Speciale gevallen van de laatste stelling van Fermat

Bachelorproject, Leiden
Ronald van Luijk

De laatste stelling van Fermat zegt dat voor alle gehele exponenten $n \geq 3$ de vergelijking

$$a^n + b^n = c^n$$

geen niet-triviale gehele oplossingen heeft, waarbij een oplossing (a, b, c) triviaal wordt genoemd als er geldt $abc = 0$.

Deze stelling is bewezen door Andrew Wiles in 1994, nadat er een gat in zijn eerste bewijs van een jaar eerder was gevonden. De stelling draagt de naam van Pierre de Fermat omdat Fermat in 1637 (ruim 350 jaar eerder) in de margin van een boek (*Arithmetica* van Diophantos) schreef dat hij een prachtig bewijs had dat helaas niet in de marge paste.

Het bewijs van deze stelling is (veel) te geavanceerd om in een bachelorscriptie te behandelen, maar we kunnen wel naar speciale gevallen kijken. Het makkelijkste geval is $n = 4$ (bewezen door Fermat zelf). Zelfs als we een van de exponenten vervangen door een 2 zijn er nog geen niet-triviale oplossingen, wat bewezen kan worden door slim herschrijven en factoriseren. Ook het geval $n = 3$ (bewezen door Euler, 1770) kan door slimme truuks elementair worden bewezen. In beide gevallen wordt uit een hypothetische niet-triviale oplossing een kleinere niet-triviale oplossing geconstrueerd. Omdat dit niet oneindig vaak herhaald kan worden (de gehele getallen zijn welgeordend) geeft dit een tegenspraak. Deze bewijsmethode wordt ook wel *oneindige afdaling* genoemd (Engels: *infinite descent*).

In beide gevallen kunnen de op het eerste gezicht getruukt lijkende bewijzen geïnterpreteerd worden in termen van elliptische krommen. Dit zijn krommen met een groepsstructuur op de punten. Dit project zal eruit bestaan om in elk geval deze twee gevallen $n = 3$ en $n = 4$ in deze terminologie te beschrijven. Als er genoeg tijd is, dan kunnen we daarna ook naar andere gevallen kijken.

Overigens spelen elliptische krommen ook een grote rol in het bewijs van Wiles voor het algemene geval, maar op een heel andere manier dan voor de zojuist beschreven gevallen.

[1] Z.I. Borevich and I.R. Shafarevich, *Number Theory*, Academic Press, New York, 1966.
[2] J. Silverman, *The Arithmetic of Elliptic Curves*, GTM **106**, Springer-Verlag, New York, 1986.