

Samenvatting

Inleiding

Een wiskundig bewijs is in principe uiteen te rafelen in stappen die slechts bestaan uit het toepassen van een logische afleidingsregel of een wiskundig axioma. Evenals in het schaakspel is op elk moment het aantal mogelijke ‘zetten’ relatief klein. Het succes van de computer in het schaakspel (bijna 10 jaar geleden versloeg ‘Deep Blue’ de regerend wereldkampioen Kasparov in 7 duels), doet vermoeden dat de computer ook in het bewijzen van wiskundige stellingen een significante rol zou kunnen spelen. Dit blijkt ook - ten dele - het geval te zijn.

Om de computer daadwerkelijk wiskunde te laten ‘bedrijven’, dient de wiskunde eerst in een taal uitgedrukt te worden die de computer kan interpreteren. Daarnaast moet overeenstemming bereikt worden welke logische en wiskundige grondwaarheden de computer mag gebruiken om mee te redeneren. Dit is het *formalisieren* van de wiskunde. In de afgelopen decennia zijn diverse automatische stellingbewijzers ontwikkeld die hiermee kunnen werken. Toch zijn deze stellingbewijzers in het algemeen niet in staat om een gemiddeld bewijs dat in eerstejaarscolleges wiskunde voorkomt automatisch te bewijzen. Wél zijn er goede resultaten geboekt met zogenaamde bewijsassistenten: programma’s die met behulp van tactieken die door een gebruiker worden ingevoerd steeds kleine stukjes van een bewijs zelfstandig kunnen doen.

De laatste stelling van Fermat

Prof. dr. Jan Bergstra geeft in [20] een opsomming van de, volgens hem, 10 meest gezichtsbepalende problemen voor het informaticaonderzoek. De eerste daarvan luidt als volgt: *Formaliseer en controleer per computer een bewijs van het door Wiles aangetoonde vermoeden van Fermat*. Dit vermoeden staat ook wel bekend als Fermat’s Laatste Stelling, waarin hij stelt dat de vergelijking $x^n + y^n = z^n$ voor het geval $n > 2$ geen oplossingen heeft in gehele getallen x, y, z ongelijk aan nul. Hoewel hij beweert een bewijs voor deze stelling te hebben is dit zeer onaannemelijk. In ieder geval bewees hij de stelling zelf voor het geval $n = 4$ en wist Euler enkele decennia later het geval $n = 3$ te bewijzen. Wiskundigen hebben vervolgens bijna 300 jaar tevergeefs gezocht naar een bewijs van het algemene geval. Pas in 1993 weet Andrew Wiles met een bewijs te komen, maar dit bleek een belangrijk ‘gat’ te bevatten. Een jaar later weet hij dit op te lossen, waarmee de stelling uiteindelijk bewezen is. Wiles’ bewijs bouwt overigens voort op vele moderne resultaten uit de wiskunde die zeker nog niet bij Fermat bekend waren.

Dit onderzoek

Met name vanwege dit laatste is het formaliseren van Wiles' bewijs een zeer omvangrijk project. Op dit moment is, afgezien van enkele specifieke projecten, alleen relatief elementaire wiskunde geformaliseerd. In dit onderzoek beperken we ons daarom tot de gevallen $n = 3$ en $n = 4$ van Fermat's laatste stelling. De redenen om deze gevallen te formaliseren zijn als volgt:

- Wiles' bewijs gaat alleen over de gevallen waar n een priemgetal groter of gelijk aan 5 is. Pas samen met het bewijs voor de gevallen $n = 3$ en $n = 4$ is het bewijs van Fermat's laatste stelling compleet.
- Het formaliseren van deze relatief eenvoudige gevallen kan meer inzicht geven in de bruikbaarheid van stellingbewijzers in het algemeen en Isabelle in het bijzonder om wiskundige bewijzen mee te formaliseren, met een focus op de getaltheorie.

Er is gekozen voor de bewijsassistent 'Isabelle' omdat deze een relatief krachtig mechanisme heeft om kleine stappen in een bewijs zelfstandig te bewijzen, maar vooral vanwege de zeer leesbare in- en uitvoer van wiskundige bewijsteksten.

Resultaten

De resultaten van dit onderzoek zijn positief. Allereerst bleek Isabelle een zeer toegankelijk bewijsprogramma, waarin al snel de eerste kleine stappen van het bewijs van het geval $n = 4$ bewezen konden worden. Niettemin bleek het formaliseren een tijdrovend proces te zijn waarbij relatief eenvoudige stappen soms nog veel werk kostten. Om die reden is er ook voor gekozen om het bewijs van het geval $n = 3$ op een zo elementair mogelijke manier te formaliseren. Na een succesvolle afronding hiervan zijn nog een aantal gerelateerde getaltheoretische bewijzen geformaliseerd, namelijk die van onder andere de volgende stellingen:

- elk priemgetal dat van de vorm $4m + 1$ is, kan geschreven worden als de som van twee kwadraten;
- elk natuurlijk getal kan geschreven worden als de som van vier kwadraten.

Samen met de resultaten over Pythagoreïsche drietallen, die nodig waren voor het geval $n = 4$ van Fermat's laatste stelling, zijn hiermee drie resultaten uit de 'top 100 van wiskundige stellingen' geformaliseerd, zie [34]. Het geheel heeft bovendien geleid tot twee publicaties in de *Archive of Formal Proofs* [14], een online tijdschrift waarin de belangrijke resultaten met Isabelle gepubliceerd worden.

De formele, automatisch geverifieerde bewijzen zijn te vinden in de appendix van deze scriptie. In totaal beslaan de formele bewijsteksten zo'n 4300 regels over 85 pagina's. Dit is ruim 10 keer zoveel als dezelfde bewijzen zoals ze 'informeel' zijn opgeschreven in de voorgaande hoofdstukken. Voor de formele bewijzen van de stellingen over de sommen van kwadraten was ongeveer 4 á 5 keer zoveel tijd nodig als voor het uitwerken van hun informelere versie in deze scriptie. Vergeleken met resultaten in andere stellingbewijzers betekent dit dat bewijzen in Isabelle/Isar relatief lang zijn, maar dat het produceren ervan relatief snel kan.