Constructie van eindige lichamen

Op de website

http://www.math.leidenuniv.nl/∼desmit/papers/standard_models.pdf

vindt men een expliciete constructie van "alle" eindige lichamen en hun algebraïsche afsluitingen. Deze constructie heeft allerlei gunstige algoritmische eigenschappen, zoals uitgelegd in het artikel

Bart de Smit, Hendrik W. Lenstra jr., *Standard models for finite fields*, pp. 401–404 in: G. L. Mullen, D. Panario (eds), *Handbook of finite fields*, CRC Press, Boca Raton, 2013.

In de genoemde bronnen worden geen bewijzen gegeven.

Het project bestaat eruit, ten eerste, een bewijs te leveren dat de op de website gegeven constructie correct is, en ten tweede, voorzover de tijd het toelaat, aan te tonen dat deze constructie inderdaad de in het artikel genoemde algoritmische eigenschappen heeft.

Voor de eerste helft van het project is enige bedrevenheid in het werken met groepen, ringen en lichamen voldoende. Kennis van algebraïsche getaltheorie is ook nuttig, maar deze is strikt genomen niet noodzakelijk, en kan ook tijdens het project verworven worden.

Voor de tweede helft van het project dient de student op de hoogte te zijn van een aantal fundamentele begrippen uit de informatica, en te weten hoe men de rekentijd van een algoritme afschat. Kennis van een aantal fundamentele algoritmen voor eindige lichamen komt eveneens van pas, maar in deze materie kan de student zich tijdens het project verdiepen.

Begeleider: Hendrik Lenstra