Az idei Arany Dániel tanulóversenyben a kezdők 3. kategóriájának döntőjében a következő feladatot kellett megoldani:

Melyik sorozatok teljesítik a következőket:

(1) a_n *szigorúan monoton növekvő;*

(2) $a_2 = 2$*;*

(3) *a sorozat minden tagja egész; végül*

(4) $a_{nm} = a_n a_m$*, valahányszor* $(n, m) = 1$*, vagy szavakkal: a sorozat* nm*-edik tagja az* n*-edik és* m*-edik tag szorzata, valahányszor* n *és* m *relatív prímek.*

Az $a_n = n$ sorozat nyilván kielégíti a feltételeket. Némi próbálkozás után az az érzésünk, hogy más sorozat nem felel meg. Az mindenesetre világos, hogy $a_1 = 1$, hiszen $2 = a_2 = a_1 a_2 = 2a_1$. Ebből, és a sorozat monotonitásából következik, hogy a sorozat minden tagja pozitív egész. Így $a_n \geq n$ minden n-re, hiszen a_n a sorozat n-edik tagja, és (1) szerint a sorozat minden tagja különböző. Ha pedig valamely k-ra $a_k > k$, akkor minden k-nál nagyobb n-re is $a_n > n$. Elég tehát *végtelen* sok olyan k-t mutatni, amelyre $a_k = k$, ebből már következik, hogy *minden* n-re $a_n = n$.

Valójában csak az első lépés nehéz, tudniillik annak belátása, hogy $a_3 = 3$. Ha ugyanis ezt be tudjuk látni, akkor $a_6 = a_2 a_3 = 2 \cdot 3 = 6$ (mert 2 és 3 relatív prímek). Ebből következik, hogy minden hatnál kisebb n-re is $a_n = n$. De $a_{30} = a_5 a_6 = 5 \cdot 6 = 30$, mert 5 és 6 relatív prímek, s ekkor minden harmincnál kisebb n-re is $a_n = n$. Általában is igaz, hogy ha $a_k = k$, akkor $a_{k-1} = k - 1$, másrészt $k - 1$ és k relatív prímek, tehát $a_{(k-1)k} = a_{k-1} a_k = (k-1)k$. Ezt az eljárást minden határon túl folytatva kapunk végtelen sok olyan n-et, amelyre $a_n = n$, tehát minden n-re $a_n = n$. (Érdemes megjegyezni, hogy szükség van az $a_3 = 3$ egyenlőségre is, $a_1 = 1$ és $a_2 = 2$ ugyanis még nem elég ahhoz, hogy „elinduljon" az eljárás, ilyenkor $k = 2$ és $(k-1)k$ nem nagyobb k-nál.)

Elég tehát azt belátni, hogy $a_3 = 3$. Ez a legegyszerűbben talán a következőképp történhet:

$$a_3 a_5 = a_{15} < a_{18} = a_9 a_2 = 2a_9 < 2a_{10} = 2a_2 a_5 = 4a_5,$$

ahonnan $a_5 > 0$ miatt következik, hogy $a_3 < 4$. Másrészt láttuk, hogy $a_3 \geq 3$, tehát $a_3 = 3$.

Ezzel befejeztük annak bizonyítását, hogy az (1)–(4) feltételeket egyetlen sorozat elégíti ki: az $a_n = n$ sorozat. (A bizonyítás Paulin Dánieltől származik.)

A bizonyított állítást más formában is kimondhatjuk. Nevezzük *számelméleti függvénynek* az olyan valós értékű függvényeket, amelyek értelmezési tartománya a pozitív egész számok halmaza. Ilyen számelméleti függvény például

$d(n)$, ami n (pozitív) osztóinak a számát jelöli,

$\sigma(n)$, ami n (pozitív) osztóinak összegét jelöli,

$\varphi(n)$, ami az n-nél kisebb, n-hez relatív prím pozitív egészek számát jelöli.

Ismeretes, hogy $d(n)$-t úgy lehet kiszámolni, hogy tekintjük n prímtényezős felbontásában az egyes prímek kitevőjét, mindegyikhez hozzáadunk egyet, majd az így kapott számokat összeszorozzuk. Ebből következik, hogy ha n és m prímtényezői különbözőek, vagyis n és m relatív prímek, akkor $d(n)d(m) = d(nm)$. (Ha viszont n és m nem relatív prímek, tehát van közös prímtényezőjük, akkor $d(n)d(m) > d(nm)$. Ha ugyanis n és m prímtényezős felbontásában e prím kitevője a illetve b, akkor nm-ben $a + b$, így e prím „adaléka" $d(n)d(m)$-ben $(a+1)(b+1)$, míg $d(nm)$-ben $a + b + 1$. Márpedig ha a és b pozitív, akkor $(a+1)(b+1) > a + b + 1$.)

Nem sokkal nehezebb belátni, hogy a $\sigma(n)$ függvényre is teljesül, hogy $\sigma(n)\sigma(m) = \sigma(nm)$, ha n és m relatív prímek. Ehhez mindössze annyit kell meggondolni, hogy ha n és m relatív prímek és d osztója nm-nek, akkor egyértelműen írható fel $d = d_1 d_2$ alakban, ahol d_1 osztója n-nek, d_2 pedig m-nek. (Megint igaz, hogy ha n és m nem relatív prímek, akkor $\sigma(n)\sigma(m) > \sigma(nm)$.)

Azokat a számelméleti függvényeket, amelyekre $f(n)f(m) = f(nm)$, ha n és m relatív prímek, *multiplikatív* függvényeknek nevezzük.

Nehezebb annak bizonyítása, hogy a harmadikként említett $\varphi(n)$ függvény is multiplikatív. A számelméletben még sok más multiplikatív függvényt is használnak. Az ilyen függvények aránylag jól kezelhetőek, mert minden értéküket ki tudjuk számítani, ha ismerjük értéküket minden olyan n-re, amely valamely prímszám hatványa. Így például könnyen kiszámolható, hogy ha p prím, akkor

$$\sigma(p^\alpha) = 1 + p + p^2 + \cdots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1}.$$

Ebből a σ függvény multiplikativitása miatt következik, hogy ha

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

akkor

$$\sigma(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \, \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdots \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}.$$

Segít a multiplikativitás a φ függvény értékének meghatározásánál is. Ha p prím, akkor $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$, hiszen p^α-hoz pontosan azok a nála kisebb pozitív egészek relatív prímek, amelyek nem oszthatók p-vel, s ezekből pontosan $p^{\alpha-1}$ van. Tehát $\varphi(p^\alpha) = p^\alpha\left(1-\frac{1}{p}\right)$. Ebből, továbbá abból, hogy φ multiplikatív, következik, hogy ha $n = p^\alpha q^\beta$, ahol p és q különböző prímek, akkor $\varphi(n) = p^\alpha q^\beta\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)$, és általában is, ha n prímosztói $p_1, p_2, \ldots, p_k$, akkor $\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_k}\right)$. Ezt egyébként közvetlenül, a logikai szita módszerével is be lehet látni.

Visszatérve a versenyfeladatra, az tehát a következő állítás igazolását kívánta:

1. tétel. *Ha az $a(n)$ multiplikatív számelméleti függvény minden értéke egész és szigorúan monoton növekszik, továbbá $a(2) = 2$, akkor minden n-re $a(n) = n$.*

A fent említett három függvényről könnyen látható, hogy nem monotonak: az osztók száma minden prímszámra 2, ha viszont $n > 2$ páros, akkor legalább három osztója van. Minthogy prímből is, páros számból is végtelen sok van, a $d(n)$ függvény nem monoton.

Hasonlóan derül ki az is, hogy $\sigma(n)$ sem monoton. Ha p prímszám, akkor $\sigma(p) = p+1$. Másrészt a $p-1$ számnak osztója 1, 2 és $p-1$ (ha $p > 3$, akkor e három szám különböző is), és $p+1$-nek osztója $1, 2, p+1$ (e három szám is különböző), tehát $\sigma(p-1) > p+2$ és $\sigma(p+1) > p+4$, mindkettő nagyobb $\sigma(p) = p+1$-nél, így a σ függvény sem monoton.

A φ függvény sem monoton, ezt is a prímszámok segítségével láthatjuk be: ha p prím, akkor minden nála kisebb pozitív egész relatív prím hozzá, másrészt ha $p > 2$, akkor p páratlan, tehát $p-1$ is, $p+1$ is páros, így a páros számok nem relatív prímek egyikhez sem. Ezért $\varphi(p-1) \le \frac{p-1}{2}$ és $\varphi(p+1) \le \frac{p+1}{2}$, mindkettő kisebb $\varphi(p) = p-1$-nél, ha $p > 3$.

Az 1. tétel bizonyítása során többször is kihasználtuk, hogy az a_n sorozat szigorúan monoton és tagjai egész számok, vagyis azt a feltételt, hogy az $a(n)$ számelméleti függvény szigorúan monoton és értékei egészek. Felmerül a kérdés, hogy nem lehet-e gyengíteni e két kikötésen. Tekintsük először a monotonitást. Láttuk, hogy vannak egyáltalán nem monoton multiplikatív számelméleti függvények. De vajon van-e monoton, ám nem szigorúan monoton multiplikatív számelméleti függvény? Ez bizonyításunkból nem derül ki, mi ugyanis már $a(3) = 3$ bizonyításánál is használtuk, hogy a függvény szigorúan monoton. Az egyszerű monotonitásból csak az jön ki, hogy $a(3)$ értéke $a(2) = 2$, 3 vagy 4. Először megmutatjuk, hogyan lehet kizárni az $a(2) = a(3)$ esetet.

Tegyük fel tehát, hogy $a(2) = a(3) = 2$. Minthogy 2 és 7, 3 és 5 relatív prímek, és $a(n)$ monoton nő, ezért $a(2)a(7) = a(14) \le a(15) = a(3)a(5)$. Itt $a(2) = a(3) > 0$, ezért $a(7) \le a(5)$. Mivel $a(n)$ monoton nő, így $a(7) = a(5)$. A monotonitásból az is következik, hogy mindkettő egyenlő $a(6)$-tal is, ami viszont az a függvény multiplikativitása miatt egyenlő $a(2)a(3) = 4$-gyel.

A következő lépésben azt mutatjuk meg, hogy $a(10) = a(21) = 8$. Ehhez használjuk, hogy 2 és 5, illetve 3 és 7 relatív prímek: $a(10) = a(2)a(5) = 8 = a(3)a(7) = a(21)$. Következésképp minden 10 és 21 közötti i-re is $a(i) = 8$. Végül megmutatjuk, hogy $a(22) = a(60) = 16$: $a(22) = a(2)a(11) = 16 = a(3)a(20) = a(60)$ (mert 2 és 11, illetve 3 és 20 relatív prímek). De akkor minden 22 és 60 közötti i-re is $a(i) = 16$, így $i = 55$-re is. Viszont $a(55) = a(5)a(11)$, mert 5 és 11 relatív prímek, és $a(5) = 4$, $a(11) = 8$, vagyis $a(55) = 32$, ami ellentmondás. Ezzel beláttuk, hogy ha a multiplikatív és monoton nő, akkor $a(2) < a(3)$. A bizonyításban nem használtuk, hogy $a(2) = 2$, csak azt, hogy $a(2)$ pozitív és nem 1. Azt sem használtuk, hogy a értékei egészek.

Hasonló módszerrel látható be az is, hogy ha az a függvény multiplikatív és monoton nő, akkor egyáltalán nincs olyan k, amelyre $a(k) = a(k+1)$. Tegyük fel, hogy mégis van ilyen k. Ha $k = 1$, azaz $a(1) = a(2)$, akkor $a(3) = a(1)a(3) = a(2)a(3) = a(6)$, s így $a(3) = a(4) = a(5) = a(6)$. Feltehető tehát, hogy $k > 1$.

Tegyük fel tehát, hogy $a(k) = a(k+1) = \alpha > 0$ valamely 1-nél nagyobb k egészre. A $k = 2$ esetre alkalmazott módszer szerint járunk el most is: a multiplikativitásból és a monotonitásból következik, hogy

$$a(k)a(k^2+k+1) = a(k^3+k^2+k) \le a(k^3+2k^2-1) = a(k+1)a(k^2+k-1),$$

mert k^2+k+1 és k relatív prímek (mert k^2+k osztható k-val, így az eggyel nagyobb számmal nincs 1-nél nagyobb közös osztója), illetve $k+1$ és k^2+k-1 is (ugyanígy: $k+1 \mid k^2+k$, ezért az eggyel kisebb számmal nincs 1-nél nagyobb közös osztója). Leosztva $a(k) = a(k+1)$-gyel (ami pozitív) azt kapjuk, hogy $a(k^2+k-1) = a(k^2+k+1)$. De akkor a monotonitás miatt mindkettő megegyezik a köztük levő $a(k^2+k)$-val. Ez viszont a multiplikativitás miatt éppen $a(k)a(k+1) = \alpha^2$. Azt kaptuk, hogy ha

$$k^2+k-1 \le i \le k^2+k+1, \quad \text{akkor} \quad a(i) = \alpha^2.$$

Az eljárást a $k = 2$ esethez hasonlóan folytatjuk. Nyilván k és k^2+k-1 is relatív prímek és $k+1$ és k^2+k+1 is relatív prímek. De akkor az a függvény multiplikativitása miatt

$$a(k^3+k^2-k) = a(k)a(k^2+k-1) = \alpha^3 = a(k+1)a(k^2+k+1) = a(k^3+2k^2+2k+1),$$

a monotonitás miatt pedig igaz, hogy

$$\text{ha} \quad k^3+k^2-k \le i \le k^3+2k^2+2k+1, \quad \text{akkor} \quad a(i)=\alpha^3.$$

Ebből minket csak annyi érdekel (mert erre lesz egyszerű teljes indukciót alkalmazni), hogy

$$\text{ha} \quad k^3+k^2-1 \le i \le k^3+2k^2+k+1, \quad \text{akkor} \quad a(i)=\alpha^3.$$

Ez ilyen alakba is írható: ha $k^2(k+1)-1 \le i \le k(k+1)^2+1$, akkor $a(i)=\alpha^3$. Most (j-re vonatkozó) teljes indukcióval megmutatjuk, hogy általában is igaz, hogy

$$(*) \qquad \text{ha} \quad k^j(k+1)-1 \le i \le (k+1)^j k+1, \quad \text{akkor} \quad a(i)=\alpha^{j+1}.$$

A $k=2$ esetben ugyanis a bizonyítás lényege az volt, hogy ha ezt az eljárást elég sokszor ismételjük, tehát j elég nagy ($k=2$ esetben ehhez négy lépésre volt szükség), akkor az α^{j+1}-re és α^{j+2}-re kapott intervallum egymásba ér, s ez $\alpha \ne 1$ esetén ellentmondás.

$j=1,2$-re már bizonyítottuk az állítást. Tegyük fel, hogy $j=l$-re igaz a $(*)$ állítás, tehát $a\big(k^l(k+1)-1\big)=a\big((k+1)^l k+1\big)=\alpha^{l+1}$. Most is igaz, hogy k és $k^l(k+1)-1$ relatív prímek, hiszen $k^l(k+1)$ osztható k-val, az eggyel kisebb számnak tehát nem lehet 1-nél nagyobb közös osztója k-val; ugyanígy $k+1$ és $(k+1)^j k+1$ is relatív prímek. Használhatjuk a multiplikativitást:

$$\begin{aligned} a\big(k^{l+1}(k+1)-k\big) &= a(k)a\big(k^l(k+1)-1\big)=\alpha^{l+2}=a(k+1)a\big((k+1)^l k+1\big)= \\ &= a\big((k+1)^{l+1}k+k+1\big). \end{aligned}$$

A monotonitásból adódik, hogy minden $k^{l+1}(k+1)-k$ és $(k+1)^{l+1}k+k+1$ közötti i-re is $a(i)=\alpha^{l+2}$. Nekünk azt kell bizonyítanunk, hogy ez minden $k^{l+1}(k+1)-1$ és $(k+1)^{l+1}k+1$ közötti i-re igaz. Mivel e két határ $k^{l+1}(k+1)-k$ és $(k+1)^{l+1}k+k+1$ között van, a bizonyítást befejeztük.

Most már elég annyit belátnunk, hogy ha j elég nagy, akkor az α^{j+1}-re és α^{j+2}-re kapott intervallum egymásba ér, azaz az utóbbi intervallum alsó végpontja kisebb az előbbi felső végpontjánál: $k^{j+1}(k+1)-1 \le (k+1)^j k+1$. Ennél kissé erősebb állítást bizonyítunk, nevezetesen azt, hogy $k^{j+1}(k+1) \le (k+1)^j k$, ha j elég nagy. Ezt az egyenlőtlenséget átrendezve azt kapjuk, hogy $k+1 \le (1+1/k)^j$. Itt k rögzített szám, $1+1/k$ egynél nagyobb szám, tehát hatványai tetszőleges számnál, így k-nál is nagyobbak lesznek, ha a j kitevő elég nagy.[1] Ezzel beláttuk, hogy az α^{j+1}-re és α^{j+2}-re kapott intervallum egymásba ér, azaz $\alpha^{j+1}=\alpha^{j+2}$. Ez csak akkor nem ellentmondás, ha $\alpha=1$. Ekkor viszont a $(*)$ állítás szerint végtelen sok i-re $a(i)=1$. A monotonitásból pedig következik, hogy ekkor *minden* i-re $a(i)=1$. Igaz tehát a következő tétel:

2. tétel. *Ha a mindig pozitív $a(n)$ számelméleti függvény multiplikatív és monoton nő, de nem szigorúan monoton, akkor $a(n)=1$ minden n-re.*

A bizonyításban nem kellett kihasználni, hogy $a(n)$ függvény értékei egészek. Felmerül tehát a kérdés, hogy az 1. tételben szükség van-e erre a kikötésre. Az a bizonyítás, amit adtunk rá, kihasználja ezt a feltételt egyrészt akkor, amikor $a(n)$ szigorú monotonitásából arra következtettünk, hogy $a(n) \ge n$, másrészt ott, hogy $a(4)<4$-ből $a(3)=3$ következik. Ezért első pillanatban talán meglepő, hogy mégis elhagyható a feltétel, igaz ugyanis a következő, ERDŐS PÁLtól származó tétel:

3. tétel. *Ha az $a(n)$ multiplikatív számelméleti függvény monoton növekszik, továbbá $a(2)=2$, akkor minden n-re $a(n)=n$.*

A bizonyítás gondolatmenetét először egy egyszerűbb eseten szemléltetjük: feltesszük, hogy $a(n)a(m)=a(nm)$ minden pozitív egész n-re és m-re fennáll, nemcsak akkor, ha n és m relatív prím. Az ilyen számelméleti függvényeket *totálisan multiplikatív* számelméleti függvénynek nevezzük. Ezekből is végtelen sok van: minden prím helyen tetszőlegesen adhatjuk meg az értékét, abból viszont már az összes többi helyen felvett értéke kiszámítható.

Tegyük fel tehát, hogy a totálisan multiplikatív és $a(2)=2$. Az erősebb feltételünk szerint $a(4)=a(2)a(2)=4$, $a(8)=a(4)a(2)=8$, és teljes indukcióval $a(2^j)=2^j$. Ugyanígy igazolható tetszőleges c pozitív egészre, hogy

$$a(c^j)=a(c)^j.$$

Másrészt ha $2^l<c^j<2^{l+1}$, akkor a monotonitás miatt $a(2^l) \le a(c^j) \le a(2^{l+1})$. Ebből következik, hogy

$$\text{ha} \quad 2^l<c^j<2^{l+1}, \quad \text{akkor} \quad 2^l \le a(c)^j \le 2^{l+1}.$$

Az előbbi egyenlőtlenséget írjuk $2^{-l}>c^{-j}>2^{-l-1}$ alakba, és szorozzuk össze az utóbbival. Így azt kapjuk, hogy

$$\frac{1}{2} \le \left(\frac{a(c)}{c}\right)^j \le 2.$$

[1] Ha $x>1$, tehát $x=1+h$ és $h>0$, akkor az úgynevezett Bernoulli-egyenlőtlenség szerint $(1+h)^j \ge 1+hj$ (ami j-re vonatkozó teljes indukcióval bizonyítható). Eszerint $j>(k-1)/h$ esetén $x^j>k$. Később tetszőleges A konstansra fogjuk használni, hogy ha j elég nagy, akkor $x^j>A$, azaz x^j „minden határon túl nő".

Említettük már, hogy ha egy szám 1-nél nagyobb, akkor a hatványai minden határon túl nőnek, ha tehát $a(c) > c$, akkor elég nagy j-re $\left(\frac{a(c)}{c}\right)^j$ nagyobb lesz kettőnél. Ha viszont $c > a(c)$, akkor $\left(\frac{c}{a(c)}\right)^j$ lesz nagyobb kettőnél elég nagy j-re, tehát $\left(\frac{a(c)}{c}\right)^j$ kisebb lesz $\frac{1}{2}$-nél. A fenti egyenlőtlenség mindkettőt kizárja, így az az egyetlen eset marad, hogy $a(c) = c$.

Ezzel már beláttuk a következőt:

Ha az $a(n)$ totálisan multiplikatív számelméleti függvény monoton növekszik, továbbá $a(2) = 2$, akkor minden n-re $a(n) = n$.

Ha az a függvény multiplikatív, de nem totálisan multiplikatív, akkor a fenti bizonyításban megakadunk annál a pontnál, hogy $a(2^j) = 2^j$ és $a(c^j) = a(c)^j$, ez ugyanis közvetlenül nem bizonyítható. Ha azonban az előző bizonyítást végignézzük, találunk egy kiutat.

A bizonyítás annak belátásán múlt, hogy ha $2^l < c^j < 2^{l+1}$, akkor $2^l \le a(c)^j \le 2^{l+1}$, mert ekkor $\frac{1}{2} \le \left(\frac{a(c)}{c}\right)^j \le 2$, és az 1 kivételével minden pozitív szám j-edik hatványa vagy minden határon túl nő, vagy a reciprokára igaz ugyanez. Ez viszont azt is jelenti, hogy az utóbbi egyenlőtlenségben $\frac{1}{2}$ és 2 helyett tetszőleges pozitív szám állhat, a bizonyítás akkor is működik. Az egyetlen, amire vigyázni kell, hogy e pozitív számok ne függjenek k-tól, vagyis ne változzanak, ha k-t növeljük, hiszen csak így juthatunk arra a következtetésre, hogy sem $\frac{a(c)}{c}$, sem a reciproka nem lehet 1-nél nagyobb.

Elég tehát azt belátni, hogy vannak olyan j-től nem függő A és B pozitív számok, amelyekre $A \le \left(\frac{a(c)}{c}\right)^j \le B$. Ehhez viszont elég azt belátni, hogy

$$(**) \qquad \text{ha} \quad 2^l < c^j < 2^{l+1}, \quad \text{akkor} \quad 2^{l+1}A \le a(c)^j \le 2^l B,$$

ahol A és B nem függ j-től. Ekkor ugyanis az utóbbi egyenlőtlenséget a $2^{-l-1} < c^{-j} < 2^{-l}$ egyenlőtlenséggel szorozva éppen a kívánt $A \le \left(\frac{a(c)}{c}\right)^j \le B$ egyenlőtlenséget kapjuk.

Ezt a $(**)$ egyenlőtlenséget fogjuk tehát bebizonyítani. A bizonyítás azon múlik, hogy találni fogunk egy olyan egyenlőtlenséget, amely szerint $a(c^j)$ ha nem is egyenlő $a(c)^j$-vel, de beszorítható $a(c)^j$-nek két konstansszorosa közé, ahol a két konstans megint csak független j-től. Azt állítjuk tehát, hogy minden v pozitív egészhez vannak olyan j-től független E_v és D_v konstansok, amelyekre igaz, hogy

$$(***) \qquad E_v a(v)^j \le a(v^j) \le D_v a(v)^j.$$

Nézzük először, miért elég ez a $(**)$ egyenlőtlenség bizonyításához. Tegyük fel tehát, hogy $2^l < c^j < 2^{l+1}$. Ekkor a monotonitás miatt $a(2^l) \le a(c^j)$ és $a(c^j) \le a(2^{l+1})$. Az első egyenlőtlenségben alkalmazzuk $(***)$ első felét $v = 2$, $j = l$-re, majd alkalmazzuk $(***)$ második felét $v = c$-re:

$$E_2 a(2)^l \le a(2^l) \le a(c^j) \le D_c a(c)^j,$$

Ebből $a(2) = 2$ felhasználásával azt kapjuk, hogy $\frac{E_2 2^l}{D_c} \le a(c^j)$, tehát $A = \frac{E_2}{2D_c}$ választással $(**)$ első felét kapjuk.

Egész hasonlóan kapjuk az $a(c^j) \le a(2^{l+1})$ egyenlőtlenségből $(**)$ második felét. Ehhez $(***)$-ban először $v = c$-t, majd $v = 2$-t és $j = l + 1$-et helyettesítünk:

$$E_c a(c)^j \le a(c^j) \le a(2^{l+1}) \le D_2 a(2^{l+1}) = D_2 2^{l+1}.$$

Innen átrendezéssel azt kapjuk, hogy $a(c)^j \le \frac{2D_2 2^l}{E_c}$, s ez $B = \frac{2D_2}{E_c}$ választással éppen $(**)$ második fele.

Most már csak $(***)$ bizonyítása van hátra. Ez a következő ötleten múlik. Keresünk v^j-hez közel olyan számot, amelyet már „le tudunk bontani" úgy, ahogyan a totálisan multiplikatív függvények esetében magát v^j-t tudjuk „lebontani". Tekintsük a $v^j + v = v(v^{j-1} + 1)$ számot. Itt v és $v^{j-1} + 1$ relatív prímek, hiszen $v \mid v^{j-1}$. Tehát az a függvény multiplikativitása miatt

$$(1) \qquad a(v^j + v) = a(v)a(v^{j-1} + 1).$$

A monotonitás miatt

$$(2) \qquad a(v^{j-1} + 1) \le a(v^{j-1} + v).$$

Ez utóbbira megint alkalmazhatjuk a (1) egyenlőséget j helyett $j-1$-re:

$$a(v^{j-1}+v)=a(v)a(v^{j-2}+1),$$

tehát összességében a következő egyenlőség és egyenlőtlenség-láncot kapjuk:

$$a(v^j)\le a(v^j+v)=a(v)a(v^{j-1}+1)\le a(v)a(v^{j-1}+v)=a(v)^2a(v^{j-2}+1).$$

Ha itt megint a (2) egyenlőtlenséget alkalmazzuk $j-1$ helyett $j-2$-t írva, majd az (1) egyenlőséget j helyett $j-2$-t írva, akkor azt kapjuk, hogy

$$a(v^j)\le a(v)^3a(v^{j-3}+1).$$

Az eljárást folytatva összesen $j-1$ lépés után arra jutunk, hogy

$$a(v^j)\le a(v)^{j-1}a(v+1)=a(v)^j\frac{a(v+1)}{a(v)}.$$

Ezzel beláttuk az (1) egyenlőtlenség második felét $\dfrac{a(v+1)}{a(v)}=D_v$ választással.

Pontosan ugyanezzel a gondolatmenettel kapjuk, ha v^j+1 helyett v^j-1-et, v^j+v helyett v^j-v-t írunk és az egyenlőtlenség irányát megfordítjuk, hogy

$$a(v^j)\ge a(v)^{j-1}a(v-1)=a(v)^j\frac{a(v-1)}{a(v)}.$$

Ez pedig (***) első fele $E_v=\dfrac{a(v-1)}{a(v)}$ választással.

Ezzel a tétel bizonyítását befejeztük.

A tételhez még pár kiegészítő megjegyzést fűzünk. Először megjegyezzük, hogy ha van olyan n, amelyre $a(n)\neq 0$, akkor $a(1)=1$, hiszen $a(n)=a(1)a(n)$ (mert 1 és n relatív prímek). Ebből máris következik, hogy ha a monoton nő, akkor minden értéke pozitív. Tegyük fel most, hogy az a függvény monoton csökken, és $a(n)<0$ valamely n-re. Ekkor $a(n+1)$ is negatív. Másrészt n és $n+1$ relatív prímek, tehát $a(n)a(n+1)=a(n^2+n)>0$, ami ellentmond annak, hogy a monoton csökken. Tehát egy monoton multiplikatív függvény minden értéke nemnegatív, kivéve ha $a(1)$ negatív és $a(n)=0$ minden $n\ge 2$-re.

Tegyük fel most, hogy $a(n)$ monoton és $a(2)\neq 0$. Ekkor minden értéke nemnegatív. Nyilvánvaló, hogy ha $a(n)$ multiplikatív, akkor multiplikatív az a^c függvény is. (Ez a függvény létezik, mert az a függvény értékei nemnegatívak.) Alkalmas c választással nyilván elérhető, hogy $a^c(2)=2$ legyen. Másrészt az a^c függvény is monoton, ha az a függvény monoton volt (legfeljebb a monotonitás iránya fordul meg, ha c negatív). Másrészt $a^c(1)=1<2=a^c(2)$, tehát az a^c függvény monoton nő. De ekkor a 3. tétel szerint minden n-re $a^c(n)=n$, vagyis minden n-re $a(n)=n^{\frac{1}{c}}$. A következő általánosabb, szintén ERDŐS PÁLtól származó tételt nyertük:

4. tétel. *Ha az $a(n)$ számelméleti függvény monoton és multiplikatív, akkor vagy $a(n)=0$ minden $n>1$-re, vagy van olyan t, amely mellett $a(n)=n^t$ minden n-re.*