2005:14
Självständigt arbete i matematik
Matematiska institutionen
Stockholms universitet

Per Westerlund: AKS-algoritmen för att bestämma om ett tal är ett primtal eller inte

Sammanfattning

AKS-algoritmen undersöker om ett tal är ett primtal eller inte. Den presenterades i augusti 2002 av Agrawal, Kayal och Saxena. Det är den första algoritmen som är både deterministisk och polynomiell, alltså för alla tal ger den rätt svar inom en tid som är ett polynom av antalet siffror.

Liksom flera andra algoritmer är den baserad på Fermats lilla sats, som inte kan användas direkt eftersom både alla primtal och vissa sammansatta tal uppfyller den. Här testar man några polynom upphöjda till det undersökta talet och de är väl valda så att inga sammansatta tal kan slinka igenom. Både antalet polynom och deras grad är små i förhållande till det undersökta talet.

Först visar jag algoritmen i pseudokod. För den senare analysen introducerar jag grundläggande talteori och algebra, bland annat moduloräkning, ringar och kroppar. Därefter beräknar jag algoritmens komplexitet rad för rad. Slutligen bevisar jag att den svarar rätt för både primtal och sammansatta tal.