A BONYOLULTTÓL AZ EGYSZERÛ FELÉ (A MATEMATIKÁBAN)

Katona Gyula
az MTA rendes tagja, intézetigazgató,
MTA Rényi Alfréd Matematikai Kutató Intézet – ohkatona@renyi.hu

Kedvesem! Hogy mondjam el Neked,
mit érzek, ha Rád gondolok?
A tenger millió apró szélcsendes recéje,
vihargó, dübörgõ, romboló hullámai
mind végigsuhannak lelkemen.
A virágzó rét szépsége,
a sötét erdõ rejtelmei,
az égbe ugró sziklák izgalmai,
érzelmeim tobzódásának
csak piciny részét tükrözik.
Szemedbe nézve egy csillag mögül
millió másik bukkan elõ,
elmondhatatlan, kimondhatatlan,
csak annyit súgok helyettük:
Szeretlek! Talán megérted...

Ismeretlen költõ,
lengyelbõl fordította Zsolnyezs Gyula

Az emberi gondolkodás talán legfontosabb vonulata a bonyolult felől az egyszerű felé törekszik. Pici unokám a cica után fut, és azt mondja: *Vau, vau*. Megalkotta a „négylábú emlősállat” fogalmát. Lehetetlen lenne felsorolni, elnevezni a rengeteg idetartozó állatfajt, annak különböző színű, méretű egyedeit. A bonyolult, valódi helyzetet leegyszerűsítette *vau*ra. Az absztrakció tehát általában lépés a bonyolulttól az egyszerű felé.

Az absztrakció egy következő, magasabb foka, amikor unokám rájön (neki ez már csak néhány év), hogy a vauk, autók és hasonlók halmazainak van egy-egy közös tulajdonságuk, hogy mennyi elemből állnak. Az új fogalmak az *egy, kettõ, három, …*, a természetes egész számok, és máris ott vagyunk a matematikánál.

A természettudós – amikor modellt alkot – hasonló utat követ. A természeti jelenség bonyolultságából próbálja kivenni a lényeget, ami már egyszerű, leírható, elmondható. Ha egy tárgy leesik, az bizony pörög, a légellenállás, sőt légörvények befolyásolják esését. Nagyon bonyolultakat csinál. A fizikus egyszerűsít, amikor elképzeli, hogy mindez légüres térben történik, konstans gravitációval. Természetesen az igazán hasznos modell a matematikai, amikor a modellben számolni is lehet, azaz egy további egyszerűsítés történik – a rendkívül bonyolult valóságot számokkal, függvényekkel írjuk le.

Miután megérkeztünk a matematikához, vizsgáljuk meg az egyszerűség-bonyolultság kérdését a matematikán belül. Még ott is gyakran lejátszódik a fenti példákban leírt absztrakció, ami a bonyolulttól az egyszerű felé megy. Ha például azt nézzük, hogy mi a közös a számok összeadásában, összeszorzásában, a geometriai transzformációk egymás utáni alkalmazásaiban és sok más hasonló jelenségben, akkor eljutunk az absztrakt *mûvelet* fogalmához; ha még azt is megfigyeljük, hogy a fenti fontos példákban a műveletek milyen tulajdonságokat elégítenek ki, akkor megkapjuk a *csoport* fogalmát. A csoport tehát egy végtelenül leegyszerűsített közös általánosítása nagyon sok matematikai jelenségnek.

Egy matematikai elméleten belül a tételek játsszák a „egyszerű"' szerepét. Egy szép mondás szerint (sajnos nem tudom, kitől származik, én Makkai Mihálytól, az MTA külső tagjától hallottam) egy matematikai elmélet olyan, mint egy kirándulóterület, amin a tételek játsszák a kilátók szerepét. Vagyis a többnyire rettentően bonyolult elméletben a tételek azok az egyszerűen megfogalmazható állítások, amelyek, valahogyan, az elmélet lényegét fejezik ki. A bizonyítások a kilátók közötti fáradságos utak. Egy tételt akkor nevez egy matematikus szépnek, ha a feltételei és az állításai nagyon egyszerűen megfogalmazhatók, de egyáltalán nem nyilvánvaló, hogy igaz. Tehát a bizonyítása nehéz, hosszadalmas. Erre jó példa a négyszíntétel.

A négyszíntétel a gráfelmélet egyik tétele, de most eredeti formájában ismertetem. Egy (síkon lévő) térkép országait szeretnénk kiszínezni úgy, hogy a közös határszakasszal bíró országok különböző színűek legyenek. Ezt az igazán egyszerűen megfogalmazható állítást több mint száz évig nem tudták bebizonyítani, csak 1976-ban sikerült Kenneth Appelnek és Wolfgang Hakennek számítógépek intenzív használatával (két hónap futási idő!).

De egy bonyolult bizonyítás is lehet szép, ha vannak benne meglepő, váratlan egyszerűsítések. A matematikusok egy részének az a véleménye, hogy a szép tételek bonyolult bizonyításai a jövőben egyre gyakrabban olyan bonyolultak lesznek, hogy csak számítógép segítségével végezhetők el, mint az a négyszíntétel esetén is történt. (Figyelem: a bizonyítást nem a számítógép találta ki!) A matematikusok másik részének ez egy rémálom.

A szép tételek esztétikai élményt nyújtanak a hozzáértőnek, mert meglepőek, akárcsak egy jó vicc csattanója. De a meglepő az, hogy a szép tételek rendszerint nagyon hasznosak is. Az egyszerű feltételek ugyanis könnyebben teljesülnek egy véletlen szituációban. Nagy a valószínűsége annak, hogy (a matematikán belül vagy külső alkalmazásnál) előfordul egy olyan helyzet, ahol a szép tétel feltételei teljesülnek. Ezért van az, hogy a matematikus, amikor szépérzékére hagyatkozva, csupán azért keres és bizonyít tételeket, mert azok szépek (egyszerűek!), akkor hallatlan hasznos tevékenységet végez. Előbb vagy utóbb mások majd találnak olyan helyzeteket, ahol a tétel használható is. E sorok írója például még a 60-as évek közepén észrevette, hogy adott számú (mondjuk 1000) ***k*** elemű (mondjuk 7-elemű) halmazban lévő ***k-1*** elemű részhalmazok (tehát 6 elemű részhalmazok) száma akkor minimális, ha a halmazokat minél kisebb halmaz részhalmazaiként választjuk. A cél akkor csak egy szép matematikai tétel megtalálása volt. Azóta rengeteg alkalmazását találták, csak egy példa a sok közül: a nagyfeszültségű távvezeték-hálózat megbízhatóságának meghatározásában. Erdős Pál munkássága ilyen példák seregét adja.

A fentieket egy kicsit más nézőpontból úgy is meg lehet fogalmazni, hogy a matematika a bonyolultban keresi az egyszerűt, a szabályosat. Erre talán a legjobb példa a valószínűségszámítás. Ha egy dobókockával sokszor dobunk, és felírjuk az eredményeket, egy nagyon szabálytalan sorozatot kapunk. A matematika mégis talál ebben a szabálytalanban valami egyszerűt, szabályosat. Például a ***nagy számok törvénye*** szerint a kapott számok átlaga majdnem mindig közel lesz 3,5-hez (persze itt pontosan meg kell mondani, mi az, hogy „majdnem mindig", és mi az, hogy „közel"). De ennél többet is lehet találni. Ha száz dobás összegét vesszük, akkor – az előzőek szerint – ezek összege körülbelül 350 lesz, de úgy, hogy a legtöbb összeg – mondjuk – 330 és 370 között lesz, 310 és 330 között már lényegesen kevesebb van, mint 330 és 350 között, 290 és 310 között még kevesebb, és így tovább, a 90-nél kisebb összeg már nagyon kevés. Egy harang

alakú görbéhez jutunk. Ha 100 helyett egyre nagyobb tagú összegeket véve, egyre pontosabb közelítését kapjuk (persze egyre jobban elnyújtva) egy ún. „harang-görbének". Ezt úgy mondjuk, hogy a nagyszámú, független, egyforma, véletlen szám összege a „normális eloszláshoz" tart. Ez az egyszerű szabály az oka annak, hogy a természetben nagyon sok véletlen szám éppen ezt az eloszlást követi. Ebben a sorban a mai legerősebb szabályosságot Komlós János, Major Péter és Tusnády Gábor egy tétele írja le.

Most egy kissé hihetetlen „egyszerű szabály" következik, amit nagyon pongyolán így írhatunk le: nemcsak a véletlenben, hanem az akármilyenben is van szabályosság. Mégpedig a gráfokban. Egy gráf pontokból és élekből áll. Például az ország minden emberét egy-egy ponttal ábrázoljuk, és két ilyen pontot összekötünk egy vonallal (ún. éllel), ha azok kölcsönösen ismerik egymást. Szemerédi Endre híres tétele szerint, ha a gráf pontjainak száma elég nagy, akkor a pontokat össze lehet rendezni viszonylag kisszámú kupacba úgy, hogy a kupacok legtöbb párja között az élek úgy mennek, mintha a gráf véletlen lenne, tehát – valamilyen értelemben – szabályos.

No, persze azért a matematikusok sem értenek mindig mindenben egyet, abban sem, hogy mi az egyszerű és mi a szép. Nem csak a szépérzéktől függ, hanem a tudástól, az ismeretanyagtól is. Ha valaki nem otthonos egy témakörben, nem ismeri a tételeit, akkor annak nem lehet abban a témakörben szép tételt mondani, mint ahogy az őserdei indián se érti a szőke nős viccet.

Nem szeretném félrevezetni az olvasót prekoncepcióimmal. Be kell vallanom, hogy vannak olyan matematikai eredmények, amelyek, mintha az egyszerűtől vezetnének a bonyolult felé. Ilyen példa a Takashi-függvény: állítsunk a *[0,1]* intervallumra egy egyenlő oldalú háromszöget, ez legyen az első függvény. A második legyen két egyenlő oldalú háromszög, a *[0, 1/2]* illetve az *[1/2,1]* intervallumra állítva. A harmadik függvény már álljon négy kis háromszögből. Ezt folytatva, és a kapott végtelen sok függvényt összeadva egy nagyon bonyolult függvényt kapunk, ami például folytonos, de sehol sem differenciálható. Általában a fraktálok ilyenek: egyszerű konstrukcióval valami bonyolultat kapunk. De ilyen az álvéletlen számok konstrukciója is. „Véletlen" számokat kell konstruálnunk egy számítógépes algoritmussal. Ez nyilván valami szabályosat kell hogy adjon, mégis olyan bonyolultnak néz ki, mintha véletlen volna.

Mielőtt továbbmennénk, meg kell említenünk a matematika alkalmazásának legnagyobb problémáját, ami szintén összefüggésben van a bonyolultsággal-egyszerűséggel. Az alkalmazás rendszerint egy szép észrevétellel kezdődik. A valóság egy darabjára egyszerű matematikai modellt találtunk: a Föld gömb alakú! Alaposabb vizsgálat után kiderül, hogy ez nem egészen igaz. Mivel a Föld forog a tengelye körül, és viszonylag puha, a centrifugális erő kinyomja az egyenlítőnél, a sarkoknál viszont belapul. A ható erőket figyelembe véve szépen kiszámolható a Föld alakja. A matematikus boldog, mert – bár a dolog nem olyan egyszerű – viszonylag egyszerűen sikerült meghatározni az alakot. De az alaposabb vizsgálat azt mutatja, hogy ez a modell sem tökéletes, mert a Föld anyaga nem homogén. Ha ezt is figyelembe akarjuk venni, akkor ismernünk kell a tömegeloszlást, és jó közelítéssel, rengeteg adattal fel is kell használnunk. A számítások csak számítógéppel végezhetők el, az eredmény sem lesz teljesen pontos, csak az adatok pontosságának megfelelően. Elveszett az egyszerűség, a szépség. De mégis meg kell csinálni! A matematikai alkalmazások túlnyomó többségénél fellép ez jelenség.

Az utóbbi két-három évtizedben lett centrális kérdés a számítások, algoritmusok bonyolultsága. A matematika ókori kezdetei-

től voltak algoritmusok, hiszen a többjegyű számok szorzására az iskolában tanult módszer is egy kis algoritmus. De a múltban az algoritmusok egyszerűek, normális időben befejezhetők voltak. Vagy – mint a matematikai analízis algoritmusai esetében – ha kevés ideig számoltunk, az eredmény pontatlan volt, ha sokáig, egyre pontosabb. Az elektronikus számítógépek belépésével és a nagy tömegű véges matematikai feladat megjelenésével egy új jelenség lépett fel. Addig valahogy úgy érezte mindenki, hogy egy véges, sok adattal megadott feladat a gyors számítógépekkel mindig megoldható, csak elég sokáig kell számolni. Ezzel szemben a gyakorlatban is kiderült az a nyilvánvaló tény, hogy ha az algoritmus lépésszáma a bemenő adatok exponenciális függvénye, akkor elég sok bemenő adat esetén emberi mértékű idő alatt a leggyorsabb számítógép sem képes a feladat elvégzésére. Ha n bemenő adatból az algoritmus például $1000n$ lépés alatt befejezi a számolást, az nagyon gyors. Ha konstansszor n^2 vagy n^3 lépés kell, az még mindig rendkívül jó. Ismertek olyan algoritmusok, amelyek n^7 lépést igényelnek. Ezek még mindig nagy reménnyel elvégezhetők nagy n esetén is. Ezeket hívjuk polinomiális algoritmusoknak. A lényeges változás 2^n-nél következik be, ennyi lépést nagy n esetén nem lehet elvégezni. Az ilyen algoritmust exponenciálisnak nevezzük.

A számítási feladatok többnyire polinomiális sok lépésben visszavezethetők olyan feladatokra, amelyek eredménye „igen-nem". Például ilyen a Hamilton-kör feladata: adott gráfról el kell dönteni, hogy az éleket használva, pont egyszer végig lehet-e menni az összes ponton, a végén visszaérve a kezdőpontba. Ha az utat valaki megsúgja, akkor könnyen ellenőrizhető, hogy az Hamilton-kör-e. A legtöbb ismert és fontos probléma ilyen, hogy ha ismertjük az eredményt, akkor arról polinomiális sok lépésben eldönthető, hogy megfelel-e a feltételeknek. Az ilyen problémákat NP-belieknek nevezzük. Ezek között sok olyan van, amit polinomiális algoritmussal meg tudunk oldani. A problémák ezen osztályát P-vel jelöljük. Tehát P része NP-nek. Máig eldöntetlen, hogy vannak-e NP-nek olyan elemei, amelyek nincsenek P-ben. Ez a híres „P=NP?" probléma. Persze a matematikusok túlnyomó többsége úgy hiszi, hogy nem egyenlő a két osztály. (Jelen cikk írása közben jött egy még távolról sem ellenőrzött híresztelés, hogy egy japán matematikus bebizonyította, hogy valóban nem egyenlőek. A korábbi hasonló híresztelések nem voltak megalapozottak.) Az viszont bizonyított, hogy ha például a Hamilton-kör problémájára csak exponenciális algoritmus van, akkor több tízezer más NP-belire is csak exponenciális létezik. (Ezeket a problémákat NP-nehéznek nevezzük.) Ez azt jelenti, hogy rengeteg probléma esetén nincs remény használható algoritmus készítésére.

A „P=NP?" probléma nem csak a számítások bonyolultságánál fontos. Ha egy matematikai állítás teljesülésére jól meghatározott szükséges és elégséges feltételt találunk, az többnyire egy polinomiális algoritmushoz is vezet az állítás eldöntésére. Ha tehát P≠NP, és sikerül bebizonyítani, hogy az állítás ellenőrzése NP-nehéz, akkor ezzel beláttuk, hogy reménytelen az állítást egy jó, szükséges és elégséges feltétellel jellemezni. Tehát a „P=NP?" probléma nem csak a számítástudomány, de a matematika egyik legfontosabb problémája.

Mit tehetünk, ha egy NP-nehéz problémát kell megoldanunk? A pontos helyett végezhetünk közelítő számítást. De – sajnos – sokszor a jó közelítés is NP-nehéz. A másik út: új típusú számítógépek kitalálása. Az ún. kvantumszámítógépek vagy a kémiai/biológiai számítógépek alapötlete már létezik, technikai megvalósításuk még (?) nem. Mindkettő azon az alapötleten működne, hogy a molekuláris vagy fotonos méretű részecskékből egyszerre olyan mennyiség számol,

hogy azt a mi számításaink szempontjából exponenciálisnak lehet tekinteni, vagyis „egy lépés” alatt gyakorlatilag „exponenciális sok” lépést lehet elvégezni. Ha sikerül ezeket a számítógépeket a gyakorlatban megvalósítani, akkor egy nagyon nagy lépést teszünk előre a számítási lehetőségek kibővítésére, de sok nagyságrend után ugyanazzal a problémával fogjuk magunkat szembetalálni. Egy másik, kísérletek alatt álló út: speciális problémákra speciális (esetleg analóg) gépeket kidolgozni. Ezzel a számítógépek univerzalitása tűnik el. Végül is a „P=NP?” probléma matematikai jelentősége sem változik az új számítógépek esetleges megjelenésével.

Van a matematikának, illetve alkalmazásának egy olyan területe, ahol a bonyolultság a cél. A kriptográfia. Üzenetet küldünk valakinek, és azt akarjuk, hogy csak a címzett tudja elolvasni, más semmi esetre sem. A címzettnek egy „kulcs” van a birtokában. Tehát az üzenetet egy olyan módon kell kódolni, hogy a visszakódolási algoritmus NP-nehéz legyen (ami nagy valószínűséggel exponenciális sok lépést igényel, tehát hosszabb üzenet esetén gyakorlatilag megoldhatatlan), így illetéktelen nem tudja dekódolni, de az, akinek az üzenetet szántuk, olyan plusz információ birtokában van, amelynek segítségével már polinomiális időben képes az üzenet dekódolására. A jelenleg alkalmazott leggyakoribb módszer azon alapszik, hogy egy nagy (például sok ezer számjegyből álló) egész szám prímszámok szorzatára való bontására nem ismeretes polinomiális algoritmus. Tehát a kódolás olyan, hogy ezt az egész számot ügyesen használja, de a dekódolás csak akkor egyszerű, ha a prímfelbontás ismert. Vagyis csak annak mondjuk meg a felbontást, akinek az üzenetet szánjuk. Ezzel az eljárással van egy kis baj: nem bizonyított, hogy a prímfelbontás elkészítése NP-nehéz. Tehát előfordulhat, hogy (annak ellenére, hogy P≠NP) valaki talál egy polinomiális felbontó algoritmust, és akkor a kódoló egész szám ismeretében mindenki el tudja olvasni a titkos üzeneteket.

Nagyon remélem, hogy a fejemben a bonyolultságról szóló gondolatokat sikerült oly módon kódolni e kis írásban, hogy az olvasó polinomiális időben képes azokat saját számára dekódolni.

Kulcsszavak: *matematika, alkalmazás, bonyolultság, gráf, véletlen, absztrakció, modell, számítás, kriptográfia*