Kivonat

Bartha Zsolt

A szakdolgozatban az elliptikus görbék elméletével és kriptográfiai alkalmazásaival foglalkozunk. A második fejezetben definiáljuk az elliptikus görbék fogalmát, megadjuk különböző egyenleteiket. Ezután bevezetünk rajtuk egy műveletet, mellyel Abel-csoportot alkotnak. Kitérünk a 2 karakterisztikájú testek feletti görbékre, ismertetve ezeknek a többi görbétől eltérő egyenleteit és műveleteit. A kriptográfiai alkalmazások szempontjából fontos, hatékony algoritmusokat mutatunk a görbéken való számolásra a projektív koordinátázás segítségével. Ezután bevezetjük a görbék mint csoportok endomorfizmusaival kapcsolatos fogalmakat, ismertetünk néhány fontos eredményt, többek között a számmal való szorzás mint endomorfizmus tulajdonságait. Ezek segítségével belátjuk a görbék n-talpának struktúrájára vonatkozó tételt.

A harmadik fejezetben az alkalmazásokat tekintve fontos, véges test feletti elliptikus görbékkel foglalkozunk. Leírjuk ezek algebrai struktúráját, ismertetjük a rendjükre becslést adó Hasse-tételt. Ezután egy fontos endomorfizmusukkal, a Frobenius-leképezéssel foglalkozunk, megadjuk ennek minimálpolinomját, amely a Schoof-algoritmusnál jut szerephez. A fejezet további részében módszereket mutatunk be a véges test feletti görbék rendjének meghatározására: egyes görbék rendjét expliciten megadó tételeket mondunk ki, illetve algoritmusokat ismertetünk, köztük a leghatékonyabb Schoof-algoritmust.

A negyedik fejezetben az elliptikus görbéken megadott diszkrét logaritmus problémát tárgyaljuk. Ennek megoldására szintén több algoritmust ismertetünk, és rámutatunk, hogy ha a görbe mint csoport rendje egy nagy prím, akkor a probléma megoldása a tudásunk mai szintjén algoritmikus értelemben nehéznek látszik.

Az ötödik fejezetben ismertetjük a kriptográfiai rendszerek fajtáit, működését, majd több, titkosításra, illetve digitális aláírásra szolgáló módszert mutatunk be, melyek biztonságossága a diszkrét logaritmus probléma nehézségén alapul, és amelyek standardként is elfogadottak. Rámutatunk arra, hogy ezek a rendszerek hatékonyabbak, és nagyobb biztonságot nyújtanak, mint a korábbi nyilvános kulcsú módszerek.