point counting on nondegenerate curves

het tellen van punten op niet-gedegenereerde krommen

Samenvatting

Een belangrijk probleem in de computationele getaltheorie is het volgende: ontwerp een efficiënt algoritme dat, gegeven een eindig veld F en een bivariate veelterm f(x,y) over dat eindig veld, het aantal oplossingen van de vergelijking f(x,y) = 0 als uitvoer geeft. Het spreekt voor zich dat de naïeve methode, die alle mogelijke waarden voor x en y uitprobeert en telkens nagaat of het om een oplossing gaat, *niet* efficiënt is wanneer F veel elementen bevat. Daarom zijn slimmere methodes nodig.
Het aantal oplossingen van vergelijkingen over eindige velden houdt wiskundigen al zo'n 200 jaar bezig. In de praktijk blijkt het een grillig en schijnbaar lukraak gekozen getal te zijn, dat veel van zijn wiskundige geheimen nog niet heeft prijsgegeven. Ons belangrijkste theoretische inzicht hebben we te danken aan André Weil, die vermoedde dat dit aantal oplossingen bepaald wordt door het spoor van de actie die het Frobeniusendomorfisme

$$A \rightarrow A : a \mapsto a^q$$

(waarbij A = F[x,y]/(f(x,y)) en q = #F) induceert op een nader te bepalen vectorruimte die we aan f(x,y) associëren. Later werden daadwerkelijk voorbeelden van zo'n vectorruimte gevonden. Eén van die voorbeelden is de zogenaamde eerste Monsky-Washnitzercohomologieruimte van f(x,y), genoteerd $H^1_{MW}(f)$, die waarden aanneemt in een p-adisch veld, waarbij p de karakteristiek is van F. Kiran Kedlaya was de eerste die vaststelde dat $H^1_{MW}(f)$ uitstekend geschikt is voor computationele doeleinden, op voorwaarde dat p klein is. Hij gebruikte dit in 2001 om een algoritme te ontwerpen dat het aantal oplossingen kan bepalen van bepaalde vergelijkingen van de vorm

$$y^2 - Q(x) = 0$$

over velden van kleine karakteristiek.
In deze thesis veralgemenen we het algoritme van Kedlaya naar bijna willekeurige vergelijkingen. Bijna, omdat er een technische voorwaarde moet voldaan zijn: de vergelijking moet niet-gedegenereerd zijn ten opzichte van zijn Newtonpolytoop. We bewijzen we dat de kans dat een willekeurige vergelijking met gegeven Newtonpolytoop niet-gedegenereerd is, naar 1 streeft als q groot wordt. Ons algoritme heeft in het algemeen $O(n^3g^{6.5})$ stappen en $O(n^3g^4)$ geheugenplaatsen nodig om tot het antwoord te komen. Hierbij is n gelijk aan $\log_p q$, de uitbreidingsgraad van F, en is g gelijk aan het aantal termen van f(x,y).
Om Kedlaya's algoritme te kunnen veralgemenen hebben we een aantal nieuwe eigenschappen van niet-gedegeneerde krommen bewezen die op zichzelf interessant zijn, zoals een effectieve versie van Hilbert's Nullstellensatz.