

ELLIPTIKUS GÖRBÉK

PETHŐ ATTILA
DEBRECENI EGYETEM, INFORMATIKAI KAR

Abstract

Az $y^2 = x^3 + ax + b$ egyenletnek eleget tevő (x, y) pontok halmazát elliptikus görbének nevezzük. Attól függően, hogy milyen alaphalmazon felett dolgozunk más-más érdekes kérdéseket tehetünk fel az elliptikus görbékkel kapcsolatban. Előadásomban három esetet vizsgálunk meg részletesebben, ha az alaphalmaz a valós, a racionális számok illetve ha a modulo p maradékosztályok halmaza, ahol p prímszám. Megnézzük az elliptikus görbék formáját, definiáljuk pontok "összegét" és megvizsgáljuk ezen összeadás tulajdonságait.