(1. közlemény)

A múlt század közepe táján kezd Magyarországon rendszeres kutatómunka kialakulni, és ennek nyomán hamarosan szervezett matematikai élet: társulat, folyóirat, stb. alakul. Ennek egyik vezető személyisége volt Rados Gusztáv, akinek tevékenységével ma ifjú olvasóinkat megismertetjük. Lényeges része volt a Matematikai és Physikai Társulat megalapításában, folyóiratának a Mathematikai és Physikai Lapok matematikai részének kezdettől fogva 23 éven át szerkesztője volt. Azután a Társulat alelnöke, majd elnöke lett. Kora ifjúsága – 1894 – óta a Magyar Tudományos Akadémiának levelező, később nagy tekintélyű rendes, majd tiszteleti tagja lett. A kolozsvári egyetem tiszteletbeli doktorává avatta. Nem volt a matematikai életnek olyan mozgalma, amelyben – legtöbbször mint kezdeményező – részt ne vett volna. Az 1894-ben megindított évi Eötvös Loránd matematikai versenyek (a jelenlegi Kürschák József versenyek elődjei) bizottságának kezdettől fogva tagja (1913-tól kezdve elnöke) 1939-ig.

Rados Gusztáv, mint a múlt század hetvenes–nyolcvanas éveinek majdnem minden magyar matematikusa, tanulmányait a Műegyetemen végezte. Nem csoda, hiszen a Műegyetemen a matematikát oly nagyszerű matematikusok tanították, mint Hunyady Jenő és Kőnig Gyula, akik minden tehetséget magukhoz vonzottak. Itt hamar feltűnt tehetségével és szorgalmával úgy, hogy tanulmányai végeztével a Műegyetemen maradt, ahol igen hamar (1885-ben) magántanár, majd, Hunyadi Jenő korai halála után, 1891-ben rendkívüli, 1893-ban pedig rendes tanár lett, és nyugdíjazásáig ott is maradt. A Műegyetem tanári testülete tehát Rados Gusztávval, majd néhány év múlva Réthy Mórral, Kürschák Józsefel és Bauer Mihálylyal egészült ki, így tehát továbbra is a magyar matematika centruma maradt.

Rados Gusztáv munkássága – amint ez modern matematikusnál szinte magától értetődő – főleg a felsőbb matematikába tartozik, de azért megkísérlem őt röviden jellemezni, sőt néhány elemibb eredményét ismertetni. Munkásságának legnagyobb része az algebra és számelmélet területére esik, még geometriai eredményei is többnyire ilyen vonatkozásúak.

Az *algebra* szón az iskolai matematika egyszerűen a betűszámtant érti. A tudományban hosszú ideig az

$$a_0x^n + a_1x^{n-1} + \ldots + a_n = 0 \tag{1}$$

alakú egyenletek (az a együtthatók adott számok, x az ismeretlen), az úgynevezett algebrai egyenletek vizsgálatát értették. Ezt ma „funkcionális algebrá”-nak is szokták nevezni, és kétségtelenül a legszebb matematikai diszciplinák közé tartozik, amelyből több magyar matematikus is kivette a részét. Az algebra újabb fejlődése egészen új problémaköröket vetett fel a műveletek tulajdonságainak vizsgálatával és általánosításával kapcsolatban. Az ilyen irányú rendszeres vizsgálatok megindulásában különösen Emmy Nöther, hírneves matematikusnőnek volt nagy szerepe, és továbbfejlesztésében ma mindhárom egyetemünkön számos magyar matematikus is jelentős részt vesz.

Hogy a funkcionális algebra körébe vágó kérdések sokféleségéről is képet adjunk, néhány eredményt bizonyítás nélkül megemlítünk. IV. osztályosok tanulják, hogyan lehet, ha az (1) egyenlet a_i együtthatói egészek, az egyenlet racionális gyökeit megkeresni. Ezek csak olyan törtek lehetnek, amelyeknek számlálója a_n-nek, nevezője pedig a_0-nak osztója.

Először Gaussnak sikerült 21 éves korában, 1798-ban bebizonyítania, a következő tételt, melyet az algebra alaptételének szokás nevezni, és amelyet már évszázadok óta igaznak hittek a matematikusok: *a komplex számok körében minden algebrai egyenletnek van gyöke.* Ebből a gyöktényezők leválasztása segítségével már könnyen következik, hogy a többszörös gyököket megfelelően számítva, *minden egyenletnek annyi gyöke van, ahányad fokú.*

A gyökök megkeresését megkönnyítik a gyökök nagyságára korlátot adó tételek. Egy egyszerű ilyen tétel a következő:

Ha az a_i-k az (1) egyenlet együtthatói, és legyen az

$$\frac{a_1}{a_0}, \quad \frac{a_2}{a_0}, \quad \ldots, \quad \frac{a_n}{a_0}$$

számok abszolút értékei között előforduló legnagyobb érték M, ekkor az (1) egyenlet bármely gyökének abszolút értéke kisebb az

$$M + 1$$

értéknél.

A funkcionális algebra legrégibb (1637-ből származó) tételei közé tartozik a „Descartes jelszabálya” néven ismeretes tétel, amely ismét egy szélesebb kérdéskör egyik részeredménye.

Ha egy (1) alakú egyenlet együtthatói valós számok, és az x hatványai szerint rendezett egyenletben két egymásra következő együttható előjele ugyanaz, *jelkövetkezés*ről beszélünk, ha két egymásra következő tag előjele különböző, *jelváltás* van. Descartes jelszabálya ekkor így fogalmazható: Az egyenletnek legfeljebb annyi pozitív gyöke van, mint a jelváltások száma, és ha kevesebb, akkor páros számmal kevesebb. Ha tehát az egyenletben csak egy jelváltás van, okvetlen van egy és csak egy pozitív gyöke.

Descartes jelszabálya a negatív gyökökre is kiterjeszthető, ha x-et $-x$-szel pótoljuk.

*Irreducibilis*nek hívunk egy racionális együtthatós algebrai egyenletet, ha nincs valamely alacsonyabb fokú racionális együtthatós egyenlettel közös gyöke. Igen sok szép tétel van, amelyek az irreducibilitásra elegendő feltételeket állapítanak meg. Közülük csak egyet idézünk, „Eisenstein tételét”. Ha az

$$x^n + a_1x^{n-1} + \ldots + a_n = 0$$

algebrai egyenlet egész együtthatós, legmagasabb fokú tagjának együtthatója 1, és a többi együttható osztható valamely p prímszámmal, de a_n nem osztható p^2-tel, akkor az egyenlet irreducibilis.

Az algebrának elsőfokú (lineáris) több ismeretlenes egyenletrendszerek megoldásával, elsőfokú többváltozós helyettesítése tulajdonságaival és rokon kérdésekkel foglalkozó részét *lineáris algebrá*nak hívjuk. Idetartoznak tehát a determinánsok is (melyeket Lapunk egy régebbi számában röviden ismertettünk[1]), mert a lineáris egyenletrendszer minden megoldása két determináns hányadosaképpen állítható elő.

Rados műveinek túlnyomó többsége a lineáris algebra körébe tartozik; némelyiknek nagy sikere volt, és lényegesen hatott a magyar (sőt részben a külföldi) matematikára.

Rados egy fiatalkorú munkájának ismertetéséhez röviden ismertetjük a kongruenciákat.

Két egész számot valamely m pozitív egész számra – modulusra – vonatkozólag *kongruens*nek nevezünk, ha a modulussal való osztásnál ugyanazt a maradékot adják, vagyis ha különbségük osztható a modulussal. Jelekben

$$a \equiv b \pmod{m},$$

és így olvassuk: a kongruens b-vel, moduló m.

A kongruenciákkal nagyjában úgy számolhatunk, mint az egyenletekkel, de van különbség is, amelyről majd szólni fogunk. Pl. rögtön látni, hogy

$$a \equiv a \pmod{m},$$

és azt is: hogy ha

$$a \equiv b \pmod{m},$$

akkor egyszersmind

$$b \equiv a \pmod{m}$$

(hiszen ha $a-b$ osztható m-mel, akkor $b-a$ is osztható m-mel). Szabad mindkét oldalhoz ugyanazt a számot hozzáadni, vagy mindkét oldalból kivonni, (hiszen a különbségből kiesik), és mindkét oldalt, ugyanazzal a számmal szorozni (mert a különbségük szorzódik a számmal).

Ha

$$a \equiv b \pmod{m} \qquad \text{és} \qquad b \equiv c \pmod{m},$$

akkor egyszersmind

$$a \equiv c \pmod{m},$$

hiszen ha $a-b$ és $b-c$ osztható m-mel, akkor összegük $a-c$ is osztható m-mel. Általában azonban nem szabad a kongruencia mindkét oldalát ugyanazzal a számmal elosztani. Pl. $2 \cdot 6 \equiv 9 \cdot 6 \pmod{14}$, de $2 \not\equiv 9 \pmod{14}$. Ebben tehát különböznek a kongruenciák műveletei szabályai az egyenletek műveleti szabályaitól. Fennáll azonban a tétel: ha d relatív prim m-hez és

$$ad \equiv bd \pmod{m},$$

akkor mindkét oldalon oszthatunk d-vel. Ugyanis

$$ad - bd = d \quad (a-b),$$

de d-nek és m-nek nincs 1-nél nagyobb közös osztója, és ismeretes, hogy ekkor a másik tényező $a-b$ osztható m-mel.

Ha

$$a \equiv b \pmod{m}, \qquad c \equiv d \pmod{m},$$

akkor egyszersmind

$$a + c \equiv b + d \pmod{m} \qquad \text{és} \qquad ac \equiv bd \pmod{m}.$$

A bizonyítást az olvasóra bízzuk.

A kongruencia fogalmát Gauss ifjúkori főművében vezette be a tudományba, és ezt a felfedezését önmaga is oly nagyra becsülte, mint a betűszámtan feltalálását.

A kongruenciák körében is nagy érdekessége van az algebrai egyenleteknek megfelelő kérdéseknek, amelyekben tehát keresnünk kell oly számokat, amelyeket az ismeretlen helyébe helyettesítve a kongruencia helyes lesz. Világos, hogy ha valamely x szám kielégíti a kongruenciát, minden vele mod *kongruens* szám is kielégíti.

Itt már nagy különbség mutatkozik a kongruencia és az egyenlet között. Míg az egyenletnek, amint már említettük, az algebra alaptétele szerint mindig van megoldása, addig pl. már a következő elsőfokú kongruenciának nincs megoldása:

$$2x \equiv 5 \pmod{4}.$$

Az

$$ax \equiv b \pmod{m},$$

[1] *Obláth R.:* Képek a magyar matematika múltjából. V. Beke Manó (1862. ápr. 24–1946. jún. 27.) Lapunk X. kötet, 1955. 33–42. old. A Függelék 41–42. old.

általános elsőfokú kongruencia megoldhatóságának szükséges és elégséges feltétele, hogy b osztható legyen a és m legnagyobb közös osztójával.

Magasabb fokú kongruenciákra már ilyen megoldhatósági kritériumok nincsenek általában, még abban a legtöbbet tárgyalt nevezetes esetben sem, ha a modulus egy p prímszám. A számelmélet, egy igen nevezetes tétele, az ún. FERMAT tétel biztosítja azt, hogy az általánosságon semmi csorba nem esik, ha prím modulus esetén olyan kongruenciákra szorítkozunk, amelyek fokszáma legfeljebb $p-2$, mert minden ennél magasabb fokú kongruencia legfeljebb $p-2$ fokúra redukálható. Feltételezzük továbbá, hogy a tiszta tag nem osztható p-vel, mert ellenkező esetben

$$a_n \equiv 0 \pmod{p}$$

lenne, és így e tagot elhagyva x-szel egyszerűsíthetnénk, és alacsonyabb fokú kongruenciát kapnánk.

A pontosan $p-2$-edfokú kongruenciák esetén a König–Rados tétel[2] megadja a választ arra a kérdésre, hogy mi annak a szükséges és elégséges feltétele, hogy a

$$c_0 x^{p-2} + c_1 x^{p-3} + \ldots + c_{p-3} x + c_{p-2} \equiv 0 (\bmod p) \tag{2}$$

kongruencia ($c_0,\ c_{p-2} \neq 0 \pmod{p}$) megoldható legyen.

A (2) *alatti kongruencia megoldhatóságának szükséges és elégséges feltétele, hogy a*

$$D = \begin{vmatrix} c_0, & c_1, & c_2, & \ldots, & c_{p-3}, & c_{p-2} \\ c_1, & c_2, & c_3, & \ldots, & c_{p-2}, & c_0 \\ c_2, & c_3, & c_4, & \ldots, & c_0, & c_1 \\ \vdots & & & & & \\ c_{p-2}, & c_0, & c_1, & \ldots, & c_{p-4}, & c_{p-3} \end{vmatrix} \tag{3}$$

ún. *ciklikus determináns osztható legyen* p-vel, *azaz*

$$D \equiv 0 \pmod{p}.$$

A tétel kibővíthető úgy is, hogy arra a kérdésre is megfeleljen, mi annak a feltétele, hogy a (2) kongruenciának k számú gyöke legyen. Ez esetben Rados felelete így szól:

Ahhoz, hogy a (2) *kongruenciának* k *számú különböző gyöke legyen, szükséges, hogy* D-*nek összes* p-k-*adrendű aldeterminánsai oszthatók legyenek* p-*vel* ($p-k$-alrendű aldeterminánsalatt azt értjük, ha a determinánsból csak $p-k$ számú sort és $p-k$ számú oszlopot tartunk meg), *ha a* p-k-*alrendű aldeterminánsok a legalacsonyabbrendűek, amelyekre ez a feltétel teljesül, akkor a* (2) *kongruenciának pontosan* k *számú gyöke van.*

Ez a két tétel König Gyulától származik, aki műegyetemi előadásában közölte, de a pontos bizonyítás Rados Gusztáv műve. A tétel jelentőségét és érdekességét mutatja, hogy KRONECKERnek (az eddig élt algebristák egyik legnagyobbikának) a berlini egyetemen tartott, és könyvalakban kiadott, számelméleti előadásaiban egész fejezetet szentel neki[3]. Kronecker itt, más bizonyítást ad rá, és a tétel második felét egyszerűbben (algebrailag) fogalmazza meg, de erre nem térhetünk ki.

Radosnak ezen kívül is igen sok dolgozata foglalkozik kongruenciákkal, de közülük csak még két eredményét ismertethetjük.

Már a XVIII. század közepén EULER tudta, hogy

$$x^2 \equiv D \pmod{p}$$

(p prímszám) másodfokú ún. binomkongruencia megoldhatóságának szükséges és elégséges feltétele

$$D^{\frac{p-1}{2}} = 1 \pmod{p}$$

teljesülése. Rados ehhez hozzáfűzi, hogy *ha ez a feltétel teljesül, és* p *valamely* $4n+3$ *alakú prímszám, akkor a megoldást az*

$$x \equiv \pm D^{\frac{p+1}{4}} \pmod{p}$$

kongruencia szolgáltatja[4]. Rados eredményét az n-edfokú binom kongruenciára is kiterjeszti, de ennek ismertetése túl messzire vezetne.

A másik tétel, amelyet ismertetek[5], összefüggést állapít meg az egyenletek és kongruenciák gyökei között. *Ha az* (1) *algebrái egyenlet minden gyöke racionális, akkor az*

$$a_0 x^n + a,\ x^{n-1} + \ldots + a_{n-1} x + a_n = 0 \pmod{p} \tag{4}$$

[2] *Raussnitz G.:* A felsőbb fokú kongruenciák elméletéhez. *Math. és Termtud. Értesítő* 1., 1883, 8–9. füzet 14. old. *Raussnitz G.:* Zur Theorie der Congruenzen höheren Grades, *Math. u. naturwiss. Berichte aus Ungarn* 1., 1883. 266–278. old., *Rados G.:* Zur Theorie der Congruenzen höheren Grades. *Journal für die reine und angewendete Mathematik* 99., 1886., 258–260. old.

[3] *Kronecker L.:* Vorlesungen über Zahlentheorie, Leipzig, 1901, 28. előadás, 389–90. old.

[4] *Rados G.:* Adalék a binom kongruenciák elméletéhez. *Mat. és Termtud. Ért.* 55., 1936., 309–319. old

[5] *Rados G.:* Über Kongruenzbedingungen der rationalen Lösbarkeit von algebraischen Gleichungen. *Math. Annalen* 87., 1922. 78–83. old.

kongruenciának minden prímszám modulusra, amely nem osztója a_0-nak, pontosan n gyöke van. (Persze, itt feltesszük, hogy $n \leq p-2$).

Ennek megfordítása, és ez a nehezebb:

Ha a (4) *alatti kongruenciában* $a_0 = 1$ *és minden* p *prímszám modulusra pontosan* n *gyöke van, akkor az* (1) *algebrai egyenlet minden gyöke egész szám.*