Modellen voor eindige lichamen

Eindige lichamen komt men in verscheidene onderdelen van de zuivere wiskunde tegen, zoals groepentheorie, getaltheorie en algebraïsche meetkunde. Bovendien hebben ze belangrijke toepassingen, onder andere in de coderingstheorie en de cryptologie. Deze toepassingen kunnen niet zonder efficiënte algoritmen, en het is de theoretische bestudering van deze algoritmen waar het onderhavige project aan gewijd is.

De uitvoerder van het project doet er goed aan niet alleen op de hoogte te zijn van de fundamentele algebraïsche eigenschappen van eindige lichamen, maar ook kennis te nemen van de inhoud van het college *Complexity theory* dat D. Hofheinz in het voorjaar van 2009 geeft.

Elk eindig lichaam heeft een *karakteristiek*, die een priemgetal is, en een *graad*, die een positief geheel getal is; als de karakteristiek p is, en de graad n, dan is p^n het aantal elementen van het lichaam. Voor elk priemgetal p en elk positief geheel getal n bestaat er een eindig lichaam van karakteristiek p en graad n, en zo'n lichaam is op isomorfie na eenduidig bepaald.

Hier zijn een aantal fundamentele algoritmische vragen over eindige lichamen: (a) hoe modelleert men een eindig lichaam? (b) hoe kan men een model voor een eindig lichaam van gegeven karakteristiek en graad efficiënt construeren? (c) hoe kan men snel testen of iets dat gepresenteerd wordt als model van een eindig lichaam, dat ook werkelijk is? (d) kan men, gegeven twee modellen voor eindige lichamen van dezelfde karakteristiek en dezelfde graad, efficiënt een isomorfisme tussen deze modellen construeren? en (e) kan dat laatste ook, in een nader te definiëren zin, op een *consistente* manier gebeuren?

Al deze vragen hebben bevredigende antwoorden, deels als resultaat van zeer recent onderzoek.

Een geschikt bachelorproject kan bestaan uit de bestudering van vraag (c). In het geval van *priemlichamen* komt deze vraag neer op het construeren van een snelle primaliteitstest, maar voor het geval van algemene eindige lichamen komt er meer bij kijken. Om een karakterisering van eindige lichamen te vinden die bruikbaar is voor een snelle algoritme, dient men niet alleen wat de abstracte algebra betreft goed beslagen ten ijs te komen maar ook enige fundamentele kennis te verwerven op het gebied van algebraïsche algoritmen en hun complexiteit.

Begeleider: H. W. Lenstra