**RÉNYI ALFRÉD MATEMATIKAI KUTATÓINTÉZET**
1053 Budapest, Reáltanoda u. 13-15, 1364 Budapest, Pf. 127.
telefon: + 36 1 4838302, fax: + 36 1 4838333
e-mail: ppp@renyi.hu, honlap: http://www.renyi.hu

# ÁTTEKINTÉS A KIEMELTEN SIKERES KUTATÁSI TERÜLETEKRŐL

Az intézet kutatói 2009-ben is számos, a részletes jelentésben ismertetett, kimagasló matematikai eredményt értek el, különösen a számelmélet és a diszkrét matematika területén, de ezek az eredmények csak nagyon nehezen fogalmazhatók meg nem szakemberek számára.

## Számelmélet

*Ikerprímszám sejtés*

A prímszámok vizsgálata több ezer éves múltra tekint vissza. A prímszámok fogalma egyszerű, a problémák könnyen megfogalmazhatóak, ugyanakkor rendkívül nehezek. Éppen ezek a nehézségek adják az alapját a prímszámokra épülő modern alkalmazásoknak.
Az intézet kutatója külföldi társszerzőkkel közösen bebizonyította, hogy a híres ikerprím sejtés egy gyengített formája bizonyos természetes feltételek teljesülése mellett igaz. Ez áttörést jelent a már Euklidesz által 2300 évvel ezelőtt megfogalmazott ikerprím sejtéssel kapcsolatban, amit a matematika egyik legreménytelenebb problémájának tartanak. A kérdés fontosságát és a kutató által korábban elért eredmények jelentőségét jelzi, hogy az intézet kutatója ezek alapján nyerte el „Gaps between primes and almost primes. Pattern in primes and almost primes. Approximations to the twin prime and Goldbach conjecture" című pályázatával a European Research Council legnagyobb presztízsű Advanced Grants kategóriájában a matematika területén egész Európában odaítélt összesen 14 matematikai projekt támogatás közül az egyiket 2008 novemberétől.
A fent említett eredmény az 1,4 millió euró támogatású projekt szebbnél szebb gyümölcsei közül is kiemelkedik. Az intézetben kialakított műhely matematikai potenciálja – külföldi matematikusok bevonásával – további hasonlóan fontos eredmények elérésével kecsegtet. A téma és a kérdések nehézségét, a műhely erősségét mutatja, hogy több cikkük is félszáz oldal terjedelmű (a bizonyítások is több tucat oldalasak), és a legrangosabb matematikai folyóiratokban jelentek meg, a fent említett dolgozat például az Annals of Mathematics-ben.

## Diszkrét matematika

*Hipergráfok*

Már évek óta a diszkrét matematikai kutatások középpontjába került a Rényi Intézet munkatársai által először a Microsoft és az ELTE, majd további kutatóhelyek munkatársaival karöltve végzett vizsgálatai nagy gráfok struktúrájának leírására vonatkozóan. A híres regularitási lemma nagy számú extremális gráfelméleti alkalmazása után gráfsorozatok határértékének definiálásában és meghatározásában tett szert egyre nagyobb jelentőségre. Legújabban pedig már a hipergráfokra való különböző általánosítási lehetőségeket vizsgálták. Ezek közül emelkedik ki az intézet kutatói által bizonyított tétel, ami forradalmasítja az ezekben alkalmazott bizonyítási technikát, nagy hatékonysággal alkalmazva az algebrai logikában definiált ultraszorzatok fogalmát. Az elért eredmények jelentőségét az is mutatja, hogy a 2009-es dél-amerikai matematika kongresszus egyik plenáris előadója a Rényi Intézet munkatársa volt erről a kérdésről szóló előadásával.

**Kriptográfia**
*Lendület program*

A kriptográfia az intézet két sikertémája, a diszkrét matematika és a számelmélet talaján születő, a biztonságos számítógépes kommunikáció igényének korában rohamosan fejlődő alkalmazás orientált matematikai kutatási terület. Az eddigi kiváló eredményeknek (digitális vízjel, számítógépes dokumentum hitelesítése) köszönhető, hogy eredményesen szerepeltek az Akadémia *Lendület* pályázatán.
Az elnyert támogatás új lendületet adott a korábban már megkezdett titkosírási, értelemszerűen nagyobb részt alkalmazott kutatások folytatásához. A projekt segítségével és a belső erők átcsoportosításával létrehozott 11 tagú kriptográfiai kutatócsoport a második félévben jött létre és egymás kutatásai ilyen irányú eredményeinek és a lehetséges kutatási témák megismerése után máris fontos eredményeket ért el a különböző titokmegosztási protokollok, az ún. anonym broadcast protokollok és az ujjlenyomat kódok vizsgálatának területén.