

Bevezetés

Az 1986. évi *Kürschák-verseny*en szerepelt az alábbi feladat:

A és B a következő játékot játssza: Az első 100 pozitív egész közül véletlenszerűen kiválasztanak k darabot és ha ezek összege páros, akkor A, egyébként pedig B nyer. A k milyen értékeire lesz egyenlő A és B nyerési esélye?

A válasz: páratlan k esetén a nyerési esélyek egyenlők, páros k esetén pedig nem: ha $k/2$ páros, akkor A, ha pedig $k/2$ páratlan, akkor B nyerési esélye nagyobb.

A KÖMAL 1987/2 számában közölt I. megoldás akkor is alkalmazható, ha valamilyen páros n -re A és B nem az első 100, hanem az első n pozitív egész közül választ ki k darabot (érdemes meggondolni, mit ad a módszer páratlan n -re).

Természetesnek tűnt a következő általánosítás: mit mondhatunk akkor, ha nem kettő, hanem m játékos játszik, úgy, hogy az m valamilyen n többszörösére az első n pozitív egész közül véletlenszerűen kiválasztanak k darabot, ezek összegét maradékosan elosztják m -mel, és a maradék határozza meg a nyertes személyt: 0 maradék esetén az első, 1 maradék esetén a második és általában, r maradék esetén az $(r + 1)$ -edik játékos nyer?

Egy speciális eset

Viszonylag könnyű volt megtalálnom a választ akkor, ha az m prímszám: ebben az esetben a játék pontosan akkor igazságos, ha a k nem osztható m -mel, azaz $(k, m) = 1$.

Osszuk be ugyanis az első n pozitív egészt n/m darab m elemű „blokkba”: $(1, 2, \dots, m), (m+1, \dots, 2m), \dots, (n-m+1, \dots, n)$, és tekintsük azokat a k -asokat, amelyek mindegyikéhez található olyan blokk, amelynek a k -as tartalmazza legalább egy, de nem az összes elemét. Az ilyen k -asokat m elemű osztályokra fogjuk bontani úgy, hogy egy-egy osztályban a k -asok elemeinek összegei minden lehetséges maradékot kiadnak m -mel osztva.

Úgy kapjuk meg egy k -ashoz a vele egy osztályban levő további $(m - 1)$ darabot, hogy megkeresve a legelső olyan blokkot, amelynek legalább egy, de nem az összes elemét kiválasztottuk, az adott k -asnak az ebbe a blokkba eső elemeit minden lehetséges módon „elforgatjuk”: azaz mindegyiküket növeljük ugyanazzal a 0 és $m - 1$ közé eső egésszel, majd azokat az elemeket, amelyek ezáltal kikerülnek a blokkból, m -mel csökkentjük, hogy visszakerüljenek. Tegyük fel, hogy a kiinduló k -as a blokkból d darab elemet tartalmaz $(1 \leq d < m)$ és e k -asban az elemek összege S . Ekkor a k -ast tartalmazó osztályban a k -asok összegei m -mel osztva az $S, S + d, S + 2d, \dots, S + (m - 1)d$ számokkal egyenlő maradékokat adnak, hiszen ha a d darab blokkbeli elem mindegyikéhez i -t adunk $(0 \leq i < m)$, majd néhányat m -mel csökkentünk, egy $S + id$ -vel kongruens számot kapunk $(\text{mod } m)$. Ez az m darab szám pedig csupa különböző maradékot ad m -mel osztva, mert ha $S + id \equiv S + jd \pmod{m}$, akkor m osztója $(i - j)d$ -nek, ami $-m < i - j < m$ és $1 \leq d < m$ miatt csak úgy lehetséges, ha $i - j = 0$, azaz $i = j$, hiszen az m prím. Mivel pedig a lehetséges maradékok száma éppen m , valóban előáll az összes lehetséges maradék. Az eddig vizsgált (nem üres – nem teli blokkokat tartalmazó) k -asokon játszva tehát igazságos a játék.

A fennmaradó k -asok azok, amelyek minden blokknak vagy mind az m elemét tartalmazzák, vagy egyet sem; ilyenek csak akkor vannak, ha m , a blokk mérete osztója a k -as elemszámának, azaz k -nak. Az ilyen k -asokban az elemeket m -mel osztva minden lehetséges maradékot egyaránt k/m esetben kapunk, így az elemek összege kongruens

$$(0 + 1 + 2 + \dots + (m - 1)) \cdot k/m = \frac{k(m - 1)}{2} - \text{vel } (\text{mod } m).$$

Ez viszont azt jelenti, hogy az ilyen k -asok összegei m -mel osztva ugyanazt a maradékot adják, az m darab játékos közül tehát egynek nagyobb a nyerési esélye a játékban, annak, aki a fenti maradéknál nyer.

Ha tehát m nem osztója a k -nak, akkor a játék igazságos, egyébként pedig nem.

A bizonyítás $m = 2$ esetén megegyezik az eredeti feladat megoldásával.

Most már könnyű volt megadni a játék igazságosságának egy szükséges feltételét az általános esetre: az m -nek és a k -nak relatív prímnek kell lennie. Tegyük fel ugyanis, hogy a játék igazságos, de m -nek és k -nak mégis van egy közös p prímosztója. Osszuk be a játékosokat p csapatba úgy, hogy az i -edik csapatba az i -edik, a $(p + i)$ -edik, $(2p + i)$ -edik, $\dots$, $(m - p + i)$ -edik játékos kerüljön $(i = 1, 2, \dots, p)$. Ekkor minden csapatban m/p játékos lesz.

1988-04-146-1.eps

1. ábra

Játsszák most a játékot úgy, hogy ne egy játékos nyerjen, hanem az a csapat, amelyiknek tagja az illető játékos. Mivel feltevésünk szerint az „egyéni” játék igazságos és minden csapat ugyanannyi játékosból áll, a játék a csapatok között is igazságos.

Ugyanakkor azt, hogy melyik csapat nyer, az dönti el, hogy milyen maradékot ad a kiválasztott k darab szám összege p -vel osztva: a i -edik csapat ugyanis akkor nyer, ha az összeg m -mel osztva $i - 1, p + i - 1, \dots, m - 2p + i - 1, m - p + i - 1$, azaz p -vel osztva $i - 1$ maradékot ad. Láttuk viszont, hogy az ilyen játék nem lehet igazságos – mert k osztható p -vel –, és így az eredeti egyéni játék sem az.

Azt sem volt nehéz bebizonyítani, hogy a kapott szükséges feltétel elégséges is: ha k és m relatív prímek, akkor a játék igazságos: az $m = \text{prim}$ esetben talált „forgatásos” bizonyítás ugyanis most is működik, ennek végiggondolását az Olvasóra hagyjuk.

Hogyan tovább?

Ezután természetesen azzal kezdtem foglalkozni, mit mondhatunk akkor, ha nem kötjük ki, hogy m , a játékosok száma, osztója legyen n -nek. '87 februárjában sikerült bebizonyítanom a következőket:

- ha m prímszám, akkor a játék igazságosságának szükséges és elégséges feltétele, hogy k adjon m -mel osztva nagyobb maradékot, mint n ad m -mel osztva; (a már vizsgált $m \mid n$ esetben ez a talált $m \nmid k$ feltételt jelenti)
- ha $m = p^\alpha$, ahol p prímszám és α pozitív egész, akkor a feltétel az, hogy minden $1 \leq i \leq \alpha$ -ra k adjon p^i -nel osztva nagyobb maradékot, mint n ad p^i -nel osztva.

Ezekből az általános esetre is kaptam egy szükséges feltételt: ha a játék igazságos, akkor minden olyan p prímszámra és i pozitív egészre, amelyre p^i osztója m -nek, k nagyobb maradékot kell, hogy adjon p^i -nel osztva, mint n (a bizonyítást a csapatba rendezési módszerrel gondolja meg az Olvasó).

A továbbiakban jelöljük egy a szám b -vel való osztásakor kapott maradékát $a \pmod{b}$ -vel.

A fenti feltétel nem elégséges: például ha $m = 10$, $n = 6$ és $k = 3$, akkor teljesül, hiszen $3 \pmod{2} = 1 > 6 \pmod{2} = 0$ és $3 \pmod{5} = 3 > 6 \pmod{5} = 1$, a játék viszont nem igazságos: az első 6 pozitív egészből kiválasztható számhármaskok összegét 10-zel elosztva rendre 3, 3, 3, 2, 1, 1, 1, 1, 2, 3 esetben kapunk 0, 1, ..., 9 maradékot.

A valódi feltétel és az elégségesség bizonyítása

A prímszám m -ekre kapott feltétel lényegibb általánosításának látszott, ha a maradékok nagyságviszonyára vonatkozó előírást nem csak az m prímszám osztóira kötjük ki, hanem az összes 1-nél nagyobb osztóra:

„Az m minden 1-nél nagyobb d osztójára adjon a k nagyobb maradékot d -vel osztva, mint az n , azaz legyen $k \pmod{d} > n \pmod{d}$.”

A vizsgált példán ez a $d = m = 10$ esetre nem teljesül, hiszen $3 \pmod{10} = 3 < 6 \pmod{10} = 6$.

Sikerült bebizonyítanom, hogy ez a feltétel elegendő, de azt akkor még nem, hogy valóban szükséges. A szükségeséget csupán arra az esetre tudtam visszavezetni, ha $n < m$; elég lett volna igazolni, hogy ha ilyenkor nem teljesül, akkor a játék nem igazságos. Ez csak több, mint fél év múlva sikerült.

Nyáron megbeszéltem Reiman tanár úrral, hogy előadom az addigi eredményeket az *Ifjúsági Matematikai Körben*. Szerencsére sikerült megtalálnom a hiányzó bizonyítást – két nappal (!) az előadás előtt. Ehhez a komplex számokat használtam fel, és később ezek segítségével új bizonyítást találtam arra, hogy a feltétel szükséges és elégséges. Ezeket a cikknek egy későbbi számban megjelenő második részében írom le.

És most következnek a feltétel elégségességének bizonyításai!

A továbbiakban azt a játékot, melynek során m játékos az első n pozitív egész közül véletlenszerűen kiválaszt k darabot ($k \leq n$), ezek összegét maradékosan elosztják m -mel, és a maradék dönti el a nyertes személyét, $J(m, n, k)$ -val fogom jelölni. (Az eredeti Kürschák-feladatbeli játék eszerint $J(2, 100, k)$.)

Megengedjük az olyan elfajuló játékokat is, amikor $m = 1$, vagy $k = 0$, esetleg $n = k = 0$. Az $m = 1$ esetben a játékot igazságosnak tekintjük.

ÁLLÍTÁS: A $J(m, n, k)$ játék igazságos, ha teljesül a következő

FELTÉTEL: Ha d az m -nek egy 1-nél nagyobb osztója, akkor k nagyobb maradékot ad d -vel osztva, mint n , azaz $k \pmod{d} > n \pmod{d}$.

A bizonyítást m – a játékosok száma – szerinti teljes indukcióval végezzük. Ha $m = 1$, akkor a játék igazságos, a feltétel pedig ekkor semmitmondó: mindig teljesül, mert az m -nek nincs 1-nél nagyobb osztója.

Legyen az m egy 1-nél nagyobb egész szám és tegyük fel, hogy az állítást már igazoltuk minden olyan $J(m', n', k')$ játékra, amikor $m' < m$. Most bebizonyítjuk, hogy ha a Feltétel teljesül a $J(m, n, k)$ játékra, akkor az igazságos.

Most is osszuk be az első n pozitív egészt $[n/m]$ darab m elemű és egy darab $n - m \cdot [n/m] = n_0$ elemű blokkra:

$$\{1, 2, \dots, m\}, \{m+1, \dots, 2m\}, \dots, \{[n/m]m - m + 1, \dots, [n/m]m\}, \\ \{[n/m]m + 1, [n/m]m + 2, \dots, n\}$$

Az m elemű blokkokat „teljes”, az utolsó, n_0 elemű pedig „csonka” blokknak nevezzük. Ha m osztója az n -nek, akkor a csonka blokk természetesen üres. A teljes blokkokat megszámozzuk: az i -edik teljes blokk az $im - m + 1, im - m + 2, \dots, im$ számokból áll.

Tekintsünk egy tetszőleges k -ast. Azt állítjuk, hogy ha a Feltétel teljesül, akkor található hozzá olyan teljes blokk, amellyel valódi metszete van, tehát nem üres és nem is az egész blokk.

Ha nincs ilyen blokk, akkor a kiszemelt k -as minden teljes blokkból 0 vagy m elemet tartalmaz és így

$$k \pmod{m} \leq n_0 = n \pmod{m}.$$

Ezt viszont a Feltétel kizárja ($d = m$).

Most is osztályokba rendezzük a k -asokat, mégpedig úgy, hogy egy adott k -as – hívjuk mintának – azokkal a k -asokkal legyen egy osztályban, amelyeket úgy kaphatunk, hogy a mintának – a legkisebb sorszámú teljes blokkban, legyen ez a b -edik – amelyből legalább egy elemet tartalmaz, de nem az összeset – levő elemeit elforgatjuk; – a magasabb sorszámú blokkokban lévő – tehát a bm -nél nagyobb – elemeit tetszés szerint megváltoztatjuk arra vigyázva, hogy bm -nél nagyobbak maradjanak.

Ha megmutatjuk, hogy bármelyik ilyen osztályban a k -asok összegét m -mel maradékosan elosztva a $0, 1, \dots, m-1$ maradékok mindegyikét ugyanannyiszor kapjuk meg, készen vagyunk: ugyanez igaz lesz az összes k -asra is.

Hívjuk egész számok egy véges H halmazát mod d *egyenletesnek*, ha minden, a H elemeit d -vel osztva fellépő maradék ugyanannyiszor fordul elő, és *teljesen egyenletesnek*, ha a $0, 1, \dots, d-1$ maradékok mindegyike ugyanannyiszor fordul elő. Ha pl. H minden eleme egyenlő és $d > 1$, akkor H egyenletes, de nem teljesen egyenletes mod d . Így azt kell megmutatnunk, hogy az egy osztályba eső k -asok összegeinek halmaza teljesen egyenletes mod m .

Tartalmazzon a minta T darab elemet a b -edik blokkból ($0 < T < m$), a b -nél nagyobb sorszámú blokkokban pedig legyen összesen k' eleme ($0 < k' < k$). Szükségünk lesz az m és a T legnagyobb közös osztójára – legyen ez q – és a relatív prím $p = T/q$ és $t = m/q$ mennyiségekre. Jelölje még n' a b -edik blokk utáni blokkok elemszámának összegét, azaz legyen $n' = n - bm$.

1988-04-149-1.eps

2. ábra

A minta bm -nél nagyobb k' darab elemét $\binom{n'}{k'} = S$ féleképpen rendezhetjük át, ezekben az elemek összegei legyenek $y_1, y_2, \dots, y_S$.

Mivel q osztója m -nek, ezért $n' \equiv n \pmod{q}$. Másfelől az első b darab blokk mindegyikében $0, m$ vagy T – azaz q -val osztható – a minta elemeinek száma, ezért $k' \equiv k \pmod{q}$. Így $n' \pmod{q} = n \pmod{q}$ és $k' \pmod{q} = k \pmod{q}$.

A minta osztályában a b -edik blokk utáni elemeken tulajdonképpen egy másik játék zajlik: itt n' szomszédos egész közül választunk ki minden lehetséges módon k' darabot. Azt állítjuk, hogy ez a játék q résztvevő között igazságos, azaz az $\{y_1, y_2, \dots, y_S\}$ halmaz teljesen egyenletes mod q .

Ehhez nyilván elég megmutatnunk hogy a $J(q, n', k')$ játék igazságos, ami viszont az indukciós feltevésből következik. Ez alkalmazható, mert $q \leq T < m$, másrészt a $J(q, n', k')$ játékra teljesül a Feltétel: ha d a q -nak 1-nél nagyobb osztója, akkor a $q|m$ miatt $d|m$, így a $J(m, n, k)$ játékra felírt Feltételből $k \pmod{d} > n \pmod{d}$. Másfelől $d|q$ -ből és $n \equiv n' \pmod{q}$ -ből

$$n \pmod{d} = n' \pmod{d}$$

és hasonlóan $k \equiv k' \pmod{q}$ -ből

$$k \pmod{d} = k' \pmod{d}$$

adódik, vagyis valóban

$$k' \pmod{d} > n' \pmod{d}$$

A játéknak a b -edik blokk utáni q személyes részére tehát valóban teljesül a feltétel, így az igazságos, és vegyük észre, hogy megszabadultunk a kellemetlen csonka bloktól.

Nézzük ezután az egy osztályba eső k -asoknak az első b blokkba eső részét. Ha a minta b -edik blokkbeli elemeinek r darab elforgatott képe van ($r \leq m$), akkor ezeket előállítják a $0, 1, 2, \dots, (r-1)$ mértékű forgatások. Azt állítjuk, hogy ekkor $p = T/(m, T)$ osztója r -nek.

Ha az i mértékű forgatás után a bm -nél nem nagyobb elemek összege x_i ($i = 0, 1, 2, \dots, r-1$), akkor az elforgatás tulajdonságai alapján

$$x_i \equiv x_0 + iT = x_0 + itq \pmod{m}.$$

Mivel pedig az r mértékű elforgatás eredeti állapotába viszi a b -edik blokkot, $x_0 \equiv x_0 + rtq \pmod{m}$, azaz $m = pq$ osztója rtq -nak, vagyis p osztója rt -nek. Mivel p és t relatív prímek, ezért valóban $p|r$.

Hogyan írhatjuk fel ezután egy, a mintával egy osztályban lévő k -as elemeinek az összegét? A bm -nél nem nagyobb elemek összege a b -edik blokk elforgatásai révén $x_0, x_1, \dots, x_{r-1}$ valamelyike, a bm -nél nagyobbak összege pedig $y_1, y_2, \dots, y_S$ valamelyike. A k -asok összegei tehát az $x_i + y_j$ ($i = 0, 1, \dots, r-1, j = 1, 2, \dots, S$) alakú összegek lesznek, mert teljesen függetlenül választhatjuk i -t és j -t.

Az állítást ezzel a következő segédtételezre vezettük vissza:

Egy segédétel

Ha $m = pq$, r, S, t pozitív egészek, p és t relatív prímek, p osztója r -nek, $x_0, x_1, \dots, x_{r-1}$ olyan egész számok, amelyekre $x_i \equiv x_0 + itq \pmod{m}$ – tehát valamennyien ugyanazt a maradékot adják q -val osztva – végül az

$\{y_1, y_2, \dots, y_S\}$ teljesen egyenletes mod q , akkor az $x_i + y_j$ ($i = 0, 1, \dots, r-1$; $j = 1, 2, \dots, S$) alakú összegek halmaza is teljesen egyenletes mod m

A segédétel csak első ránézésre tűnik ijesztőnek. Először is vegyük észre, hogy az $\{x_0, x_1, \dots, x_{r-1}\}$ halmaz is egyenletes mod m .

Tudjuk ugyanis, hogy $p|r$, osszuk be tehát az r darab x_i -t p elemű csoportokba:

$$(x_0, x_1, \dots, x_{p-1}), (x_p, x_{p+1}, \dots, x_{2p-1}), \dots (x_{r-p}, \dots, x_{r-1}),$$

Mivel $x_i \equiv x_0 + itq \pmod{m}$, $m = pq$, ezért az

$$x_i \equiv x_j \pmod{m}$$

feltételből a q -val való osztással

$$it \equiv jt \pmod{p}$$

adódik. Ez utóbbi pedig $(t, p) = 1$ miatt akkor és csak akkor igaz, ha $i \equiv j \pmod{p}$. Az egyes csoportokon belül így nincsenek egyenlő maradékok, ezek p -esével ismétlődnek, így minden fellépő maradék annyiszor fordul elő, ahány csoport van: r/p -szer.

1988-04-150-1.eps

Vegyük szemügyre ezután a táblázatot. Itt négy $\left(\frac{S}{q} \cdot \frac{r}{p}\right)$ darab teljes maradékrendszer elemei állnak mod 6 ($m = 6$). Ezeket úgy kapjuk, hogy az y -okból egy-egy teljes mod q maradékrendszer elemeihez – az $\{y_1, y_2, \dots, y_S\}$ halmaz $\frac{S}{q}$ darab ilyenre bontható – hozzáadjuk az m szerint különböző maradékot adó x -ek egy-egy p elemű csoportjának az elemeit – ilyen csoport r/p darab van.

Elég tehát belátnunk, hogy ha a q elemű Y halmaz teljes maradékrendszer mod q , a p elemű X halmaz elemei pedig valamennyien ugyanazt a maradékot adják q -val osztva, de m -mel osztva bármely kettő különböző maradékot ad, akkor az $x + y$ ($x \in X$, $y \in Y$) alakú összegek teljes maradékrendszert alkotnak mod m .

Mivel összesen $p \cdot q = m$ darab ilyen összeg van, ezért azt kell megmutatnunk, hogy semelyik kettő nem adhat ugyanolyan maradékot m -mel osztva.

Ez viszont nyilvánvaló, hisz ha

$$(*) \quad x' + y' \equiv x'' + y'' \pmod{m},$$

akkor $m = pq$ miatt a fenti kongruencia $\pmod{q}$ is fennáll, és mivel bármely két x ugyanazt a maradékot adja q -val osztva,

$$y' \equiv y'' \pmod{q},$$

ami csak úgy lehet, ha $y' = y''$, hiszen az y -ok teljes maradékrendszert alkottak mod q . Ekkor viszont $(*)$ -ből

$$y' \equiv y'' \pmod{m}$$

adódik, ami az x -ek kiválasztása miatt $\pmod{m}$ különböző maradékot adtak) csak az $x' = x''$ esetben lehetséges.

Ezzel a felhasznált segédételt bebizonyítottuk és így a Feltétel elégséges voltának bizonyítása teljes.

Kísérlet a megfordításra

Most visszavezetjük a Feltétel szükségességét arra az állításra, hogy ha $n < m$ esetén nem teljesül, akkor $J(m, n, k)$ nem igazságos (kivéve, ha $m = 1$).

Ideje kimondani egy apró segédételt, amit tulajdonképpen már ismerünk és a csapatokba rendezés módszerével be is bizonyítottunk:

Ha $J(m, n, k)$ igazságos és m' osztója m -nek, akkor $J(m', n, k)$ is igazságos.

Tegyük fel ezután, hogy a $J(m, n, k)$ játékra nem teljesül a Feltétel. Legyen m' az m legkisebb 1-nél nagyobb osztója, amely a feltételt elrontja, tehát amellyel osztva a k legfeljebb akkora maradékot ad, mint az n . A fenti segédétel alapján ekkor elég bebizonyítani, hogy $J(m', n, k)$ nem igazságos.

Az m' kiválasztása miatt ha $1 < d < m'$ és d osztója m' -nek (tehát m -nek is), akkor k a d -vel osztva már nagyobb maradékot ad, mint az n , ezért elég a következőt igazolni:

Ha az m minden d osztójára, amelyre $1 < d < m$, a k nagyobb maradékot ad d -vel osztva, mint az n , de az m -re ez már nem igaz, tehát $k \pmod{m} \leq n \pmod{m}$, akkor $J(m, n, k)$ nem igazságos.

Bontsuk fel az első n pozitív egészet m -elemű blokkokra úgy, mint az elégségeség bizonyításánál tettük és tekintsük azokat a szám k -asokat, amelyekhez találhatók olyan teljes blokkok, amelyekből legalább egy, de legfeljebb $m-1$ elemet tartalmaznak.

Az indukciós lépéshez teljesen hasonlóan kapjuk, hogy ezekben az elemek összegét m -mel osztva minden lehetséges maradék ugyanannyiszor fordul elő, így ezeken a játék igazságos.

A többi k -as ezután olyan, hogy minden teljes blokkból vagy az összes elemet tartalmazza, vagy egyet sem. Legyen egy ilyen k -asnak k_0 eleme az n_0 elemű csonka blokkban. Ekkor $k_0 \equiv k \pmod{m}$, mert $k - k_0$ osztható m -mel (a teljes blokkban lévő elemek száma), másrészt $k_0 \leq n_0 < m$, ami csak úgy lehet, hogy k_0 az a maradék, amelyet k ad m -mel osztva.

A fennmaradó k -asok tehát olyanok, hogy a teljes blokkok közül $[k/m]$ -et tartalmaznak, a csonka blokkból pedig k_0 elemet.

A teljes blokkban levő elemek összege m -mel osztva mindig ugyanannyi maradékot ad; legyen ez r .

Az ilyen k -asokon zajló játékot úgy is felfoghatjuk, mintha az csak a csonka blokkon belül folyna, innen kellene k_0 elemet kiválasztani. (Az eredeti játékban k_0 ilyen elem összegéhez még r -et hozzá kell adnunk és minden ilyen k_0 -ast $\binom{[n/m]}{[k/m]}$ -féleképpen ki kell egészíteniünk $[k/m]$ teljes blokkal, de ez a játék igazságos voltán nem változtat, $J(m, n, k)$ akkor és csak akkor igazságos, ha a „csonka blokkban” zajló $J(m, n_0, k_0)$ az.

Elég tehát $J(m, n_0, k_0)$ -ról bebizonyítani, hogy nem igazságos, ebben pedig valóban $n_0 < m$.

Ha $m = p^\alpha$, ahol p prím és α pozitív egész, akkor a bizonyítás könnyen befejezhető egy ismert számelméleti eredmény felhasználásával:

Ha $p^\alpha \mid \binom{n}{k}$, akkor $p^\alpha \leq n$.

Ha ugyanis ilyenkor $J(p^\alpha, n, k)$ igazságos, akkor az $\binom{n}{k}$ darab k -asban az elemek összegét p^α -val osztva minden maradék ugyanannyiszor fordul elő, így p^α osztója $\binom{n}{k}$ -nak. Mivel pedig ez nem teljesülhet, ha $n < p^\alpha$, ilyenkor $J(p^\alpha, n, k)$ valóban nem igazságos.

A módszer az általános esetben ezen a ponton ($n < m$) elakad: nem látni reményt, hogy tovább lehetne lépni vele. Jelenlegi alakjában is alkalmas viszont más számelméleti feladatok megoldására:

Egy következmény

Ha $n = \overline{n_S n_{S-1} \dots n_1 n_0}$ és $k = \overline{k_S k_{S-1} \dots k_1 k_0}$

egy p alapú számrendszerben felírva, ahol p prímszám, akkor

$$\binom{n}{k} \equiv \binom{n_0}{k_0} \binom{n_1}{k_1} \dots \binom{n_S}{k_S} \pmod{p},$$

ahol az $\binom{a}{b}$ binomiális együtthatóban megengedjük a $b > a$ esetet is; ilyenkor $\binom{a}{b} = 0$.

Az eredmény *Lucas lemma* néven ismert és messzemenő általánosítása annak az *F. 2597.* feladat megoldásában kimondott állításnak (KÖMAL 1987/3 108. o.), mely szerint $\binom{n}{k}$ akkor és csak akkor páratlan, ha az n -et és a k -t kettes számrendszerben felírva mindazokon a helyiértékeken, ahol a k -ban 1-es áll, az n -ben is 1 áll.

A bizonyításhoz nyilván elég megmutatni, hogy

$$\left(\frac{\overline{n_S n_{S-1} \dots n_1 n_0}}{\overline{k_S k_{S-1} \dots k_1 k_0}} \right) \equiv \left(\frac{\overline{n_S n_{S-1} \dots n_1}}{\overline{k_S k_{S-1} \dots k_1}} \right) \cdot \binom{n_0}{k_0} \pmod{p}.$$

Ha $k_0 > n_0$, akkor $J(p, n, k)$ igazságos és így $p \mid \binom{n}{k}$, valamint $\binom{n_0}{k_0} = 0$ miatt az állítás igaz. Ha $k_0 \leq n_0$, akkor $\binom{n}{k}$ kongruens modulo p azoknak a $J(p, n, k)$ -beli szám k -asoknak a számával, amelyek az $\overline{n_S n_{S-1} \dots n_1} = [n/p]$ teljes blokk közül $[k/p] = \overline{k_S k_{S-1} \dots k_1}$ darabot teljes egészében, az n_0 elemű csonka blokkból pedig k_0 darab elemet tartalmaznak. A többi k -asokon, mint láttuk, a játék igazságos, így azok száma osztható p -vel.

Az ilyen k -asok száma pedig éppen

$$\left(\frac{\overline{n_S n_{S-1} \dots n_1}}{\overline{k_S k_{S-1} \dots k_1}} \right) \cdot \binom{n_0}{k_0}.$$

Ezzel az állítást igazoltuk.