

Foglalkoztatok CSEBYSEV tételének ERDŐS Páltól származó bizonyításával, mely szerint bármely szám és a két-szerese közt van prímszám. Ebből a tételből következik persze, hogy végtelen sok prímszám van. (A tétel maga természetesen ennél lényegesen többet mond.) Ennek az egyszerűbb tételnek egy nagyon szellemes bizonyítását adta már EUKLIDES. Eljárását legtöbbször ismeritek. Ő megadott prímszámokhoz olyan számot talál, mely az adott prímszámok egyikével sem osztható. Mivel pedig minden szám vagy maga prímszám, vagy prímszámokból – mint azok szorzata – van összetéve, így következik, hogy az adottakon kívül még létezik prímszám.

Kínálkozik egy harmadik út is ennek az állításnak bebizonyítására. Ismét induljunk ki abból, hogy ismerünk valahány prímszámot. Próbáljuk megszámolni, hány olyan szám van egy elég nagy K számig, amelyek csak az adott prímszámokkal oszthatók. Ha azután sikerül egy olyan K -t találni, amelyig az ilyen egész számok száma nem éri el K -t, ez azt jelenti, hogy van olyan szám, mely más prímszámokkal is osztható. Még azt is remélhetjük, hogy kapunk egy becslést azon számok számára, amelyek nemcsak az adott prímszámokkal oszthatók, és ebből ismét további következtetéseket vonhatunk le a prímszámokra.

Meg kellene tehát becselnünk az olyan K -nál kisebb számok számát, melyek csak a megadott p_1, p_2, \dots, p_n prímszámokkal oszthatók, ahol K egyelőre közelebből nincs még meghatározva. Később fogjuk alkalmasan nagy-nak választani. A megszámlálандó számoknak két követelményt kell kielégíteniük. K -nál kisebbnek kell lenniök, és törzstényezőik csak az adott prímszámok közül lehetnek. E két követelmény igen különböző természetű s így nehéz őket egyidejűleg figyelembe venni. ERDŐS ezt a nehézséget úgy oldotta fel, hogy a számokat is kettéválasztotta. Pl.: $3780000 = 2^5 \cdot 3^3 \cdot 5^4 \cdot 7 = 2 \cdot 3 \cdot 7 \cdot 2^4 \cdot 3^2 \cdot 5^2$. Az így visszamaradt tényezőben minden prímszám páros hatványon szerepel, ez tehát négyzetszám, példánkban $3780000 = (2^2 \cdot 3 \cdot 5^2)^2 \cdot 2 \cdot 3 \cdot 7 = 300^2 \cdot 42$. Hasonlóan felbonthatunk minden számot két tényezőre, melyek közül egyikben az előforduló törzstényezők csak első hatványon szerepelnek – ezt *négyzetes osztó nélküli számnak* fogjuk nevezni, mert nem lehet osztója 1-nél nagyobb négyzetszám – a másik tényező meg négyzetszám. A két tényező bármelyike lehet 1 is, pl. $1225 = 35^2 = 35^2 \cdot 1$, vagy $1001 = 1^2 \cdot 7 \cdot 11 \cdot 13$, vagy $1 = 1^2 \cdot 1$. Most már azzal oldja meg Erdős Pál a nehézségeket, hogy a négyzetszámokról elég csak annyit megkövetelni, hogy kisebbek legyenek K -nál, a négyzetes osztó nélküli számról pedig csak annyit, hogy törzstényezői csak a p_1, p_2, \dots, p_n számok legyenek. Ezzel ugyan nagyon bőven számolunk, mert pl. a második tényezőnél még azt sem néztük, hogy K -nál kisebb legyen, még kevésbé vigyáztunk arra, hogy a két tényező szorzata is kisebb legyen K -nál, de a nyert egyenlőtlenség még így is igen hasznos lesz.

A K -nál kisebb négyzetszámok alapja kisebb \sqrt{K} -nál (egyenlő is lehet vele, ha e szám egész), és minden K négyzetgyökénél kisebb szám négyzete K -nál kisebb négyzetszám. Így a négyzetszámok száma \sqrt{K} , amennyiben K teljes négyzet, ha nem az, akkor valamivel még kevesebb is ennél.

Számoljuk össze most a lehetséges négyzetes osztó nélküli számokat. Hacsak egy p_1 prímszám szerepelhetne bennük, akkor vagy 1-et veszünk, vagy ezt a prímszámot. Ez két eset. Ha hozzáveszünk még egy p_2 prímszámot, akkor is szerepelhetnek az előbb kapott számok négyzetes osztó nélküli tényezőként, de szerepelhetnek ezeknek p_2 -szőrösei is, ez összesen 4 szám – 1, p_1, p_2 és $p_1 \cdot p_2$. Ha mindig újabb és újabb számokat veszünk figyelembe, ezek mindig meg fogják kétszerezni az ilyen számok számát. Ebből a megfontolásból az következik, hogy n törzsszámból összesen 2^n különböző négyzetes osztó nélküli szám alkotható. A pontos bizonyításra a teljes indukciót lehet felhasználni. Azt már láttuk, hogy $n = 1$ esetén valóban $2^1 = 2$ négyzetes osztó nélküli szám szerepel. Tegyük fel most, hogy tudjuk már: k számú prímszámból 2^k négyzetes osztó nélküli szám alkotható. Vegyük most hozzá a $(k + 1)$ -edik prímszámot p_{k+1} -et is. Az eddig szereplő 2^k darab négyzetes osztó nélküli szám továbbra is szerepelhet; továbbá ezek mindegyikét p_{k+1} -gyel szorozva újabb, egymástól is különböző négyzetes osztó nélküli számokat kapunk, melyek mindegyike az előzőktől különböző. Ezek száma ismét 2^k lesz. Így $k + 1$ törzstényezőből összesen $2 \cdot 2^k = 2^{k+1}$ négyzetes osztó nélküli számot képeztünk, vagyis $k + 1$ -re is érvényes állításunk.

Ezzel bebizonyítottuk, hogy n prímszámból 2^n négyzetes osztó nélküli szám alkotható.

Vegyük most az összes kapott négyzetszámnak és négyzetes osztó nélküli számnak a szorzatát. Így meg fogjuk kapni az összes K -nál kisebb és csak p_1, p_2, \dots, p_n -nel osztható számokat (esetleg ezenkívül más számokat is, például K -nál nagyobbakat). Az így kapott számok száma a megengedett négyzetszámok és a négyzetes osztó nélküli számok számának a szorzata lesz, mert bármelyik négyzetszámnak szerepel a szorzata minden négyzetes osztó nélküli számmal. Így összesen legfeljebb $2^n \cdot \sqrt{K}$ számot kaptunk. Legfeljebb ennyi a K -nál kisebb és csak p_1, p_2, \dots, p_n -nel osztható számok száma. Kérdésünk az volt, hogy választható-e K olyan nagyra, hogy K -ig ne minden szám legyen ilyen. Ez biztosan teljesül, ha $2^n \cdot \sqrt{K} < K$. Vagyis $2^n < \sqrt{K}$, $K > 2^{2n}$. $2^{2n} + 1$ tehát már biztosan olyan szám, hogy az első $2^{2n} + 1$ számú szám közül legalább egy nemcsak a p_1, p_2, \dots, p_n törzsszámok hatványainak szorzata. Egy ilyen számot kiválasztva ez is törzstényezőik szorzatára bontható, ezek közt kell a megadottaktól különböző törzsszámnak is lennie, tehát van még prímszám p_1, p_2, \dots, p_n -en kívül is.

Azt is megkaptuk, hogy a p_1, p_2, \dots, p_n -től különböző prímszámokkal is osztható számok száma legalábbis $K - 2^n \cdot \sqrt{K}$, hiszen itt általában olyan számokat is számbavettünk a levonandók közt, amelyek nemcsak az adott n prímszámmal oszthatók, és olyanokat is, amelyek nagyobbak K -nál.

K -t $2^{2n} + 1$ -nek választva azt kapjuk, hogy $K - 2^n \sqrt{K}$ határozottan pozitív, és mivel ennél nagyobb a nemcsak a p_1, p_2, \dots, p_n -nel osztható számok száma, ami mindenesetre egész szám, tehát e szám legalább 1. Ha azonban K -t nagyobbak választjuk, még meglepőbb eredményt is kaphatunk. Legyen pl. $K \geq 2^{2n+2}$, ekkor $\sqrt{K} \geq 2^{n+1}$, vagyis $2^n \leq \frac{\sqrt{K}}{2}$, s így a p_1, p_2, \dots, p_n adott n prímszámon kívül más prímszámmal is osztható számok száma K -ig legalábbis

$$K - 2^n \cdot \sqrt{K} \geq K - \frac{\sqrt{K}}{2} \cdot \sqrt{K} = K - \frac{K}{2} = \frac{K}{2}.$$

Vagyis azt kaptuk, hogyha adva van n darab prímszám p_1, p_2, \dots, p_n , akármilyen nagy szám is az n , ha $K \geq 2^{2n+2}$, akkor már biztos, hogy a K -nál kisebb számoknak legalább a fele az adott prímszámoktól különböző prímszámmal is osztható.

Ezeknek a számoknak a számát még egy módon megbecsülhetjük az adott n prímszámtól különböző prímszámok segítségével. Az egyszerűség kedvéért legyen p_1, p_2, \dots, p_n a továbbiakban az első n prímszám, a többi K -nál kisebb prímszámok pedig sorra $p_{n+1}, p_{n+2}, \dots, p_{n+m}$. Nézzük meg, hány olyan K -nál kisebb szám van, mely p_{n+1} -gyel osztható. Mivel minden p_{n+1} -edik szám osztható p_{n+1} -el, ezen számok száma legfeljebb $\frac{K}{p_{n+1}}$. (Pontosan $\left\lfloor \frac{K}{p_{n+1}} \right\rfloor$ volna.) Hasonlóan p_{n+2} -vel legfeljebb $\frac{K}{p_{n+2}}$, ... végül p_{n+m} -mel legfeljebb $\frac{K}{p_{n+m}}$ számú szám osztható K -ig. A $p_{n+1}, p_{n+2}, \dots, p_{n+m}$ számoknak legalább egyikével osztható számok száma legfeljebb $\frac{K}{p_{n+1}} + \frac{K}{p_{n+2}} + \dots + \frac{K}{p_{n+m}}$. Általában sokkal kevesebb, hiszen ha egy szám több ilyen prímszámmal is osztható, akkor ezt a számot mindegyik ilyen prímszám-osztójánál külön figyelembe vettük. Az előbbi összegből K kiemelésével $K \cdot \left(\frac{1}{p_{n+1}} + \frac{1}{p_{n+2}} + \dots + \frac{1}{p_{n+m}} \right)$ lesz.

Jelöljük a zárójelben lévő kifejezést a rövidség kedvéért egyelőre R_{nm} -mel. Az eddigiekből az következik, hogy $K \cdot R_{nm}$ nagyobb, mint azon K -nál kisebb számok száma, melyeknek az első n prímszámon kívül még más prímosztója is van; ez a szám viszont nagyobb, mint $\frac{K}{2}$, ha $K \geq 2^{2n+2}$. Ebből az következik, hogy $K \cdot R_{nm} \geq \frac{K}{2}$. Vagyis $R_{nm} = \frac{1}{p_{n+1}} + \frac{1}{p_{n+2}} + \dots + \frac{1}{p_{n+m}} \geq \frac{1}{2}$, tehát az n -edig prímszámtól a 2^{2n+2} -ig lévő prímszámok reciprok értékeinek összege feltétlenül eléri az $\frac{1}{2}$ -et. Ha ebben a sorban előforduló utolsó prímszám az $(n+m)$ -edik, akkor ugyanezen egyenlőtlenség szerint a 2^{2n+2} és a $2^{2n+2m+2}$ közti prímszámok reciprok értékének összege újból eléri az $\frac{1}{2}$ -et. Ha ebben a számközben további r prímszám volt, akkor a $2^{2n+2m+2}$ és a $2^{2n+2m+2r+2}$ közti prímszámok reciprok értékeinek összege ismét nagyobb lesz, mint $\frac{1}{2}$, és így tovább. Bármeddig is megyünk tehát el a prímszámok sorában, mindig találhatunk még annyi és akkora prímszámot, hogy reciprok értékeik összege nagyobb legyen, mint $\frac{1}{2}$, ezek az $\frac{1}{2}$ -ek pedig összeadva akármilyen nagyra felnövekedhetnek.

Az egymás utáni prímszámok reciprokait összeadva, ez az összeg tehát bármilyen nagyra is felnövekedhetik.

Ez az eredmény már lényegesen többet mond, minthogy végtelen sok prímszám van. A számelmélet egy újabb klasszikus tételéhez jutottunk el, melyet először Leonhard EULER svájci származású pétérvári matematikus bizonyított be.