Kleiner maken van binaire vormen.

BSc-project. Begeleider: Marco Streng

Een **binaire vorm** is een homogeen polynoom in twee variabelen, zoals

$$\begin{aligned} f = \ & 389563013118404936902656613482370301436284913062096870883427309559 76\ X^6 \\ & + 83853419742316763942127252814649835964165153930406595462369589996 1041\ X^5Z \\ & + 75206018941964418941076033379844863952217222080650297032788470407528 74\ X^4Z^2 \\ & + 35973537648466058783566365210341872099879116742459308573671342028630076\ X^3Z^3 \\ & + 96791277998458685042239493022180105321183100932676702721797229646064456\ X^2Z^4 \\ & + 13889545273527870633338971427934915604340787142382030561908039751656560 2\ XZ^5 \\ & + 83047887464118272394504416684068431409615867045083754396559720862496820\ Z^6 \end{aligned}$$

of

$$g = X^5Z + 3X^4Z^2 - 2X^3Z^3 - 6X^2Z^4 + 3XZ^5 + Z^6 \in \mathbf{Z}[X, Z].$$

Deze twee voorbeelden van binaire vormen zijn **equivalent**, in de zin dat ze uit elkaar te verkrijgen zijn door middel van een $\mathbf{Z}$-lineaire verandering van variabelen:

$$g = f(816549163549X + 146986510561Z, -227609574056X - 40971858835Z).$$

Vraag: als iemand je een binaire vorm geeft, hoe vind je dan een lineaire verandering van variabelen die een zo 'klein' mogelijke equivalente binaire vorm oplevert?

Toepassing: In mijn onderzoek komen bijvoorbeeld complex-analytische constructies voor waaruit polynomen zoals f komen, terwijl voor praktische toepassingen kleine polynomen als g veel bruikbaarder zijn. Het antwoord op de vraag is daarvoor dus nuttig. Die praktische toepassingen vindt men rond algebraïsche krommen, cryptografie en algebraïsche getaltheorie, maar komen in dit project niet aan bod. De technieken die wel aan bod komen zijn vooral gerelateerd aan de vakken Algebra 1 en 2 en geven een voorproefje van dingen die je later bij vakken over algebraïsche getaltheorie en modulaire vormen in meer detail kan leren.

Het antwoord op de vraag wordt voor binaire vormen over $\mathbf{Z}$ gegeven door een algoritme van Stoll en Cremona [2].

In dit project bestudeer je eerst [2], en daarna:

(1) Stoll en Cremona geven in [2] al aan dat een variant van hun methode ook werkt voor bepaalde andere getallenringen. Werk dit uit voor $\mathbf{Z}[\sqrt{-1}]$.

(2) Mogelijk vervolg op (1): kun je voor $\mathbf{Z}[\sqrt{-1}]$ ook bewijzen dat je de kleinste equivalente vorm kan vinden, zoals voor $\mathbf{Z}$ wordt gedaan door Hutz en Stoll [1]?

(3) Mogelijk vervolg op (1): nu algemene(re) imaginair kwadratische getallenringen, zoals $\mathbf{Z}[\zeta_3]$ en $\mathbf{Z}[\sqrt{-2}]$.

(4) Mogelijk vervolg op (1): programmeer dit in het open source softwarepakket SageMath.

Referenties:

[1] Benjamin Hutz and Michael Stoll. Smallest representatives of $\mathrm{SL}(2, \mathbf{Z})$-orbits of binary forms and endomorphisms of $\mathbf{P}^1$. *Acta Arith.*, 189(3):283–308, 2019.

[2] Michael Stoll and John E. Cremona. On the reduction theory of binary forms. *J. Reine Angew. Math.*, 565:79–99, 2003.

Appendix: meer details.

Voor wie nu al wat details wil zien, vat ik hier kort de methode van [2] samen.

We kunnen lineaire verandering van variabelen zien als een werking van de groep $\mathrm{SL}_2(\mathbf{Z}) = \{M \in \mathbf{Z}^{2\times 2} : \det(M) = 1\}$ op de verzameling $B_n \subset \mathbf{Z}[X, Z]$ van homogene polynomen van graad n. Dezelfde groep werkt op het *bovenhalfvlak* $\mathcal{H} = \{\tau \in \mathbf{C} : \mathrm{Im}(\tau) > 0\}$ door

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \frac{a\tau + b}{c\tau + d}.$$

Deze laatste werking is belangrijk in de theorie van modulaire vormen, en er is bekend dat elke baan hooguit twee elementen bevat van het *fundamentele domein*

$$\mathcal{F} = \left\{ \tau \in \mathcal{H} : \begin{array}{l} |\tau| \geq 1, \\ |\mathrm{Re}(\tau)| \leq \frac{1}{2}, \end{array} \right\}.$$

Bovendien bestaat er een snel algoritme dat voor elke $\tau \in \mathcal{H}$ een element $A \in \mathrm{SL}_2(\mathbf{Z})$ vindt met $A \cdot \tau \in \mathcal{F}$.

Stoll en Cremona geven een afbeelding van $\mathrm{SL}_2(\mathbf{Z})$-verzamelingen

$$z : B_n \to \mathcal{H},$$

en hun algoritme is als volgt. Gegeven $f \in B_n$, bereken een $A \in \mathrm{SL}_2(\mathbf{Z})$ met $A \cdot z(F) \in \mathcal{F}$. Voor $g = A \cdot F$ geldt dan $z(g) = A \cdot z(f) \in \mathcal{F}$ en dit is volgens [1] één van de 'kleinste' elementen van de baan van F.

Voor (1) moet gekeken worden naar een werking van $\mathrm{SL}_2(\mathbf{Z}[i])$ op een zeker driedimensionaal analogon van $\mathcal{H}$.