Szakdolgozat kivonat

Bognár Dávid

Szakdolgozatom a számelmélet témakörének egyik érdekes csoportjával, a prímszámokkal, azon belül is a számokat tesztelő algoritmusokkal foglalkozik. Az új technológiák bevezetése miatt egyre több helyen találkozhatunk adatok titkosításával. Talán észre sem vesszük, de nagy prímszámokkal nap mint nap találkozhatunk.

Napjaink leggyakrabban használt titkosítási folyamata az RSA-eljárás. Az eljárás kiinduló pontjában két nagy prímszám kiválasztása, valamint ezek összeszorzása áll. A művelet hatékony elvégzése megköveteli a prímszámok gyors, és hatékony tesztelését, ezért az elmúlt évtized egyik fontos matematikai céljává vált a gyors tesztek előállítása.

Dolgozatomban a teszteket működésüket tekintve három nagy csoportba osztom: determinisztikus, valószínűségi valamint modern determinisztikus prímtesztek. Minden teszt esetén egy kis történelmi áttekintés után megismerhetjük magát a tesztet és zárásként megvizsgáljuk a futási időket is. Az itt bemutatott tesztek több évszázadot ölelnek fel hiszen a kezdetleges naiv prímteszttől eljutunk az egészen modern, 2002-ben publikált AKS algoritmushoz is.

A szakdolgozatban bemutatott tesztek:

Determinisztikus módszerek:

- Naiv-módszer
- Wilson-prímteszt
- Lucas-prímteszt
- Lucas-Lehmer prímteszt

Valószínüségi módszerek:

- Solovay-Strassen-prímteszt
- Rabin-Miller

Modern determinisztikus módszerek:

- Agrawal-Biswas-teszt
- AKS-teszt