A SZÁMELMÉLET ALAPTÉTELÉRŐL.

Bevezetés.

1. Az *elemi számelmélet alaptételét* — amely szerint *minden természetes szám lényegében*[1] *csak egyféleképpen állítható elő törzsszámok szorzataként* — a tankönyvek legtöbbnyire vagy a legnagyobb közös osztó, vagy a legkisebb közös többszörös alaptulajdonságainak felhasználásával bizonyítják be. A legnagyobb közös osztón alapuló tárgyalás[2] abból indul ki, hogy két egész számnak, a-nak és b-nek,[3] legnagyobb közös osztója, d, előállítható

$$d = ax + by \tag{1}$$

alakban, ahol x és y egész számok. Ezt vagy a legnagyobb közös osztó meghatározására szolgáló EUKLIDES-féle algoritmus segitségével bizonyítják be, vagy úgy, hogy megmutatják, hogy a legkisebb pozitív egész szám, mely az (1) alakban előállítható, osztója a-nak is, b-nek is. A legkisebb közös többszörösön alapuló tárgyalás[4] kiindulópontja az a tétel, hogy két egész szám legkisebb közös többszöröse[5] osztója bármely közös többszörö-

---

[1] Azaz a tényezők sorrendjétől eltekintve.

[2] L. pl. P. G. LEJEUNE DIRICHLET: *Vorlesungen über Zahlentheorie*, Braunschweig (4. kiadás, 1894), 4., 5., 8. §; P. BACHMANN: *Niedere Zahlentheorie*, erster Teil, Leipzig (1902), 34., 35., 40., 41. old.

[3] Egész számon mindig racionális egész számot értek; latin kis betű mindig ilyent jelöl.

[4] L. pl. GROSSCHMID LAJOS: *Előadások a mathematika elemeiből*, Budapest (1923), 2., 6., 7. §; E. LANDAU: *Vorlesungen über Zahlentheorie*, erster Band, Leipzig (1927), 5—12. old.

[5] Azaz pozitív közös többszöröseik legkisebbike.

süknek. Mind a két tárgyalásmód a *törzsszámok alaptulajdonságának* bebizonyításával folytatódik, amely szerint *egész számok szorzata csak úgy lehet osztható egy törzsszámmal, ha valamelyikük osztható vele.*

Ebből viszont a számelmélet alaptétele — amely nyilván így is fogalmazható: *ha*

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s, \tag{2}$$

ahol $p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s$ *mind törzsszámok, akkor* $r = s$ *és* $p_1, p_2, \ldots, p_r$ *sorrendtől eltekintve ugyanazok, mint* $q_1, q_1, \ldots, q_s$ — például r szerinti teljes indukcióval adódik. Ha $r = 1$, akkor a tétel evidens:[6] ekkor ugyanis (2) szerint

$$p_1 = q_1 q_2 \cdots q_s,$$

ami, minthogy p_1 törzsszám, csak úgy állhat fenn, ha a jobboldalon is csak egy tényező van s az egyenlő p_1-gyel. Tegyük fel, hogy igaz a tétel, ha a baloldalon r tényező van; akkor $r+1$ tényező esetére így adódik: ha

$$p_1 p_2 \cdots p_r p_{r+1} = q_1 q_2 \cdots q_s, \tag{3}$$

akkor a $q_1 q_2 \cdots q_s$ szorzat osztható p_{r+1}-gyel, tehát, minthogy p_{r+1} törzsszám, valamelyik tényezője is; de mivel ezek is törzsszámok, valamelyikük, például q_k, egyenlő kell hogy legyen p_{r+1}-gyel. De akkor (3)-ból

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_{k-1} q_{k+1} \cdots q_s;$$

itt már csak r tényező áll a baloldalon, tehát a feltevés szerint $r = s - 1$ és a baloldalon álló tényezők sorrendtől eltekintve ugyanazok, mint a jobboldalon állók; így $r + 1 = s$ és $p_1, p_2, \ldots, p_r, p_{r+1}$ sorrendtől eltekintve ugyanazok, mint $q_1, q_2, \ldots, q_s$.

2. Ismeretesek azonban a számelmélet alaptételének a legnagyobb közös osztó és a legkisebb közös többszörös fogalmá-

---

[6] Még inkább evidens a tétel $r = 0$ esetében (0 tényezőből álló szorzaton 1-et szokás érteni).

tól független bebizonyításai is. Már GAUSS[7] is adott közvetlen bebizonyítást a törzsszámok alaptulajdonságára; újabban pedig F. A. LINDEMANN,[8] ZERMELO[9] és KLAPPAUF[10] közöltek nagyon egyszerű közvetlen bebizonyításokat a számelmélet alaptételére. Ez utóbbi körülmény késztet arra, hogy közöljem azt a bebizonyítást, melyet az 1932/33. tanév óta több egyetemi előadásomban is tárgyaltam. Ez a bebizonyítás a következő lemmán alapul:

Ha négy nemnegatív egész szám, a, b, c és d, teljesíti az

$$ab = cd \tag{4}$$

egyenletet, akkor van további négy oly nemnegatív egész szám, t, u, v, w, hogy

$$a = tu, \quad b = vw, \quad c = tw, \quad d = uw. \tag{5}$$

	c	d
a	t	u
b	v	w

(A t, u, v, w számokat célszerű az oldalt látható táblázatban elhelyezni.)

Ez a lemma — amelyet a továbbiakban «négyszámtétel» néven fogok említeni — nyilvánvaló következménye a számelmélet alaptételének.[11] Az 1. §-ban azonban megmutatom, hogy

---

[7] C. F. GAUSS: *Disquisitiones arithmeticae*, Sectio secunda, art. 13., 14., *Werke*, erster Band, Göttingen (Zweiter Abdruck, 1870), 14., 15. old., l. még KÜRSCHÁK JÓZSEF: *Matematikai versenytételek*, Szeged (1929), 16., 17. old.

[8] F. A. LINDEMANN: The Unique Factorization of a Positive Integer, *Quarterly Journal of Math.*, Oxford Series, **4** (1933), 319—320. old.

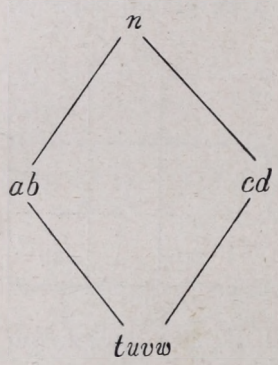
[9] E. ZERMELO: Elementare Betrachtungen zur Theorie der Primzahlen, *Nachrichten Göttingen*, Math.-Phys. Klasse, Fachgruppe I: Mathematik, Neue Folge, **1** (1934), 43—46. old., különösen 43—44. old.

[10] G. KLAPPAUF: Beweis des Fundamentalsatzes der Zahlentheorie, *Jahresbericht der Deutschen Math.-Ver.*, **45** (1935), *130.* old.

[11] Ennélfogva a négyszámtétel érvényes minden olyan integritási tartományban, amelyben az egyértelmű törzstényezős előállítás tétele érvényes; l. A. KORSELT: Vollständige Lösung einer neuen diophantischen Aufgabe, *Math. Annalen*, **112** (1936), 395—410., különösen 396—397. old. KORSELT szerint (természetes számok esetére, a számelmélet alaptételének következményeképpen) már EULER ismerte a négyszámtételben foglalt állítást.

nagyon egyszerűen be lehet bizonyítani a számelmélet alaptételének felhasználása nélkül is.

A négyszámtétel «csírájában» mutatja meg a számelmélet alaptételének okát. Ha ugyanis valamely n pozitív egész számot kétféleképpen kezdünk el szorzatra bontani: $n = ab$, $n = cd$, akkor alkalmas továbbontás útján: $a = tu$, $b = vw$, illetőleg $c = tv$, $d = uw$, mindkettőből ugyanahhoz az $n = tuvw$ felbontáshoz juthatunk (mint ezt az 1. ábra szemlélteti). Minthogy hasonlóan minden, a további szétbontás közben lehetséges «elágazás» után következik be ilyen «összetalálkozás», plauzibilis, hogy a legvégén minden szétbontás ugyanabba a végső szétbontásba torkollik. Ez a gondolatmenet megfogalmazható úgy, hogy a számelmélet alaptételének bebizonyítását adja: kitűnik innen a négyszámtételnek a számelmélet alaptételével való tisztán kombinatorikai kapcsolata. E kapcsolat kombinatorikai természetének kidom-borítására a 2. §-ban a négyszámtételről a számelmélet alaptételére való áttérést szemléletesen, *gráfelméleti tételként* fogom megfogalmazni, mégpedig kétféleképpen is. Ugyanitt megmutatom, hogy ez az átmenet, ha nem helyezünk súlyt a meggondolás kombinatorikai jellegére, minden gráfelméleti megfogalmazás nélkül is, nagyon egyszerűen elvégezhető.



1. ábra.

A 3. §-ban a négyszámtételt általánosítom többtényezős szorzatokra és ez általánosítás segítségével újból bebizonyítom a a számelmélet alaptételét. A 4. §-ban pedig megmutatom, hogy a négyszámtétel nem tekinthető a számelmélet alaptételének bebizonyítására szolgáló *ad hoc* módszernek, hanem az elemi számelmélet számos más tétele is könnyen következik belőle. Olyan tételekről van szó, amelyeket rendesen a legnagyobb közös osztó (1) előállításából, néha a legkisebb közös többszörös fentemlített alaptulajdonságából szoktak bebizonyítani; a négy-

számtétel segítségével való bebizonyításuk azonban didaktikai szempontból előnyösebb, mert könnyebben megjegyezhető: ugyanis minden egyes esetben nyilvánvaló, hogy melyik az a négy szám, amelyre a négyszámtételt alkalmazni kell.

1. §.

3. A négyszámtételt a szerint menő teljes indukcióval fogom bebizonyítani; azaz egyrészt megmutatom, hogy igaz e tétel négy oly a, b, c, d számra, amelyek közül $a = 0$, másrészt, hogy, ha (adott pozitív a mellett) igaz a tétel bármely négy oly a', b', c', d' számra, ahol $a' < a$, akkor igaz (tetszőleges b, c, d mellett) az a, b, c, d számokra is.[12]

Ha $a=0$, akkor (4) szerint $cd=0$, tehát vagy $c=0$, vagy $d=0$.

$a = 0, \quad c = 0.$

	c	d
a	0	d
b	b	1

Az első esetben a baloldali, a másodikban a jobboldali táblázatból olvashatók le t, u, v, w oly értékei, amelyek az (5) egyenletnek eleget tesznek.

$a = 0, \quad d = 0.$

	c	d
a	c	0
b	1	b

Tegyük fel most már, hogy a négyszámtétel igaz négy oly a' b', c', d' számra, ahol $a' < a$; feladatunk megmutatni érvényességét az a, b, c, d számokra ($a > 0$) is. Osszuk el c-t a-val, legyen a hányados[13] q, a maradék r; akkor

$$c = aq + r, \quad 0 \leqq r < a. \tag{6}$$

---

[12] Az alkalmazások szempontjából elég volna a négyszámtételt abban az esetben bebizonyítani, ha a, b, c, d egyike sem 0; azonban épp a teljes indukcióval való bebizonyítás megkönnyítésére célszerű azt is megengedni, hogy valamelyikük 0 legyen. — Szimmetria-okokból fel lehetne tenni, hogy a a legkisebb a, b, c, d közül; ez azonban nem egyszerűsítené lényegesen a bebizonyítást.

[13] Ha $a > c$, akkor természetesen $q = 0$ (és $r = c$).

Innét és (4)-ből
$$ab = cd = aqd + rd,$$
$$rd = a(b - qd). \tag{7}$$

Minthogy $r < a$, alkalmazhatjuk a négyszámtételt az $a' = r$, $b' = d$, $c' = a$, $d' = b - qd$ számokra;[14] van tehát négy oly i, j, k, l szám, hogy (l. a jobboldali táblázatot)

	a	$b-qd$
r	i	j
d	k	l

$$r = ij,\ d = kl,\ a = ik,\ b - qd = jl. \tag{8}$$

(8) második és negyedik egyenletéből
$$b = qd + jl = (qk + j)\,l, \tag{9}$$

	c	d
a	i	k
b	$kq+j$	l

(6)-ból, (8) harmadik és első egyenletéből
$$c = ikq + ij = i(kq + j). \tag{10}$$

(8) harmadik egyenlete, (9), (10) és (8) második egyenlete[15] mutatja, hogy a baloldalt álló táblázatból leolvasható $t = i$, $u = k$, $v = kq + j$, $w = l$ számok eleget tesznek az (5) egyenleteknek, qu. e. d.

4. Az (5) egyenletekből nyilvánvaló, hogy, ha a, b, c, d egyike sem 0, akkor t, u, v, w is *pozitív* egész számok; továbbá, hogy, ha a, b, c, d mind nagyobbak 1-nél és sem $a = c$, $b = d$, sem pedig $a = d$, $b = c$ nem áll, akkor t, u, v, w közül legfeljebb egyik lehet egyenlő 1-gyel.

2. §.

5. Legyen n adott, 1-nél nagyobb egész szám. Az n szám *faktorizációs gráf*-ján a következő $\mathfrak{F}_n$ irányított gráfot[16] értjük. Feleltessünk meg n minden
$$n = n_1 n_2 \ldots n_r$$

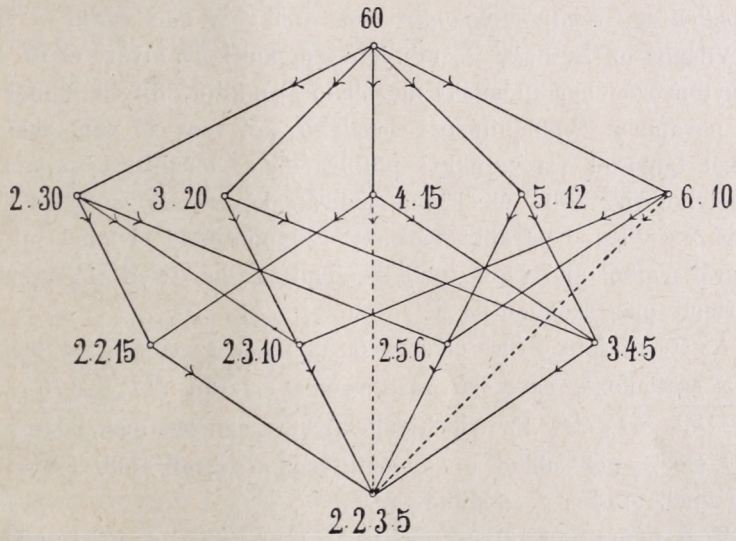
---

[14] Ezek egyike sem negatív; a', b', c'-re ez világos, d'-re pedig (7)-ből következik.

[15] Ha $a \neq 0$, akkor (4)-ből és (5) első, harmadik és negyedik egyenletéből már következik (5) második egyenlete is, úgy hogy (9) tulajdonképpen nélkülözhető.

[16] A gráfelmélet itt felhasznált alapfogalmaira nézve l. D. König: *Theorie der endlichen und unendlichen Graphen*, Leipzig (1936) 1. §-át.

1-nél nagyobb egész tényezők szorzataként való előállításának (beleértve az $r = 1$ esetnek megfelelő $n = n$ előállítást is) egy-egy pontot, mégpedig két előállításnak akkor és csak akkor ugyanazt a pontot, ha azok csak a tényezők sorrendjében térnek el egymástól. A P és Q pontokat akkor és csak akkor kössük össze egy $\overrightarrow{PQ}$ irányított éllel, ha a P-nek megfelelő szorzatelőállításból (röviden: a P előállításból) a Q előállítás úgy



2. ábra.

jön létre, hogy valamelyik tényezőjét tovább bontjuk két tényezőre. Pl. a 60 faktorizációs gráfját, $\mathfrak{F}_{60}$-at, a 2. ábra szemlélteti (a két pontozott él itt figyelmen kívül hagyandó). Ha p prímszám, $\mathfrak{F}_p$ egyetlen egy szögpontból áll s éle nincs.

Nyilvánvaló, hogy $\mathfrak{F}_n$ *véges* gráf. Ugyanis n előállításainál csak véges számú szám jöhet figyelembe tényezőként (minden tényező kisebb lévén n-nél); s a tényezők száma nyilván (jóval) kisebb, mint n. E szerint $\mathfrak{F}_n$-nek véges számú szögpontja van,[17] tehát

[17] $\mathfrak{F}_n$ szögpontjainak száma az az $f(n)$ függvény, amellyel két dolgozatomban: A «factorisatio numerorum» problémájáról, *Mat. és Fiz. Lapok*, 38

(minthogy két-két szögpont legfeljebb egy éllel van összekötve) éleinek száma is véges.

Ha n valamely P szorzatelőállításánál valamelyik tényező összetett szám, akkor ennek két tényezőre való szétbontásával oly előállításhoz jutunk, amelybe visz P-ből $\mathfrak{F}_n$-nek éle.[18] Fordítva is, ha $\mathfrak{F}_n$-nek P-ből indul ki éle, akkor a P előállításnál legalább egy tényező összetett szám. E szerint a számelmélet alaptétele úgy fejezhető ki, hogy *az $\mathfrak{F}_n$ faktorizációs gráfnak egyetlen egy olyan szögpontja van, amelyből nem indul ki él.*

Világos az is, hogy $\mathfrak{F}_n$ minden szögpontjába, kivéve az $n=n$ «egytényezős előállításnak» megfelelő P_0 pontot, fut éle $\mathfrak{F}_n$-nek; ha ugyanis a P előállításnál legalább két tényező van, akkor e két tényezőt szorzatukkal pótolva oly Q előállítást kapunk, amelyből visz P-be él. Ebből nyilván következik, hogy az $\mathfrak{F}_n$ gráf *összefüggő;* ugyanis bármely szögpontjából el lehet jutni a gráf éleiből álló úton (nyilellenében) P_0-ba, tehát (P_0-on át) bármely más szögpontba is.

Az $\mathfrak{F}_n$ gráfnak *nincs ciklusa* (azaz irány szerint is egymáshoz csatlakozó, egyszerű zárt vonalat alkotó $\overrightarrow{P_1P_2}$, $\overrightarrow{P_2P_3}, \ldots,$ $\overrightarrow{P_{k-1}P_k}$, $\overrightarrow{P_kP_1}$ élei). Ez nyilvánvaló következménye annak, hogy, ha $\overrightarrow{PQ}$ éle $\mathfrak{F}_n$-nek, akkor a Q előállításnál (eggyel) több tényező szerepel, mint a P előállításnál.

6. A négyszámtétel folyományaként a $\mathfrak{G} = \mathfrak{F}_n$ gráfnak a következő tulajdonsága van:

T tulajdonság. Ha $\overrightarrow{PQ}$ és $\overrightarrow{PR}$ a $\mathfrak{G}$ gráfnak valamely szögpontjából kiinduló, két különböző szögpontba futó élei, akkor van $\mathfrak{G}$-nek oly S pontja, amelybe Q-ból is, R-ből is visz $\mathfrak{G}$-nek pályavonala[19] (l. 3. ábra).

(1931), 1—15. old. és Über die mittlere Anzahl der Produktdarstellungen der Zahlen, erste Mitteilung, *Acta Scientiarum Math.*, **5** (1930—32), 95—107. old. foglalkoztam.

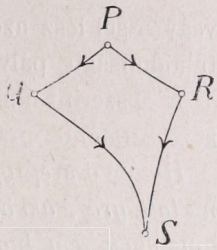
[18] A $\overrightarrow{PQ}$ élt P-ből *kiinduló*, Q-ba *futó*, P-ből Q-ba *vivő* élnek mondom; hasonlóan később pályavonalak esetén.

[19] Azaz irány szerint is egymáshoz csatlakozó éleinek önmagát nem metsző nyitott vonalat alkotó sorozata. (Ciklus nélküli gráfnál az önmagát

Legyen ugyanis a P előállítás

$$n = n_1 n_2 \ldots n_r$$

és keletkezzék ebből a Q előállítás azáltal, hogy n_i-t ab-re, az R előállítás pedig azáltal, hogy n_j-t cd-re bontjuk fel ($i, j = 1, 2, \ldots$, vagy r). Ha $i \neq j$, akkor állításunk evidens: Q-ban n_j-t cd-re bontva ugyanahhoz az S előállításhoz jutunk, mintha R-ben n_i-t ab-re bontjuk, úgy, hogy $\overrightarrow{QS}$ és $\overrightarrow{RS}$ élei $\mathfrak{F}_n$-nek. Tegyük fel tehát, hogy $i = j$; akkor



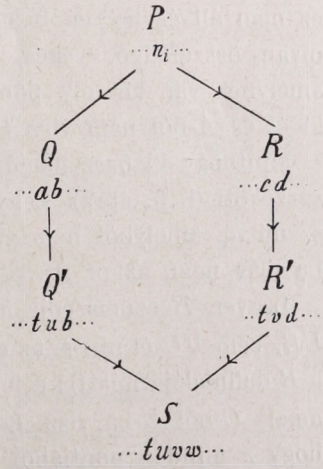
3. ábra.

$$n_i = n_j = ab = cd,$$

tehát a négyszámtétel szerint van négy oly szám, t, u, v, w, hogy

$$a = tu, \; b = vw, \; c = tv, \; d = uw.$$

Minthogy Q és R különböző pontok, sem $a = c$, $b = d$, sem $a = d$, $b = c$ nem állhat, tehát a **4.** megjegyzése szerint t, u, v, w közül legfeljebb egyik lehet 1. Ha egyik sem 1, akkor jelentse Q' a Q-ból a-nak tu-val, R' az R-ből c-nek tv-vel való pótlásával keletkező előállítást; akkor Q'-ben b-t vw-vel, R'-ben pedig d-t uw-vel pótolva ugyanahhoz az S ellőállításhoz jutunk, úgy, hogy $\overrightarrow{QQ'S}$ és $\overrightarrow{RR'S}$ a kívánt tulajdonságú pályavonalak (4. ábra). Hasonlóan járhatunk el, ha t, u, v, w közül valamelyik 1; ekkor ezt az 1-gyel egyenlő tényezőt el kell hagynunk, úgy, hogy Q' vagy Q-val, vagy S-sel, R' vagy R-rel,



4. ábra.

nem metszés feltétele magától teljesül.) Az irányitást nem tekintve egymáshoz csatlakozó élek önmagát nem metsző nyitott vonalat alkotó sorozatát *út*nak nevezik.

vagy S-sel lesz azonos; ekkor tehát a $\overrightarrow{QS}$ és $\overrightarrow{RS}$ élek a kívánt tulajdonságú pályavonalak.

7. E szerint a számelmélet alaptétele bennefoglaltatik a következő általános gráfelméleti tételben:

Ha $\mathfrak{G}$ összefüggő, véges, ciklus nélküli, T tulajdonságú irányított gráf, akkor $\mathfrak{G}$-nek egyetlen egy olyan U pontja van, amelyből nem indul ki él.

Hogy *van* ilyen U pont,[20] az közvetlenül belátható. Válasszuk ugyanis P_1-et $\mathfrak{G}$ pontjai közül tetszőlegesen, P_2-t, P_3-at,... pedig sorra úgy, hogy $\mathfrak{G}$-nek legyenek $\overrightarrow{P_1P_2}$, $\overrightarrow{P_2P_3}$,... élei. E pontok sorozatában nem fordulhat elő ismétlődés (mert $\mathfrak{G}$-nek nincs ciklusa), tehát a sorozatnak vége szakad (mert $\mathfrak{G}$ véges); utolsó pontja a kívánt tulajdonsággal bír.

Annak megmutatására, hogy ilyen U pont csak *egy* van, bebizonyítom, hogy, ha $\mathfrak{G}$ valamely U pontjából nem indul ki él, akkor bármely más A pontjából visz U-ba pályavonal. (Ebből persze következik, hogy A-ból indul ki él.) Tegyük fel, hogy ez nem áll és legyen $\mathfrak{G}$ egy lehető legkevesebb ponttal bíró olyan összefüggő, véges, ciklus nélküli, T tulajdonságú gráf, amelynek van két oly pontja, U és A, hogy U-ból nem indul ki él és A-ból nem visz U-ba pályavonal.

Minthogy $\mathfrak{G}$ összefüggő, van oly ω útja, amely A-t U-val összeköti (l. 5. ábra). Legyen ω-n B az első olyan pont U-tól számítva, amelyből nem visz U-ba pályavonal (ilyen pont van, ha más nem, akkor A).

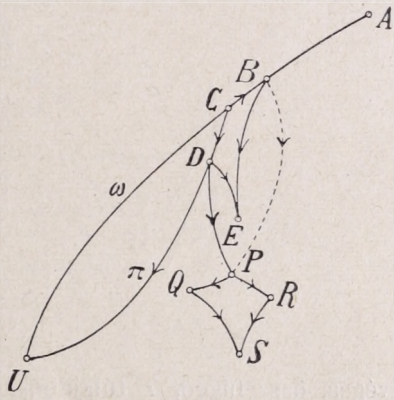
Legyen B szomszédja az ω úton U felé C ($C \neq U$, mert sem $\overrightarrow{UB}$, sem $\overrightarrow{BU}$ él nincs, az előbbi az U-ra tett feltevés, az utóbbi a B definíciója miatt); a feltevés szerint van olyan π pályavonal, amely C-ből U-ba visz. Legyen π C-ből kiinduló éle $\overrightarrow{CD}$. Minthogy π minden pontjából visz U-ba pályavonal, B nincs rajta π-n; továbbá az ω út BC élének irányítása szükségképpen $\overrightarrow{CB}$,

---

[20] Ez a tény, $\mathfrak{F}_n$-re alkalmazva, annak felel meg, hogy n felbontható törzstényezők szorzatára.

különben a $\overrightarrow{BC}$ él és π a B-ből U-ba vivő pályavonalat adna. Ennélfogva a T tulajdonság miatt $\mathfrak{G}$-nek van oly E pontja, ahova B-ből is, D-ből is visz pályavonal (ebből egyébként nyilvánvaló, hogy $D \neq U$).

Tekintsük most azt a $\mathfrak{G}'$ irányított gráfot, amelyet B, D, továbbá $\mathfrak{G}$-nek azok a *pontjai* alkotnak, amelyekbe vagy B-ből, vagy D-ből visz $\mathfrak{G}$-nek pályavonala, továbbá $\mathfrak{G}$-nek azok az *élei*, amelyeken legalább egy ilyen pályavonal átmegy. A π pályavonal DU szakasza, valamint a BE, DE pályavonalak $\mathfrak{G}'$-höz tartoznak. Ennélfogva $\mathfrak{G}'$ összefüggő; ugyanis bármelyik szögpontja összeköthető vagy B-vel, vagy D-vel, tehát, minthogy ezek (E-n át) egymással is összeköthetők, $\mathfrak{G}'$ bármely szögpontja összeköthető bármely másik szögpontjával is. Minthogy $\mathfrak{G}'$ része $\mathfrak{G}$-nek, világos, hogy véges és ciklus nélküli gráf. Továbbá $\mathfrak{G}'$ is T tulajdonságú. Legyenek ugyanis $\overrightarrow{PQ}$ és $\overrightarrow{PR}$ ($Q \neq R$) élei $\mathfrak{G}'$-nek; minthogy ezek $\mathfrak{G}$-nek is élei, van $\mathfrak{G}$-nek oly S pontja, amelybe Q-ból is, R-ből is visz pályavonala. Azonban e pályavonalak (s így az S pont is) hozzátartoznak $\mathfrak{G}'$-höz is; ugyanis a $\overrightarrow{DP}$ vagy $\overrightarrow{BP}$ pályavonalat (ilyen van, mert P pontja $\mathfrak{G}'$-nek) akár a $\overrightarrow{PQ}$ éllel és a $\overrightarrow{QS}$ pályavonallal, akár a $\overrightarrow{PR}$ éllel és az $\overrightarrow{RS}$ pályavonallal meghosszabbítva $\mathfrak{G}$-nek D-ből, illetőleg B-ből kiinduló pályavonalát kapjuk.

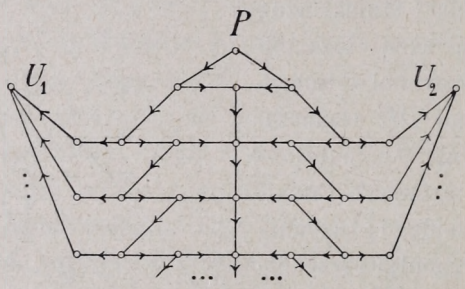


5. ábra.

Minthogy $\mathfrak{G}'$-nek kevesebb szögpontja van, mint $\mathfrak{G}$-nek (ugyanis C nem lehet pontja $\mathfrak{G}'$-nek. mert $\mathfrak{G}$-nek nincs ciklusa), $\mathfrak{G}'$-re áll a bebizonyítandó állítás. U-ból $\mathfrak{G}'$-nek sem indulhat ki éle, tehát adódik, hogy $\mathfrak{G}'$ minden pontjából visz $\mathfrak{G}'$-nek

pályavonala U-ba. Ez azonban ellentmond annak, hogy B-ből nem visz U-ba pályavonala $\mathfrak{G}$-nek, tehát $\mathfrak{G}'$-nek sem.

8. Az imént bebizonyított tétel végtelen gráfokra nem érvényes, amint ezt a 6. ábrán szemléltetett, lefelé határtalanul meghosszabbítandó gráf mutatja. Ennek az összefüggő, T tulajdonságú gráfnak nincs ciklusa; mégsem indul ki sem az U_1, sem az U_2 szögpontjából éle.[21] Könnyen meg lehet adni olyan



6. ábra.

véges, összefüggő, T tulajdonságú, de ciklussal bíró gráfot is, amelynek két ilyen szögpontja van.[22]

9. Annál meglepőbb viszont, hogy a T tulajdonság egy kis módosításával olyan tételhez jutunk, amelynél nem kell a gráfról feltennünk sem azt, hogy véges, sem azt, hogy nincs ciklusa. Ez a módosított T' *tulajdonság* a következő:

Ha PQ és PR a $\mathfrak{G}$ gráfnak valamely szögpontjából két különböző pontjába vivő élei, akkor vagy van $\mathfrak{G}$-nek ($\overrightarrow{QR}$ vagy $\overrightarrow{RQ}$ irányítású) QR éle, vagy pedig van olyan S pontja $\mathfrak{G}$-nek, amelybe Q-ból is, R-ből is visz éle $\mathfrak{G}$-nek.

Be fogom tehát bizonyítani a következő tételt:

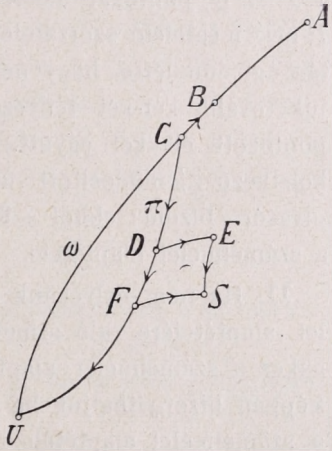
---

21 A P pontot és a belőle kiinduló két élt el lehetne hagyni; azért vettem ezeket hozzá a gráfhoz, hogy, a faktorizációs gráfokhoz hasonlóan, csak egy olyan pontja legyen, amelybe nem fut él.

22 Ilyen gráf keletkezik pl. a 6. ábrán látható gráfból, ha P és a belőle kiinduló élek elhagyása után azt hengerre rajzoljuk úgy, hogy a «pagoda» legfelső «emelete» egybeessék valamelyik alsó «emelettel».

Ha a $\mathfrak{G}$ összefüggő irányított gráf T' tulajdonságú, akkor legfeljebb[23] *egy olyan U pontja lehet, amelyből nem indul ki él.*

Ismét elegendő bebizonyítanunk, hogy, ha a $\mathfrak{G}$ gráf U pontjából nem indul ki él, akkor $\mathfrak{G}$ bármely másik A pontjából visz U-ba pályavonal. Tegyük fel ugyanis, hogy ez $\mathfrak{G}$ valamely A pontjára nem áll. Kössük össze A-t U-val ismét $\mathfrak{G}$ egy ω útjával és legyen ezen, U-tól számítva, B az első pont, amelyből nem visz pályavonal U-ba, legyen továbbá C a B pont szomszédja az ω úton U felé. Akkor C-ből visz π pályavonal U-ba és a BC él irányítása $\overrightarrow{CB}$.



7. ábra.

Legyen π-n, U-tól számítva, D az első olyan pont, amelyből indul ki olyan $\overrightarrow{DE}$ él, hogy E-ből nem visz pályavonal U-ba (l. 7. ábra); ilyen D pont van, ha más nem, akkor C. Világos, hogy $D \neq U$; legyen F a D pont szomszédja π-n U felé. E nincs rajta π-n (különben vinne E-ből pályavonal U-ba), így mindenesetre $E \neq F$. A T' tulajdonság szerint a következő három eset közül valamelyiknek állnia kell:

a) $\mathfrak{G}$-nek van $\overrightarrow{FE}$ éle. Ez ellentmond D definíciójának, mert ekkor F-ből is indulna ki oly $\overrightarrow{FE}$ él, amelynek másik végpontjából nem visz U-ba pályavonal.

b) $\mathfrak{G}$-nek van $\overrightarrow{EF}$ éle. Ez az él π $\overrightarrow{FU}$ szakaszával együtt E-ből U-ba vivő pályavonalat adna, ellentétben E definíciójával.

c) $\mathfrak{G}$-nek van E-ből és F-ből ugyanabba az S pontba vivő $\overrightarrow{ES}$ és $\overrightarrow{FS}$ éle. D definíciója szerint S-ből visz U-ba pálya-

---

[23] Könnyen látni, hogy ha $\mathfrak{G}$ végtelen gráf, akkor nem feltétlenül van ilyen U pont.

vonal; ez $\overrightarrow{ES}$-sel együtt (ill., ha e pályavonal átmenne E-n, ennek egy része) E-ből U-ba vivő pályavonalat adna, ellentétben E definiciójával.

10. A most bebizonyított gráfelméleti tételt is fel lehet használni a számelmélet alaptételének bebizonyítására. E célból az n szám faktorizációs gráfjának fogalmát úgy módosítjuk, hogy a P és Q pontokat akkor is összekötjük egy $\overrightarrow{PQ}$ éllel, ha a P-nek megfelelő szorzatelőállításból a Q-nak megfelelő előállítás úgy jön létre, hogy nem egy, hanem több tényezőjét bontjuk tovább két-két tényezőre. (L. $n = 60$ esetén a 2. ábrát, a pontozott élekkel együtt.) Annak bebizonyítását, hogy az így keletkező $\mathfrak{F}'_n$ módosított faktorizációs gráf T' tulajdonságú, az olvasóra bízom; ebből a **9.** tétele segítségével újból következik a számelmélet alaptétele.

11. Ha nem helyezünk súlyt a négyszámtételről a számelmélet alaptételére való átmenet tiszta kombinatorikai jellegére, akkor a számelmélet alaptételét legegyszerűbben a következőképpen bizonyíthatjuk be a négyszámtételből. Tegyük fel, hogy a számelmélet alaptétele nem áll, és legyen n a legkisebb oly pozitív egész szám, amelynek két, lényegesen különböző, törzstényezős előállítása van: P és Q. Foglaljuk össze tetszésszerint P bizonyos tényezőit (nem valamennyit) és legyen ezek szorzata a, míg P többi tényezőinek szorzata b; hasonlóan legyen Q bizonyos tényezőinek szorzata c, a többi tényezőjének szorzata pedig[24] d. Akkor a, b, c, d kisebbek n-nél, úgy hogy ezek csak lényegében egy-egyféle módon bonthatók fel törzstényezők szorzatára. Az n szám P felbontását megkapjuk, ha $n=ab$-ben a és b helyébe törzstényezős felbontásukat írjuk; hasonlóan megkapjuk a Q felbontást, ha $n=cd$-ben c és d helyébe törzstényezős felbontásukat írjuk.

---

[24] Pl. a legyen P egyik törzstényezője, b a többiek szorzata; hasonlóan c és d a Q előállításra nézve.

Minthogy $ab = cd$, a négyszámtétel szerint van négy oly pozitív egész szám, t, u, v, w, hogy

$$a = tu, \quad b = vw, \quad c = tv, \quad d = uw. \tag{11}$$

Nyilván t, u, v, w is kisebbek n-nél, így ezeknek is egy-egy törzstényezős felbontásuk van.[25] Ha e törzstényezős felbontásokat t, u, v, w helyére a (11) egyenletekbe beírjuk, megkapjuk a, b, c, d egy-egy törzstényezős előállítását, tehát ezek *egyetlen* törzstényezős előállítását. E szerint n-nek P előállítását úgy kapjuk meg, hogy az $n = tu.vw$ egyenletbe, a Q előállítást pedig úgy, hogy az $n = tv.uw$ egyenletbe beírjuk t, u, v, w helyébe ezek törzstényezős előállítását. Igy tehát P és Q, a feltevéssel ellentétben, csak a tényezők sorrendjében különböznek egymástól.

3. §.

12. A négyszámtételt többtényezős szorzatokra a következőképpen általánosíthatjuk:[26]

Legyenek $a_1, a_2, \ldots, a_r$; $b_1, b_2, \ldots, b_s$ *olyan nemnegatív egész számok, amelyek között fennáll az*

$$a_1 a_2 \ldots a_r = b_1 b_2 \ldots b_s$$

egyenlet. Akkor van oly, nemnegatív egész számú elemekkel bíró, r sorból és s oszlopból álló mátrix, amelynek az egyes soraiban álló elemek szorzata rendre $a_1, a_2, \ldots, a_r$, *az egyes oszlopaiban álló elemek szorzata pedig rendre* $b_1, b_2, \ldots, b_s$.

---

[25] Ha valamelyikük 1, akkor törzstényezős előállításán a «0 tényezős» szorzatot értjük; tehát 1 helyébe törzstényezős előállítását beírni annyit jelent, mint elhagyni az 1-et.

[26] KORSELT szerint (l. a [11] lábjegyzetben idézett helyet) ez az általánosítás szerepel KRONECKER «Vorlesungen über Zahlentheorie»-jában. Azonban e mű egyetlen általam ismert kiadásában (L. KRONECKER: *Vorlesungen über Zahlentheorie*, erster Band [több nem jelent meg], herausgegeben von K. HENSEL, Leipzig (1901)) nem található erre vonatkozó rész. A Korseltnél álló szövegből világos, hogy e tételre, mint a számelmélet alaptételének következményére gondol.

Ha $r=1$ vagy $s=1$, akkor a tétel tautologikus. Ha $r=s=2$, akkor éppen a négyszámtételbe megy át. Elegendő tehát a következő két dolgot megmutatnom:

a) Ha a tétel igaz $r=2$, $s=2$, valamint egy bizonyos r és $s=2$ esetére, akkor igaz r helyett $r+1$-gyel $s=2$ esetére.

b) Ha a tétel igaz — egy bizonyos r érték mellett — $s=2$, valamint egy bizonyos s esetére, akkor igaz s helyett $s+1$-gyel is.

Elegendő *b)*-t megmutatnom, hiszen *a)* ebből az $r=2$ specializálással, a szóbanforgó mátrix sorainak oszlopaival való felcserélésével és s helyébe r tételével keletkezik.

Legyen tehát igaz a tétel r egy bizonyos értéke mellett $s=2$-re, valamint egy bizonyos s-re. Legyen $a_1, a_2, \ldots, a_r$; $b_1, b_2, \ldots, b_s, b_{s+1}$ $r+s+1$ olyan nemnegatív egész szám, amelyek között fennáll az

$$a_1 a_2 \ldots a_r = b_1 b_2 \ldots b_s b_{s+1} \tag{12}$$

egyenlet. Alkalmazzuk a bebizonyítandó tételt mindenekelőtt az $a_1, a_2, \ldots, a_r$; $b_1, b_2, \ldots, b_{s-1}, b'_s = b_s b_{s+1}$ számokra. Adódik, hogy van oly (t_{ij}) $(i=1, 2, \ldots, r;\ j=1, 2, \ldots, s)$ mátrix, amelynek elemei nemnegatív egész számok, úgy, hogy

$$a_i = t_{i1} t_{i2} \ldots t_{is}, \quad \text{ha} \quad i=1, 2, \ldots, r; \tag{13}$$

$$b_j = t_{1j} t_{2j} \ldots t_{rj}, \quad \text{ha} \quad j=1, 2, \ldots, s-1, \tag{14}$$

míg

$$t_{1s} t_{2s} \ldots t_{rs} = b_s b_{s+1}.$$

Alkalmazzuk most a bebizonyítandó tételt a $t_{1s}, t_{2s}, \ldots, t_{rs}$; b_s, b_{s+1} számokra. Adódik, hogy van $2r$ olyan nemnegatív egész szám, $u_1, u_2, \ldots, u_r, v_1, v_2, \ldots, v_r$, hogy

$$t_{is} = u_i v_i, \quad \text{ha} \quad i=1, 2, \ldots, r; \tag{15}$$

$$b_s = u_1 u_2 \ldots u_r; \tag{16}$$

$$b_{s+1} = v_1 v_2 \ldots v_r. \tag{17}$$

A (13) és (15) egyenletekből

$$a_i = t_{i1} t_{i2} \ldots t_{i,s-1} u_i v_i, \quad \text{ha} \quad i=1, 2, \ldots, r;$$

ez az egyenlet, továbbá (14), (16) és (17) mutatja, hogy a tétel a (12) egyenlet bal- és jobboldalán álló számokra is igaz: a keresett mátrix

$$\begin{pmatrix} t_{11} & t_{12} & \dots & t_{1,s-1} & u_1 & v_1 \\ t_{21} & t_{22} & \dots & t_{2,s-1} & u_2 & v_2 \\ & & \dots & & & \\ t_{r1} & t_{r2} & \dots & t_{r,s-1} & u_r & v_r \end{pmatrix}.$$

13. A négyszámtétel ez általánosításából a számelmélet alaptétele nagyon egyszerűen adódik. Tegyük fel ugyanis, hogy

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

ahol $p_1, p_2, \dots, p_r, q_1, q_2, \dots, q_s$ törzsszámok. A négyszámtétel általánosítása szerint van olyan nemnegatív egész számú elemekből álló mátrix, amelynek első, második, ..., r-edik sorában álló elemek szorzata rendre $p_1, p_2, \dots, p_r$, első, második, ..., s-edik oszlopában álló elemek szorzata pedig rendre $q_1, q_2, \dots, q_s$ (és több sora vagy oszlopa nincs). De akkor e mátrix minden sorában vagy oszlopában, egy-egy elem kivételével, csupa 1 áll; az egyetlen, 1-től különböző elem a kérdéses sorhoz vagy oszlophoz tartozó p_i, illetőleg q_j. De akkor r is, s is egyenlő a mátrix 1-től különböző elemeinek számával; maguk ez elemek, a mátrix sorai szerint rendezve, rendre p_1-gyel, p_2-vel, ..., p_r-rel, a mátrix oszlopai szerint rendezve pedig rendre q_1-gyel, q_2-vel, ..., q_s-sel egyenlők; azaz $p_1, p_2, \dots, p_r$ csak sorrendben különböznek $q_1, q_2, \dots, q_s$-től.

4. §.

14. Megmutatom, hogy a négyszámtétel nagyon jól használható néhány, az elemi számelméleti előadásokban szerepelni szokott további tétel bebizonyítására is. E §-ban szám mindenütt pozitív egész számot jelent; minthogy oszthatósági tételekről van szó, nyilvánvaló, hogyan lehet azokat tetszőleges racionális egész számokra átvinni.

Ha egy ab szorzat osztható egy c számmal, de egyik tényezője, a, relatív prímszám c-hez, akkor a szorzat másik tényezője, b, osztható c-vel.

Ugyanis a feltevés szerint van olyan d egész szám, hogy

$$ab = cd, \tag{18}$$

a négyszámtétel szerint van négy oly t, u, v, w egész szám, hogy

$$a = tu, \quad b = vw, \quad c = tv, \quad d = uw. \tag{19}$$

Minthogy a-nak és c-nek nincs más közös osztója, mint 1, szükségképpen $t = 1$, tehát $c = v$, $b = cw$, azaz b osztható c-vel.

Abban az esetben, ha c törzsszám, ez a tétel átmegy a törzsszámok alaptulajdonságának kéttényezős szorzatra vonatkozó speciális esetébe. A tényezők száma szerinti teljes indukcióval bebizonyíthatjuk ebből a törzsszámok alaptulajdonságát a maga általánosságában s így, a bevezetésben részletezett módon, a klasszikus mederben maradva is eljuthatunk a számelmélet alaptételéhez. (Ez az a mód, ahogyan egyetemi előadásaimban be szoktam bizonyítani a számelmélet alaptételét.)

15. *Valamely ab szorzat minden osztója előállítható a egy osztójának b egy osztójával való szorzataként.*[27] Ha ugyanis d osztója ab-nek, akkor van olyan c egész szám, hogy (18) fennáll; a négyszámtételt alkalmazva adódik, hogy van négy oly t, u, v, w egész szám, amelyekre (19) fennáll. A (19) egyenletek mutatják, hogy u osztója a-nak, w osztója b-nek és d ezeknek szorzata.

Világos, hogy fordítva, a bármely osztójának b bármely osztójával való szorzata osztója d-nek. Általában ab valamely osztója többféleképpen is előállítható a tételben említett módon. Azonban:

Ha a relatív prímszám b-hez, akkor ab minden osztója csak egyféleképpen állítható elő a és b egy-egy osztójának szorzataként. Ez belátható a **14.**-ben bebizonyított tétel segítségével is; a négyszámtételből közvetlenül így adódik: ha ab valamely osztója, d, kétféleképpen is előállítható a és b egy-egy osztójának szorzataként:

$$d = ef, \quad d = gh,$$

---

[27] A bebizonyításból látszik, hogy ez a tétel nem egyéb, mint a négyszámtételnek más (kevésbbé szimmetrikus) megfogalmazása.

ahol (azt, hogy k osztója l-nek, a szokott módon a $k|l$ jellel jelölve)

$$e|a, \quad f|b, \quad g|a, \quad h|b,$$

akkor $ef = gh$, tehát a négyszámtétel szerint van négy oly t, u, v, w szám, hogy

$$e = tu, \quad f = vw, \quad g = tv, \quad h = uw. \tag{20}$$

Minthogy $u|e$ és $e|a$, az oszthatóság ú. n. tranzitív sajátsága folytán $u|a$; hasonlóan $u|h$ és $h|b$ miatt $u|b$; tehát $u = 1$, mert a-nak és b-nek nincs más közös osztója. Hasonlóan, $v|g$ és $g|a$ miatt $v|a$, $v|f$ és $f|b$ miatt $v|b$ s így $v = 1$. E szerint (20)-ból $e = t = g$, $f = w = h$, vagyis a kétféle előállítás mégis csak ugyanaz.

Ezek az alkalmazások már eléggé mutatják a négyszámtétel használhatóságát az elemi számelmélet tárgyalásánál.

Kalmár László.

ÜBER DEN FUNDAMENTALSATZ DER ZAHLENTHEORIE.

Es werden mehrere Beweise für den Fundamentalsatz der elementaren Zahlentheorie (Satz von der eindeutigen Darstellbarkeit der natürlichen Zahlen als Produkte von Primzahlen) gegeben, unabhängig vom Begriff und Eigenschaften des größten gemeinsamen Teilers (oder der kleinsten gemeinsamen Vielfachen). Sämtliche Beweise beruhen auf dem folgenden Lemma («Vierzahlensatz»):

Genügen die nichtnegativen ganzen Zahlen a, b, c, d der Gleichung $ab=cd$, so gibt es vier weitere nichtnegative Zahlen t, u, v, w, so daß $a = tu$, $b = vw$, $c = tv$, $d = uw$.

Dieser Satz wird natürlich ohne Anwendung des Fundamentalsatzes der Zahlentheorie, durch vollständige Induktion in Bezug auf a bewiesen. Der Übergang zum Fundamentalsatz der Zahlentheorie wird sowohl graphentheoretisch, wie auch rein zahlentheoretisch geführt. Schließlich wird gezeigt, daß der Vierzahlensatz auch sonst für Vorlesungszwecke nützlich ist, da daraus auch einige weiteren elementar-zahlentheoretischen Sätze ziemlich direkt zu entnehmen sind.

László Kalmár.