*Freud Róbert* 2005. november 22-én 16.00-kor

**Prímszámok – ősi problémák, új eredmények**

címmel tart előadást.

A prímszámok témakörében hemzsegnek az egyszerűen megfogalmazható, ám jelenlegi tudásunk szerint reménytelennek látszó megoldatlan problémák. Az előadásban néhány olyanról lesz szó, amelynél az utóbbi években történt kisebb-nagyobb előrehaladás.

A Mersenne-prímek a tökéletes számok több mint 2000 éves problémájához és a nagyon nagy prímszámok kereséséhez kapcsolódnak. Nagyon közel járunk már (legalább) tízmilliójegyű prímszám előállításához; a versenybe számítógépével bárki bekapcsolódhat, és százezer dollár üti a markát, ha elsőként talál ilyen megaprímet.

Az első és ma is leginkább használt nyilvános jelkulcsú titkosírás, az RSA-séma, azon alapul, hogy viszonylag gyorsan tudjuk egy nagy számról eldönteni, hogy prím-e, azonban összetett szám esetén reménytelen megtalálnunk a prímfelbontását (kivéve, ha mi magunk szoroztuk össze a tényezőit). A korábbi gyors prímteszteknél volt egy minimális elméleti bizonytalansági faktor, ezt azonban három indiai matematikus 2002-ben egy új eljárással teljesen kiküszöbölte.

Tavaly nagy szenzációt jelentett annak igazolása, hogy a prímekből akármilyen hosszú véges számtani sorozatok képezhetők.

Az idei év újdonsága, hogy mintegy százéves szinte egy helyben topogás után egy aprócska lépéssel közelebb jutottunk az ikerprímsejtéshez; a rendkívüli eredmény egyik szerzője a magyar Pintz János. Ez még mindig fényévnyi távol van magától a sejtéstől; egy hasonlattal élve, eddig azt tudtuk, hogy egy gyufaszál rövidebb, mint az Egyenlítő és a Margit-híd távolsága, most pedig már azt is tudjuk, hogy az Egyenlítő és a Lánchíd távolságánál is rövidebb.

Friss információkkal a

`http://matek.fazekas.hu/portal/eloadas/2005/index.html`

linken jelentkezünk. Az iskola címe: 1082 Budapest, Horváth Mihály tér 8.

[1] A sorozat programja megtalálható előző számunkban.