Habilitációs és tudományos előadások vázlata

Mérai László

2017. május 8.

Tervezett habilitációs előadások vázlata

Mindhárom tervezett előadás a Számítógépes számelmélet c. tárgy egy-egy 45 perces előadása.

1. **Prímtesztek**
   - Valószínűségi és determinisztikus prímtesztek
   - Fermat-teszt, pszeudoprímek
   - Soloway-Strassen teszt
2. **Faktorizáció**
   - A faktorizáció probléma, RSA probléma
   - A faktorizáció és az Euler-féle φ függvény kiszámolásának kapcsolata
   - Pollard ρ algoritmus
3. **Diszkrét logaritmus probléma**
   - Diszkrét logaritmus probléma
   - A DDHP, CDHP és DLP problémák
   - Pollard ρ algoritmus

Tudományos előadás vázlata

Pszeudovéletlen sorozatok

Az előadásban elliptikus görbék segítségével definiált sorozatok pszeudovéletlen tulajdonságait vizsgálom. A témában elért eredményeimet a habilitációs tézisfüzet 2. részében foglaltam össze.

Először röviden ismertetem az elliptikus görbék fogalmát, majd a pszeudovéletlenség lehetséges megközelítéseit foglalom össze.

Ezután elliptikus görbék segítségével definiált sorozatokat vizsgálok a korábban definiált pszeudovéletlenségi mértékek segítségével. Az előadásban három, klasszikusnak mondható generátort tárgyalok, nevezetesen a *lineáris kongruencia generátort* a *hatványgenerátort* és a *Frobenius generátort*.

Az előadásomat a jelenlegi kutatási témám ismertetésével zárom.