A cikk első részének végén (KÖMAL 1985. 4. szám 145–146. old.) Laci és Kálmán magukra maradtak azzal a problémával, hogy folytathatják-e kettesben a kártyapartit telefonon. Nos, a válasz tagadó, két játékos részére már nincs olyan osztási eljárás, amely rendelkezik mindazokkal a tulajdonságokkal, amelyeket természetes módon elvárnánk.

A bizonyításhoz gondoljuk át még egyszer ezeket a követelményeket. A leosztás végeztével mindkét játékosnak ismernie kell a saját lapjait, semmit sem tudhatnak viszont az ellenfél lapjáról. Az eljárásnak biztosítania kell, hogy kettejük lapjai különbözők legyenek, továbbá bármely leosztás egyformán valószínű legyen függetlenül attól, hogy éppen ki milyen lapot kapott. A parti végén a játékosoknak kölcsönösen meg kell tudniuk győződni arról, hogy ellenfelük valóban azokkal a lapokkal játszott, amelyeket az eljárás számára előírt, nem „húzott elő egy ászt a mellényzsebéből".

Tegyük fel, hogy mégis létezik kétszemélyes osztási eljárás. Ez valahogy úgy nézhet ki, hogy a két játékos előzetes megegyezés szerint feldolgozandó üzeneteket vált egymással egészen addig, amíg mindketten megtudják a saját lapjukat. Ha például éppen Lacin a sor, akkor újabb üzenetét – amelyről föltehető, hogy egy szám –, az addig váltott üzenetek, továbbá bizonyos számítások, illetve adott véletlen kísérletek kimenetele alapján készíti el. Ilyen kísérlet lehet például bizonyos számok véletlen sorbarendezése, egy halmaz néhány elemének véletlenszerű kiválasztása – gondoljunk csak az előző részben ismertetett négyszemélyes osztási eljárásra –, de akár egy érme feldobása is. A parti végén épp e kísérletek kimenetelét nyilvánosságra hozva kerülhet sor annak kölcsönös ellenőrzésére, hogy a felek betartották-e az előírásokat.

Képzeljük most el, hogy lezajlott a párbeszéd, Laci „megkapta" a lapjait, de nincs velük megelégedve –, mondjuk nagyon hiányzik neki a pikk ász. Vajon ki tudja-e cserélni valamelyik lapját a pikk ászra anélkül, hogy ezt Kálmán a játék végén lezajló ellenőrzéskor észrevenné ?

Nem egészen arról van szó, hogy a leosztás végeztével Laci esetleg többféle lap közül is válogathat: a lezajlott párbeszéd, a véletlen kísérletek ugyancsak adott kimenetelével együtt egyértelműen kell hogy meghatározza a Lacinak jutó lapokat. Elképzelhető viszont, hogy Laci, visszapergetve az eseményeket, talál a párbeszéd szüneteiben lezajlott véletlen kísérleteinek olyan, az eredetitől különböző kimenetelét, amelynek eredményeként ő egyrészt szóról szóra a valóban elhangzott üzeneteit közölheti Kálmánnal, másrészt az eljárás végén, az információk kiértékelése után a pikk ász kerül a kezébe. Ha így áll a dolog – amiről Laci talán csak csillagászati méretű számítások árán szerezhet tudomást –, akkor Kálmán az utólagos ellenőrzések során sem veheti észre a „cserét". Laci ugyanis ekkor a véletlen kísérleteknek számára kedvező kimenetelét fedheti fel; amennyiben ez is összhangban van az elhangzott párbeszéddel és Laci lapjaival, akkor Kálmánnak el kell fogadnia, hogy így történt a dolog.

Az a kisebbik baj, hogy így földeríthetetlen visszaélésre nyílhat alkalom – hisz megeshet; hogy Laci csak lapjait gyengítve tudja az elhangzott párbeszéddel összhangban „megváltoztatni" a leosztást; ami nyilván nem érdeke. Sokkal komolyabb gond a következő: ha az eljárás garantálja, hogy a két fél kezébe különböző lapok kerülnek, akkor eredeti lapjaival a kezében Laci a fenti vizsgálatokat *jóhiszeműen* elvégezve is megtudja, hogy egy lap, ami nincs a kezében, *Kálmánnál sem lehet:* lehetséges lett volna ugyanis, hogy az eljárás keretein belül ugyanilyen üzenetváltás mellett nála, Lacinál legyen a pikk ász.

Ha tehát vannak olyan lapok – és ha vannak, akkor Laci, ha nem is egykönnyen, de meg tudja határozni ezeket –, amelyek az éppen neki kiosztottakon kívül is hozzá kerülhettek volna, miközben a kettejük közti párbeszéd ugyanaz marad, akkor ezek nem kerülhettek Kálmánhoz sem. Miután pedig az ilyen lapokra Laci rátalálhat, jogosulatlan információhoz jut !

Az eljárásnak tehát mindenképp ki kell zárnia ezt a lehetőséget. Más szóval: csak egyetlen olyan leosztás létezhet, amely összhangban van az elhangzott párbeszéddel, annak ellenére, hogy a lefolytatott véletlen kísérleteknek esetleg több különböző kimenetele is eredményezheti ugyanazt a párbeszédet, és ezen keresztül persze ugyanazt a leosztást.

Most azonban ugyancsak baj van: Laci tudja, hogy mindez Kálmán lapjaira is igaz. Mivel ismeri az elhangzott párbeszédet, rendre próbát tehet Kálmán véletlen kísérleteinek minden egyes kimenetelével. Ezekből csak véges sok van – bár lehet, hogy nagyon sok –, olyan viszont feltétlenül van köztük, amely összhangban van az elhangzott párbeszéddel: az, amelyik valójában bekövetkezett. Így ha Laci egy másik ilyet talál – az egész csak türelem kérdése –, akkor biztos lehet abban, hogy csak azok a lapok lehetnek Kálmán kezében, amelyeket e kimenetelek és a párbeszéd alapján az osztási eljárás utasításai szerint most már ő is ki tud számolni. Láttuk ugyanis, hogy ha az osztási eljárás igazságos, akkor egy adott párbeszéd bármely vele összhangban lezajlott kísérletsorozattal együtt ugyanazt a leosztást határozza meg.

Laci tehát megtudhatja, milyen lapok vannak Kálmán kezében és ugyanez, fordítva is igaz – így viszont nem érdemes kártyázni.

Az említett módszeres próbálgatás természetesen csak elvben teszi lehetővé, hogy a felek valóban megismerjék egymás lapjait. A bizonyításhoz ennyi elég, a valóságban viszont megtörténhet, hogy ezek a számítások még a ma létező leggyorsabb számológépekkel is évmilliókig tarthatnak, ami gyakorlati szempontból tökéletesen kielégítő garancia. Többek között az ilyen méretű számítási feladatok gyakorlati kivihetetlensége az alapja az utóbbi években a figyelem előterébe került, úgynevezett nyilvános kulcsú titkosírási módszereknek is. Ha elfogadjuk ilyen titkosírás létezését, akkor már két résztvevő esetén is megadható megfelelő osztási eljárás.

A szemléletesség kedvéért képzeljük úgy, hogy az egyes lapok kódolása a következőképpen valósul meg: betesszük őket egy-egy dobozba, amelyekre ezután olyan lakat kerül, amelyet kizárólag az tud kinyitni, aki rátette – azaz, a kódot csak a kód tulajdonosa tudja megfejteni. Egy dobozon több lakat is lehet, azaz a kódolt üzenetek továbbkódolhatók.

Az osztási eljárás ezután a következő. Laci véletlen sorrendben beteszi a 32 kártyát 32 dobozba, minden dobozt lelakatol, majd elküldi őket Kálmánnak – azaz megtelefonálja neki a kódolt lapokat. Kálmán véletlenszerűen kiválaszt öt dobozt, amelyeket visszaküld; ezekben vannak Laci lapjai, aki természetesen hozzájuk tud férni. Kálmán egy kicsit küzdelmesebben jut a lapjaihoz. A nála maradt dobozok közül kiválaszt ötöt, ezeket ő is lelakatolja és az öt, duplán lelakatolt dobozt elküldi Lacinak, aki leveszi róluk a *saját* lakatjait, majd visszaküldi a dobozokat. Ezeket így már csak Kálmán lakatjai zárják, aki kinyitva őket, kézbe veheti a lapjait.

A történetben szereplő lakatok – illetve kódok – itteni alkalmazása azon múlik, hogy használatuk sorrendje felcserélhető, a két lakat nem ugyanabban a sorrendben kerül le a dobozokról, mint ahogyan rákerültek. Ilyen tulajdonságú kódokról olvashatunk [3]-ban, illetve [4]-ben.

Ami a feleségek életkorának sorrendjét illeti, előrebocsátjuk, hogy a megoldás nem felel meg minden tekintetben az elvárásoknak: szükség van ugyanis a lehetséges életkorok egy felső korlátjára, azaz egy olyan értékre, amelynél egyetlen résztvevő sem lehet idősebb. A sorrenden túl ehhez az értékhez is mindenki hozzájut majd, ezt nem tudjuk megakadályozni. Ha ezt a számot a résztvevők jó nagynak választják, – például 100-nak –, akkor ugyan mindegyikükről kiderül, hogy legfeljebb 100 éves lehet, de ez talán nem túl bizalmas információ.

A korábbiakhoz hasonlóan most is szükség lesz a szóba jöhető életkorok – az első 100 darab pozitív egész – kódolásaira, továbbá az egyes kódok közötti bizonyos szótárakra. Valakinek ezen kívül össze kell tudnia hasonlítani az egyes életkorokat – a lényeg most is az, hogy ezt az összehasonlítandó értékek érthetetlen kódjai alapján is megtehesse.

Készítse el Anna – az egyik feleség – az 1-től 100-ig terjedő számok egy-egy véletlen permutációját – azaz a lehetséges élétkorok egy-egy kódolását – mind a négyük számára. Jelölje Anna saját kódját $\alpha(i)$ $i = 1,\ 2,\ \ldots,\ 100$. Ez a kód hasonló szerepet játszik, mint az első cikkben a kínai nyelv.

Gondolja végig az olvasó, hogy ezután alkalmas szótárak felhasználásával, melyeket ugyancsak Anna készít el és oszt szét, a négyszemélyes kártyaosztáshoz hasonlóan elérhető, hogy valaki más – például Bea – mind a négyük életkorának megtudakolhassa az α-kódját anélkül, hogy eközben bárki többlet-információhoz jutna.

Bea tehát ismeri az $\alpha(A)$, $\alpha(B)$, $\alpha(C)$ és az $\alpha(D)$ értékeket – a másik két feleség neve Cili és Dóra –, tudja, hogy melyik szám kinek az életkorát kódolja, de a sajátján kívül egyiknek sem ismeri a jelentését. (Föltehető, hogy a négy érték között nincsenek egyenlők.)

Az életkorok összehasonlítását Bea végzi majd el anélkül, hogy eközben megismerné a kódok jelentését. A nagyságviszonyokat nyilván nem kérdezheti meg közvetlenül Annától, de egy közvetítő segítségével már megtudhatja mindazt, amire szüksége van. Annának ehhez el kell készítenie az összes $\big(\alpha(i),\ \alpha(j),\ \alpha(k),\ \alpha(l)\big)$ számnégyesek listáját – ez összesen $\binom{100}{4}$ számnégyes –, minden egyes esetben pénzfeldobással döntve el, hogy a négy számot milyen sorrendben írja föl. Ezt a listát közli Beával, majd ugyanabban a sorrendben, ahogyan ezeket a számnégyeseket felsorolta, rendre elmondja Cilinek, hogy mi az egyes számnégyesek által kódolt négy érték valódi nagyságviszonya. Tehát például azt, hogy az 587-ik négyesben a legnagyobb szám kódja a második, a második legnagyobb számé a negyedik, a harmadik legnagyobb számé az első, végül a legkisebb szám kódja a harmadik helyen áll stb.

A kapott listán most már Bea megkeresheti azt a négyest, amelyik éppen az általa ismert $\alpha(A)$, $\alpha(B)$, $\alpha(C)$ és $\alpha(D)$ értékeket tartalmazza valamilyen sorrendben. E négyes sorszáma alapján megtudakolhatja Cilitől a valódi nagyságviszonyokat és kihirdetheti az életkorok sorrendjét.

Befejezésül az olvasóra hagyjuk annak átgondolását, hogy ez a feladat sem oldható meg akkor, ha csak két hiú feleség szeretné tisztázni, melyikük az idősebb. Megemlítünk ezenkívül még két változatot a fenti témára. Az egyik: $n \geq 3$ résztvevő mindegyike gondol egy 1 és 100 közé eső természetes számra. Mindegyikük szeretné megtudni, hogy az ő száma nagyság szerint hányadik az n darab szám közül, de azt akarják, hogy ennél többet senki se tudjon meg. A másik: $n \geq 3$ résztvevő titkos szavazással szeretne eldönteni egy vitás kérdést telefonon.

Ami a bevezetőben említett hiányt illeti, érdekes volna egy olyan eljárás, amelynek során a résztvevők nem ismernek korlátot a sorba rendezendő számokra.

Irodalom

[1] *Bárány Imre–Füredi Zoltán:* How to play Mental Poker?

[2] *A. Shamir–R. Rivest–L. Adleman:* Mental Poker. *The Mathematical Gardner.*

[3] *Babai László:* Prímszámok és titkosírás. *A Természet Világa,* 1981/6.

[4] *Lovász László:* Számítógépek, algoritmus, matematika. KÖMAL, 1982/3.

[5] *A. Yao:* Protocols for Secure Computations.