Populärvetenskaplig sammanfattning

I denna kandidatuppsats visas vissa grundläggande satser inom algebraisk geometri. Satserna tillämpas slutligen på elliptiska kurvor, vilka är intressenta, bland annat för deras tillämplighet inom talteori, och speciellt kryptografi.

Bezouts, Max Noethers, Pappus, Pascals och Chasles satser, vilka visas här, har varit kända länge. Det äldsta resultatet, Pappus sats, visades nämligen redan på 300-talet e. Kr., visserligen utan de metoder som används här. Cirka 1500 år senare visade Max Noether sin fundamentalsats, vilket är det nyaste resultatet som visas här. Trots åldern är resultaten oumbärliga verktyg för att verkligen förstå de moderna tillämpningarna inom elliptiska kurvor.

Även om viktiga resultat, som bland annat Lenstras algoritm för snabb primtalsfaktorisering av stora heltal, och asymmetrisk kryptering med hjälp av elliptiska kurvor, inte visas här, så har dessa tillämpningar gemensamt att de bygger på att man kan definiera addition på elliptiska kurvor, vilket visas rigoröst i denna uppsats.

Metoderna som används är elementära och kräver endast förkunskaper inom linjär algebra och grundläggande ringteori. Bevisen kommer från böcker (se referenslistan) i algebraisk geometri, men de som hittas i dessa är mycket mer kortfattade, än de som presenteras här. Detta arbete fyller i detaljerna i resonemangen, för att göra materialet tillgängligt för människor med grundläggande matematisk skolning.