Snelle algoritmen in de algebra

Dit project gaat over algoritmen in de algebra en getaltheorie die een betere *asymptotische complexiteit* hebben dan de standaardmethoden.

Een voorbeeld is het vermenigvuldigen van polynomen. Als f en g twee polynomen van graad m respectievelijk n zijn over een ring R, dan zijn er op de voor de hand liggende manier $(m+1)(n+1)$ vermenigvuldigingen en mn optellingen in R nodig om het product fg te berekenen. Voor het product van twee polynomen van graad n zijn asymptotisch (d.w.z. als $n \to \infty$) dus een constante maal n^2 operaties nodig. In 1960 ontdekte Anatoly Karatsuba een verrassende alternatieve methode voor het vermenigvuldigen van polynomen die voor grote waarden van n slechts ongeveer $n^{1,585}$ operaties nodig heeft. In de loop van de tijd zijn hierop meerdere verbeteringen gevonden.

Een andere belangrijk probleem is hoe snel twee matrices vermenigvuldigd kunnen worden. De methode om twee $n \times n$-matrices te vermenigvuldigen die direct uit de definitie van het product van matrices volgt, heeft asymptotisch een constante maal n^3 operaties nodig. Volker Strassen vond in 1969 als eerste een snellere methode, die voor $n \to \infty$ slechts ongeveer $n^{2,81}$ operaties nodig heeft. Ook voor dit probleem zijn in de tussentijd algoritmen ontwikkeld die asymptotisch nog sneller zijn.

Een bachelorscriptie in deze richting zou kunnen gaan over het beschrijven van een aantal van deze algoritmen. Voor studenten die interesse hebben in programmeren is het ook een optie om bijvoorbeeld verschillende algoritmen experimenteel te vergelijken.

Begeleider: Peter Bruin