, și aceștia decid să călătorească pe traseul a1 – b2, deci toți 4000 de șoferi urmează
 același drum, cu timpul până la destinație:

$$\frac{4000}{100} + \frac{4000}{100} = 80 \text{ min}$$

În concluzie, drumul adăugat a creat mai multe probleme decât soluții și a transformat o
 călătorie de 65 de minute într-una de 80 .

Exemplu cu alte valori



Bibliografie

- https://en.wikipedia.org/wiki/Braess's_paradox
- https://en.wikipedia.org/wiki/Dietrich_Braess
- <https://www.youtube.com/watch?v=8mIH9bnvWVE>
- https://www.youtube.com/watch?v=cALeZV_Fwi0
- https://www.youtube.com/watch?v=cALeZV_Fwi0

Banda lui Möbius

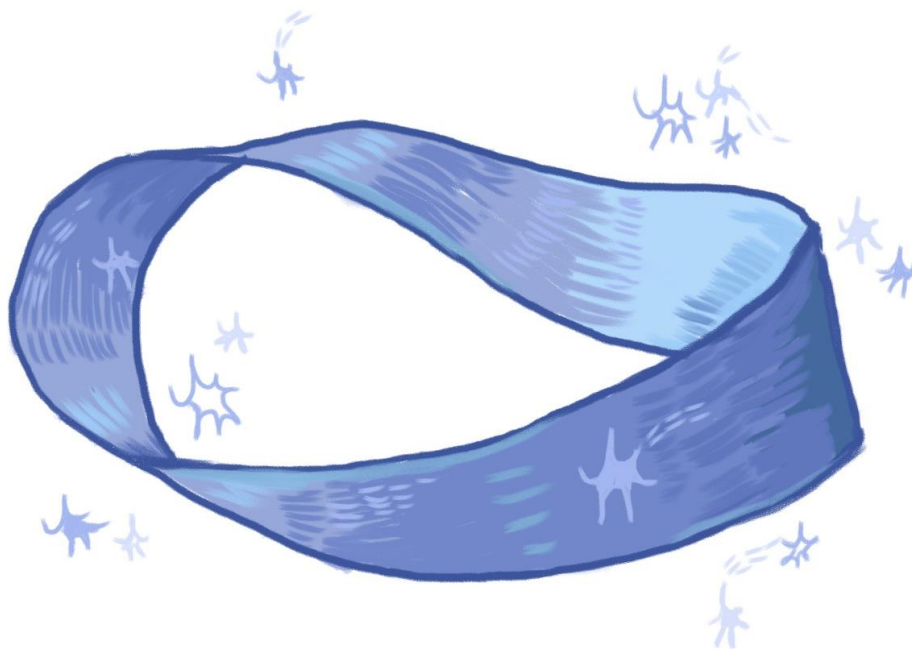
Dănoiu Dragoș și Ciovică Ianis

August Ferdinand Möbius a fost un matematician și astronom german, care alături de Johann Benedict Listing a studiat pentru întâia oară banda care avea să îi poarte numele în viitor.

Cei doi au descoperit banda în 1858. Banda se obține în practică prin lipirea capetelor unei benzi dreptunghiulare, astfel încât vârful de pe aceeași diagonală să se suprapună.

Câteva caracteristici interesante ale benzii sunt: are o singură margine, dacă se taie după o linie mediană se obține un inel răsucit de 360 de grade.

Toate benzile Möbius cu un număr impar de semirăsuciri sunt homomorfe între ele. Și toate benzile cu un număr par de semirăsuciri sunt homomorfe între ele. Dar o bandă cu un număr par de semirăsuciri nu este homomorfă cu una cu un număr impar de semirăsuciri. De asemenea, banda Möbius apare în două forme: dextrogiră și levogiră (de mână dreaptă și mână stângă).



Bibliografie:

https://ro.wikipedia.org/wiki/Banda_lui_M%C3%B6bius

https://math.fandom.com/ro/wiki/Banda_lui_M%C3%B6bius

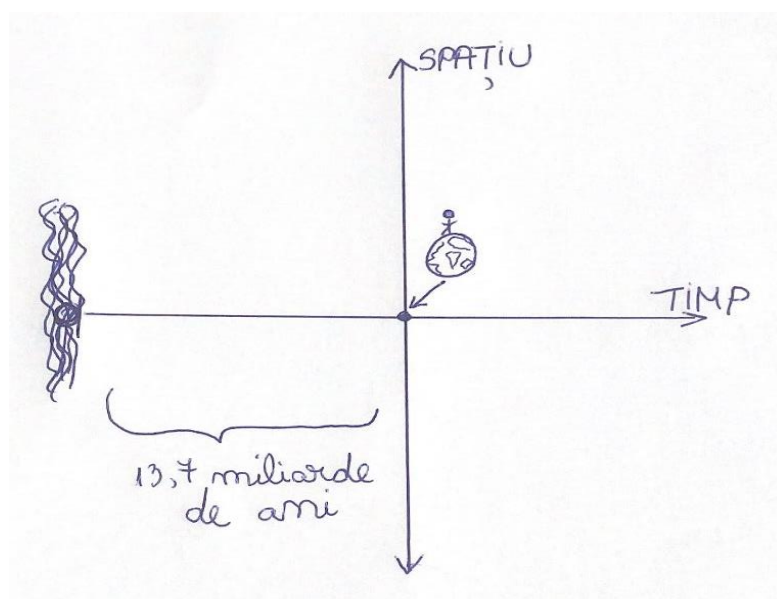
Paradoxul Olbers

Andra Dachin

De ce este cerul/spațiul întunecat noaptea?

Un prim răspuns ar fi că noaptea suntem în umbra Pământului creată de soare și putem vedea doar stelele care luminează ușor. Ziua lumina soarelui este dispersată pe atmosfera astfel încât cerul este luminat, dacă nu am avea atmosferă, cerul ar fi mereu întunecat (cum este de exemplu pe Lună).

Heinrich Wilhelm Olbers (cel de la care paradoxul a luat naștere) trăia într-un timp când i se spunea constant că Universal este infinit. El a realizat că din moment ce stelele sunt și ele infinite, în orice direcție în care ne uităm noaptea pe cer, trebuie să se afle o stea, fie că e departe, fie că e aproape. Astfel el a concluzionat că cerul ar trebui să fie complet acoperit de stele noaptea, adică să fie complet luminat, alb.



Dar dacă cerul nu este luminat, înseamnă totuși că stelele și galaxiile NU sunt infinite?

Nu, Universul NU are o limită spațială, dar are una temporală.

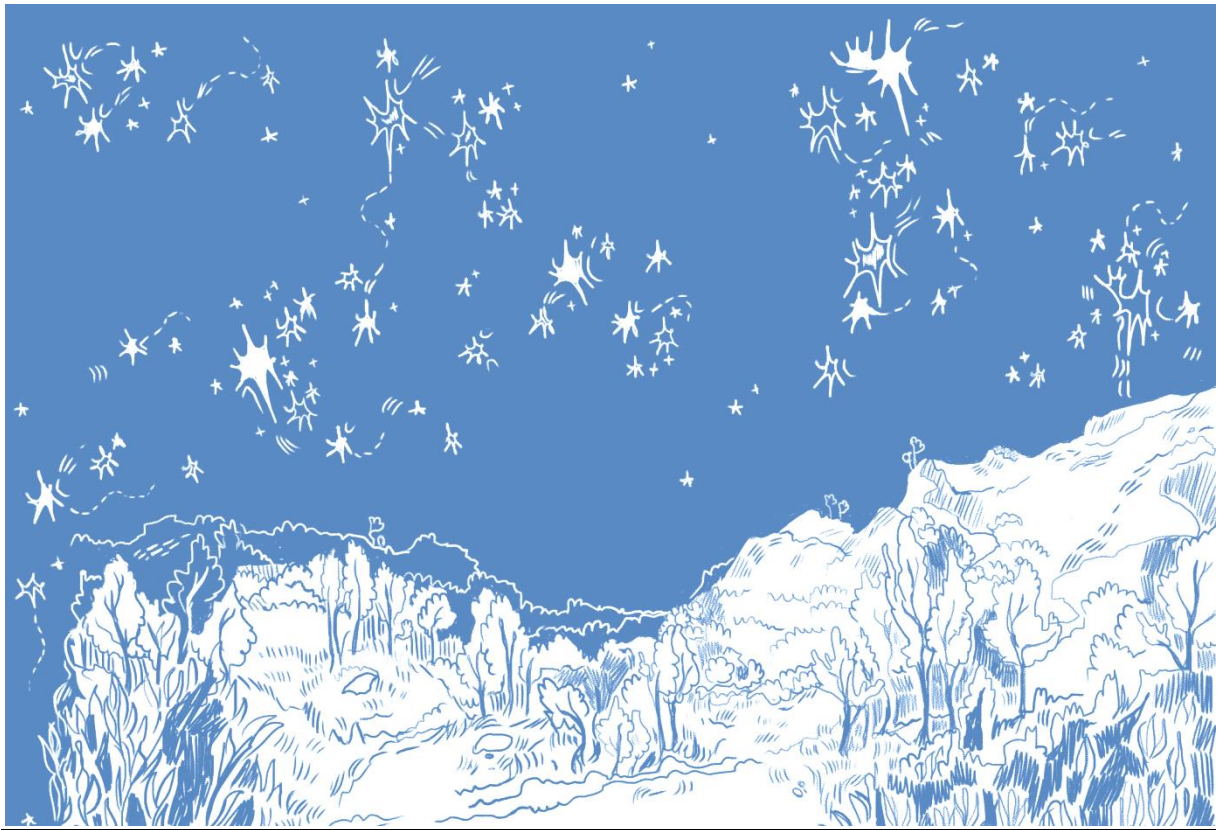
Înseamnă că unele stele sunt atât de departe încât lumina lor nu a avut timp să ajungă la noi.

Deoarece lumina are nevoie de timp pentru a călători în univers, atunci când ne îndreptăm telescoapele spre ceva foarte departe, noi vedem de fapt acea parte a Universului așa cum era atunci când lumina a fost emisă. Deci, când ne uităm la lumina veche de 13.5 miliarde de ani,

nu este vorba că nu vedem stele doar pentru că lumina de la ele nu a ajuns la noi încă - nu vedem stele și pentru că aruncăm o privire asupra Universului înainte ca stelele să se fi format!

Dar chiar și atunci când telescoapele noastre se uită înainte de primele stele, încă se mai vede lumină. Nu lumina stelelor, ci lumina rămasă de la Big Bang. Astfel observăm această "radiație cosmică de fond" cum formează un fundal luminos dincolo de stele. Deci, cerul noaptea NU ESTE de fapt întunecat. Dar atunci de ce arată întunecat?

Când Telescopul Hubble a fotografiat stelele îndepărtate ale frumosului Câmp Ultra-Profund Hubble, a făcut fotografia folosind o cameră cu infraroșu pentru că stelele și galaxiile se îndepărtează de noi datorită faptului că Universul se extinde constant. Stelele care se îndepărtează de noi devin tot mai roșii și cu cât sunt mai departe, cu atât sunt mai rapide și astfel ajung... infraroșii încât noi nu le mai pot vedea cu ochii noștri umani - **și de aceea noaptea cerul pare întunecat!**



Bibliografie

<https://www.youtube.com/watch?v=gxJ4M7tyLRE&list=TLPQMzAwNzIwMjlrCaWREJfqUQ&index=3>

https://ro.wikipedia.org/wiki/Paradoxul_lui_Olbers

<https://www.youtube.com/watch?v=yQz0VgMNGPQ>

fotografia 2- NASA, ESA, S. Beckwith (STScI) HUDF Tea

Paradoxul zilelor de naștere

Daniel Bischin

Paradoxul zilelor de naștere este o problemă propusă de matematicianul englez Harold Davenport, care a pus următoarea întrebare: care este probabilitatea ca într-un grup de n persoane, două dintre acestea să aibă aceeași zi de naștere?

Rezultatele sunt de-a dreptul surprinzătoare, obținând pentru un grup de 23 de persoane o probabilitate de peste 50%, iar pentru unul de 50 de persoane, această rată ajungând la 97%. Dar oare cum este posibil așa ceva? Nu ar trebui să fie rezultate mult mai mici, ținând că într-un an nebisect sunt 365 de zile? Propun astfel pentru următoarea parte a articolului o demonstrație care afirmă rezultatele spuse anterior.



Pentru simplitate, nu vom lua în considerare anii bisecți, gemenii și variațiile sezoniere și săptămânale ale natalității, iar grupul la care vom face referire are n persoane. Atsfel vom vorbi de anii în care sunt 365 de zile de naștere. Este ușor de dedus din principiul lui Dirichlet că pentru $n \geq 366$, probabilitatea este de 100%. Vom lucra acum cu $n \leq 355$.

La problema de față este mai ușor să determinăm probabilitatea ca două persoane din acest grup să **nu** aibă aceeași zi de naștere. Pentru asta, vom calcula pentru fiecare persoană probabilitatea să nu aibă aceeași zi de naștere cu una dintre persoanele din fața acestuia. Bineînțeles, pentru prima persoană aceasta va fi de 100%. A doua persoană nu poate avea aceeași zi de naștere cu prima, deci poate avea una dintre cele 364 de zile de naștere rămase, adică probabilitatea acestuia este de $\frac{364}{365}$. A treia persoană nu poate avea aceeași zi de naștere cu primele două persoane, așadar poate avea una dintre cele 363 de zile de naștere rămase, deci probabilitatea este $\frac{363}{365}$. Vom proceda analog pentru fiecare persoană până ajungem la a n -a persoană, pentru care probabilitatea va fi $\frac{365 - n + 1}{365}$.

Paradoxul Grand Hotel al lui Hilbert

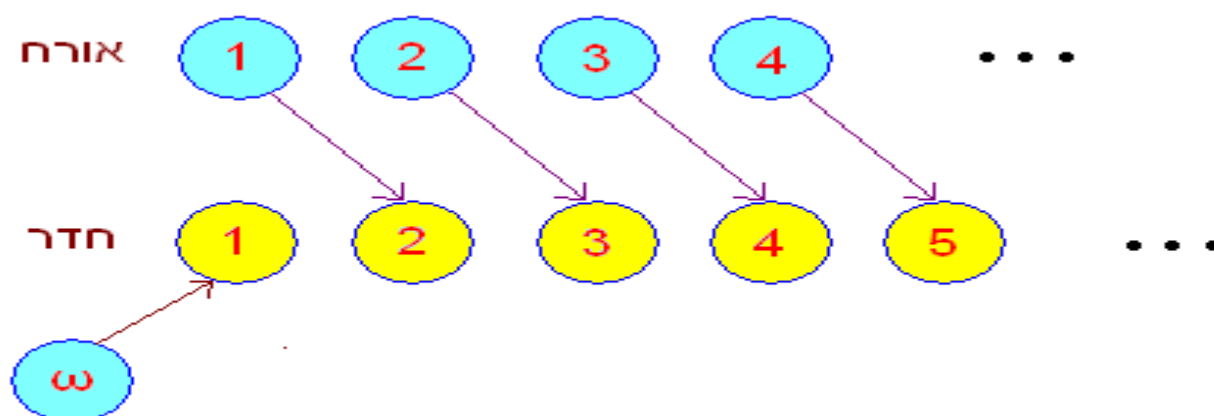
Dănoiu Dragoș și Ciovică Ianis

În secolul al XX-lea, matematicianului german David Hilbert îi vine ideea perfectă pentru a arăta unele caracteristici ale conceptului de infinit și diferențele dintre operațiuni cu seturi finite și infinite.

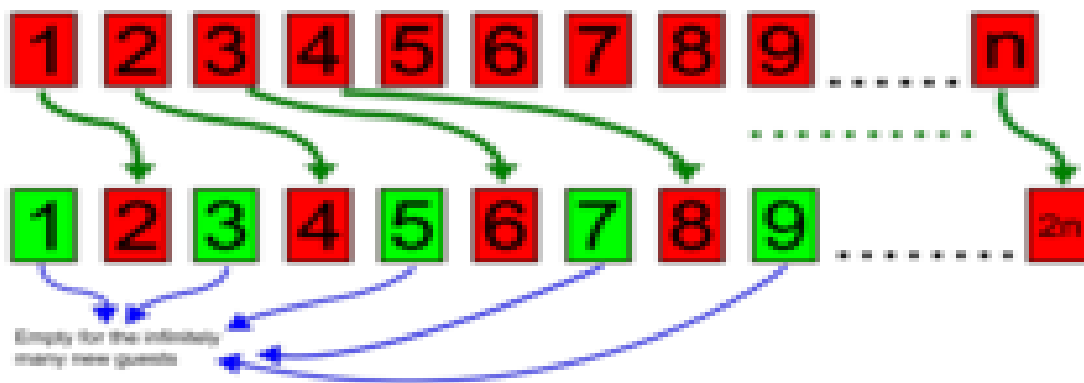
Paradoxul se prezintă în următorul fel:

Principiul sertarului spune că într-un hotel cu un număr finit de camere nu mai pot fi primiți oaspeți de îndată ce toate camerele sunt ocupate. Hotelul lui Hilbert însă, are un număr infinit de camere numerotate cu numere întregi, începând cu 1.

Dacă sosește un nou client, acesta nu poate fi trimis în ultima cameră, deoarece aceasta nu există! Așadar, fiecare client este mutat cu o cameră mai departe, oaspetele din camera 1 se mută în camera 2, cel din camera 2 se mută în camera 3 și așa mai departe. Așa noul oaspete va ocupa camera 1, care va deveni liberă și nu va exista problema ca ultimul oaspete să aibă camera, deoarece acesta va trece în următoarea, neexistând “ultima” cameră. Dacă repeți acest lucru, ai loc pentru un număr arbitrar, dar finit de noi oaspeți, astfel ocupantul camerei n se va muta în camera $n+1$.



Dacă sosește un autobuz infinit de lung cu un număr infinit de noi clienți, fiecare dorind să primească câte o cameră, fiecare oaspete trebuie să meargă în cameră cu număr dublu față de numărul camerei sale actuale. Oaspetele din camera 1 merge în camera 2, cel din camera 2 merge în camera 4, cel din camera 3 în camera 6 și așa mai departe, deci clientul n se va muta în camera $2n$. În acest caz, toate camerele cu număr impar vor fi libere. Știind că există un număr infinit de numere impare, dovedește faptul că numărului infinit de noi clienți li se va atribui câte o cameră, fiecare în parte. La această abordare, este important ca toți oaspeții să schimbe camera în același timp, de exemplu la semnalul dat de portarul prin bătaia unui gong. Dacă acest lucru s-ar face secvențial, cu un număr infinit de oaspeți și un număr infinit de camere, ar dura o perioadă infinită de timp.



Paradoxul hotelului infinit este, de asemenea, găsit în cartea „Infinitul“ de John Barrow David în capitolul III, intitulat „Bine ați venit la Hotel Infinit“ și a fost preluat în spectacol infinitati de către Barrow și Luca Ronconi.

Bibliografie:

https://ro.wikipedia.org/wiki/Hotelul_lui_Hilbert

https://koaha.org/wiki/Paradosso_del_Grand_Hotel_di_Hilbert

Paradoxul frunzelor de ceai

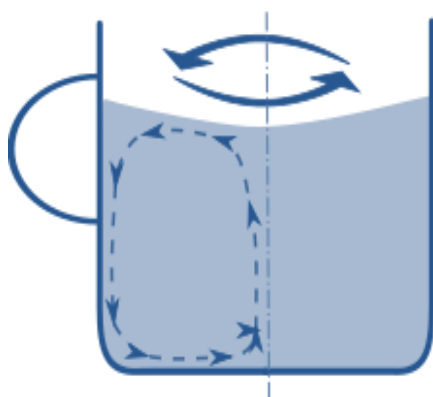
Săulescu Valentin

Forța centripetă aruncă un corp din mișcare de rotație

Forța centrifugă ține un corp în mișcare de rotație

Paradoxul frunzei de ceai este un fenomen în care frunzele de ceai dintr-o ceașcă de ceai migrează spre centrul și fundul cănii, după ce sunt amestecate, mai degrabă decât să se deplaseze către marginile ceștii, așa cum ar fi de așteptat într-un vârtej de lichid.

Agitarea lichidului crează o curgere spiralată, prin acțiune centrifugă. Prin urmare,



așteptarea este ca frunzele de ceai să se mute, din cauza masei lor, pe marginea ceștii. Cu toate acestea, frecarea dintre apa în mișcare și ceașcă crește presiunea apei, rezultând un strat de contact de înaltă presiune. Forța exercitată de acest strat de apă asupra frunzelor este mai mare și opusă față de forța centrifugă. Astfel, frecarea crează forța centripedă.

Stratul sub presiune afectează și curgerea apei după cum se poate vedea în imagine.

Paradoxul Calului

Spada Matteo

Paradoxul calului, afirmat prima data de George Pólya, este un paradox fals care spune că „Toți caii sunt de aceeași culoare”.

Demonstrație

Argumentul reiese din inducție matematică. Cazul cu un singur cal este trivial. Dacă în grup există un singur cal ($n=1$), atunci toți caii din acel grup au aceeași culoare.

Presupunem că n cai au aceeași culoare. Să considerăm un grup format din $(n+1)$ cai.

Mai întâi, se exclude ultimul cal și se analizează primii n cai; despre care s-a presupus anterior că toți au aceeași culoare. De asemenea, se exclude primul cal și se analizează ultimii n cai. Prin același raționament, și aceștia trebuie să aibă aceeași culoare. Prin urmare, primul cal din grup este de aceeași culoare ca și caii din mijloc, care la rândul lor sunt de aceeași culoare ca ultimul cal. Prin urmare, primul cal, caii din mijloc și ultimul cal sunt de aceeași culoare și am dovedit că:

Dacă n cai au aceeași culoare atunci $(n+1)$ cai vor avea, de asemenea, aceeași culoare.

Astfel, prin inducție matematică, s-a demonstrat că în orice grup de cai, toți caii trebuie să aibă aceeași culoare.

Explicație

Acest paradox fals este aparent dovedit prin inducție matematică. Dar aceasta este o metodă de verificare matematică folosită pentru a stabili veridicitatea unei afirmații pentru toate numerele naturale. În plus, nu are niciun sens afirmația că "primul cal din grup este de aceeași culoare ca și caii din mijloc" deoarece nu există "cai din mijloc" (aceasta este o legătură logică întreruptă).

Demonstrația a pornit de la un grup în care există un singur cal (pasul de inducție $n=1$). Dacă demonstrația începe cu un grup format din 2 cai, nu se mai poate afirma că cei doi cai au exact aceeași culoare (pasul de inducție $n=2$). Demonstrația cu pasul de inducție 2 nu este posibilă, deoarece primul 1 cal și ultimul 1 cal nu au cai în comun, și prin urmare s-ar putea să nu aibă toți aceeași culoare.



Bibliografie

https://ro.wikipedia.org/wiki/Paradoxul_calului

Efectul Mpemba

Gușe Tudor Ovidiu, Săulescu Valentin

“Efectul Mpemba” este numele care a fost dat unei observații , care constă în faptul că, un lichid (ex : apa) care este inițial fierbinte îngheață mai rapid decât același fel de lichid dar care este inițial rece.

Numele ii provine de la studentul tanzanian Erasto Bartholomeo Mpemba (născut în 1950) a cărui poveste devine popularizată în 1963. Descoperirea și observațiile notate despre efect originează în antichitate, Aristotel a menționat că este o informație uzuală.

Deoarece nu este sigură cauza efectului Mpemba, oamenii de știință au ajuns la mai multe soluții care ar putea să explice de ce se întâmplă acest fenomen.

De exemplu:

- * Transfer de căldură indus de microbule
- * Evaporare; evaporarea reduce masa apei care trebuie sa înghețe
- * Convecție: Accelerarea transferurilor de căldură. Reducerea densității apei sub 4 °C (39 °F) tinde să suprime curenții de convecție care răcesc partea inferioară a masei lichide
- * Substanțe dizolvate: Carbonatul de calciu, carbonatul de magneziu și alte săruri minerale dizolvate în apă se pot precipita atunci când apa este fiartă, ceea ce duce la o creștere a punctului de înghețare în comparație cu apa nefiartă care conține toate mineralele dizolvate.

Bibliografie

https://en.wikipedia.org/wiki/Mpemba_effect

De la pisica lui Schrödinger la multivers

Radu Andra

Cine a fost Schrödinger?

Erwin Rudolf Josef Alexander Schrödinger (1887-1961) a fost un fizician teoretician austriac și laureat al premiului Nobel pentru contribuția avută în fizica cuantică, cele mai renumite descoperiri ale sale fiind ecuația fundamentală ce determină probabilitatea distribuției rezultatelor posibile unui eveniment la scară atomică și experimentul care ilustrează efectul observatorului, respectiv conceptul de superpoziție cuantică.

$$\frac{-\hbar^2}{2m} \frac{\partial^2 \Psi}{\partial x^2} = i\hbar \frac{\partial \Psi}{\partial t}$$

*Schrodinger equation for free particle
in one dimension.*



Paradoxul "pisicii lui Schrödinger"

Experimentul teoretic propus de Schrödinger prezintă un paradox al superpoziției cuantice, proprietate a mecanicii cuantice care descrie posibilitatea unei particule de a coexista simultan în diferite stări. Fizicienii care au realizat primele experimente de bază ale mecanicii cuantice au ajuns în final la concluzia că **nicio proprietate a unui sistem cuantic (precum poziția unui electron) nu poate fi totuși precizată cu exactitate înainte de a fi măsurată**. Experimentul propus de Schrödinger s-a născut de fapt ca o încercare de a evidenția absurditatea acestor teorii privind mecanica cuantică. Acesta a ajuns în final să ridice o serie de întrebări cu privire la natura realității și la relația dintre observator și lumea înconjurătoare.

Schrödinger și-a imaginat o pisică închisă într-o cameră ce nu putea fi observată din exterior, în interiorul căreia a plasat un container plin cu o substanță otrăvitoare, un detector de particule, un ciocan și un material radioactiv. Pe măsură ce materialul suferă fenomenul de descompunere radioactivă, detectorul pune în mișcare „trăgaciul” radioactiv care eliberează în cele din urmă ciocanul; ca urmare a căderii ciocanului sticla umplută cu o substanță toxică (cianură, în versiunea imaginată de Schrödinger) se sparge, iar pisica moare otrăvită. Precizația principală este că sunt 50% șanse ca materialul radioactiv să se fi descompus, adică sunt probabilități egale ca pisica să fie vie sau moartă. Aplicând mecanica cuantică, deoarece până nu desfacem capacul cutiei nu putem ști dacă dezintegrarea a avut loc sau dacă pisica mai trăiește, nu doar mostra radioactivă va fi într-o superpoziție a două stări posibile, ci întregul experiment.

Astfel pisica, în condițiile în care nu analizăm sistemul cu ochii noștri, poate fi considerată atât vie, cât și moartă, în același timp.



Trecerea de la o pisică imaginară la universuri paralele; Sinuciderea cuantică

Pornind de la experimentul lui Schrödinger, unii fizicieni își imaginează consecințele aplicării teoriilor cuantice la scară universală. În cazul în care pisica se află într-o stare de superpoziție cuantică înainte să o observăm, momentul deschiderii cutiei ar trebui să nu "distrugă" posibilitatea existenței simultane a celor două stări, ci doar să o "fractureze", adică să o împartă în alte două posibile cadre de evenimente, mai precis în două posibile universuri paralele. Atunci când ne uităm în cutie, suntem incluși în "superpoziția" pisicii, observând-o moartă într-un univers posibil și vie în altul paralel. Această teorie a coexistenței universurilor paralele legate cuantic unul de celălalt poartă numele de multivers.

Sinuciderea cuantică este o ipoteză adoptată cu privire la posibilitatea ca moartea noastră dintr-o versiune de univers să fie de fapt doar una din stările ce alcătuiesc proprietatea de superpoziție în cadrul multiversului. Aceasta descrie cum, în cazul în care murim într-un univers, putem continua să existăm în continuare în altul, această supraviețuire putând să descrie un fel de imortalitate, în cazul în care există o infinitate de universuri paralele. În cazul acestor teorii, ne putem imagina că noi suntem pisica din experimentul inițial descris de Schrödinger, putând să ne aflăm în stare de viață și moarte simultan.

Deși aceste ultime teorii menționate pot fi explicate mult mai complex iar dovezile pentru acestea sunt căutate încă, majoritatea fizicienilor recunoscând aparențele absurde ale multitudinii de posibile descoperiri pe care fizica cuantică ni le va putea aduce.



Bibliografie

https://www.youtube.com/watch?v=n7RHv_MIIT0
https://en.wikipedia.org/wiki/Quantum_suicide_and_immortality
https://en.wikipedia.org/wiki/Schr%C3%B6dinger%27s_cat
https://ro.wikipedia.org/wiki/Interpretarea_Copenhaga
<https://www.youtube.com/watch?v=kTXTPe3wahc>
<https://www.youtube.com/watch?v=UjaAxUO6-Uw>
https://ro.wikipedia.org/wiki/Erwin_Schr%C3%B6dinger

Paradoxul lui Russell

Cichi David

Paradoxul lui Russell sau paradoxul mulțimii tuturor mulțimilor este un paradox logic și se referă în special la teoria mulțimilor, la existența unei *mulțimi a tuturor mulțimilor*. Formularea sa, de către Bertrand Russell în 1902, a marcat la un moment de criză în lumea matematicii și a logicii. Depășirea acestui moment a condus la revizuri, dezvoltări și chiar la apariția a noi teorii științifice.

Istoric

În 1872, Georg Cantor, fondatorul teoriei naive a mulțimilor, consideră mulțimea drept o colecție de obiecte ce posedă o proprietate comună. În primul volum al lucrării *Grundgesetze der Arithmetik* ("Legile de bază ale aritmeticii"), apărută în 1893, Gottlob Frege se exprimă într-o manieră similară, susținând că tot ce poate fi exprimat printr-o proprietate poate constitui o mulțime. Mai mult, Frege construiește o teorie axiomatică a mulțimilor, care va sta la baza matematicii și a logicii începutului de secol XX.

Bertrand Russell își manifestă rezervele față de această teorie și pe 8 decembrie 1900, într-o scrisoare adresată lui Louis Couturat, formulează o primă versiune a paradoxului ce ulterior îi va purta numele. Doi ani mai târziu, pe 16 iunie 1902, într-o scrisoare adresată lui Frege, Russell editează o altă versiune a paradoxului, foarte asemănătoare cu cea cunoscută astăzi, ca apoi să o publice în 1903 în celebrul său volum *The Principles of Mathematics*.

Publicarea paradoxului a stârnit largi ecouri în lumea științifică a epocii. Frege scria într-o postfață a unei lucrări

Paradoxul lui Russell, varianta cu predicate, 1905

Orice predicat își aplică propria lui proprietate, sau îi este aplicată din exterior. Dacă un predicat își aplică propria lui proprietate, vom spune că el are proprietatea **predicabil**; în caz contrar, vom spune că el este **impredicabil**. Însă **predicabil** și **impredicabil** sunt la rândul lor predicate, astfel că putem face același raționament și despre ele.

În particular, **impredicabil** este sau predicabil, sau impredicabil.

Dacă **impredicabil** este predicabil, atunci el își aplică propria lui proprietate, deci este impredicabil. Dacă **impredicabil** este impredicabil, atunci își aplică propria lui proprietate și, deci, este predicabil. În fapt este un semiparadox deoarece dacă se ia formal în considerare o proprietate, ea nu poate fi decât predicabilă, noțiunile în sine fiind în exclusivitate o abstractizare a minții umane.

Bibliografie

https://ro.wikipedia.org/wiki/Paradoxul_lui_Russell

Matematica jocurilor de noroc

Iacob Diana, Timofte Ana

Probabilitatea este ramura matematicii care determină cât de probabil este să se producă un eveniment sau cât de probabil este ca o propoziție să fie adevărată.

Matematica jocurilor de noroc este o colecție de aplicații probabilistice specifice jocurilor de noroc. Jucătorii pricepuți nu numai că iau în calcul caracterul uman din jocurile de noroc, dar înțeleg și probabilitățile matematice ale acestora, pentru a elabora strategii de joc.

Concepte de bază

Toate evenimentele din jocurile de noroc au probabilități absolute care depind de numărul total de rezultate posibile. De exemplu, dacă aruncați un zar cu șase fețe, probabilitatea de a ateriza pe orice latură anume este $1/6$. Jocurile cu spații de probă uriașe, cum ar fi pokerul, au evenimente cu probabilități și mai mici. De exemplu, în pokerul cu cinci cărți, probabilitatea de a trage patru de un fel este de $0,000240$, în timp ce șansa de a trage o chintă regală, cea mai rară mână, este de doar $0,00000154$.

Jucătorii adevărați sunt interesați nu numai de probabilități, ci și de câți bani pot câștiga teoretic dintr-un joc sau eveniment. Suma medie pe care vă puteți aștepta să o câștigați/pierdeți se numește valoarea așteptată – EV (eng-expected value) și este definită matematic ca suma tuturor probabilităților posibile înmulțită cu câștigurile sau pierderile asociate acestora.

De exemplu, dacă de fiecare dată când arunci o monedă și aceasta arată cap câștigi 1 leu, iar când aceasta arată coadă pierzi 1 leu, valoarea așteptată ar fi zero, deoarece probabilitatea ca moneda să arate cap este echivalentă cu probabilitatea monezii de a arăta coadă.

$$EV = 1/2 * 1.00lei + 1/2 * (-1.00lei) = 0 lei$$

Acesta este considerat un joc „corect” deoarece niciunul dintre jucători nu are un avantaj monetar dacă joacă jocul de mai multe ori.

Însă dacă schimbăm regulile jocului, astfel încât să pierzi tot 1 leu când moneda arată coadă, dar să câștigi abia 90 de bani când aceasta arată cap, jocul nu mai este „corect”, cazinoul având acum un avantaj, numit avantajul casei (house edge).

$$EV = 1/2 * 0.90lei + 1/2 * (-1.00lei) = -0.05 lei \Rightarrow \text{avantajul casei este de } 5\%$$

\Rightarrow dacă arunci moneda de 500 de ori, pariind așadar 500 lei, te poți aștepta la o pierdere de aproximativ 25 de lei, adică $5\% * 500$.

Toate jocurile de cazinou prezintă un avantaj al casei, iar valoarea așteptată negativă a lor explică modul în care cazinourile profită pe termen lung de pe urma jucătorilor.

Atunci de ce mai joacă oamenii jocuri de noroc? Și cum pot unii dintre ei să câștige sume uriașe? Ei bine, EV dictează cât de mult ar trebui să se aștepte un jucător să câștige pe

termen lung, o perioadă de timp arbitrară, perioadă pentru care majoritatea jucătorilor nu joacă. În schimb, jucătorii sunt mai interesați de valorile reale ale fiecărei mâini și de fluctuația de la EV a acesteia. Indicele de volatilitate, un termen tehnic pentru deviația standard, îi spune unui jucător șansa de a câștiga mai mult sau mai puțin decât EV, pentru un anumit număr de runde. Jocurile sau mâinile cu volatilitate ridicată au o variație mai mare între rezultatele așteptate și cele reale și, prin urmare, o posibilitate mai mare de a câștiga peste EV, ceea ce îi atrage în cele din urmă pe jucători la cazinouri.

Probabilitatea în jocul de ruletă

Roulette este un cuvânt francez însemnând "roată mică". Reguli: Un coupier învârte roata, care are 37(Europa) sau 38(S.U.A) de buzunare numerotate unde se poae opri o bilă. Principalele buzunare sunt numerotate de la 1 la 36, culorile lor alternând roșu cu negru. De asemenea, există 1 sau 2 buzunare verzi, numerotate cu cifra 0. Un jucător poate paria pe culoarea buzunarului unde se oprește bila, pe paritatea numărului, pe valoarea ridicată/scăzută a numărului, pe un interval de 2-12 numere, sau chiar pe un singur număr.

Majoritatea jucătorilor ar fi tentați să afirme că pariatur pe o culoare este cel mai promițător, datorită faptului că există mai multe șanse de câștig. Dar este acesta adevărul?

- Pariu pe roșu/negru sau pe par/impar:

Probabilitatea de câștig, $P(\text{win } \$1) = 18/38$; Probabilitatea de pierdere, $P(\text{lose } \$1) = 20/38$

=> $EV = 18/38 * \$1 + 20/38 * (-\$1) = -\$0.0526$

- Pariu pe un interval 1-12/13-24/25-36:

$P(\text{win } \$2) = 12/38$; $P(\text{lose } \$1) = 26/38$

=> $EV = 12/38 * \$2 + 26/38 * (-\$1) = -\$0.0526$

- Pariu pe un singur număr:

$P(\text{win } \$35) = 1/38$; $P(\text{lose } \$1) = 37/38$

=> $EV = 1/38 * \$35 + 37/38 * (-\$1) = -\$0.0526$

Așadar, orice pariu ai face în timpul jocului de ruletă, în timp, te poți aștepta să pierzi aceeași sumă de bani, casa având mereu un avantaj de 5,26%.

Probabilități pentru începutul jocului de Poker

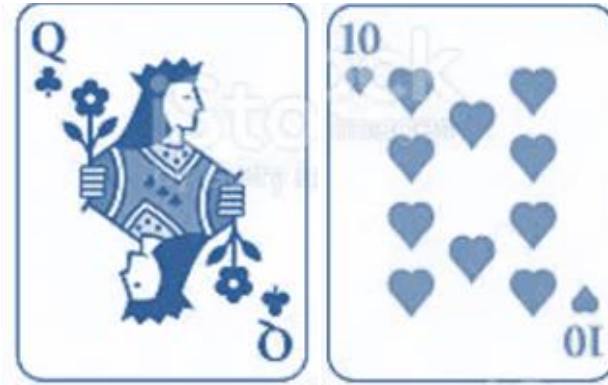
Primul pas în jocul de poker (variantea texană) este împărțirea a câte două cărți fiecărui jucător. Jucătorii își privesc perechea și apoi trebuie să parieze pe ea (să intre mai departe în joc) sau să abdice. În această etapă jucătorii se întreabă dacă merită sau nu pariul. Pentru asta, trebuie să prezică dacă vor fi sau nu *în avantaj* față de restul (se gândesc la cât de puternice/mari sunt cărțile pe care le au). Un mod de abordare ar fi să calculeze probabilitatea ca unul dintre *ceilalți* jucători să aibă *cărți mai mari decât perechea din propria mână*.

Cum se face asta?

Pentru a înțelege calculul de probabilitate vom folosi exemple. Ne imaginăm că jucăm noi înșine cu prietenii :)

- A. Presupunem la început că jocul se desfășoară în 2, deci se împart în total 4 cărți dintr-un pachet de 52 de cărți. Noi știm însă doar 2 dintre acestea, adică rămân 50 de cărți necunoscute.

Cărțile cunoscute:



Cărțile mai mari decât regina din mână sunt regii (K) și așii (A). În cele 50 de cărți necunoscute se află 4 regi și 4 ași. Adică sunt 8/50 cărți „periculoase” și 42/50 cărți „inofensive”.

⇒ Pentru prima carte a oponentului este o șansă de 42/50 ca el să NU aibă K sau A

Acum că am luat în considerare una dintre cărțile oponentului, rămân 49 de cărți în pachet (necunoscute). De asemenea, presupunând că prima oară nu a nimerit un K sau un A, și a extras din cărțile „inofensive”, au rămas 42-1=41 cărți „inofensive” și 8 cărți „periculoase”. De aici, mai are o probabilitate de 41/49 să extragă o carte „inofensivă”.

⇒ Pentru întreaga pereche este o probabilitate de $\frac{42}{50} \cdot \frac{41}{49} \approx 70,3\%$ să fie „inofensivă”, deci noi avem o șansă destul de mare să câștigăm/să fim în avantaj cu mâna pe care o avem

⇒ Scăzând dintr-un procent de 100% ne rezultă că oponentul are șanse de 29,7 % să se afle în avantaj.

⇒

B. Acum jocul se desfășoară în 3, deci avem 2 oponenti (noi primim aceleași cărți de început).

Pentru a calcula mai departe probabilitatea ca adversarii tăi să fie „inofensivi” se urmează aceeași raționament ca mai sus. Nu trebuie să percepem cărțile celorlalți ca pe mai multe perechi, ci ca pe 2,4,6...etc cărți (ca un pachet).

Așadar, rămân 8 cărți „periculoase”, 40 cărți „inofensive”, 48 cărți în pachet. Apoi, pentru patra carte adversară avem tot 8 regi și ași, 39 cărți mai mici (sau egale) decât regina, 47 cărți rămase.

⇒ Ecuația: $\frac{42}{50} \cdot \frac{41}{49} \cdot \frac{40}{48} \cdot \frac{39}{47} \approx 48,7\%$ - probabilitate ca restul perechilor să fie „inofensive”.

⇒ Adică 51,3% șanse de avantaj pentru UNUL dintre ceilalți.

Așa se poate continua până la maximum jucătorilor de Poker. Bineînțeles că aceste calcule sunt greu de făcut în minte, dar un reper ar fi numărul de jucători. Cu cât sunt mai mulți, cu atât este mai probabil ca unul dintre ei să aibă cărți mai bune ca tine.

Aici este un tabel pentru restul numărului de jucători, în cazul în care începem cu cărți si mai slabe decât o regină.

1 adversar	Aprox. 30%
2 adversari	Aprox. 51%
3 adversari	Aprox. 67%
4 adversari	Aprox. 78%
5 adversari	Aprox. 85%
6 adversari	Aprox. 90%
7 adversari	Aprox. 94%
8 adversari	Aprox. 96%

Pentru un ultim calcul ne vom imagina că avem un AS și o carte mică, precum un 7. În acest caz ne întrebăm care e probabilitatea ca adversarul nostru (unul singur) să aibă *tot* un AS.

Avem 50 de cărți necunoscute, 3 ași rămași, deci 47 de cărți slabe. Ulterior – 49 cărți necunoscute, 3 ași, 46 cărți slabe (una tocmai a fost extrasă de jucător)

⇒ $\frac{47}{50} \cdot \frac{46}{49} \approx 88,2\%$ probabilitate să nu aibă un AS.

⇒ 11.8% să mă înfrunte cu un AS.

Bibliografie:

<https://ro.wikipedia.org/wiki/Poker>

<https://www.youtube.com/watch?v=GE7qGgosago>

<https://www.youtube.com/watch?v=iPwN3BPBpwo>

https://en.m.wikipedia.org/wiki/Gambling_mathematics

<https://www.yalescientific.org/2010/02/should-you-bet-on-it-the-mathematics-of-gambling/>

<https://youtu.be/eHgbkeaRkEQ>



Riemann și numerele prime

Prof.Dorca Doriana

Ipoteza Riemann (1859) este una din cele mai celebre și mai importante probleme nerezolvate din matematică (conjectură).

Toată lumea știe ce sunt numerele prime - sunt numere care sunt divizibile cu 1 și cu ele însele. Dar, în mod interesant, până acum s-a dovedit imposibil de identificat vreo regularitate în plasarea lor. Riemann a încercat să găsească o formulă (funcție) de distribuție a lor printre numerele naturale.

Ipoteza Riemann este o conjectură care spune că distribuția numerelor prime nu este aleatorie, ci ar putea urma un model descris de o lege denumită funcția Zeta Riemann. Provocarea era de a dovedi că această ecuație se aplică tuturor numerelor prime.

Riemann a propus propria sa versiune, convenabilă pentru identificarea numerelor prime mari. Riemann a descoperit că numărul numerelor prime care nu depășește un anumit număr x este exprimat în termenii distribuției zerourilor netriviiale ale funcției zeta Riemann $Z(s)$. Riemann a exprimat conjectura, care nu a fost dovedită sau infirmată până acum, că toate zerourile netriviiale ale funcției zeta se află pe linia dreaptă $\text{Re}(z) = (1/2)$. În general, prin demonstrarea ipotezei Riemann (dacă este posibil) și alegând algoritmul adecvat, va fi posibilă spargerea multor parole și coduri secrete.

Conform lui Euclid orice număr întreg pozitiv este produsul de un singur set de numere prime. În 1737, marele matematician german Leonhard Euler și-a exprimat în primul teorema lui Euclid pe infinitatea cu formula prezentată mai jos.

$$\frac{1}{1-2^{-s}} \times \frac{1}{1-3^{-s}} \times \dots \times \frac{1}{1-p^{-s}} \dots = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \frac{1}{6^s} + \frac{1}{7^s} + \dots$$

Formula lui Euler, la o inspecție mai atentă, este absolut uimitoare, deoarece definește relația dintre numere prime și numere întregi. La urma urmei, pe partea stângă, se înmulțesc infinit de expresii care depind doar de numere prime, iar în partea dreaptă există o sumă asociată tuturor numerelor întregi pozitive. Riemann a mers mai departe decât Euler. Pentru a găsi cheia problemei distribuției numerelor, el și-a propus definirea unei formule atât pentru variabile reale, cât și pentru variabile complexe. Ea a fost cea care a primit ulterior numele funcției zeta Riemann. În 1859, omul de știință a publicat un articol intitulat „Despre numărul de numere prime care nu depășesc o valoare dată”, unde și-a rezumat toate ideile.

$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ este funcția zeta Riemann pentru toate numerele complexe s

Se numește funcția zeta, în cazul în care s - o constantă și n este toate valorile simple. Din aceasta au urmat în mod direct și aprobarea unicitatea expansiunii lui Euclid. Funcția Zeta Riemann este un tip de funcție.

Riemann a continuat ideea lui Euler. În scopul de a găsi cheia problemei distribuției numerelor, se propune să se definească formula atât variabila reală și complexă. Mai târziu a devenit cunoscută sub numele de funcția zeta Riemann.

La această funcție, numărul care se introduce se numește "intrare". Numărul pe care îl primești înapoi se numește "valoare". Fiecare intrare introdusă în funcția Riemann zeta oferă o valoare specială. De cele mai multe ori, se obține o valoare diferită pentru fiecare intrare. Dar fiecare intrare oferă aceeași valoare de fiecare dată când este utilizată. Atât intrarea dată, cât și valoarea primită de la funcția Riemann zeta sunt numere speciale numite numere complexe. Un număr complex este un număr format din două părți, parte reală și parte imaginară.

Ipoteza Riemann afirmă că toate zerourile netriviiale ale funcției zeta se află pe dreapta verticală $\text{Re}=0,5$ a planului complex. Ipoteza Riemann este importantă nu numai pentru matematica pură - funcția zeta apare constant în probleme practice legate de numerele prime, de exemplu, în criptografie.

Uneori, atunci se introduce o intrare în funcția zeta Riemann, primiți înapoi numărul zero. Când se întâmplă acest lucru, se numește acea intrare o rădăcină a funcției Riemann zeta. Se numește "rădăcină" atunci când se obține zero. Au fost găsite o mulțime de rădăcini. Dar unele rădăcini sunt mai ușor de găsit decât altele. Numim rădăcinile "triviale" sau "netriviiale". Numim o rădăcină "trivială" dacă este ușor de găsit. Dar numim o rădăcină "netrivială" dacă este greu de găsit. Rădăcinile triviale sunt numere numite "numere întregi pare negative". Motivul pentru care credem că sunt ușoare este că sunt ușor de găsit. Există reguli clare care spun care sunt rădăcinile triviale. Știm care sunt rădăcinile triviale datorită ecuației date de Bernhard Riemann. Această ecuație a fost numită "ecuația funcțională a lui Riemann".

Rădăcinile netriviiale sunt mai greu de găsit. Ele sunt mai greu de găsit decât rădăcinile triviale. Ele nu au aceleași reguli clare care să spună ce sunt. Chiar dacă sunt greu de găsit, au fost descoperite multe rădăcini netriviiale. Amintiți-vă că valoarea funcției zeta Riemann a fost un tip de număr numit număr complex. Și amintiți-vă că numerele complexe au două părți. Una dintre aceste părți se numește "partea reală". Se observă un lucru interesant în legătură cu partea reală a rădăcinilor netriviiale. Toate rădăcinile netriviiale pe care le-am găsit au o

parte reală care este același număr. Acest număr este $1/2$, care este o fracție. Acest lucru ne conduce la marea întrebare a lui Riemann, care se referă la cât de mari sunt părțile reale. Această întrebare reprezintă ipoteza Riemann. Întrebarea este "au toate rădăcinile non-triviale partea reală $1/2$?". Încă încercăm să aflăm dacă răspunsul este "da" sau "nu".

Există o modalitate prin care putem afla date despre părțile reale ale rădăcinilor ne-triviale. Aceasta este cu ajutorul ecuației speciale a lui Riemann (ecuația funcțională a lui Riemann). Ecuația funcțională a lui Riemann ne vorbește despre mărimea părților reale. Ea spune că toate zerourile netriviale au o parte reală apropiată de $1/2$. Aceasta spune cât de mici pot fi părțile reale și cât de mari pot fi. Dar nu spune *exact* care sunt acestea. Mai exact, se spune că părțile reale trebuie să fie mai mari decât 0 . Dar trebuie să fie mai mici decât 1 . Dar tot nu știm dacă ar putea exista o rădăcină non-trivială cu o parte reală foarte apropiată de $1/2$. Poate că există, dar nu am găsit-o încă. Grupul de numere complexe care au partea reală mai mare decât 0 , dar mai mică decât 1 se numește "banda critică".

Independent unul de celălalt, Hadamard și Poussin au dedus o teoremă privind distribuția numerelor prime. Hadamard și Poussin au reușit să demonstreze că toate funcțiile zeta netriviale 0 se află în banda critică.

Datorită muncii acestor oameni de știință, a apărut o nouă direcție în matematică - teoria analitică a numerelor. Mai târziu, mai multe dovezi primitive ale teoremei la care lucra Riemann au fost obținute de alți cercetători. În special, Pal Erdős și Atle Selberg au descoperit chiar și un lanț logic foarte complex care o confirmă, care nu a necesitat utilizarea unei analize complexe. Cu toate acestea, până la acest punct, mai multe teoreme importante fuseseră deja demonstrate prin intermediul ideii lui Riemann, inclusiv aproximarea multor funcții ale teoriei numerelor. În acest sens, noua lucrare a lui Erdős și Atle Selberg nu a avut practic niciun efect asupra nimic.

Deși nu s-a găsit niciun model care să descrie distribuția primelor între naturi, Riemann a descoperit că numărul de prime mai mici decât x - funcția de distribuție a numerelor prime, notată $\pi(x)$ - este exprimat în termenii distribuției așa-numitelor „non -zerouri triviale” ale funcției zeta.

Ipoteza Riemann este unul dintre cele șapte „Premii ale Mileniului” oferite de institut, fiecare având o valoare de un milion de dolari.

Bibliografie

- www.claymath.org - "[The Riemann Hypothesis - official problem description](#)"
- science.sciencemag.org - "[Prime Time for the Riemann Hypothesis](#)"
- [doi.org](http://doi.org/10.1126/science.1089660) - [10.1126/science.1089660](http://doi.org/10.1126/science.1089660)

Articolele au fost culese și selectate de elevii:

Albescu David	Fleacă Anastasia Maria
Alexandrov Alexandru	Gușe Tudor
Apostol Vlad	Iacob Diana
Bischin Daniel	Iagăru Dragoș
Bîja Alexandra	Ihora Vlad
Ciovică Ianis	Junger Ernest
Cichi David	Orza Anamaria
Corabian Andrei	Penteleiciuc Maria-Lavinia
Crețu Victor	Radu Andra
Dachin Andra	Săulescu Valentin
Dănoiu Dragoș	Spada Matteo
Dospinescu Miruna	Timofte Ana
Dospinescu Tudor	Țeposu Vlad

Coordonator: prof. Dorca Doriana

Editor și ilustrator: Dospinescu Miruna

Copertă: Dospinescu Miruna

