HOOFDSTUK 2 paragraaf 1

Rekenkunde betreft de natuurlijke getallen (N) en de bekende operaties daarmee middels optellen en vermenigvuldigen. Binnen een dergelijke elementaire taal van de rekenkunde kunnen de meest frappante vermoedenen gesteld en bewezen worden. Een paar voorbeelden:

> *Goldbach's Conjecture* stelt dat elk even getal groter dan 2 de som is van twee priemgetallen.
>
> *Twin Prime Conjecture* stelt dat er oneindig veel priemgetallen p zijn zodat $p + 2$ ook een priemgetal is.
>
> *Collatz Conjecture:* Neem een willekeurig positief getal n. Bereken nu $n/2$ als n even is, en $3n+1$ als n oneven is, en herhaal dit voor het zo verkregen nummer. Uiteindelijk kom je, zo stelt dit vermoeden, bij 1 uit.

Om begripsverwarring te voorkomen: met 'vermoeden' bedoel ik een uitspraak die nog niet bewezen is, met 'stelling' bedoel ik een uitspraak die bewezen is.

Sommige uitspraken zijn zo te (her)formuleren dat ze de volgende vorm aannemen:

> ***elk natuurlijk getal heeft de eigenschap* P**.

Goldbach's vermoeden luidt dan: *elk natuurlijk getal heeft de eigenschap kleiner dan 3 te zijn, of oneven te zijn, of de som van twee priemgetallen te zijn.* Het punt van deze herformulering is dat er een **algoritme** is om te bepalen of een bepaald getal deze eigenschap heeft. Een algoritme is een mechanische, computationele procedure waarmee vast te stellen is of een bepaald getal een bepaalde eigenschap heeft – dat impliceert dus dat een algoritme *eindig* moet zijn. Voor de eigenschap uitgedrukt in de herformulering van Goldbach's vermoeden hierboven is een mogelijke procedure voor een bepaald getal n hieronder gegeven. De eigenschap is een disjunct dus het vaststellen van één van de drie eigenschappen in het disjunct is voldoende. Het interessantst is natuurlijk het geval waarbij n een even getal groter dan 2 is, uitgewerkt onder het derde streepje. Het algoritme gebruikt twee variabelen, x en y, die steeds in waarde verhoogd worden tot ze een priemgetal zijn (bepaald door stap 1 voor x en door stap 2 voor y), totdat ze opgeteld n zijn (waarmee n dus aan het vermoeden voldoet) of beide even groot worden als n (en dan is n een **tegenvoorbeeld** tegen het vermoeden, een geval dat dus niet zal voorkomen als het vermoeden klopt).

Voor elk natuurlijk getal n:

- Geldt $n = 0$, $n = 1$ of $n = 2$: dan is n kleiner dan 3 en heeft dus de gegeven eigenschap, en dus mag het algoritme afgebroken worden. ●
- Levert $n \div 2$ een rest 1 op dan is n een oneven getal en heeft dus de gegeven eigenschap (waarbij voor een deling $a \div b$ weer een algoritme gegeven kan worden, bijvoorbeeld staartdeling). Het algoritme mag afgebroken worden. ●
- Laat getal x de beginwaarde 2 hebben, en getal y ook. Ga naar stap 3.
  1. Laat w de beginwaarde 2 hebben.
     a. Is $w = x$? Geef dan y de waarde van x en ga naar stap 3, anders:
        Is $x \div w$ zonder rest?
        Ja: Verhoog dan de waarde van x met 1 en keer terug naar stap 1.
        Nee: Verhoog dan de waarde van w met 1 en herhaal stap 1.a.
  2. Laat w de beginwaarde 2 hebben.
     a. Is $w = y$? Ga dan naar stap 3, anders:
        Is $y \div w$ zonder rest?
        Ja: Verhoog dan de waarde van y met 1 en keer terug naar stap 2.
        Nee: Verhoog dan de waarde van w met 1 en herhaal stap 2.a.
  3. Is $x + y$ gelijk aan n?
     Ja: Dan heeft n de gegeven eigenschap, en het algoritme mag afgebroken worden. ●
     Nee: Verhoog de waarde van y met 1.
        Is y groter dan n - 2?
        Ja: Verhoog dan de waarde van x met 1.
           Is x groter dan n - 2?
           Ja: n heeft de eigenschap ***niet***, het algoritme afgebroken worden. ○
           Nee: Geef dan y weer beginwaarde 2 en keer terug naar stap 1.
        Nee: Keer terug naar stap 2.

Deze eigenschap is dus *computable*, berekenbaar. Goldbach's vermoeden heeft dus de vorm *Elk natuurlijk getal heeft de eigenschap* P, waarbij P een berekenbare eigenschap is. Alle uitspraken van die vorm worden in het boek **Goldbachachtige uitspraken** genoemd. Ook de uitspraken *Elke eindige reeks* $k_1, \ldots, k_n$ *van natuurlijke getallen heeft de eigenschap* P, en *Elk natuurlijk getal heeft de eigenschap* ¬P zijn Goldbachachtige uitspraken.

Interessant aan zulke uitspraken is dat ze gemakkelijk te weerleggen zijn als ze onwaar zijn: met een *tegenvoorbeeld*. We hoeven bijvoorbeeld alleen maar een *n* te vinden die in de hierboven gegeven procedure tot het (enige) afbreekpunt ○ leidt en niet tot een afbreekpunt ● om te concluderen dat Goldbach het verkeerd had. We hoeven alleen maar systematisch alle mogelijkheden 0, 1, 2, 3, etc. af te gaan. – De onwaarheid van het vermoeden zou dan een logisch *gevolg* van de basisregels van de rekenkunde zijn, aangezien ze uit een berekening met uitsluitend die regels noodzakelijk volgt.

Een berekening zoals in het voorbeeld kan dus als **bewijs** dienen voor bepaalde rekenkundige vermoedens binnen een bepaald formeel systeem.

De **Logica** bestudeert zulke **formele systemen**, en Gödels theorema is een theorema *over* zulke formele systemen.

Concluderend: In elk formeel systeem *S* dat genoeg rekenkunde bevat, te weten de basisregels om berekeningen uit te voeren zoals hierboven, is elke onware Goldbachachtige uitspraak in principe weerlegbaar.

Over het *bewijzen* van *ware* Goldbachachtige uitspraken kunnen we echter niets dergelijks zeggen, de geschiedenis leert dat daar soms hooggecompliceerde wiskunde voor nodig is.

Een **Diophantus-vergelijking** is een vergelijking, notatie $D(x_1, \ldots, x_n) = 0$, die beweert dat er *n* getallen zijn (niet noodzakelijk verschillende) die, indien overeenkomstig ingevuld in de vergelijking, ervoor zorgen dat deze waar is. Bijvoorbeeld: $x + y - xy = 0$, met oplossing $x = 2$ en $y = 2$, of $x = 0$ en $y = 0$.

Een vermoeden als *De Diophantische vergelijking* $D(x_1, \ldots, x_n) = 0$ *heeft geen oplossing in natuurlijke getallen* is altijd een Goldbachachtige uitspraak, maar dan niet betreffende de eigenschap van één getal *n*, maar betreffende een groep getallen. Je hoeft dus alleen maar alle mogelijke groepen getallen af te gaan tot je een groep vindt die de vergelijking kloppend maakt, die groep is dan weer een **tegenvoorbeeld**. Als de stelling waar is kun je, net als bij de Goldbach-stelling, natuurlijk eeuwig blijven zoeken, zoals gezegd.

Maar de *Twin Prime*-stelling is *geen* Goldbach-like stelling. Hij is te omschrijven als *Elk natuurlijk getal* n *heeft de eigenschap dat er een getal* m *groter dan* n *is waarvoor geldt dat* m *een priemgetal is en tevens dat* m+2 *een priemgetal is*. Maar deze 'eigenschap' is niet om te zetten in een algoritme waarmee je in principe een tegenvoorbeeld kunt vinden: er komt geen einde aan de zoektocht naar zo'n getal als er geen is.

HOOFDSTUK 2 paragraaf 2

Hoewel makkelijk te stellen blijken bekende rekenkundige stellingen, zoals de laatste stelling van Fermat, slechts middels zeer complexe wiskunde te bewijzen te zijn – en er zijn nog genoeg onbewezen vermoedens, zoals de drie aan het begin genoemde.

Hilbert was ervan overtuigd dat met genoeg tijd en inspanning alle problemen opgelost zullen gaan worden, dat er dus geen reden is problemen als *in principe* onoplosbaar te beschouwen – '*their solution must follow by a finite number of purely logical processes*'. Geen 'ignorabimus'.

Gödels eerste onvolledigheidsstelling ontkracht Hilberts positieve vertrouwen geenszins, het stelt slechts dat er niet *één bepaald* formeel systeem is waarbinnen *alle* rekenkundige problemen opgelost kunnen worden. Dat is belangrijk.

De stelling luidt:

> ***Elk consistent formeel systeem S waarin een bepaalde hoeveelheid rekenkunde uitgevoerd kan worden is onvolledig m.b.t. elementaire rekenkundige uitspraken: er zijn uitspraken die niet bewezen noch weerlegd kunnen worden in S.***

Een paar verdere begripsdefinities en –omschrijvingen zijn nodig om duidelijk te maken wat dit nu precies zegt.

Een **formeel systeem** is een systeem van **axiomata** en **inferentieregels** waarmee **stellingen** (*theorems*) uit de axiomata afgeleid kunnen worden. Een **stelling** is een uitspraak in de **formele taal** van het systeem die resulteert uit een reeks toepassingen van de inferentieregels, uitgaande van de axiomata. Een **bewijs** in het systeem is dus een eindige reeks van dergelijke toepassingen van inferentieregels die de bewezen stelling als zijn conclusie heeft. Het woord **theorie** (*theory*) wordt als synoniem voor 'formeel systeem' gebruikt in de huidige context. Een **axioma** heeft alleen *binnen het systeem* een speciale functie maar geen intrinsieke eigenschap waardoor het noodzakelijk een axioma *moet* zijn – in principe kan elke zin in de taal van het formele systeem tot axioma binnen dat systeem benoemd worden. Een notatie-detail: als S een formeel systeem is, dan wordt met S + A het formele systeem aangeduid dat identiek is aan S maar een extra axioma kent, namelijk A. In S + A is de uitspraak A uiteraard eenvoudig te bewijzen.

Onvolledigheid in de zin van Gödels onvolledigheidsstelling houdt in dat er in het systeem uitspraken zijn die niet bewezen noch weerlegd kunnen worden, die worden **onbeslisbaar** (*undecidable*) genoemd. **Consistent** is een systeem als er geen enkele bewering in het systeem gedaan kan worden die zowel bewezen als weerlegd kan worden. Een inconsistent systeem kan overigens alles bewijzen èn weerleggen middels de *ex falso quodlibet*-regel, zodat een inconsistent systeem nooit onvolledig *kan* zijn. Daaruit volgt tevens dat *A bewijsbaar is in S desda S + ¬A inconsistent is, en dat A onbeslisbaar is in S desda S + ¬A èn S + A beide consistent zijn.* (intuïtionistische logica laten we hier even buiten beschouwing).

Een eis die Gödels eerste onvolledigheidsstelling dus aan de taal van een formeel systeem stelt is dat **negatie** mogelijk moet zijn zodat voor elke zin A ook de ontkenning daarvan, ¬A, mogelijk is. Verder eist Gödels stelling dat het systeem consistent moet zijn. Dat is geen sterke eis: consistentie heeft op zichzelf nog niets met waarheid te maken, net zoals er consistente leugenaars kunnen bestaan. Men spreekt van **eigenschappen van soundness** van een systeem, waarbij consistentie een heel zwakke eigenschap is, terwijl waarheid van alle rekenkundige theoremata in het systeem de sterkste eigenschap is. Er tussenin ligt de eigenschap die **Σ-soundness** wordt genoemd, wat inhoudt dat het systeem geen enkele *ware* Goldbachachtige uitspraak *weerlegt*. Zoals reeds duidelijk werd bij het bespreken van Goldbachachtige uitspraken is een weerlegging ervan binnen een consistent rekenkundig systeem immers altijd mogelijk, terwijl een *bewijs* binnen het systeem vaak onmogelijk is. Daaruit volgt tevens dat *elke Goldbachachtige uitspraak die in één consistent formeel systeem (met genoeg rekenkunde) bewezen is, waar is.* En daaruit volgt weer dat een bewijs van de onbeslisbaarheid van een Goldbachachtige uitspraak in zo'n systeem tevens een bewijs van de waarheid van die stelling is. Als de stelling onwaar is, is er tenslotte op mechanische wijze een tegenvoorbeeld te vinden en kan er dus niet van onbeslisbaarheid gesproken worden.

Gödel spreekt tevens van een "bepaalde hoeveelheid rekenkunde". Als de taal van een systeem een representatie van natuurlijke getallen en van de bewerkingen + en x bevat en wat basisgegevens betreffende natuurlijke getallen dan is aan deze definitie voldaan. Om nog algemener te zijn: het systeem moet alle rekenkundige uitspraken kunnen bewijzen die middels een mechanische berekening zoals besproken m.b.t. Goldbachachtige uitspraken opgesteld kunnen worden. Het is dus een vrij algemene eis aan wat *uitgedrukt* kan worden en aan wat *bewezen* kan worden in het systeem.

Er is dus een duidelijke connectie tussen deze algemene notie van formele systemen en de eerder geïntroduceerde notie van berekenbaarheid: het herkennen van een axioma en het toepassen van een inferentieregel moet puur mechanisch uitgevoerd kunnen worden. Maar daarover meer in hoofdstuk 3.

HOOFDSTUK 2 paragraaf 3

Als wordt gezegd dat Gödel bewijst dat bepaalde uitspraken **onbewijsbaar** zijn dan moet dat altijd begrepen worden als *onbewijsbaar binnen het formele systeem* en niet als *onbewijsbaar in het algemeen*. Want elke uitspraak A die onbewijsbaar is in S is wel degelijk bewijsbaar in S+A. De eerste onvolledigheidsstelling zegt dus **niet** dat er ware rekenkundige uitspraken zijn die onbewijsbaar zijn in absolute zin.

Evenmin zegt de stelling dat *elk* consistent formeel systeem onvolledig is – de elementaire theorie van de reële getallen is bijvoorbeeld compleet en consistent, maar bevat niet de middelen om aritmetische uitspraken te bewijzen – de natuurlijke getallen kunnen niet eens in termen van de theorie van reële getallen gedefinieerd worden.

Verwarring komt vaak voort uit Gödels *volledigheidsstelling*, waarin 'volledigheid' echter een compleet andere betekenis heeft dan in de onvolledigheidsstelling. Deze stelling zegt in feite dat de inferentieregels van predicatenlogica voldoende zijn voor het afleiden van alle logische consequenties van een set axiomata in een eerste-orde formele logische taal. In die zin zijn genoemde inferentieregels 'volledig' – meer daarover in hoofdstuk 7. De *onvolledigheid* uit de eerste onvolledigheidsstelling kan dan preciezer benoemd worden als negatie-onvolledigheid.

Tenslotte dient nog gesteld te worden dat de onvolledigheidsstelling alleen iets zegt over de *rekenkundige* component en dito stellingen van een bepaald systeem, en niets over de (eventuele) niet-rekenkundige stellingen.

HOOFDSTUK 2 paragraaf 4

Wanneer de eerste onvolledigeidsstelling toepasbaar is op een systeem S, dan is er in S een uitspraak die niet bewijsbaar is, maar wel waar (Stel dat A niet bewijsbaar is, dan is niet-A ook niet bewijsbaar. Maar een van beide moet waar zijn.). We hebben namelijk al gezien dat ieder systeem waar de eerste onvolledigheidsstelling op toepasbaar is, een bepaalde hoeveelheid rekenkunde bevat. Precies in dit rekenkundige component is, dus onafhankelijk van de uitspraken van S, een dergelijke ware onbewijsbare uitspraak te vinden. Dit wil echter niet zeggen dat onvolledigheid een notie van waarheid voor uitspraken in S verondersteld. Integendeel, want onvolledigheid is een **syntactisch concept**.

In de rekenkunde wordt er veel gewerkt met de term "waar(heid)" Ondanks dat er veel filosofische discussies bestaan over het definiëren, gebruiken en toepassen van deze term, is dit binnen de wiskunde veel minder problematisch. De filosofische ideeën over deze term zijn irrelevant voor de rekenkunde. Er bestaan hier twee verschillende gevallen waar "waarheid" op van toepassing kan zijn.

(1) Uitspraken binnen een systeem. Een voorbeeld: "goldbach's conjecture is waar". In dit geval komt het beweren dat deze uitspraak waar is neer op het stellen/formuleren van deze uitspraak. "X is waar", waarbij X een dergelijke uitspraak is, komt dus neer op het beweren van de inhoud van X.

(2) Uitspraken over een systeem. Een voorbeeld: " elke stelling van PA is waar". Deze zin kan niet worden vervangen door een uitspraak die alle beweringen van PA opnoemt. Hiervoor beroept men zich op het waarheidscriterium van Tarski.

Soms wordt er ook gesproken over "waar in het systeem" of "waar binnen de verzameling van axioma's". Dit betekent niet dat het bewijsbaar is in het systeem, maar dat men met behulp van het systeem tot deze waarheid kan komen zonder een formele afleiding.

Verder wordt er soms gesproken over *stellingen* die onbepaalbaar zijn door te beweren dat als een systeem consistent is, dat het een ware onbewijsbare *stelling* bevat. Dit is analytisch incorrect doordat een stelling gedefinieerd wordt als een uitspraak waartoe gekomen kan worden door vanuit de axioma's de regels van rederneren toe te passen. Elke stelling van S is dus ook bewijsbaar in S. Op een zelfde manier kan een *axioma* ook niet onbewijsbaar zijn.

HOOFDSTUK 2 paragraaf 5

Er zijn twee mogelijkheden met betrekking tot de onbeslisbaarheid van rekenkundige uitspraken: Of er bestaan onmogelijk beslisbare uitspraken of elke uitspraak is in principe beslisbaar. Deze laatste opvatting valt samen met Hilbert's "*non ignorabimus*". Godel's onbeslisbaarheid sluit geen van beide opvattingen uit. Zo is er bijvoorbeeld nooit bewezen dat er onbeslisbare rekenkundige problemen bestaan in ZFC. Zelfs al is er geen formeel die alle rekenkundige problemen beslist, bestaat er nog steeds de mogelijkheid om de problemen op te lossen door uitbereiding van de wiskunde. Een voor Systeem S onbeslisbare uitspraak kan wellicht door een ander systeem beslist worden. Er is dus geen reden om skeptisch te owrdne met betrekking tot Hilbert's optimisme.