

A fizikai, kémiai törvények kutatásának igen fontos módszere a próbálgatás, kísérletezés, de a matematikában is juthatunk próbálgatás segítségével törvények felfedezésére. Csak egy egyszerű példát említek. Tudjuk, hogy a többtagúak négyzetét úgy alakíthatjuk polinomná, hogy vesszük minden tag négyzetét és mindegyik kétszeres szorzatát minden más taggal. Hogy honnan tudjuk? Két tagra egyszerű szorzással nyertük:

$$(a + b)^2 = (a + b)(a + b) = a^2 + ab + ab + b^2 = a^2 + 2ab + b^2.$$

Három tag esetén ezt már felhasználhatjuk, úgy, hogy két tagot egybefoglalunk először:

$$(a + (b + c))^2 = a^2 + 2a(b + c) + (b + c)^2$$

Ha tovább folytatjuk a tagokra bontást, akkor a második tagból két 2-szeres szorzat adódik, a harmadik meg még két négyzetet szolgáltat és az utolsó kétszeres szorzatot a két tag négyzetére nyert eredmény szerint.

Négytagúaknál ezek után megint csak az utolsó kettőt kell összefoglalni és akkor úgy emelhetjük négyzetre, mint egy háromtagút. A maradó zárójelek felbontása után megint csak olyan szerkezetű kifejezést kapunk, amilyent bevezetőben mondtunk. És ezt nyilván így folytathatjuk tovább akárhány tagú kifejezésig.

Próbálgatás vezette a következő meggondolást is. Ha azt akarjuk tudni, hogy egy szám osztható-e egy egyjegyű számmal, ennek eldöntésére egyszerű módszerünk van minden egyjegyű szám esetén, csak a 7-tel való oszthatóságra nincs. Egyik matematikusunk ebbe nem akart belenyugodni második gimnazista korában és sok mindennel próbálkozott. 7-tel való oszthatóságra ugyan nem talált próbát, de észrevett valamit a $3 \cdot 7 = 21$ -gyel osztható számoknál: elhagyta a szám utolsó jegyét és a maradó számhoz hozzáadta ezt a jegyet. Ha az így kiszámított számot megszorozta 7-tel, visszakarta azt a számot, amiből kiindult. Pl. mindjárt $21 = (2 + 1)7$, vagy $3 \cdot 21 = 63 = (6 + 3)7$, vagy $6 \cdot 21 = 126 = (12 + 6)7$, vagy $8 \cdot 21 = 168 = (16 + 8)7$ stb. Kipróbáltunk két- és háromjegyű számokat is, és még a közbeesőkkel is kiegészíthetnénk próbálgatásainkat. Úgy látszik, használható módszerre akadtunk

Ha 7-re nem, hát legalább a $3 \cdot 7$ -tel való oszthatóság eldöntésére módszert találtunk. Kérdés még, hogy jól használható-e a módszer gyakorlatban. Vegyünk egy nagyobb számot, pl. $(57 \cdot 21 =) 1197$: $(119 + 7)7 = 882$. Hát itt mi történt? Csak az, hogy a kísérlet becsapott. 1197-re már nem jó ez a próba. Ha utána nézünk, kiderül, hogy $1 \cdot 21$ -re, $2 \cdot 21$ -re, s. í. t. egészen $9 \cdot 21$ -ig jó ez a próba, de $10 \cdot 21$ -től kezdve már mindig csődöt mond. Ez nem is olyan csodálatos. Végeredményben magában az, hogy valamit 9 esetben kipróbáltunk, mindössze arról biztosít, hogy ebben a 9 esetben érvényes, de már a tizedik esetben sem következik belőle semmi.

Akkor lehet, hogy a többtagúak négyzeténél is tévedtünk, hogy nem akárhány tag összegének négyzete számítható úgy ki, ahogy mondtuk? Pedig ebben sohasem szoktunk kételkedni. Van talán valami különbség abban, ahogy a négyzetreemelést próbáltuk ki 2, 3, 4 tagra, meg ahogy a 21-gyel való oszthatóságot próbálgattuk? Bizony hogy van. A négyzetreemelésnél nem kezdtük mindig előről a számolást, hanem lépésről-lépésre vettünk mindig egy taggal többet és felhasználtuk, hogy már tudjuk, eggyel kevesebb tagot úgy emelhetünk négyzetre, ahogy azt előbb elmondtuk. Nem is azért hagytuk abba, mert „annyi esetben kipróbáltuk és mindig igaz volt, hogy biztos igaz lesz minden esetben”. Négy próba nem is „annyi eset”, hogy kár volna tovább próbálgatni. Ellenben abbahagytuk a próbálgatást akkor, amikor észrevettük azt is, hogy ezen a módon, ahogy a próbálgatásokat végeztük, mindig tovább tudunk menni egy többtagú négyzetéről eggyel több tagéra; akkor hagytuk abba, amikor jogunk volt leírni ezt a mondatot: „És ezt nyilván így folytathatjuk tovább akárhány tagú kifejezésig.” Akár a háromtagúak négyzeténél megállhattunk volna, ha már ott megláttuk volna, hogy az, amit használtunk, az utolsó két tag összefoglalása, az egyre több tagú kifejezésekkel mindig megismételhető.

*

A négyzetreemelés nagyon unalmas példa. A könyökünkön jön ki. Keressünk helyette érdekesebbet. Az egymásutáni egész számokat össze tudjuk adni akármeddig. Talán még a négyzetszámok összegezésével is találkozhatók. Próbáljuk hasonló képletet nyerni a köbszámok összegére.¹

$$\begin{array}{ll} 1^3 = 1 & 1^3 + 2^3 + 3^3 + 4^3 = 100 \\ 1^3 + 2^3 = 9 & 1^3 + 2^3 + 3^3 + 4^3 + 5^3 = 225 \\ 1^3 + 2^3 + 3^3 = 36 & 1^3 + 2^3 + 3^3 + 5^3 + 6^3 = 441 \end{array}$$

Szembeötlő egy szabályossága az összegeknek: csupa négyzetszámot kaptunk:

$$1^2, 3^2, 6^2, 10^2, 15^2, 21^2.$$

Nézzük az alapot: 1, 3, 6, 10, 15, 21: mindig eggyel nő a különbség két egymás utáni szám közt. Akkor ezek nem mások, mint az első, első két, első három, négy, öt, hat, stb. egész szám összege. Ezt általában is tudjuk összegezni:

$$1 + 2 + 3 + 4 + 5 + \dots + n = \frac{n(n+1)}{2}$$

¹Lapunk első évfolyama tárgyalta annak egy módját hogyan lehet egymásutáni egész számok akárhányadik hatványai összegének kiszámítására képletet találni: Lásd Kalmár László: *A számok hatványainak összegéről*, I. évfolyam, 5 – 10., 39 – 47., 169 – 176. lap.

így az első n köbszám összegét is fel tudjuk könnyen írni:

$$(1) \quad 1^3 + 2^3 + 3^3 + \dots + n^3 = \left(\frac{n(n+1)}{2} \right)^2,$$

feltéve, hogy a szabályosság, amit találtunk, nem csak látszólagos, mint a 21-gyel való oszthatóságnál. Eddig csak észre vettük a szabályosságot, de nem látszik, hogy miért maradt ez érvényes sorban az egymásutáni számokra, mint a négyzetreemelésnél látszott.

Próbáljuk meg még az utolsó eredményhez a következő köbszámot hozzáadni, hogy továbbra is az a szabályosság marad-e érvényben, amit eddig találtunk:

$$21^2 + 7^3 = (7 \cdot 3)^2 + 7^2 = 7^2 \cdot (3^2 + 7) = 7^2 \cdot (3^2 + 2 \cdot 3 + 1) = 7^2 \cdot 4^2 = 28^2$$

és $1 + 2 + 3 + 4 + 5 + 6 + 7 = 28$. Itt már valami szabályosság sejthető, de még mindig nem látjuk világosan, hogy mi is az oka annak, hogy 21-ből 28 lesz. Nem tudnánk előre megmondani, milyen átalakítást lehetne alkalmazni, ha még a következő köbszámot is hozzáadnánk. Próbáljuk meg ezt is végig számolni. Háttha utólag látunk valamit:

$$\begin{aligned} 28^2 + 8^3 &= (7 \cdot 4)^2 + (2 \cdot 4)^2 = 4^2 \cdot (7^2 + 4 \cdot 2^3) = 4^2 \cdot (7^2 + 4 \cdot 8) = \\ &= 4^2 \cdot (7^2 + 4 \cdot 7 + 4) = 4^2 \cdot 9^2 = 36^2 \end{aligned}$$

és $28 + 8 = 36$. Itt egy kicsit mesterkétebben sikerült csak négyzetté alakítani azt, ami a zárójelben maradt. Ez azt engedné sejtetni, hogy csak véletlen, hogy megint az jött ki, amit vártunk. Abba viszont nem nyugodhatunk bele, hogy az egész csak véletlen, mikor már nyolc esetben ugyanezt a szabályosságot találjuk és még egyetlen olyan esetet sem tapasztaltunk, ahol ez a szabályosság nem volna érvényes.

Azt akarjuk eldönteni, hogy akárhányadik köbszám hozzáadásakor is érvényben marad-e a talált szabályosság, vagy sem. Ha ilyesmi nem közvetlenül nyilvánvaló, akkor segít az algebra nyelve. Tegyük fel, hogy valamely k számig már kipróbáltuk a szabályosságot, tehát k -t téve (1)-ben n helyett, tudjuk, hogy még helyes az összefüggés:

$$1^3 + 2^3 + 3^3 + \dots + k^3 = \left(\frac{k(k+1)}{2} \right)^2.$$

Adjuk hozzá a következő köbszámot, $(k+1)^3$ -t:

$$\begin{aligned} (1^3 + 2^3 + 3^3 + \dots + k^3) + (k+1)^3 &= \frac{k^2(k+1)^2}{4} + (k+1)^3 = \\ &= \frac{(k+1)^2}{4} (k^2 + 4k + 4) = \frac{(k+1)^2(k+2)^2}{4} = \left(\frac{(k+1)(k+2)}{2} \right)^2. \end{aligned}$$

Valóban azt kaptuk, amit az első $k+1$ szám köbének összegére vártunk. Ezzel sikerült bebizonyítani, hogy a talált szabályosság tovább öröklődik bármely számról a következőre. 8-ra láttuk az állítás helyességét. A fenti megfontolást $k=8$ -ra alkalmazva következik, hogyha 8-ra helyes volt, helyes 9-re is. De ha 9-re helyes, akkor alkalmazhatjuk $k=9$ -cel is az utolsó átalakítást és kapjuk, hogy 10-re is helyes az állítás, s. í. t. A főnti átalakítással tehát sikerült próbálgatásunkat bizonyító erejűvé tenni. Az (1) összefüggés helyes minden n -re.

*

Ez a bizonyításmód erősen elüt a matematika egyéb bizonyításaitól. Mindenek előtt abban, hogy nem derít arra fényt, hogy miért igaz a tétel. Más bizonyításnál, ha a felmerült probléma megoldását el is felejtjük, de a megoldáshoz vezető alapgondolatra emlékszünk, akkor többnyire sikerül rekonstruálni ennek segítségével a megoldást is. Hiába emlékezünk azonban a számok köbének összegezéséből annyira, hogy az eredményt a főnti módon minden számról az eggyel nagyobbba következtetve bizonyítottuk, ennek a módszernek segítségével nem lehet az eredményre rátalálni, csak ha már valahonnan sejtjük az eredményt, azt igazolni sikerül.

Ez a bizonyítás az egész számok sorának egyszerű szabályosságát használja fel. Azt, hogy mindegyiknek van egy szomszédja és szomszédától és szomszédig menve egyszer minden pozitív számhoz eljutunk. Így, ha az egyiknek van valamilyen tulajdonsága (pl. az, hogy odáig a köbszámok (1) szerint adhatók össze) és ez a tulajdonság átöröklődik róla a következőre is és bármelyik számról, amelynek megvan, átöröklődik a következőre, akkor biztos hogy minden pozitív egész számnak megvan ez a tulajdonsága.

A bizonyítás ezek szerint két kérdést kell, hogy tisztázzon. Először is kell keresni egy egész számot, amire igaz az állítás. Ez szokott a bizonyítás könnyebb része lenni, de éppen olyan lényeges, mint a másik: megmutatni, hogy minden számról, amelynek megvan ez a tulajdonsága, átöröklődik a rákövetkezőre.

Összehasonlítottuk a matematikai próbálgatásokat a természettudományok kísérleti módszerével. Ott bőséges kísérleti anyag alapján keresik meg az azokban közös törvényszerűséget. Ezt a következtetési módot nevezik indukciónak. A természettudósok a jelenségeket igyekeznek minél változatosabb körülmények közt megfigyelni és minél több esetben, nehogy olyanféle látszatigazságokat véljenek természeti törvényeknek, mint a mi próbálkozásainkban a 21-gyel

osztható számok próbája volt. Ennek ellenére a természettudományok útja az hogy a megfigyelések finomodásával és a mélyebb összefüggések felismerésével tapasztalati törvényeinkről is kiderül, hogy nem pontosak s így újabbakkal kell helyettesíteni őket, amelyeknek a régiek csak bizonyos feltételek melletti speciális esetei.

Az elmondott matematikai következtetés ehhez csak nagyon kevésben hasonlít. Igaz, hogy próbálgatással sikerült megtalálni a fenti példában a törvényszerűséget, de azután éppen nem a sokszori kísérletre alapítottuk a bizonyítást. Ha már tudjuk, hogyan szól a törvényszerűség, amit be akarunk bizonyítani, akkor elég akár csak egyetlen esetben is kipróbálni és azután megmutatni, hogy ha egy számra teljesül, akkor a következőre is teljesül ez a törvényszerűség. Ezt a bizonyításmódot mégis *teljes indukciónak* szokás nevezni.

Lényegesen különbözik abban is a természettudományok kutatási módszerétől ez a módszer, hogy csak egész számokra vonatkozó tételek bizonyítására alkalmas, hisz alapját éppen az egész számok sorának egyszerű szerkezete adja.

*

Gyakorlásul bizonyítsuk be a következő azonosságot:

$$\frac{x}{1-x^2} + \frac{x^2}{1-x^4} + \frac{x^4}{1-x^8} + \dots + \frac{x^{2^{n-1}}}{1-x^{2^n}} = \frac{1}{1-x} \frac{x-x^{2^n}}{1-x^{2^n}}$$

Próbáljuk ki az állítást $n = 1$ -re. Ekkor a baloldalon csak az első tag áll, a jobbon

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

tehát az állítás ebben az esetben igaz.

Meg kell még mutatnunk, hogy ha valamilyen $n = k$ -ra helyes az egyenlőség, akkor igaz az $n = k + 1$ esetén is. $n = k + 1$ esetén a következő összeget kell átalakítani:

$$\frac{x}{1-x^2} + \frac{x^2}{1-x^4} + \frac{x^4}{1-x^8} + \dots + \frac{x^{2^{k-1}}}{1-x^{2^k}} + \frac{x^{2^k}}{1-x^{2^{k+1}}}$$

Feltevés szerint az első k tag összegéről már tudjuk, hogy így írható: $\frac{1}{1-x} \frac{x-x^{2^k}}{1-x^{2^k}}$. Ehhez kell még $\frac{x^{2^k}}{1-x^{2^{k+1}}}$ -et adni. Vonjuk össze a két törtet, lehetőleg alacsony fokú közös nevezőt használva: A második tört nevezője így írható:

$$\begin{aligned} 1-x^{2^{k+1}} &= 1-x^{2^k \cdot 2} = 1-(x^{2^k})^2 = (1-x^{2^k})(1+x^{2^k}) \\ \text{s így } \frac{1}{1-x} \frac{x-x^{2^k}}{1-x^{2^k}} + \frac{x^{2^k}}{1-x^{2^{k+1}}} &= \frac{(x-x^{2^k})(1+x^{2^k}) + x^{2^k}(1-x)}{(1-x)(1-x^{2^k})(1+x^{2^k})} = \\ &= \frac{x-x^{2^k} + x^{2^{k+1}} - x^{2^{k+1}} + x^{2^k} - x^{2^{k+1}}}{(1-x)(1-x^{2^{k+1}})} = \frac{1}{1-x} \cdot \frac{x-x^{2^{k+1}}}{1-x^{2^{k+1}}} \end{aligned}$$

és $k + 1$ tagra is ez a várható összeg. Ezzel megmutattuk, hogy a tétel érvényessége nem szakadhat meg semmilyen egész számnál, tehát igaz bármely egész számra

*

Egész számokra vonatkozó tételek bizonyítására alkalmas a teljes indukció, egész számokra vonatkozó tételek azonban nemcsak az egész számok tanában, az úgynevezett számelméletben fordulnak elő. Egész számokra vonatkozik például a következő geometriai kérdés is: adott számú egyenes hány részre oszthatja maximálisan a síkot? Ez a maximális szám csak az egyenesek számától, tehát egy pozitív egész számtól függ. Némi próbálgatással rájövünk, hogy a második egyenes 2-vel a harmadik 3-mal, a negyedik 4-gyel növeli „legjobb esetben” a részek számát és pedig akkor, ha nem megy át az előző egyenesek egyetlen metszéspontján sem. Az első egyenesnél egy kis eltérés van, mert két részre osztja a síkot. (Ha tetszik, eggyel szaporítja a részeinek számát, mert kezdetben is állt egy részből a sík.) Így n egyenes a síkot maximálisan

$$1 + (1 + 2 + 3 + \dots + n) = 1 + \frac{n(n+1)}{2} = \frac{1}{2}(n^2 + n + 2)$$

részre osztja. Ha minden tévedés lehetőségét ki akarjuk zárni, akkor megint nem addig fogjuk próbálgatni különböző n -ekre, míg meg nem unjuk, hanem csak egy esetre próbáljuk ki, pl. $n = 1$ -re: $\frac{1}{2}(1^2 + 1 + 2) = 2$ és egy egyenes valóban két részre osztja a síkot. Nézzük most meg, hogy igaz marad-e akárhányszor is! Jelöljük ezt az „akárhányszor”-at k -val tehát tegyük fel, hogy $k - 1$ egyenesről már tudjuk, hogy maximálisan $\frac{1}{2}[(k - 1)^2 + (k - 1) + 2]$ részre osztják a síkot. Ez két állítást foglal magában: „van $k - 1$ olyan egyenes, amely ennyi részre osztja, a síkot” és „ $k - 1$ egyenessel több részre osztani nem lehet”. Azt kell megmutatnunk, hogy az állítás mindkét fele érvényben marad k számú egyenesre is, persze $k - 1$ helyére mindenütt k -t írva.

Legyen meghúzva valahogy $k - 1$ egyenes. A k -adik egyenes azáltal szaporítja a részek számát, hogy egyeseken áthalad azokat kettéosztja. Annyit oszt szét, ahány szakaszra a $k - 1$ egyenes a k -adikat osztja. Ez akkor lesz a legnagyobb, ha a k -adik egyenes nem megy át az első $k - 1$ egyenes közül semelyik kettőnek a metszéspontján sem, és nem párhuzamos egyikkel sem. Ekkor $k - 1$ metszéspont keletkezik rajta, s ez k részre osztja az egyenest, tehát az egyenes hozzávétele ez esetben k -val szaporítja a sík részeinek a számát, ennél többel viszont semmiképpen sem.

Ebből következik, hogy k egyenes akkor osztja legtöbb részre a síkot, ha az első $k - 1$ annyi részre osztja, amennyire csak $k - 1$ egyenessel lehet, tehát $\frac{1}{2}(k^2 - k + 2)$ -re, a k -adik egyenes pedig metszi mind a $k - 1$ egyenest és pedig különböző pontokban. Ekkor a síkot összesen

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

részre osztottuk. Ennyire tehát fel lehet osztani k számú egyenessel a síkot, többre pedig nem amint ezt vártuk. Tételünk tehát minden n -re igaz.

*

Egy baj azért van a teljes indukcióval: be lehet vele bizonyítani, hogy a síkban akárhány egymást páronként metsző egyenest veszünk, ezek mindig egy közös pontban metszik egymást. Először is próbáljuk ki a legegyszerűbb esetben: két egyenesnél ez magától értetődő: ha metszik egymást, akkor egy pontban. Tegyük most föl, hogy valamilyen k számig már bebizonyítottuk a tételt; tehát bárhogy veszünk k számú, vagy kevesebb egyenest, ezek egy ponton mennek keresztül. Mit tudunk mondani $k + 1$ egyenesről? Vegyük el a $k + 1$ -ediket. A maradó k számú a feltétel szerint egy közös ponton megy át. De a $k + 1$ -edik helyett vegyünk el most egy másik egyenest. Megint k számú marad, ezek tehát szintén egy ponton mennek keresztül, és köztük van most már az előbbi $k + 1$ -edik is. Az is nyilvánvaló, hogy ez a két pont ugyanaz, mert vegyük el most mind a két egyenest, feltétel szerint a maradó $k - 1$ egyenesről is tudjuk, hogy egy ponton mennek keresztül, tehát ezen a ponton kell a maradó két egyenesnek is átmennie.

Ezzel az állítást be is bizonyítottuk, ez azonban mit sem változtat, azon a tényen, hogy az állítás nem igaz. Hol van tehát a hiba? Mielőtt a teljes indukció módszerét kétségbe vonnánk, nézzük meg jobban a bizonyítást, hogy kiáll-e minden kritikát? Jó lesz először is pontosan elmondani magunknak, hogy milyennek is kell egy helyes indukciós bizonyításnak lennie, mert akkor tudjuk jól ellenőrizni, hogy ez a bizonyítás valóban olyan-e.

Egy teljes indukciós bizonyítás két elég egyszerű lépésből áll. Egy egész számokról szóló állításról először is megmutatjuk, hogy igaz 1-re vagy valamilyen más egész számra, amelytől kezdve helyes az állítás. Ezután megmutatjuk, hogy ha valamilyen egész számra már igaz az állítás, akkor igaz a rákövetkezőre is. (Ezt a két egymás utáni számot szoktuk k -val és $k + 1$ -gyel, vagy $k - 1$ -gyel és k -val jelölni, ahogy kényelmesebb. Ez nem változtat a lényegen.)

Ezt a bizonyításmódot azért ítéljük helyesnek, mert van egy kezdőérték, amelyikre igaz a tétel és ettől elindulva következtethetünk arra, hogy mindig a következő egész számra is igaz a tétel. Már pedig így előbb-utóbb bármely, a kiindulási értéknél nagyobb egész számhoz eljutunk egyszer, tehát a tétel ettől kezdve minden egész számra igaz.

A fenti példánál 2-re még helyes az állítás. Keressük meg az első számot, amire nem igaz, ha erre megpróbáljuk az általános módszer szerint bizonyítani az állítást, akkor ki kell, hogy derüljön, hol jutottunk hibás következtetésre. Esetünkben már 3-ra nem igaz a tétel, tehát nézzük meg, hogyan kellene a bizonyítást második lépése szerint 2-ről 3 egyenesre átvinni a tételt. Legyen adva 3 egyenes, vegyük el a harmadikat, a maradó két egyenes egy ponton megy keresztül. – Ez valóban helyes, mert két egyenesre még igaz a tétel. – Vegyük el most valamelyik másik egyenest. Megint kettő marad, tehát megint egy ponton mennek keresztül. – Ez is igaz. – Most már csak azt kellene belátni, hogy ez a két pont mindig ugyanaz. – Na vajon hogyan? – Vegyük el mind a két egyenest, mind a kettő ugyanazon a ponton megy keresztül, amin a visszamaradók.

– Na itt a hiba. Egy egyenes marad vissza, és ez nem határoz meg egyértelműen egy pontot, amin a másik kettőnek át kellene mennie. A bizonyításban kifejezetten felhasználtuk, hogy nem csak a kérdéses számot megelőzőre, hanem az azelőttire is igaz az állítás. Ekkor már ahhoz, hogy valamely számra az előzőkről átvigyük állításunkat, mindig az kell, hogy előzőleg már két egész számra tudjuk a tétel helyességét. Minden rendben is volna, ha háromra igaz volna az előbbi állítás, csak éppen hogy nem igaz háromra. És ez nemcsak olyan kis szépséghiba, mert ennek folytán azután már egyetlen nagyobb számra sem igaz.

Ez nagyon élesen mutatja azt is, hogy bármilyen egyszerű része többnyire a bizonyításnak, egy kezdő értékre megmutatni a tétel helyességét, mégis éppen olyan lényeges, mint a másik lépés. Csak a kettő együtt bizonyítja az állítást.

Ezt mindjárt megmutatjuk még egy példán, de most már nem álokoskodással. Igen sok embert érdekelnek a prímszámok tulajdonságai. Bizonyára ismeritek annak bizonyítását, hogy végtelen sok van belőlük. De nagyon szabálytalanul oszlanak el az egész számok közt. Ez azért nem jelenti azt, hogy ne lehetne sok mindent megtudni róluk. Hirtelen végiggondolva úgy látszik, pl. hogy bármeddig elmenve is a számok közt, legfeljebb a felük lehet prímszám, hiszen a másik felük páros. Ez persze így nagyon pontatlan állítás, már csak azért is, mert a 2 páros szám, de prímszám is, csak a nála nagyobb páros számok összetettek. Hozzájön az is, hogy az 1-et viszont nem szokás prímmnek nevezni. Így 3-ig 2 prímszám van, 5-ig 3; tehát több, mint a fele a számoknak. Nézzük hát meg, mit is lehet pontosan állítani.

Hogy a matematika nyelvén beszélhessünk, adjunk nevet az x -nél nem nagyobb prímszámok számának, ahol x

tetszőleges egész szám. Ennek a szokásos jele $\pi(x)$. Első kijelentésünket akkor így írhatnánk:

$$(2) \quad \pi(x) \leq \frac{x}{2}$$

Erre abból akarunk következtetni, hogy két egymásutáni számból legfeljebb az egyik lehet prímszám. Ez igaz is a 2-n túl, tehát ha $x \geq 2$, $\pi(x+2) \leq \pi(x) + 1$. Ha most x egy olyan szám, amelyre (2) igaz, akkor $\pi(x+2) \leq \frac{x}{2} + 1 = \frac{x+2}{2}$, tehát akkor $x+2$ is olyan szám. Itt tehát nagyapáról unokára öröklődő tulajdonságot találunk. Azt bizonyítottuk csak be, hogy ha valamely x -re $\pi(x) \leq \frac{x}{2}$, akkor onnan minden második egész x -re is igaz. Tehát pl. $\pi(2) = 1 = \frac{2}{2}$ s így (2) minden páros x -re igaz. A páratlanok közt azonban láttunk olyanokat, amikre nem igaz. Valamit azért a páratlan x -ekre is mond a bizonyítás. Ha találunk köztük egy olyan x -et, melyre helyes a (2) egyenlőtlenség, akkor onnan mindre, tehát onnan minden egész x -re is igaz. Próbáljuk ki: $\pi(7) = 4 > \frac{7}{2}$, de $\pi(9) = 4 < \frac{9}{2}$ s így végül kimondhatjuk, hogy a (2) egyenlőtlenség minden x -re igaz, ha $x \geq 8$, mivel páros x -ekre mindig igaz.

Tehát valóban lényeges volt itt is megkeresni, hogy honnan helyes az állítás. Mégpedig nem is egy, hanem két *szomszédos* számra kell megmutatni az állítás helyességét, mert csak onnan kezdve tudjuk, hogy tovább minden számra helyes.

1. feladat. A bebizonyított tétel még nem sokat árul el a prímszámok számáról, bár pl. a Csebysev-tétel, bizonyítására elég lesz ennyit tudni róla. Azt is be lehet bizonyítani, hogy valahonnan kezdve $\frac{x}{3}$ -nál sem lesz nagyobb $\pi(x)$. Elárulok annyit, hogy ehhez már nem 2, hanem 6 egymásutáni számot kell egyszerre figyelembe venni. A bizonyítást ezután már rátok bízom. Azt is ti állapítsátok meg, hogy melyik x -től kezdve lesz igaz.

*

Szinte minden bizonyításban kicsit más formában használtuk a teljes indukciót. Az volt a célunk, hogy lehetőleg sok oldalról világítsuk meg használatát. Most még két érdekes formáját mutatjuk az indukciónak.

A számelméletben nagyrészt a számok oszthatóságával kapcsolatos kérdésekkel foglalkozunk s így sokszor van szükségünk a számok legnagyobb közös osztójára is. Használunk is rá egy külön jelet: a számokat vesszővel elválasztva kerek zárójelbe tesszük. Tehát $(15, 72)$ egy számot jelent, amivel maradék nélkül osztható a 15, meg a 72 is mégpedig a legnagyobb ilyen számot, vagyis 3-at: $(15, 72) = 3$. Ennek a legnagyobb közös osztónak érdekes és sokszor használható tulajdonsága, hogy két szám legnagyobb közös osztója mindig előállítható úgy, mint az egyik szám egy többszörösének és a másik szám egy többszörösének különbsége, pl. $(15, 72) = 5 \cdot 15 - 1 \cdot 72$. Általában két pozitív egész szám, a és b , legnagyobb közös osztója előállítható így:

$$(3) \quad (a, b) = xa + yb,$$

ahol x és y (pozitív vagy negatív) egész számnak. (Nem tudjuk előre, melyik szám többszöröse fog pozitív, melyiké negatív előjellel szerepelni, de ez nem is fontos nekünk, azért írtuk ilyen alakba.)

Ezt az állítást számpár kisebbik száma szerint haladó teljes indukcióval fogjuk bizonyítani. Legyen a a kisebbik a két szám közül, ha, nem egyenlők, röviden legyen: $a \leq b$. Először is próbáljuk ki az állítást $a = 1$ -re:

$$(1, b) = 1 = 1 \cdot 1 + 0 \cdot b,$$

tehát $x = 1$, $y = 0$ -val teljesül az állítás.

Tegyük fel most, hogy valamely $a = k$ értékig már beláttuk az állítás helyességét, tehát ha $a \leq k$ és b tetszőleges szám, tudjuk, hogy mindig található olyan x és y egész szám, amire teljesül a (3) egyenlőség. Nézzük most, segít-e valamit a (k, b) legnagyobb közös osztó (3) alakú előállításának kereséséhez, ha ezt tudjuk. Az láthatólag nem sokat, ha a közvetlen előzőre tudjuk, hisz könnyű látni, hogy $k-1$ relatív prím k -hoz (nem lehet 1-nél nagyobb közös osztójuk) s így általában számoknak $k-1$ -gyel való közös osztójuk nem sokat mondhat k -val való közös osztójukról. Nem is úgy vezethetjük vissza kisebb számra a feladatot, ha kivonunk 1-et valamelyikből, hanem ha a kisebbet vonjuk ki a nagyobból. Ilyenkor ugyanis a különbségnek és a kisebbik számnak a közös osztója ugyanaz, mint az eredeti két számé. Gyorsabban járhatunk el, ha nem is egyszer vonjuk le a kisebbik számot, hanem ahányszor csak lehet, vagyis osztjuk a nagyobb számot a kisebbel.

Ezek szerint az indukció második lépése így végezhető el: Keressük a (k, b) legnagyobb közös osztót, ahol $k \leq b$, ha tudjuk, hogy valamennyi k -nál kisebb számnak és egy tetszőleges számnak a legnagyobb közös osztója előállítható (3) alakban.

Osszuk el b -t k -val. Lehet, hogy megvan benne maradék nélkül, ekkor $(k, b) = k = 1 \cdot k + 0 \cdot b$ a keresett előállítás. Ha nincs meg maradék nélkül, az azt jelenti, hogy b ilyen alakba írható: $b = c \cdot k + m$, ahol c valamilyen egész szám. (a hányados), m pedig a maradék, tehát k -nál, kisebb pozitív egész szám. Azt állítjuk, hogy $(m, k) = (k, b)$. Egyrészt az előbbi egyenlőség szerint b osztható m és k minden közös osztójával. Másrészt m -et kifejezve $m = b - c \cdot k$, tehát m -nek is osztója k és b legnagyobb közös osztója. Mármost az indukciós feltevésünk szerint

$$(m, k) = x_1 \cdot m + y_1 \cdot k,$$

m -et viszont épp most fejeztük ki b -vel és k -val. Ezt felhasználva végül is nyerjük, hogy

$$\begin{aligned}(k, b) &= (m, k) = x_1 m + y_1 k = x_1(b - ck) + y_1 k = \\ &= (y_1 - cx_1)k + x_1 b.\end{aligned}$$

Ezzel teljes is a bizonyításunk, csak egy kétely marad. Hát nem követtük el megint ugyanazt a hibát, mint az egy ponton átmenő egyeneseknél? Hisz itt sem csak a közvetlen előző esetre használtuk fel az indukciós feltétel helyességét a második esetben, sőt nem is az előző két esetben, hanem az összes megelőzőben, mert mindegyikre szükség lehet, a szerint, hogy b milyen érték. Ha azonban lépésről-lépésre menve próbálunk meg eljutni valamilyen értékig, akkor mindig olyan értékekre lehet csak szükségünk, amelyeket már megvizsgáltunk. Előző, hamis bizonyításunknál viszont mindig két megelőző esetre lett volna szükségünk, akkor is amikor még csak egy esetet vizsgáltunk meg, a két egyenesét, az egy egyenesre meg éppen értelme sincs a tételnek. Itt tehát nem érhet olyan meglepetés, mint ott, hogy olyan esetben is szükségünk van a tételre, amire még nincs kipróbálva.

Valójában nem is azt kell itt csinálnunk, hogy végigpróbálgatunk minden lehetőséget 1-től a -ig ahhoz, hogy (a, b) -nek megkeressük a (3) alakú előállítását. Ez nem is vihető keresztül, hisz b akármilyen szám lehet. Itt a bizonyítás második lépését használva fel, állandóan kisebbítjük a két számot osztással, míg vagy maradék nélkül meg nincs egyszer a kisebb szám a nagyobbban, vagy 1 nem lesz a maradék. Vagyis az ismert euklideszi algoritmussal megkeressük a legnagyobb közös osztót és ekkor a közben fellépő osztási hányadosokból lehet lépésről-lépésre az indukciós bizonyítás második lépésének mintájára eljutni a legnagyobb közös osztó (3) alakú előállításához.

2. feladat. A tétel alkalmazásával keressétek az

$$ax + by = c$$

elsőfokú határozatlan egyenletnek egész x, y megoldását, ha a, b és c egész számok. Mi a feltétele annak, hogy legyen ilyen megoldás?

3. feladat. Hogyan lehet az előbbi egyenlet összes megoldásait előállítani?

*

Utolsó példának egy egyenlőtlenséget bizonyítunk be számok számtani és mértani középértéke közt. Tudjuk, hogy a pozitív $a_1, a_2, a_3, \dots, a_n$ számok számtani közepének az

$$\frac{a_1 + a_2 + \dots + a_n}{n}$$

értéket, mértani közepének pedig az

$$\sqrt[n]{a_1 a_2 \dots a_n}$$

értéket szoktuk nevezni. Ezek közül mindig a számtani közép nagyobb, kivéve, ha minden szám egyenlő, mert akkor mind a két középérték is ezzel a közös értékkel egyenlő. A tagok száma szerint kínálkozik teljes indukciót végezni. Persze $n = 1$ -re nincs is értelme középértékről beszélni, tehát $n = 2$ -re kell először is bebizonyítani az állítást, vagyis azt, hogy ha a és b pozitív számok, akkor

$$(4) \quad \frac{a+b}{2} \geq \sqrt{ab}$$

Most ez a lépés sem nyilvánvaló, be kell tényleg bizonyítani. Mivel mind a két oldalon pozitív szám áll, elég bizonyítani, hogy négyzetükre fennáll az egyenlőtlenség:

$$\left(\frac{a+b}{2}\right)^2 \geq ab,$$

mert ebből négyzetgyökvonással megkaphatjuk (4)-et. Ehelyett még könnyebbnek látszik egy olyan egyenlőtlenséget bebizonyítani, melynek egyik oldalán 0 áll, tehát vigyük át ab -t másik oldalra:

$$\left(\frac{a+b}{2}\right)^2 - ab = \frac{a^2 - 2ab + b^2}{4} \geq 0.$$

Ha ezt bebizonyítjuk, abból az előbbi is következik, csak hozzá kell adni mindkét oldalhoz ab -t. Ezt viszont nem is kell bebizonyítani, hiszen a számláló $(a-b)$ -nek a négyzete, tehát nem lehet negatív. 0 is csak akkor lehet, ha $a = b$. Ebből pedig a mondottak szerint lépésről-lépésre következik a (4) egyenlőtlenség. (Kiindulhattunk volna persze mindjárt ebből a helyes egyenlőtlenségből és átalakíthattuk volna, míg megkapjuk (4)-et, de akkor az nem derült volna ki, honnan jutott eszünkbe éppen ezt az egyenlőtlenséget felírni.)

Ezzel megtettük az első lépést, bebizonyítottuk a tételt $n = 2$ -re. Baj van azonban a továbbmenettel. Ha azt gondolnánk, hogy három szám számtani közepét vehetjük úgy, hogy előbb kettőt, aztán a kapott számát és a harmadikét vesszük, akkor nagyon tévedünk, mert

$$\frac{\frac{a+b}{2} + c}{2} = \frac{a+b+2c}{4} \neq \frac{a+b+c}{3}, \text{ kivéve ha } c = \frac{a+b}{2}.$$

Három számnak nem lehet így lépésenként kiszámítani a számtani közepét, de ki lehet négyét, 4 szám esetén vehetjük kettő-kettő számtani közepét, külön és azután ezeknek a számtani közepeknek a számtani közepét. Ha a négy számot a_1, a_2, a_3, a_4 -gyel jelöljük,

$$\frac{\frac{a_1+a_2}{2} + \frac{a_3+a_4}{2}}{2} = \frac{a_1 + a_2 + a_3 + a_4}{4}.$$

Így az előbbi egyenlőtlenséget is kétszer alkalmazhatjuk:

$$\begin{aligned} \frac{a_1 + a_2 + a_3 + a_4}{4} &= \frac{\frac{a_1+a_2}{2} + \frac{a_3+a_4}{2}}{2} \geq \sqrt{\frac{a_1 + a_2}{2} \cdot \frac{a_3 + a_4}{2}} \geq \\ &\geq \sqrt{\sqrt{a_1 a_2} \sqrt{a_3 a_4}} = \sqrt[4]{a_1 a_2 a_3 a_4}. \end{aligned}$$

Igaz tehát az egyenlőtlenség négy szám számtani és mértani közepére is. Ezt a számítást most már ismételtük is, de mindig csak kétszer annyi tagra tudjuk átvinni az egyenlőtlenséget, mint amennyire már igazoltuk, tehát 2-ről 4-re, 4-ről 8-ra, stb.

Így tehát csak azt sikerül bebizonyítani, hogy ha a tagok száma $n = 2^m$, akkor igaz a tétel, hogy a számtani közép nagyobb, vagy legalább akkora, mint a mértani.

$m = 1$ -re már bebizonyítottuk a tételt. Tegyük fel, hogy valamilyen k kitevőre, tehát 2^k számú tagra igaz a tétel: ebből következik $2 \cdot 2^k = 2^{k+1}$ -re is. Legyenek u. i. a számok $a_1, a_2, \dots, a_{2^k}, a_{2^k+1}, a_{2^k+2}, \dots, a_{2^{k+1}}$. A számtani közepük, – jelöljük röviden A -val

$$\begin{aligned} A &= \frac{a_1 + a_2 + \dots + a_{2^k} + a_{2^k+1} + a_{2^k+2} + \dots + a_{2^{k+1}}}{2^{k+1}} = \\ &= \frac{\frac{a_1+a_2+\dots+a_{2^k}}{2^k} + \frac{a_{2^k+1}+a_{2^k+2}+\dots+a_{2^{k+1}}}{2^k}}{2} \geq \\ &\geq \sqrt{\frac{a_1 + a_2 + \dots + a_{2^k}}{2^k} \cdot \frac{a_{2^k+1} + a_{2^k+2} + \dots + a_{2^{k+1}}}{2^k}}, \end{aligned}$$

mert két tagra tudjuk, hogy igaz az egyenlőtlenség. De az indukciós feltevés szerint (hogy a k kitevőig már eljutottunk a bizonyításban)

$$\begin{aligned} \frac{a_1 + a_2 + \dots + a_{2^k}}{2^k} &\geq \sqrt[2^k]{a_1 \cdot a_2 \cdot \dots \cdot a_{2^k}} \\ \text{és} \quad \frac{a_{2^k+1} + a_{2^k+2} + \dots + a_{2^{k+1}}}{2^k} &\geq \sqrt[2^k]{a_{2^k+1} \cdot a_{2^k+2} \cdot \dots \cdot a_{2^{k+1}}}, \end{aligned}$$

tehát

$$\begin{aligned} A &\geq \sqrt{\sqrt[2^k]{a_1 a_2 \dots a_{2^k}} \sqrt[2^k]{a_{2^k+1} a_{2^k+2} \dots a_{2^{k+1}}}} = \\ &= \sqrt[2^{k+1}]{a_1 a_2 \dots a_{2^k} a_{2^k+1} a_{2^k+2} \dots a_{2^{k+1}}}. \end{aligned}$$

Mit csináljunk azonban a közbeeső esetekkel, tehát amikor a tagok száma pl. 3 vagy 6? Ezeket az eseteket most már elég volna bármely megoldott esetre visszavezetni. Láttuk, hogy a kevesebb tag esetére való visszavezetésnek nehézségei vannak. Hozzá lehet azonban venni új tagokat a meglévőkhöz úgy, hogy a számtani közép ne változzék meg. A számtani közép olyan szám, hogy ha az összes számokat vele helyettesítjük, akkor a számok összege nem változik. Három szám, a_1, a_2, a_3 , esetén például ha a számtani közepet A -val jelöljük,

$$A = \frac{a_1 + a_2 + a_3}{3}, \quad \text{azaz} \quad a_1 + a_2 + a_3 = 3A.$$

Ha most a három számhoz negyediket hozzávesszük A -t, akkor a négy számnak is ugyanezen A lesz a számtani közepe: $a_1 + a_2 + a_3 + A = 4A$, azaz valóban $\frac{a_1 + a_2 + a_3 + A}{4} = A$. De négy számra már bebizonyítottuk a számtani és mértani közép közti egyenlőtlenséget, tehát

$$A = \frac{a_1 + a_2 + a_3 + A}{4} \geq \sqrt[4]{a_1 a_2 a_3 A}.$$

A könnyebb számolás végett emeljük mindkét oldalt negyedik hatványra. Mivel pozitív számról van szó, érvényes marad az egyenlőtlenség:

$$A^4 \geq a_1 a_2 a_3 A, \quad \text{tehát} \quad A^3 \geq a_1 a_2 a_3,$$

Amiből következik, A -ra, ami három szám számtani közepét jelenti, hogy

$$A = \frac{a_1 + a_2 + a_3}{3} \geq \sqrt[3]{a_1 a_2 a_3}.$$

Itt tehát 4 szám esetéről sikerült visszakövetkeztetnünk 3 számra. Ugyanígy eljuthatunk most már bármely számhoz úgy, hogy keressünk egy nála nagyobb 2-hatványt és abból következtetünk vissza kevesebb tagra.

A bizonyítás teljes menete a következő: Bebizonyítjuk az állítást indukcióval 2^m számú tag esetére, ahol m tetszőleges egész szám. (Vagyis bebizonyítjuk, hogy 2 tagra igaz és bebizonyítjuk, hogy ha 2^k számú tagra igaz, akkor igaz 2^{k+1} tagra is.) Végül megmutatjuk, hogy ha valamilyen számú tagra igaz az egyenlőtlenség, akkor igaz eggyel kevesebbre is.

Ezek közül már csak az utolsó lépés van hátra. Tegyük fel, hogy valamilyen $l+1$ számú tagra fennáll az egyenlőtlenség, bizonyítsuk be, hogy akkor teljesül l számúra is. Legyen a_1, a_2, \dots, a_l , az l számú tag $l+1$ -ediknek hozzávesszük számtani közepüket, A -t: $A = \frac{a_1 + a_2 + \dots + a_l}{l}$. Mivel innen $a_1 + a_2 + \dots + a_l = l \cdot A$, tehát $a_1 + a_2 + \dots + a_l + A = (l+1)A$, vagyis $\frac{a_1 + a_2 + \dots + a_l + A}{l+1} = A$. Feltétel szerint $l+1$ számúra már tudjuk, hogy teljesül az egyenlőtlenség, tehát

$$A = \frac{a_1 + a_2 + \dots + a_l + A}{l+1} \geq \sqrt[l+1]{a_1 a_2 \dots a_l A}.$$

Innen $A^{l+1} \geq a_1 a_2 \dots a_l A$ vagyis $A^l \geq a_1 a_2 \dots a_l$ és l -edik gyököt vonva, (szabad, mert mindkét oldalon pozitív szám áll) :

$$A = \frac{a_1 + a_2 + \dots + a_l}{l} \geq \sqrt[l]{a_1 a_2 \dots a_l}.$$

*

Gyakorlásul oldjátok meg a következő feladatokat:

4. Számítsuk ki az $x^2 + x + 41$ kifejezés értékét különböző egész helyeken és bontsuk törzstényezőkre.

Igaz-e, hogy a kifejezés minden egész x -re törzsszámot állít elől?

5. Bizonyítsuk be, hogy egy egyváltozós polinom, akárhányad fokú, nem állíthat elő a változó minden egész értékére prímszámot.

6. Adva vannak a térben egyenesek, melyek páronként metszik egymást, de semelyik három, nem fekszik egy síkban. Bizonyítsuk be, hogy az összes egyenesek egy ponton mennek keresztül.

7. Mutassuk meg, hogy

$$(5) \quad \frac{a_1}{1+a_1} + \frac{a_2}{(1+a_1)(1+a_2)} + \dots + \frac{a_n}{(1+a_1)(1+a_2)\dots(1+a_n)} = 1 - \frac{1}{(1+a_1)(1+a_2)\dots(1+a_n)}.$$

8. Mutassuk meg, hogy

$$(6) \quad \sin \alpha + \sin 2\alpha + \dots + \sin n\alpha = \frac{\sin \frac{n\alpha}{2} \sin \frac{(n+1)\alpha}{2}}{\sin \frac{\alpha}{2}}.$$