

A Wilson-tételnek és megfordításának bizonyítása Bolyai Farkas kéziratos hagyatékában

Szabó Péter Gábor

1. Bevezetés

A Wilson-tételt, vagyis ha p prímszám, akkor $(p-1)! + 1$ osztható p -vel már Lagrange is bebizonyította 1771-ben. Igazolta az állítás megfordítását is, ami a tétellel együtt így azt állítja, hogy p akkor és csak akkor prímszám, ha $(p-1)! \equiv -1 \pmod{p}$. Ezt ma már a legtöbb egyetemi számelméleti kurzus tárgyalja.

A közelmúltban Kiss Elemér, marosvásárhelyi matematikus *Matematikai kincsek Bolyai János kéziratos hagyatékából* című könyve kapcsán figyelhattünk fel újra a Wilson-tételre. Kiderült, hogy a tétellel és megfordításának bizonyításával a két Bolyai is foglalkozott. Munkájuk apropóját az adta, hogy Gauss a *Disquisitiones Arithmeticae*-ben bár tárgyalta a Wilson-tételt, de annak megfordításáról Bolyai Farkas szavaival élve *“merőben hallgat”*. Kiss Elemér könyvében megtalálhatjuk Bolyai Jánosnak a megfordításra adott elegáns bizonyítását, valamint János utalásait apja megközelítéséről: *“oly szép és fontos Wilson-tétel fordítottját apám és én is bebizonyítottuk”, “A Wilson-tan fordítottjának is szigorú, bár is nem rövid okát adta.”*.

Bolyai Farkas matematikai vonatkozású kéziratos hagyatékára Oláh Anna, fizikus hívta fel a figyelmem. A kéziratok között sikerült megtalálni Bolyai Farkasnak a Wilson-tételre és annak megfordítására adott bizonyítását, amit a jelen dolgozatban teszünk közzé. Matematikai szempontból a mai olvasó újdonságot talán nem fog találni a bizonyításban, viszont maga a tárgyalás, ahogy ezt 150 évvel ezelőtt Bolyai Farkas előadta, mindenképpen kuriózumnak számít. Az eredeti kéziratok fénymásolata és azok kibetűzött változata mellett, megjegyzésekkel segítjük az olvasót. A lapok itt-ott sérültek; azokat a részeket, amelyeket a szöveggörnyezet alapján valószínűsítettünk szögletes zárójelek közé írtak. Az itt közölt oldalaknak a Teleki-Bolyai Könyvtárban a jelzetszámok BF 88/1, BF 88/1v, BF 88/2, BF 88/2v. Ezek az iratok a Magyar Tudományos Akadémia Könyvtárának Mikrofilmtárában is megvannak a 8030-as tekercsen.

Lássuk hát, hogyan is adta meg Bolyai Farkas, *A' Wilson theoremájának 's conversának is demonstratióját*.

maus alfijának kör factora volna, ugyanis
 S és S' nek; és akkor balra monve; mint
 denitnek $A' = 1$ egy ugyan a factora volna.
 Most legyen két primus approximátusnak
 jobb felől alfija K' és bal felől I' ; S kör
 factoruk c ; $K' = mc$; $I' = nc$; akkor
 mivel $K' = I' + H'$, leír $K' = nc + H' = mc$;
 tehát $H' = (m - n)c$. Melyet balra A' ig fogy.
 letni lehet.
 S és S' is prim az vr hoz. Most legyen
 péld. S kör factor vr ban $S = S' + u$; S le-
 gyen $vr = v \cdot S$; S és $S' = \gamma \cdot S$; leír $S' = \gamma \cdot S - \gamma \cdot S$
 $= (1 - \gamma) \cdot S$. Tehát vr és S' nem volnának
 primek egymáshoz.
 Hogy pedig $vr - by$ ban y nál vr nál kisebb
 lenne van -1 re, és ahelyett, az vr
 akár prim fiam magában akár nem; tehát
 Most ha $\frac{S}{y}$ páratlan páratlan, úgy
 $y = S'$, S és $S' = \frac{S}{y} = -1$; ha pedig páros $\frac{S}{y}$
 majd, akkor $vr - (vr - S') = -1$; a' mikor
 is (Fens.) $\frac{S}{y}$ de formában $q = 1$ miatt
 bit, S és $q = 2$ nem veres lehet, mert akkor
 $2vr - S' > vr$ volna.
 S' és $vr - S'$ pedig különböz; mert ha
 egyenlők volnának $S' = vr - S'$ prim vr ba
 mert $vr = 2 S'$ volna.
 De hogy y nál nagyobb y nál kisebb
 51 88/1 17

2. ábra. A BF 88/1 jelzetszámú lap másik oldala.

3. A kibetűzött szöveg

A' Wilson theoremajának 's conversájának is demonstratiója

Előre bocsáttatnak a' Tentamenbol¹

I. Ha $\mathfrak{b}$ és $\mathfrak{a}$ + egész s egymáshoz prim számok², 's $\mathfrak{b} < \mathfrak{a}$; és $\frac{\mathfrak{b}}{\mathfrak{a}}$ fractio continuába³ fejtettve ki, az approximánsok⁴ $\frac{A}{A'}, \frac{B}{B'}, \frac{C}{C'}, \frac{D}{D'}, \frac{E}{E'}, \frac{F}{F'}, \dots$ s péld. $\frac{F}{F'}$ a' végső, az első $\frac{0}{1}$ a' következő $\frac{1}{\mathfrak{a}}$ sat... Ekkor $F = \mathfrak{b}$, 's $F' = \mathfrak{a}$, 's $EF' - E'F$ azaz $E\mathfrak{a} - E'\mathfrak{b} = \pm 1$, és $\mathfrak{a}(\mathfrak{b} - E) - \mathfrak{b}(\mathfrak{a} - E') = \mp 1$; és így $\mathfrak{a}x - \mathfrak{b}y = \pm 1$ re vagy ∓ 1 re y nak becse⁵ lehet E' vagy $\mathfrak{a} - E'$.

II. Azonban $EF' - E'F$ a' szerint $= -1$ vagy $+1$, ha $\frac{A}{A'}$ tol (bezárólag) $\frac{E}{E'}$ páros vagy páratlan számadik. És mind E' a' ± 1 re mind $\mathfrak{a} - E'$ a' ∓ 1 re legkisebb + becse y nak.

Jegyzés. Ott $\mathfrak{a}\mathfrak{b}q - \mathfrak{a}\mathfrak{b}q = 0$ által arra a' végre, hogy x nek s y nak nem csak a' legkisebb hanem minden becsei kijöjjenek, könnyen lesz $[\mathfrak{a}](\pm E'c \pm \mathfrak{b}q) - \mathfrak{b}(\pm E'c \pm \mathfrak{a}q)$; de itt arra nincs szükség.

De ennek felette mind E' mind $\mathfrak{a} - E'$ prim az $\mathfrak{a}$ hoz és $< \mathfrak{a}$ [s] $\mathfrak{b}y$ az $m\mathfrak{a} + 1$ kép alá jön⁶, ha $\mathfrak{a}x - \mathfrak{b}[y] = -1$, a' mikor is $\mathfrak{b}y$ nevezettség -1rei [társ]ul[atn]ak. Hogy [mind E'] mind $\mathfrak{a} - E'$ prim az $\mathfrak{a}$ hoz, látszik [...].

E' -nek és $\mathfrak{a}$ nak köz factora⁷ nem lehet (1 et nem értve oda). Mert két szomszéd approximáns

(BF 88/1)

mans⁸ alsójának⁹ köz factora volna ugymint E' nek és F' nek; és akkor balra menve; mindeniknek $A' = 1$ ig ugyan az factora volna.

Mert legyen két szomszéd approximánsnak jobbfelöli alsója K' s balfelöli I' , 's köz factoruk c , 's $K' = mc$'s $I' = nc$; akkor mivel $K' = I'i + H'$, lesz $K' = nic + H' = mc$; tehát $H' = (m - ni)c$. Melyet balra A' ig folytatni lehet.

S $\mathfrak{a} - E'$ is prim az $\mathfrak{a}$ hoz. Mert legyen péld. 5 köz factora $\mathfrak{a}$ ban 's $\mathfrak{a} - E'$ ben; 's legyen $\mathfrak{a} = \nu 5$, 's $\mathfrak{a} - E' = \gamma 5$; lesz $E' = \nu 5 - \gamma 5 = (\nu - \gamma)5$. Tehát $\mathfrak{a}$ E' nem volnának primek egymáshoz.

Hogy pedig $\mathfrak{a}x - \mathfrak{b}y$ ban y nak $\mathfrak{a}$ nál kisebb becse van -1re, és az edjetlen, az $\mathfrak{a}$ akár prim szám magában akár nem: látszik.

Mert ha $\frac{E}{E'}$ páratlan számadik, úgy $y = E'$, s $\mathfrak{a}x - \mathfrak{b}E' = -1$; ha pedig páros számadik, akkor $\mathfrak{a}x - [\mathfrak{b}](\mathfrak{a} - E') = -1$; a' mikor is (Tent.) a' 2dik formában $q = 1$ vétetik, 's $q = 2$ nem vetetthetik, mert akkor $2\mathfrak{a} - E' > \mathfrak{a}$ volna.

E' és $\mathfrak{a} - E'$ pedig külön[böznek]; mert ha egyenlők volnának E' [nem volna] prim $\mathfrak{a}$ hoz, mert $\mathfrak{a} = 2E'$ volna.

De hogy y nál nagyobb [...] nincs péld.

(BF 88/1v)

$y + 1$ abból is látszik, hogy ha $ax - b(y + 1)$ is $= -1$; akkor $by - 1$'s $b(y + 1) - 1$ is oszolnék a val, tehát $by - 1 + b1$ is oszolnék a val; mely nem lehet; mert b prim lévén a hoz 1 nek kellene legalább akkorának lenni mint a : akkor pedig a ' b társa $>[\dots]+:[\dots]$ negatív se lehet 1 , mert az [előbbi a legkisebb] becs (Tent..).

Legyen¹⁰ már $a = \text{prim } p$. Ekkor y nem lehet $= b$, ha $b < p - 1$ vétetik. Mert ha $a = b = p - n$, a ' mikor is $n > 1$ lenne $bb - 1 = p^2 - 2np + n^2 - 1$; 's $n^2 - 1 = (n + 1)(n - 1)$; és $n + 1$'s $n - 1$ is $< p$. Tehát a szorzás nem oszlik p vel, ha p prim.

Innen mivel p prim 's páratlan, 's minden megelőző számokhoz prim (1en kívül) minden az 1 és $p - 1$ közti számok száma, és minden az azok köze -1 rei társulatnak száma is páros rendre vétetvén b nek az 1 és $p - 1$ közti számok. Tehát mivel mindenik társulat kétszer jön elé minden két egyenlő társulatnak csak edjiket véve lesz minden társulatnak szorza[ta] $= 1 + \mu p$, mert mindenik társulat ez $1 + mp$ [...]hez járulván a p nek kisebb számokból [...] $1(p - 1)$; lesz $(1 + \mu p)(p - 1) = \mu pp + p - \mu p - 1 [= p(\mu p - \mu + 1) - 1]$; melyhez adattván 1 , lesz $p(\mu p - \mu + 1)$. [Tehát] ha p prim, minden megelőző számok szorzata meg 1 oszlik p vel; azaz $\frac{1.2.3...\dots(p-1)+1}{p}$ egész szám.

(BF 88/2)

Megfordítva ha $\frac{1.2.3...\dots(a-1)+1}{a}$ egész szám: ugy a prim. Mert ha a nem prim, azon becs nem egész szám.

Mert kerestessék minden az a hoz prim, a nál kisebbnek -1 rei társulata by , s minden két $=$ társulatból vétessék csak az edjik, s ha valamely az a hoz prim b nek társa $= b$, minden bb kép alá jövő társulat hagyassék ki; s a többi társulatok szorzata legyen K . Továbbá minden bb kép alá jövő társulatból vétessék csak b , s vétessenek minden az a nál kisebb hozzá nem prim számok; 's legyen ezeknek az említett b kkal együtti szorzatuk k . Látszik, hogy Kk minden az a nál kisebb számok szorzata leend. Mert akármely az a hoz nem primek y ja, s minden bb képben is azon b nek nincs más társa, 's ha a társulat kimaradt, b belément s belé mentek az a hoz nem primek is mint szorzók a szorzatba.

Minthogy pedig minden társulat $ma + 1$ kép alá jön, tehát $K = \mu a + 1$. És így $Kk = k\mu a + k$; melyhez azután, lesz $\frac{1.2.3...\dots(a-1)+1}{a} = \frac{k\mu a + k + 1}{a}$, mely nem egész szám; mert $\frac{1}{a} < 1$, s $\frac{k}{a}$ egész szám.

Mert k ban a nak minden primfactora meg van legalább annyiszor a ' hányszor a ban van. Mert akármelyik péld. 2 legyen a ban, az meg van k ban, mert akkor azon 2 nem prim az a hoz, tehát k ban factor, ha pedig péld. d szer van meg azon 2 factor az a ban; $2^{d-1} < a$ és a hoz nem prim, tehát f. . . a k ban; s a hoz járulván maga 2 , vagy [...] factor 2 : k ban 2^d factor leend. Edjetlen [...], ha $a = 2.2$ mert akkor $k = 2$ nem oszlik 4 [el. . .] nem jöhetvén elé. De akkor látszik, hogy $[1.2.3] + 1$ nem oszlik 4 el.

(BF 88/2v)

Megjegyzések a szöveghez

1. A *Tentamen*, teljes címén *Tentamen juventutem studiosam in elementa matheseos purae, elementaris ac sublimioris, methodo intuitiva, evidenti-aeque huic propria introducendi. Cum appendice triplici.* Bolyai Farkasnak 1832–33-ban Marosvásárhelyen megjelent latin nyelvű munkája. A könyv első kötetének §41 és §42 részei a 424–457 oldalakon tárgyalják a lánc törtek elméletének alapjait. Bolyai a kéziratban is ezekre a paragrafusokra hivatkozik. A Jegyzés kezdetű szöveg a 452. oldalon található megjegyzésre utal.
2. *egymáshoz prim számok* = relatív prímek
3. *fractio continua* = lánc tört
4. *approximánsok* = a közelítő törtsorozat törtjei
5. *becse* = értéke
6. *by az ma + 1 kép alá jön* = $by \equiv +1 \pmod{a}$ [4, 184. oldal]
7. *köz factora* = közös osztója
8. *mans*, órszó
9. *alsójának* = nevezőjének
10. Itt kezdődik a Wilson-tétel tényleges bizonyítása, a korábbi megjegyzések csak felvezették azt.

2. “Ezt János találta az enyim után.”

Bolyai Farkas kéziratai között találtunk egy olyan lapot is amelynek egyik oldalán a Wilson-tétel megfordításának egy újabb bizonyítása olvasható. Ezen a BF 100/1v jelzetű lapon található indoklás egészen biztos, hogy Bolyai Jánostól származik. Ezt onnan lehet tudni, hogy az indoklás pontosan megegyezik azzal, amit Kiss Elemér talált Bolyai János kéziratok hagyatékában (három különböző helyen is), továbbá a lap alján Bolyai Farkas ezt jegyezte fel:

“Ezt János találta az enyim után.”

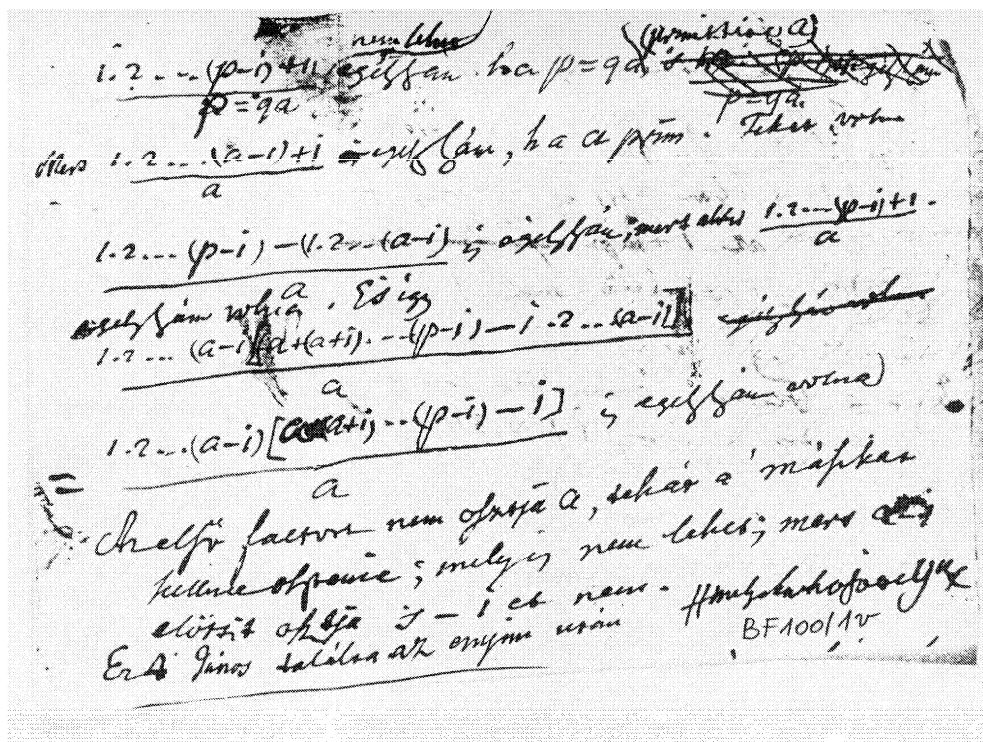
Az eredeti kézirat fénymásolatát az 5. ábrán láthatjuk, annak kibetűzése pedig a következő:

$\frac{1 \cdot 2 \dots (p-1) + 1}{p=qa}$ nem lehet egész szám ha $p = qa$ (prímet téve a). Mert $\frac{1 \cdot 2 \dots (a-1) + 1}{a}$ egész szám, ha a prim. Tehát volna $\frac{1 \cdot 2 \dots (p-1) - 1 \cdot 2 \dots (a-1)}{a}$ is egész szám, mert akkor $\frac{1 \cdot 2 \dots (p-1) + 1}{a}$ egész szám volna. És így

$\frac{1.2 \dots (a-1)a(a+1) \dots (p-1)-1.2 \dots (p-1)}{a} = \frac{1.2 \dots (a-1)a(a+1) \dots (p-1)-1}{a}$ is egész szám volna. Az első factort nem osztja a , tehát a másikat kellene osztania; mely is nem lehet; mert a -1 előtti osztja s -1 et nem.

Ezt János találta az enyim után.

(BF 100/1v)



5. ábra. A BF 100/1v jelzetszámú oldal, amely Bolyai Jánosnak a Wilson-tételre adott bizonyítását tartalmazza.

Az itt tárgyalt iratok bár nem tartalmaznak keltezéseket, mégis szinte biztosra vehetők, hogy az 1850-es évek első felében, vagyis Bolyai Farkas életének utolsó éveiben keletkeztek. Ezt Bolyai Farkasnak egy 1853. november 15.-én kelt levele [3] támasztja alá, amelyben kérdéssel fordul Vajda Dánielhez (Bolyai János egykori magántanítójához) és Szász Károlyhoz (aki a levél írása idején marosvásárhelyi tanár), hogy látta-e már a Wilson-tétel megfordítását, mert ha nem, nála "van valami". A BF 100/1v lap másik oldalán a legkisebb álrím, a 341 próbája található, amit Bolyai János talált és közölt édesapjával egy 1855. májusában írt levelében [4, 80. és 184. oldal]. A fenti kéziratok keletkezését ezen dátumok alapján valószínűsíthetjük és helyezhetjük el az időben.

Köszönetnyilvánítás

Ezúton köszönöm Oláh Anna Bolyai-kutatónak, hogy segített a kibetűzésben és mindig odaadóan támogatta a munkámat. Külön köszönöm Dr. Kiss Elemér akadémikusnak, hogy a marosvásárhelyi tartózkodásom alatt oly szívesen vezetett végig a Bolyai-emlékhelyeken. Hálás vagyok Dr. Kása Zoltánnak a Babes-Bolyai Tudományegyetem egyetemi tanárának is, a CEEPUS-ösztöndíjas kolozsvári utam során nyújtotta segítségéért.

Irodalom

- [1] Bolyai gyűjtemény, Magyar Tudományos Akadémia Könyvtára, Budapest.
- [2] Bolyai Farkas, *Tentamen juventutem studiosam in elementa matheseos purae, elementaris ac sublimioris, methodo intiutiva, evidentiaque huic propria introducendi. Cum appendice triplici*, Maros vásárhelyini, 1832-33. Az általunk megadott hivatkozások a második kiadás (1897, 1904) köteteire vonatkoznak.
- [3] Bolyai Farkas 10 levele (közli Benkő Samu), *Igaz Szó* 23:3, 1975, 262-273.
- [4] Kiss Elemér, *Matematikai kincsek Bolyai János kéziratok hagyatékából*, Akadémiai Kiadó és Typotex Kft, Budapest, 1999.