# Stellingen

behorende bij het proefschrift

*Modular curves, Arakelov theory, algorithmic applications*

van Pieter Jan Bruin

**1.** Er is een probabilistische algoritme om, gegeven een positief geheel getal $n$, een geheel getal $k \geq 2$ en een ringhomomorfisme van de Hecke-algebra $\mathbf{T}(\mathrm{S}_k(\Gamma_1(n), \mathbf{Z}))$ naar een eindig lichaam $\mathbf{F}$ van karakteristiek groter dan $k$, de bijbehorende tweedimensionale Galoisrepresentatie te berekenen, met een verwachte looptijd die polynomiaal begrensd is in $n$ en $\#\mathbf{F}$.

**2.** Er is een probabilistische algoritme om, gegeven een even positief geheel getal $k$ en een positief geheel getal $n$ tezamen met zijn priemontbinding, het aantal manieren te bepalen waarop $n$ te schrijven is als som van $k$ kwadraten, met een verwachte looptijd die onder aanname van de gegeneraliseerde Riemannhypothese polynomiaal begrensd is in $k$ en $\log n$.

**3.** Voor elke ondergroep $\Gamma \subseteq \mathrm{SL}_2(\mathbf{Z})$ zij $Y_\Gamma$ het quotiënt van het complexe bovenhalfvlak onder de werking van $\Gamma$ via Möbiustransformaties. Zij $C$ een compacte deelverzameling van $Y_{\mathrm{SL}_2(\mathbf{Z})}$. Er is een reëel getal $a$ met de volgende eigenschap. Zij $\Gamma \subset \mathrm{SL}_2(\mathbf{Z})$ een congruentieondergroep zonder elliptische elementen, en zij $C_\Gamma$ het inverse beeld van $C$ in $Y_\Gamma$. De Greense functie van $\Gamma$ op $Y_\Gamma \times Y_\Gamma$ wordt, na verwijdering van de logaritmische singulariteit langs de diagonaal, op $C_\Gamma \times C_\Gamma$ in absolute waarde begrensd door $a$.

**4.** De snijtheorie van Arakelov is een mooi voorbeeld van een opmerkelijk soort wiskundig bouwwerk: bij de eerste aanblik vooral een interessante abstractie, maar juist daardoor nuttig om concrete problemen op te lossen.

**5.** Algebraïsche krommen zijn algoritmisch goed te hanteren met methoden waarbij vergelijkingen een minimale rol spelen. Het is zelfs de moeite waard het denken in termen van vergelijkingen bewust te vermijden.

**6.** Zij $\phi$ een isogenie tussen abelse variëteiten over een eindig lichaam $k$ zodanig dat de kern van $\phi$ geannihileerd wordt door $\#k^\times$, en zij $\hat{\phi}$ de duale isogenie. Er is een kanonieke perfecte paring

$$\ker \hat{\phi}(k) \times \operatorname{coker}(\phi(k)) \to k^\times,$$

waarvan de constructie en de perfectie op vrij elementaire feiten berusten. De Frey–Rück-paring voor krommen over eindige lichamen is hiervan een speciaal geval, en is derhalve eenvoudiger te begrijpen dan de wiskundige literatuur over dit onderwerp doet vermoeden.

**7.** Zijn $p$ en $q$ priemgetallen zodanig dat $p$ oneven is en $q-1$ deelt. Zijn $\eta$ en $\lambda$ de Gaußperioden van graad $p$ in respectievelijk $\mathbf{Q}(\zeta_{p^2})$ en $\mathbf{Q}(\zeta_q)$. De Galoisgroep $G$ van de uitbreiding $\mathbf{Q} \subset \mathbf{Q}(\eta \cdot \lambda)$ is een product van twee cyclische groepen van orde $p$. De deeluitbreiding $\mathbf{Q} \subset \mathbf{Q}(\eta)$ is volledig vertakt bij $p$, en de deeluitbreiding $\mathbf{Q} \subset \mathbf{Q}(\lambda)$ is onvertakt bij $p$. Er zijn $p-1$ andere deellichamen van graad $p$ over $\mathbf{Q}$, die elk volledig vertakt zijn bij $p$. Als $K$ zo'n deellichaam is, wordt $K$ voortgebracht over $\mathbf{Q}$ door het spoor van $\eta \cdot \lambda$ naar $K$; het minimumpolynoom van dit spoor heeft de vorm

$$X^p - \binom{p}{2} q X^{p-2} + (\text{termen van lagere graad die van } K \text{ afhangen}).$$

**8.** In kabouterland staat een gevangenis waarvan de cellen genummerd zijn met de reële getallen. In elke cel zit een kabouter, met zijn celnummer op zijn boevenpak. Op een dag roept de koningin alle kabouters naar de binnenplaats en stelt hen zó op dat elke kabouter alle andere op aftelbaar veel na kan zien. (Als een kabouter een andere kan zien, is het niet vanzelf zo dat de tweede de eerste ook kan zien.) Daarna krijgt elke kabouter ofwel een rode ofwel een blauwe puntmuts op, die hijzelf niet kan zien, en een vel papier met onbeperkte capaciteit, waarop hij mag schrijven wat hij wil; dit kan gelezen worden door elke kabouter die hem kan zien. Op het teken van de koningin moeten alle kabouters tegelijk ieder 'rood' of 'blauw' zeggen. De kabouters die de kleur van hun eigen puntmuts noemen, worden vrijgelaten. Is er voor elke opstelling minstens één kabouter die zeker is van zijn redding, hoe de koningin de puntmutsen ook verdeelt?

De bovenstaande vraag is niet beantwoordbaar vanuit het gebruikelijke Zermelo–Fraenkel-axiomastelsel met het keuzeaxioma.

**9.** Dat wiskundigen het over het algemeen zonder een spier te vertrekken hebben over *perfecte lichamen*, *radicale idealen* en *blowing up the plane in six points*, heeft weinig met pokergezichten te maken.

**10.** Het zou de moeite waard zijn als er binnen de academische cultuur, in plaats van een vanzelfsprekende bevordering van het Engels als lingua franca, meer gedaan zou worden om een zekere taaldiversiteit te bewaren. Het woord 'moeite' is hier bewust gekozen.

**11.** Als neveneffect van het succes van de wetenschap kan ten onrechte de indruk ontstaan dat het tot haar doelen behoort zoiets als een wetenschappelijk mens- en wereldbeeld te construeren.

**12.** Op het eiland Kaua'i hebben architecten het makkelijker dan wiskundigen: de hoogten van hun constructies zijn uniform begrensd.