rijksuniversiteit groningen
faculteit wiskunde en natuurwetenschappen

De Mahler-maat

Bacheloronderzoek Wiskunde

April 2015

Student: T. Zijlstra

Eerste begeleider: Prof.dr. J. Top

Tweede begeleider: Dr.ir. F.W. Wubs

Samenvatting

We definiëren de Mahler-maat voor polynomen en leiden enkele eigenschappen af. Het probleem van Lehmer gaat over het vinden van een ondergrens voor deze maat. We bespreken enkele resultaten richting de oplossing van dit nog onopgeloste probleem en maken een algoritme om dit probleem voor vaste graad op te lossen.

Inhoudsopgave

Inleiding

De Mahler-maat werd geïntroduceerd door de Duitse wiskundige Kurt Mahler in [1]. Mahler, die nog twee jaar aan de universiteit van Groningen heeft gewerkt, gebruikte afschattingen van de Mahler-maat in de theorie van transcendente getallen. In 1933 schetste Lehmer het probleem van het vinden van lage waarden van de Mahler-maat. De laagste waarde die hij destijds vond, geldt nog steeds als ondergrens. In deze scriptie onderzoeken we methoden om een ondergrens te vinden.

1. Definities en notaties

Een polynoom met coëfficiënten $a_0, a_1, ..., a_{n-1}, a_n \in \mathbb{Z}$ wordt gegeven door:

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0. \tag{1}$$

Een polynoom wordt *monisch* genoemd als de kopcoëfficiënt a_n gelijk is aan 1. In deze scriptie wordt vooral geschreven over polynomen van de vorm (1) met $a_n = 1$. Een monische polynoom in $\mathbb{Z}[X]$ wordt hier daarom simpelweg een *polynoom* genoemd.
De reciproke $\hat{P}(x)$ van $P(x)$ wordt gegeven door:

$$\begin{aligned} \hat{P}(x) &= x^n P(\frac{1}{x}) \\ &= a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n. \end{aligned}$$

We noemen $P(x)$ *zelf-reciprook* als $P(x) = \hat{P}(x)$ of $P(x) = -\hat{P}(x)$.
De polynoom die wordt gegeven door (1) heeft n nulpunten $\alpha_i \in \mathbb{C}$ en kan geschreven worden als:

$$P(x) = \prod_{i=1}^{n}(x - \alpha_i). \tag{2}$$

Uit de definitie van reciproke polynomen volgt dat $\alpha_1^{-1}, \ldots, \alpha_n^{-1}$ precies de nulpunten van $\hat{P}(x)$ zijn, mits $P(0) \neq 0$.

1.1. Definitie van de Mahler-maat.

De Mahler-maat $M(P)$ van de polynoom (2) is als volgt gedefinieerd:

$$M(P) = \prod_{i=1}^{n} \max\{1, |\alpha_i|\}. \tag{3}$$

De waarde $M(P)$ hangt af van de absolute waarde van de nulpunten die buiten de eenheidscirkel liggen. De Mahler-maat van een polynoom $P(x)$ met kopcoëfficiënt -1 is gedefiniëerd als $M(P) = M(-P)$.

Voorbeeld 1.1. De polynoom $x^3 + x + 2$ heeft nulpunten

$$\alpha_1 = -1, \alpha_2 = \frac{1}{2} + \frac{i}{2}\sqrt{7}, \alpha_3 = \frac{1}{2} - \frac{i}{2}\sqrt{7}.$$

Van deze nulpunten liggen alleen de laatste twee buiten de eenheidscirkel, dus:

$$M(x^3 + x + 2) = |\frac{1}{2} + \frac{i}{2}\sqrt{7}||\frac{1}{2} - \frac{i}{2}\sqrt{7}| = 2.$$

1.2. **Het probleem van Lehmer.** D.H. Lehmer vroeg zich af of er een constante $\epsilon > 0$ bestond zodat $M(P) > 1 + \epsilon$ voor elke $P(x)$ met $M(P) \neq 1$. Daarop begon hij te zoeken naar polynomen met $M(P)$ dicht bij de 1. De laagste waarde die hij vond, was $M(P) = 1.176\ldots$, voor de zelf-reciproke polynoom gegeven door:

$$P_l(x) = x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1. \tag{4}$$

Sinds deze vondst is er geen enkele polynoom $P(x)$ gevonden waarvoor geldt

$$1 < M(P) < M(P_l).$$

Of er een dergelijke polynoom bestaat, is nog onbekend. Wel zijn er pogingen gedaan om een ondergrens te geven voor $M(P)$. Een van de eerste resultaten werd gegeven door Breusch [3], waarin wordt aangetoond dat $M(P) > 1.179$ voor niet-reciproke polynomen. In [5] wordt deze ondergrens verbeterd tot $M(P) > 1.32$. Dit resultaat zal in hoofdstuk 8 worden besproken. Voor polynomen met oneven coëfficiënten wordt in [6] het vraagstuk van Lehmer opgelost.

1.3. **Eigenschappen van $M(P)$.** Als $P(x)$ reducibel is, dan kan de polynoom geschreven worden als product van twee polynomen met graad ongelijk aan nul:

$$P(x) = Q_1(x)Q_2(x).$$

De nulpunten van $P(x)$ zijn de nulpunten van $Q_1(x)$ samen met die van $Q_2(x)$, dus er geldt

$$M(P) = M(Q_1)M(Q_2). \tag{5}$$

De Mahler-maat is voor elke polynoom groter dan of gelijk aan 1, dus $M(P)$ is groter dan of gelijk aan zowel $M(Q_1)$ als $M(Q_2)$.

Lemma 1.2. Als $M(P) < 2$ en $P(x)$ is irreducibel, dan $|P(0)| = 1$ of $P(x) = x$.

Bewijs: De coëfficiënt $a_0 = P(0) \in \mathbb{Z}$ is ongelijk aan nul, want anders geldt: $x|P(x)$. Uit vergelijkingen (1) en (2) volgt dat het product van de absolute waarden van alle nulpunten gelijk moet zijn aan $|a_0|$. Dus:

$$2 > M(P) = \prod_{i=1}^{n} \max\{1, |\alpha_i|\} \geq \prod_{i=1}^{n} |\alpha_i| = |a_0|.$$

Dan moet a_0 in absolute waarde wel gelijk zijn aan 1. ☺
We zijn op zoek naar polynomen met een kleine Mahler-maat en daarom richten we ons vanaf hier op irreducibele polynomen met $P(0) = \pm 1$.

Lemma 1.3. Laat $\hat{P}(x)$ de reciproke van $P(x)$ zijn. Dan:

$$M(\hat{P}) = M(P).$$

Bewijs: De nulpunten van de n-degraadspolynoom $P(x)$ zijn $\alpha_1, \alpha_2, ..., \alpha_n$. De constante term is gelijk aan ± 1. Uit (2) volgt dat: $\prod_{i=1}^{n} \alpha_i = \pm 1$. We rangschikken deze nulpunten zodanig dat, voor zekere $k \in \{0, 1, ..., n\}$ geldt: $|\alpha_i| < 1$ voor $0 \leq i \leq k$ en $|\alpha_i| \geq 1$ voor $k < i \leq n$. Dan kan $M(P)$ geschreven worden als:

$$M(P) = \prod_{i=1}^{n} \max\{1, |\alpha_i|\} = \prod_{i=k+1}^{n} |\alpha_i|.$$

Voor de reciproke $\hat{P}(x)$:

$$M(\hat{P}) = \prod_{i=1}^{n} \max\{1, |\frac{1}{\alpha_i}|\} = \prod_{i=1}^{k} |\frac{1}{\alpha_i}|.$$

Dan is het quotiënt:

$$\begin{aligned} \frac{M(P)}{M(\hat{P})} &= \frac{\prod_{i=k+1}^{n} |\alpha_i|}{\prod_{j=1}^{k} |\frac{1}{\alpha_j}|} \\ &= \prod_{i=k+1}^{n} |\alpha_i| \prod_{j=1}^{k} |\alpha_j| \\ &= \prod_{i=1}^{n} |\alpha_i| \\ &= 1. \end{aligned}$$

Dus $M(P) = M(\hat{P})$. ☺

Er zijn meer manieren waarop de maten van twee verschillende polynomen gelijk aan elkaar kunnen zijn. Een voorbeeld hiervan wordt uitgelegd in het volgende lemma.

Lemma 1.4. Als $Q(x) = P(x^k)$ voor een gehele $k \geq 2$, dan

$$M(Q) = M(P).$$

Bewijs: Als de graad van $P(x)$ gelijk is aan n, dan is graad$(Q) = nk$. Laat α een nulpunt zijn van $P(x)$ en β een k-demachtswortel van α. Dan:

$$Q(\beta) = P(\beta^k) = P(\alpha) = 0$$

dus de k-demachtswortels van α zijn nulpunten van $Q(x)$. Als $|\alpha| > 1$ dan zijn al zijn k wortels in absolute waarde ook groter dan 1. Het product van de absolute waarden van die wortels is weer gelijk aan α. Dus:

$$M(Q) = \prod_{j=1}^{nk} \max\{1, |\beta_j|\} = \prod_{i=1}^{n} \max\{1, |\alpha_i|\} = M(P)$$

☺

2. Cyclotomische polynomen

In dit hoofdstuk onderzoeken we welke polynomen een Mahler-maat gelijk aan 1 hebben. Het resultaat 2.7 is een gevolg van een stelling van Kronecker, die we verderop bewijzen. Eerst definiëren we cyclotomische polynomen aan de hand van primitieve eenheidswortels.

Definitie 2.1. Een n-de eenheidswortel is een $\gamma \in \mathbb{C}$ met $\gamma^n = 1$ voor een geheel getal n.

De groep van n-de eenheidswortels is een cyclische groep. De voortbrengers van deze groep noemen we *primitieve* n-de eenheidswortels.

Definitie 2.2. De n-de cyclotomische polynoom $g_n(x)$ is gedefiniëerd als:

$$g_n(x) = (x - \gamma_1)(x - \gamma_2)...(x - \gamma_k). \tag{6}$$

Waarbij $\gamma_1, \gamma_2, ..., \gamma_k$ de n-de primitieve eenheidswortels zijn.

We zullen verderop laten zien dat g_n een monisch polynoom met gehele coëfficiënten is. Uit de definitie volgt direct dat $M(g_n) = 1$.

Voorbeeld 2.3. De 3-de eenheidswortels zijn oplossingen van de vergelijking: $x^3 - 1 = 0$. De wortels zijn:

$$z_1 = 1, z_2 = \frac{-1 - i\sqrt{3}}{2}, z_3 = \frac{-1 + i\sqrt{3}}{2}$$

en er geldt: $z_2 z_3 = 1$ en $z_2^2 = z_3$. Dus z_2 en z_3 zijn voortbrengers van de cyclische groep. De 3-de cyclotomische polynoom is:

$$g_n(x) = (x - \frac{-1 - i\sqrt{3}}{2})(x - \frac{-1 + i\sqrt{3}}{2}) = x^2 + x + 1.$$

Om te laten zien dat elke $g_n(x)$ in $\mathbb{Z}[X]$ zit, maken we gebruik van het lemma van Gauss.

Lemma 2.4. Laat $f \in \mathbb{Z}[X]$ een monisch polynoom zijn. Als er monische polynomen $g(x)$ en $h(x)$ in $\mathbb{Q}[X]$ bestaan zodat $f = g \times h$, dan: $g, h \in \mathbb{Z}[X]$.

Een bewijs van dit lemma kan gevonden worden in [4].

Stelling 2.5. Cyclotomische polynomen zijn monisch en hebben gehele coëfficiënten.

Bewijs:
De polynoom $x^n - 1$ heeft alle n-de eenheidswortels als nulpunten. De n-de niet-primitieve eenheidswortels $\{\gamma_{k+1}, \ldots, \gamma_n\}$ hebben een orde die een deler is van n en ongelijk is aan n. Als orde$(\gamma_j) = m$ dan is γ_j een m-de primitieve eenheidswortel en dus een nulpunt van de m-de cyclotomische polynoom. Andersom geldt dat iedere m-de primitieve eenheidswortel een n-de niet-primitieve eenheidswortel is als $m|n$ en $m \neq n$. De polynoom $x^n - 1$ kan daarom geschreven worden als product van cyclotomische polynomen:

$$x^n - 1 = g_n(x) \prod_{m|n} g_m(x) \tag{7}$$

Het is duidelijk dat $g_1(x) = (x - 1) \in \mathbb{Q}[X]$. Hieruit volgt dat voor elke n de n-de cyclotomische polynoom in $\mathbb{Q}[X]$ zit. Uit het lemma van Gauss volgt dan dat $g_n(x)$ gehele coëfficiënten heeft.

☺

In stelling 2.7 beweren we dat $M(P) = 1$ alleen maar mogelijk is als $P(x)$ een product van cyclotomische polynomen is. Om dit te bewijzen gebruiken we de hoofdstelling over symmetrische polynomen.

2.1. **Symmetrische polynomen.** Een polynoom $f \in \mathbb{Z}[X_1, ..., X_n]$ is symmetrisch als f in zichzelf overgaat bij alle permutaties van $X_1, ..., X_n$ [4]. De elementaire symmetrische polynomen $\sigma_k(X_1, ..., X_n)$ worden gedefiniëerd als de coëfficiënten van:

$$\begin{aligned} f(z) &= \prod_{i=1}^{n}(z - X_i) \\ &= z^n - \sigma_1 z^{n-1} + \cdots + (-1)^n \sigma_n. \end{aligned}$$

Dus $\sigma_1 = X_1 + ... + X_n$, $\sigma_2 = \sum_{i,j} X_i X_j$ enzovoort: $\pm\sigma_k$ geeft de $n-k$-de coëfficiënt van $f(z)$ als functie van de X_i's. Het is duidelijk dat elke σ_k een symmetrische polynoom in $\mathbb{Z}[X_1, \ldots, X_n]$ is. De hoofdstelling van symmetrische polynomen luidt:

Stelling 2.6. Elke symmetrische polynoom $f \in \mathbb{Z}[X_1, \ldots, X_n]$ is te schrijven als polynoom in de elementaire symmetrische polynomen $\sigma_1, ..., \sigma_n$ met coëfficiënten uit $\mathbb{Z}$.

Een bewijs van deze stelling wordt gegeven in [4].

Stelling 2.7. $M(P) = 1$ dan en slechts dan, als alle nulpunten van $P(x)$ eenheidswortels zijn.

Bewijs: Eerder werd al opgemerkt dat de ($\Longleftarrow$)-richting per definitie waar is: als alle nulpunten van $P(x)$ eenheidswortels zijn dan liggen de nulpunten op de eenheidscirkel.
Het bewijs de andere kant op ($\Longrightarrow$) is minder triviaal:
We nemen aan dat $M(P) = 1$. Dan moet het zo zijn dat alle nulpunten op of binnen de eenheidscirkel liggen. We schrijven:

$$P(x) = x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 = \prod_{i=1}^{n}(x - \alpha_i). \qquad (8)$$

Het aantal polynomen van graad n met alle nulpunten in of op de eenheidscirkel is eindig. Dit volgt uit het gegeven dat voor de nulpunten $\alpha_1, \ldots, \alpha_n$ van zo'n polynoom geldt: $|\alpha_k| \leq 1$ voor $1 \leq k \leq n$. De coëfficiënten zijn dan af te schatten door de rechterzijde van (8) volledig

uit te werken:

$$\begin{aligned} |a_0| &= |\alpha_1\alpha_2...\alpha_n| \leq 1 \\ &\vdots \\ |a_{n-k}| &= \sum_{1\leq i_1\leq\cdots\leq i_k\leq n} |\alpha_{i_1}...\alpha_{i_k}| \leq \binom{n}{k} \\ &\vdots \\ |a_{n-1}| &= |\sum_{k=1}^{n} \alpha_k| \leq \binom{n}{n-1}. \end{aligned} \tag{9}$$

We definiëren voor $k \in \mathbb{N}$ de polynoom:

$$f_k(x) = \prod_{i=1}^{n}(x - \alpha_i^k). \tag{10}$$

Om te laten zien dat de coëfficënten van $f_k(x)$ geheel zijn, definiëren we:

$$h_i^{(k)}(x_1, ..., x_n) := \sigma_i(x_1^k, \ldots, x_n^k)$$

zodat de coëfficiënten van f_k worden gegeven door $h_i^{(k)}(\alpha_1, \ldots, \alpha_n)$ voor $1 \leq i \leq n$. Deze polynoom is duidelijk symmetrisch en dus volgens Stelling 2.6 bestaat $g_{i,k} \in \mathbb{Z}[X_1, \ldots, X_n]$ zodat:

$$h_i^{(k)}(x_1, \ldots, x_n) = g_{i,k}(\sigma_1, \ldots, \sigma_n).$$

We weten dat $\sigma_i(\alpha_1, \ldots, \alpha_n)$ voor elke i een geheel getal is, want dit is de $n - i$-de coëfficiënt van (8). De functie $g_{i,k}(x_1, \ldots, x_2)$ heeft gehele coëfficiënten dus is ook de waarde van $g_{i,k}(\sigma_1, \ldots, \sigma_n)$ een geheel getal. Daarom geldt voor de coëfficiënten van $f_k(x)$:

$$a_{n-i}^{(k)} = h_i^{(k)}(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}.$$

Dus voor elke $k \in \mathbb{N}$ is (10) een polynoom met gehele coëfficiënten. Bovendien heeft elke $f_k(x)$ al zijn nulpunten op of binnen de eenheidscirkel, want: $|\alpha_i^n| \leq |\alpha_i| \leq 1$. Het aantal polynomen van graad n met die eigenschap is eindig, dus er is een gehele $m > k$ te vinden zodat $f_k = f_m$. De nulpunten $\alpha_0^m, \alpha_1^m, ..., \alpha_n^m$ van $f_m(x)$ zijn, op permutatie van de indices na, gelijk aan de nulpunten $\alpha_0^k, \alpha_1^k, ..., \alpha_n^k$ van $f_k(x)$ [8]. Er bestaat een permutatie σ zodat, voor alle $1 \leq i \leq n$:

$$\alpha_i^m = \alpha_{\sigma(i)}^k.$$

Dan:

$$\alpha_i^{m^2} = (\alpha_{\sigma(i)}^k)^m = (\alpha_{\sigma(i)}^m)^k = \alpha_{\sigma(\sigma(i))}^{k^2}.$$

Als de orde van de permutatie σ gelijk is aan r, dan:

$$\alpha_i^{m^r} = \alpha_{\sigma(\ldots(\sigma(i)))}^{k^r} = \alpha_i^{k^r}.$$

Alle α_i's zijn ongelijk aan nul dus we kunnen beide zijden delen door $\alpha_i^{k^r}$:

$$\alpha_i^{m^r - k^r} = 1.$$

De exponent $m^r - k^r$ is een positief, geheel getal ongelijk aan 0, dus elk nulpunt α_i is een eenheidswortel.

☺

In het vervolg zullen we vanwege het bovenstaande resultaat de cyclotomische polynomen negeren bij het zoeken naar polynomen met lage $M(P)$-waarden.

3. Kwadratische polynomen

Gegeven de irreducibele polynoom:

$$P(x) = x^2 + ax + b. \tag{11}$$

Op grond van lemma 1.2 mogen we ons beperken tot het geval $b = \pm 1$. De discriminant van (11) wordt gegeven door: $D = a^2 - 4b$. Voor de waarde van deze discriminant onderscheiden we drie gevallen:
In het eerste geval is de discriminant negatief: $D < 0$. Dat betekent dat $P(x)$ twee niet-reële nulpunten heeft. Als $P(\alpha) = 0$ dan is het andere nulpunt bij $x = \bar{\alpha}$:

$$P(\bar{\alpha}) = \overline{P(\alpha)} = \bar{0} = 0.$$

De twee nulpunten zijn elkaars complex geconjugeerde. De polynoom kan worden herschreven als:

$$P(x) = (x - \alpha)(x - \bar{\alpha}) = x^2 - (\alpha + \bar{\alpha})x + \alpha\bar{\alpha}. \tag{12}$$

Als we aannemen dat α buiten de eenheidscirkel ligt, dan is de Mahlermaat: $M(P) = |\alpha||\bar{\alpha}| = |\alpha|^2 = |b| = 1$. Alle kwadratische polynomen met $M(P) < 2$ en een negatieve discriminant zijn dus producten van cyclotomische polynomen.

In het tweede geval is de discriminant gelijk aan nul: $a^2 - 4b = 0$. Dan is $P(x)$ reducibel en dus $M(P) < 2 \implies M(P) = 1$.
In het derde geval is de discriminant positief en heeft $P(x)$ twee verschillende reële nulpunten α en β:

$$P(x) = (x - \alpha)(x - \beta) = x^2 - (\alpha + \beta)x + \alpha\beta. \tag{13}$$

Als $1 \leq |\alpha| \leq |\beta|$ dan $M(P) = |\alpha||\beta| = |b| = 1$.

Als $|\alpha| \leq 1 \leq |\beta|$ dan $M(P) = |\beta| \geq |\alpha\beta| = |b| = 1$. Voor de coëfficiënt a geldt dan:

$$0 \neq |a| = |\alpha + \beta| < 1 + 2 = 3.$$

Er blijven $4 \times 2 = 8$ tweedegraads polynomen over die mogelijk $M(P) < 2$ hebben. Met behulp van Maple blijkt dat $M(x^2 + x - 1) = 1,618...$ de enige waarde voor $M(P)$ kleiner dan 2 is. Dus als $P(x)$ kwadratisch is en $M(P) \neq 1$, dan:

$$M(P) \geq M(x^2 - x - 1) = 1,618... \tag{14}$$

4. Derdegraadspolynomen

We schrijven de irreducibele derdegraadspolynoom als:

$$P(x) = x^3 + ax^2 + bx + c. \tag{15}$$

Net als bij kwadratische polynomen is de discriminant voor (15) gedefiniëerd. In het algemeen [4]:

Definitie 4.1. De discriminant van een (monische) n-degraadspolynoom met nulpunten $\alpha_1, \alpha_2, \ldots, \alpha_n$ wordt gegeven door:

$$D(P) = \prod_{1 \leq i \leq j \leq n} (\alpha_i - \alpha_j)^2. \tag{16}$$

Omdat $D(P)$ een symmetrisch polynoom in $\mathbb{Z}[X]$ in de α_i's is, kan men deze uitdrukken in de coëfficiënten van $P(x)$. Dit geeft de discriminant voor (11): $D = a^2 - 4b$ en voor het geval van graad 3 (15): $D = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc$. Vanuit de definitie is direct te zien dat een discriminant alleen nul is als $P(x)$ een nulpunt van multipliciteit groter dan 1 heeft. Bovendien geldt: $D > 0$ dan en slechts dan als alle 3 nulpunten reëel zijn. En $D < 0$ dan en slechts dan als $P(x)$ 1 reëel nulpunt heeft en een paar niet-reële nulpunten.

Als $D < 0$, dan heeft $P(x)$ twee niet-reële nulpunten α en $\bar{\alpha}$ en een reëel nulpunt β. Liggen alle nulpunten op of buiten de eenheidscirkel, dan $M(P) = |\alpha|^2|\beta| = |c| = 1$. Er geldt dus weer $M(P) \geq 2$ als $M(P) \neq 1$.

Polynomen waarvoor geldt $1 < M(P) < 2$ zijn wel te vinden als een nulpunt binnen de eenheidscirkel ligt en de andere twee erbuiten. Of andersom, als: $|\alpha| \leq 1 \leq |\beta|$. Het maakt voor de waarde van $M(P)$ geen verschil welke van de nulpunten binnen S^1 liggen. Als namelijk $|\beta| \leq 1 \leq |\alpha|$ dan heeft de reciproke polynoom nulpunten bij $\frac{1}{\alpha}$ en $\frac{1}{\bar{\alpha}}$, die beide binnen S^1 liggen en als derde nulpunt $\frac{1}{\beta}$, buiten de eenheidscirkel. Volgens 1.3 geldt $M(\hat{P}) = M(P)$, dus we kunnen aannemen dat

$|\alpha| \leq 1 \leq |\beta|$. Dan:

$$M(P) = |\beta| = |\frac{c}{|\alpha|^2}| \geq |c|. \tag{17}$$

Voor elke derdegraadspolynoom $P(x)$ met $P(0) = c$ is de polynoom die wordt gegeven door $\tilde{P}(x) = -P(-x)$ monisch en heeft constante term $\tilde{P}(0) = -c$ en geldt: $M(P) = M(\tilde{P})$. We kunnen dus aannemen dat $c = 1$.

Als $M(P) < 2$ dan kunnen we dus schrijven:

$$P(x) = x^3 + ax^2 + bx + 1. \tag{18}$$

De polynoom is gelijk aan zijn reciproke als $a = b$. Dan is er een nulpunt bij $x = -1$:

$$P(-1) = (-1)^3 + a(-1)^2 + a(-1) + 1 = 0.$$

En dus bestaat er een monische polynoom $Q(x)$ zodat $P(x) = (x + 1)Q(x)$. Maar we hebben aangenomen dat $P(x)$ irreducibel is, dus zelfreciproke derdegraadspolynomen met $D < 0$ hebben $M(P) \geq 2$. Om te achterhalen voor welke coëfficiënten a en b de polynoom (18) een Mahler-maat kleiner dan 2 kan hebben, gebruiken we vergelijking (17) en het feit dat $1 = c = -\alpha\bar{\alpha}\beta$ en $|\alpha| \leq 1$:

$$\begin{aligned} |b| &= |\alpha\bar{\alpha} + \alpha\beta + \bar{\alpha}\beta| \\ &= ||\alpha|^2 + \frac{-1}{\alpha\bar{\alpha}}(\alpha + \bar{\alpha})| \\ &= ||\alpha|^2 - \frac{2Re(\alpha)}{|\alpha|^2}| \\ &\leq 1 + 2 \\ &= 3. \end{aligned}$$

De gelijkheid kan alleen gelden als $\alpha = Re(\alpha)$, wat niet het geval is omdat $D < 0$. Daarom is de ongelijkheid strict: $|b| < 3$. Op dezelfde manier is de coëfficiënt a af te schatten. Als $M(P) = |\beta| < 2$, dan:

$$\begin{aligned} |a| &= |\alpha + \bar{\alpha} + \beta| \\ &< |2Re(\alpha)| + 2 \\ &\leq 4. \end{aligned}$$

Nu alle coëfficiënten zijn bepaald of afgeschat, blijft er een eindig aantal derdegraadspolynomen over waarvoor mogelijk is dat $M(P) < 2$. Het aantal polynomen van de vorm (18) met $a \in \{-3, -2, -1, 0, 1, 2, 3\}$ en $b \in \{-2, -1, 0, 1, 2\}$, die -1 niet als nulpunt hebben, is: $7 \times 5 - 5 =$

30. Van deze 30 mogelijkheden blijken, na een controle met Maple, in totaal 8 niet-cyclotomische polynomen een Mahler-maat kleiner dan 2 te hebben. De laagste waarde is $M(x^3 - x^2 + 1) = 1,324....$ In het geval dat alle drie nulpunten van (15) reëel zijn, is dit aantal volgens dezelfde methode af te schatten. De gevonden ondergrens blijft gelijk, dus voor kubische polynomen in het algemeen:

$$M(P) \neq 1 \implies M(P) \geq M(x^3 - x^2 + 1) = 1,324...$$

5. n-degraadspolynomen met lage Mahler-maat

5.1. **Afschatten van coëfficiënten.** De methode die in de voorgaande hoofdstukken is gebruikt om de ondergrens van $M(P)$ te bepalen is eenvoudig: voor alle polynomen die mogelijk $M(P) < 2$ hebben, berekenen we $M(P)$ en uiteindelijk is het minimum van de gevonden waarden de kleinst mogelijke Mahler-maat voor graad 3. Deze methode werkt omdat er maar een eindig aantal polynomen bestaan met $M(P) < 2$ en graad$(P) = 3$. In dit hoofdstuk generaliseren we deze methode. We schrijven de n-degraadspolynoom:

$$P(x) = \sum_{i=0}^{n} a_i x^i = \prod_{i=1}^{n} (x - \alpha_i). \tag{19}$$

We nemen aan dat $M(P) < 2$ en gaan de rechterzijde van (19) uitwerken op dezelfde manier als in het bewijs van stelling 2.7. Elk product van de nulpunten is in absolute waarde kleiner dan of gelijk aan $M(P)$. Dan geldt voor de coëfficiënten van $P(x)$:

$$\begin{aligned}
|a_0| &= |\alpha_1 \alpha_2 ... \alpha_n| \leq M(P) < 2 \\
&\vdots \\
|a_{n-k}| &= \sum_{1 \leq i_1 \leq \cdots \leq i_k \leq n} |\alpha_{i_1} ... \alpha_{i_k}| \leq \binom{n}{k} M(P) < 2\binom{n}{k} \\
&\vdots \\
|a_{n-1}| &= |\sum_{k=1}^{n} \alpha_k| \leq \binom{n}{n-1} M(P) < 2\binom{n}{n-1}.
\end{aligned}$$

Elke coëfficiënt a_k zit dus in de verzameling:

$$A_k := \{-2\binom{n}{k} + 1, -2\binom{n}{k} + 2, \ldots, 0, 1, \ldots, 2\binom{n}{k} - 1\}.$$

Het totaal aantal keuzes voor de k-de coëfficiënt is $\#A_k = 4\binom{n}{k} - 1$. Er is dan een totaal aantal van $d(n)$ keuzes voor polynomen van graad n

met mogelijk $M(P) < 2$:

$$d(n) = \prod_{k=0}^{n-1} \#A_k = \prod_{k=0}^{n-1} (4\binom{n}{k} - 1). \tag{20}$$

Voorbeeld 5.1. Gegeven de vierdegraadspolynoom $P(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ met $M(P) < 2$. Dan weten we van de coëfficiënten dat:

$$\begin{aligned} |a_3| &< 2\binom{4}{3} = 8 \\ |a_2| &< 2\binom{4}{2} = 12 \\ |a_1| &< 2\binom{4}{1} = 8 \\ |a_0| &< 2\binom{4}{0} = 2. \end{aligned} \tag{21}$$

De coëfficiënten kunnen $d(4) = 15 \times 23 \times 15 \times 3 = 15.525$ verschillende polynomen vormen. De ondergrens van $M(P)$ voor vierdegraadspolynomen is de laagste waarde van $M(P)$ ongelijk aan 1 die wordt bereikt voor een polynoom die voldoet aan (21).

Het aantal $d(n)$ stijgt snel met het verhogen van de graad: $d(5)$ is al groter dan een miljoen. Om voor een graad n de ondergrens van $M(P)$ te bepalen, moet er $d(n)$ maal de Mahler-maat van een n-degraadspolynoom worden berekend. Met voldoende rekenkracht is dit natuurlijk mogelijk, maar we kunnen het aantal benodigde berekeningen fors inperken door het volgende op te merken:

(1) $M(P(x)) = M(-P(x))$
(2) $M(P(x)) = M(\hat{P}(x))$
(3) $M(P(x)) = M(P(-x))$
(4) $a_0 \neq 0$.

Dit betekent dat we niet alle mogelijke combinaties van de coëfficiënten hoeven na te gaan.
Hebben we eenmaal $M(P)$ berekend voor een vierdegraadspolynoom in de vorm van 5.1, dan kunnen we $P(-x)$ negeren.

$$P(-x) = x^4 - a_3x^3 + a_2x^2 - a_1x + a_0.$$

Hieruit volgt dat nog steeds alle polynomen worden nagegaan als we ons beperken tot $a_3 \geq 0$. Dan komen we de polynomen $Q(x)$ met coëfficiënt $a_3 < 0$ niet tegen, maar wel $Q(-x)$ want die heeft immers de coëfficiënt

$\tilde{a_3} = -a_3 \geq 0$. Op dezelfde manier kunnen we opmerkingen (1) en (2) gebruiken voor de reciproke:

$$\pm\hat{P}(x) = \pm(a_0x^4 + a_1x^3 + a_2x^2 + a_3x + 1).$$

We kiezen het teken zodanig dat de kopcoëfficiënt gelijk is aan 1. Bij polynomen van even graad is $\pm\hat{P}(-x)$ ook een monische polynoom die ongelijk is aan $\pm\hat{P}(x)$ als niet alle coëfficiënten van de oneven machten nul zijn. Dit zijn allemaal gevallen equivalent aan $P(x)$. Om te voorkomen dat we deze equivalente gevallen dubbel controleren, nemen we aan dat $a_3 \geq a_2$. In het voorbeeld wordt op deze manier het aantal te controleren polynomen teruggedrongen tot $2\times(8+9+\cdots+15)\times 23 = 4232$.

Voor een gegeven graad n is Lehmer's probleem op te lossen. We kunnen in principe de eindige verzameling polynomen met mogelijk een beperkte maat bepalen en vervolgens $M(P)$ berekenen voor elk van die polynomen.

5.2. **Zoeken naar de laagste waarden van $M(P)$.** Het algoritme om polynomen met lage Mahler-maat te vinden kan verbeterd worden met behulp van het resultaat van hoofdstuk 3. Voor derdegraadspolynomen hebben we de ondergrens:

$$M(P) \geq M(x^3 - x^2 + 1) = 1,324...$$

Dan is er voor elke graad $n \geq 3$ een polynoom met $M(P)$ lager dan of gelijk aan $1,324\ldots$, namelijk:

$$P_n(x) := x^{n-3}(x^3 - x^2 + 1).$$

Voor deze n-degraadspolynoom geldt: $M(P_n) = M(x^3 - x^2 + 1) = 1,324\ldots$. Bij het afschatten van de coëfficiënten kan de aanname $M(P) < 2$ dus worden vervangen door $M(P) \leq 1,324\ldots$. Dit levert een aanzienlijke verbetering op ten opzichte van (20). Het aantal polynomen waarvoor mogelijk is dat $M(P) \leq M(x^3 - x^2 + 1)$ is dan:

$$d(n) = \prod_{k=0}^{n-1} 2,648\ldots \binom{n}{k} - 1. \tag{22}$$

Hierbij mag $2,648\ldots\binom{n}{k}$ voor elke k naar beneden worden afgerond. Passen we dit toe op voorbeeld 5.1 dan blijven er nog maar $9\times 13\times 9\times 3 = 2106$ polynomen over, een verbetering met factor 5. Meer dan de helft hiervan kan overgeslagen worden op grond van de opmerkingen in de vorige paragraaf. Het aantal overgebleven polynomen is dan: $2\times 13\times(5+6+\cdots+9) = 910$. Met behulp van Maple berekenen we $M(P)$ voor elk van deze polynomen. We vinden voor graad vier

geen lagere ondergrens dan voor graad 3. De gevonden polynomen die voldoen aan $1 < M(P) \leq 1.324\ldots$ zijn producten van $P(x) = x^3 - x^2 + 1$ of $\hat{P}(\pm x)$ met de lineaire polynomen $x \pm 1$ en x.

5.3. **Selecteren van polynomen met lage maat.** Van de verzameling polynomen die we volgens deze methode zouden moeten nagaan, hebben verreweg de meesten $M(P) > 2$. Een algoritme zou dus voor onnodig veel polynomen de nulpunten moeten berekenen. Deze tijdrovende onderneming kunnen we gelukkig omzeilen met behulp van een algoritme uit [2]. Dit algoritme is gebaseerd op het volgende lemma.

Lemma 5.2. Als $M_0 \geq 1$ zo gekozen kan worden dat elke coëfficiënt a_k van de n-degraadspolynoom $P(x)$ begrensd wordt door:

$$|a_k| \leq \binom{n}{k} M_0,$$

dan wordt de lengte $L(P) = \sum_{i=0}^{n} |a_i|$ van de polynoom begrensd door:

$$M(P) \leq L(P) \leq 2^n M_0.$$

Bewijs:
We maken gebruik van het feit dat voor elke $\alpha \in \mathbb{C}$ geldt:

$$\begin{aligned} 1 &\leq \max_{x \in S^1} |x - \alpha|, \\ |\alpha| &\leq \max_{x \in S^1} |x - \alpha|. \end{aligned}$$

Voor de linker ongelijkheid maken we de afschatting:

$$M(P) = \prod_{k=1}^{n} \max\{1, |\alpha_k|\} \leq \prod_{k=1}^{n} \max_{x \in S^1} \{|x - \alpha_k|\} = \max_{x \in S^1} |P(x)|.$$

Terwijl voor x op de eenheidscirkel geldt:

$$|P(x)| = |x^n + a_{n-1} + \cdots + a_1 x + a_0| \leq 1 + |a_{n-1}| + \cdots + |a_1| + |a_0| = L(P).$$

De rechter ongelijkheid volgt direct uit de hypothese en het feit dat $\sum_{i=0}^{n} \binom{n}{i} = 2^n$:

$$L(P) = \sum_{i=0}^{n} |a_i| \leq M_0 \sum_{i=0}^{n} \binom{n}{i} = 2^n M_0.$$

☺

We definiëren voor een polynoom $P_0(x)$ met nulpunten $\alpha_1, \ldots, \alpha_n$ een

nieuwe polynoom $P_1(x)$ met als nulpunten $\alpha_1^2, \ldots, \alpha_n^2$. De coëfficiënten van $P_1(x)$ kunnen we bepalen door op te merken:

$$\begin{aligned} P_1(y^2) &= \prod_{i=1}^{n} y^2 - \alpha_i^2 \\ &= \prod_{i=1}^{n} (y - \alpha_i)(y + \alpha_i) \\ &= (-1)^n P_0(y) P_0(-y), \end{aligned}$$

waaruit volgt $P_1(x) \in \mathbb{Z}[X]$ als $P_0(x) \in \mathbb{Z}[X]$. Op dezelfde manier definiëren we $P_k(x)$ als de monische polynoom met nulpunten $\alpha_1^{2^k}, \ldots, \alpha_n^{2^k}$ en graad n. Uit het bewijs van Stelling 2.7 volgt overigens ook dat $P_k(x)$ gehele coëfficiënten $a_j^{(k)}$ heeft. Bovendien:

$$M(P_k) = \prod_{i=1}^{n} \max\{1, |\alpha|^{2^k}\} = M(P)^{2^k}. \tag{23}$$

Als voor alle coëfficiënten geldt dat:

$$|a_j^{(k)}| \leq \binom{n}{j} M_0^{2^k}, \tag{24}$$

dan volgt uit lemma 5.2: $M(P_k) \leq 2^n M_0^{2^k}$, en dus:

$$M(P_k)^{2^{-k}} \leq 2^{n \cdot 2^{-k}} M_0.$$

Uit (23) volgt dat de linkerzijde gelijk is aan $M(P)$. Dus we hebben:

$$M(P) \leq 2^{\frac{n}{2^k}} M_0. \tag{25}$$

Naarmate k groter wordt, gaat de exponent $\frac{n}{2^k}$ naar nul. Als de rij polynomen $P_k(x)$ voor alle $k \in \mathbb{N}$ voldoet aan (24) kunnen we dus met zekerheid zeggen dat $P(x) = P_0(x)$ een lage maat heeft: $M(P) \leq M_0$.

Dit biedt de mogelijkheid om te controleren of een polynoom een lage maat heeft zonder dat de nulpunten van het polynoom uitgerekend hoeven te worden. In het voorbeeld hieronder wordt de werking van het algoritme gedemonstreerd.

Voorbeeld 5.3. We willen van $P(x) = x^3 + 3x^2 - x - 1$ weten of $M(P) < 2$. De coëfficiënten a_k zijn in absolute waarde kleiner dan $2\binom{3}{k}$, dus volgens de methode van 5.1 is $P(x)$ een kandidaat voor een lage $M(P)$-waarde. We gaan dit controleren met het algoritme dat hierboven is beschreven. De polynoom $P_1(x)$ is hier:

$$P_1(x) = x^3 - 11x^2 + 7x - 1.$$

Voor de coëfficiënten $a_1^{(1)}$ en $a_2^{(1)}$ van $P_1(x)$ gaan we na of (24) geldt:

$$|a_k^{(1)}| \leq \binom{3}{k} 2^{2^1} = 12.$$

We zien dat $a_1^{(1)} = 7$ en $a_2^{(1)} = -11$ beide voldoen aan de ongelijkheid, dus volgt uit (25) dat:

$$M(P) \leq 2 \cdot 2^{3/2} = 5,65...$$

Op dezelfde manier berekenen we:

$$P_2(x) = x^3 - 107x^2 + 27x - 1.$$

En, gegeven dat $M(P) < 2$, voor de coëfficiënten zou moeten gelden:

$$|a_k^{(2)}| \leq \binom{3}{k} 2^{2^2} = 48.$$

Maar dit geldt niet, want $|a_2^{(2)}| = 107 > 48$. We mogen concluderen dat $M(P) \geq 2$.

6. Niet-reciproke polynomen

Een belangrijke stap richting het beantwoorden van Lehmer's vraag is gedaan door Smyth in [5]. Hij laat zien dat $M(P) \geq M(x^3+x^2-1)$ voor alle niet-reciproke polynomen. Dit is een verbetering van een resultaat van Breusch [3] uit 1951. In dit hoofdstuk zullen we, Smyth's bewijs volgend, stelling 6.1 bewijzen.

Stelling 6.1. Als $P(x)$ niet-reciprook is dan

$$M(P) \geq \frac{1}{4}(1 + \sqrt{17}) = 1,28077\ldots.$$

Om deze stelling te bewijzen, zullen we gebruik maken van het volgende lemma:

Lemma 6.2. Laat $f(z) = \sum_{i=0}^{\infty} e_i x^i$, met alle $e_i \in \mathbb{R}$ en $e_0 \neq 0$, een functie zijn die analytisch is in een omgeving die de eenheidsschijf bevat. Als $|f(z)| \leq 1$ voor z op de eenheidscirkel, dan geldt voor alle coëfficienten:

$$|e_i| \leq 1 - e_0^2 \tag{26}$$

Een bewijs van dit lemma wordt gegeven in [5].

Nu kunnen we stelling 6.1 bewijzen. We nemen aan dat de constante term $b_0 = P(0) = 1$. Het bewijs van het geval dat $P(0) = -1$ gaat

analoog, en als $|P(0)| \geq 2$ dan $M(P) \geq 2$.
Gegeven is de niet-reciproke polynoom:

$$P(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + 1 = \prod_{j=1}^{n}(x - \alpha_j).$$

We zullen gebruik maken van de machtreeks van $P(x)\hat{P}(x)^{-1}$. Deze reeks is niet constant, want $P(x)$ is niet-reciprook. De reeks wordt gegeven door:

$$\frac{P(x)}{\hat{P}(x)} = 1 + a_k x^k + a_l x^l + \dots . \tag{27}$$

De indices k en l zijn de laagste indices waarvoor de coëfficiënten ongelijk zijn aan nul. Dat a_k een geheel getal is, volgt uit het herschrijven van de bovenstaande vergelijking:

$$\hat{P}(x)(1 + a_k x^k + a_l x^l + \dots) = P(x).$$

De coëfficiënt voor de term x^k is aan de rechterzijde gelijk aan b_k, en aan de linkerzijde: $a_k + b_{n-k}$. Alle termen b_j zijn gehele getallen, dus dan moet ook a_k een geheel getal zijn, en daarom: $|a_k| \geq 1$.
De reciproke $\hat{P}(x) = x^n P(\frac{1}{x})$ heeft nulpunten $\alpha_1^{-1}, \dots, \alpha_n^{-1}$ en kan geschreven worden als:

$$\hat{P}(x) = \prod_{i=1}^{n}(1 - \alpha_i x).$$

Dan volgt:

$$\begin{aligned}
\frac{P(x)}{\hat{P}(x)} &= \frac{\prod_{j=1}^{n}(x - \alpha_j)}{\prod_{i=1}^{n}(1 - \alpha_i x)} \\
&= \prod_{|\alpha_j|<1} \frac{(x - \alpha_j)}{(1 - \alpha_j x)} \prod_{|\alpha_j|\geq 1} \frac{(x - \alpha_j)}{(1 - \alpha_j x)} \\
&=: f(x)g(x)^{-1},
\end{aligned}$$

waarin

$$f(x) = \prod_{|\alpha_j|<1} \frac{(x - \alpha_j)}{(1 - \alpha_j x)} \tag{28}$$

en

$$g(x) = \prod_{|\alpha_j|\geq 1} \frac{(1 - \alpha_j x)}{(x - \alpha_j)}. \tag{29}$$

We merken op dat:

$$|g(0)| = |\prod_{|\alpha_j|\geq 1} \frac{1}{(-\alpha_j)}| = \frac{1}{M(P)}. \tag{30}$$

De rationale functies $f(x)$ en $g(x)$ hebben geen polen voor $|x| \leq 1$, dus ze zijn analytisch op een omgeving van de eenheidsschijf. We kunnen de reeksontwikkeling schrijven:

$$\begin{aligned} f(x) &= c + c_1 x + c_2 x^2 + \dots \\ g(x) &= d + d_1 x + d_2 x^2 + \dots . \end{aligned}$$

De coëfficiënten zijn reëel, want voor elke term met een complexe α die voorkomt in uitdrukking (28), komt een term voor met $\bar{\alpha}$, en hun product is:

$$\frac{(x-\alpha)}{(1-\alpha x)}\frac{(x-\bar{\alpha})}{(1-\bar{\alpha}x)} = \frac{x^2 + |\alpha|^2 - 2x \cdot Re(\alpha)}{1 + |\alpha|^2 x^2 - 2x \cdot Re(\alpha)},$$

dus $f(x)$ heeft reële coëfficiënten. Voor $g(x)$ geldt hetzelfde. Het quotiënt van de twee functies is gelijk aan $P(x)\hat{P}(x)^{-1}$. Hieruit volgt:

$$1 = P(0)\hat{P}(0)^{-1} = \frac{f(0)}{g(0)} = \frac{c}{d}.$$

Dus $c = d$ en $|c| = \frac{1}{M(P)}$. Het verband tussen de k-de coëfficiënten van $f(x), g(x)$ en $P(x)\hat{P}(x)^{-1}$ is te zien als we $f(x) = g(x)P(x)\hat{P}(x)^{-1}$ als reeks uitschrijven:

$$c + c_1 x + c_2 x^2 + \dots = (d + d_1 x + d_2 x^2 + \dots)(1 + a_k x^k + a_l x^l + \dots),$$

en dus: $c_k = a_k d + d_k$. Omdat $|a_k| \geq 1$ en $c = d$, hebben we:

$$|c| \leq |a_k c| = |c_k - d_k| \leq 2 \cdot \max\{|c_k|, |d_k|\}.$$

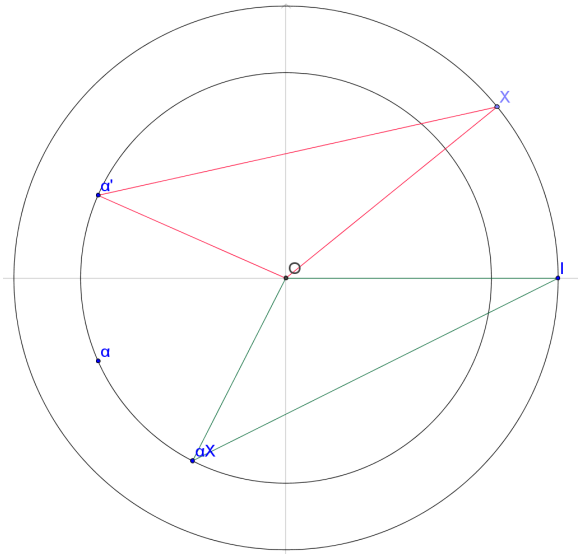
Uit figuur 1 volgt dat $|x - \bar{\alpha}| = |1 - \alpha x|$ en dus $|f(x)| = 1$ voor x op de eenheidscirkel. Volgens een vergelijkbaar argument geldt ook $|g(x)| = 1$ voor x op de eenheidscirkel. Lemma 6.2 is dan van toepassing op beide functies:

$$\frac{|c|}{2} \leq \max\{|c_k|, |d_k|\} \leq \max\{1 - c^2, 1 - d^2\} = 1 - c^2.$$

Uit (30) en $c^2 + \frac{1}{2}c - 1 \leq 0$ volgt:

$$M(P) = \frac{1}{|c|} \geq \frac{1}{4}(1 + \sqrt{17}).$$

De ondergrens $\frac{1}{4}(1 + \sqrt{17})$ is bij benadering: 1,28077.... Dit kan nog worden verbeterd. In [5] wordt een sterker resultaat bewezen: de ondergrens voor niet-reciproke polynomen is $M(x^3 + x^2 - 1) = 1.32471\dots$.



FIGUUR 1. De groene driehoek, gevormd door de punten $(1,0), \alpha x$ en de oorsprong, is congruent aan de rode, met hoekpunten $\bar{\alpha}, x$ en de oorsprong. Daarom geldt $|x - \bar{\alpha}| = |1 - \alpha x|$. De geconjugeerde $\bar{\alpha}$ van α is in de figuur aangegeven als α'.

Dit is duidelijk wel het best mogelijke resultaat omdat deze ondergrens wordt bereikt door de niet-reciproke polynoom $P(x) = x^3 + x^2 - 1$.

7. RESULTATEN

7.1. **Gevonden ondergrenzen.** We gebruiken het algoritme uit hoofdstuk 5 om de ondergrens M_k van $M(P)$ te bepalen voor polynomen met graad k. Door gebruik te maken van het resultaat van Smyth hoeven we voor $k \geq 4$ alleen maar de zelfreciproke polynomen te controleren. Hieronder staan de gevonden waarden met de bijbehorende polynomen. De waarden waar geen polynoom naast staat worden bereikt door een

product van een bovenstaande polynoom met een cyclotomische polynoom.

$$\begin{aligned}
M_2 &= 1,61803... \quad x^2 - x - 1 \\
M_3 &= 1,32471... \quad x^3 - x^2 + 1 \\
M_4 &= 1,32471... \\
M_5 &= 1,32471... \\
M_6 &= 1,32471... \\
M_7 &= 1,32471... \\
M_8 &= 1,28063... \quad x^8 - x^5 - x^4 - x^3 + 1 \\
M_9 &= 1,28063... \\
M_{10} &= 1,17628... \quad x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1
\end{aligned} \tag{31}$$

In [2] wordt nagegaan dat $M_{16} = M_{15} = \cdots = M_{10} = 1,17628\ldots$.

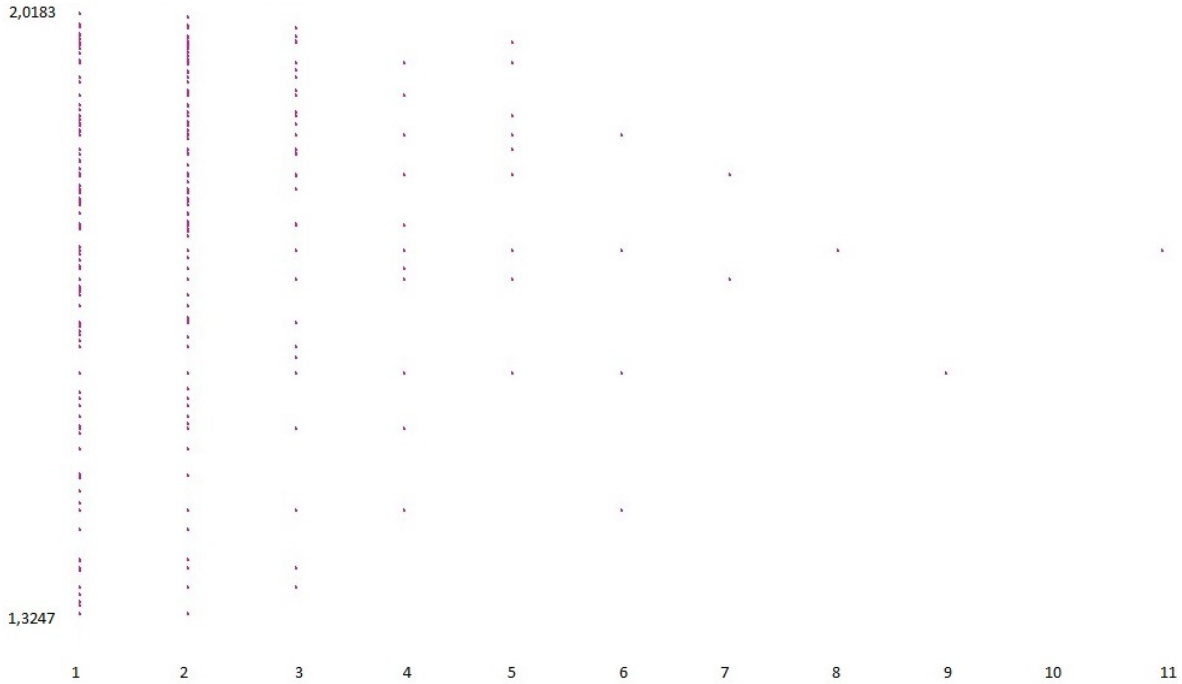
Kleine waarden worden vaak bereikt door polynomen met coëfficiënten 0 en ± 1. Het maximum van de absolute waarde van de coëfficiënten van een polynoom wordt de *hoogte* genoemd en aangeduid als $H(P)$. In figuur 2 zijn de punten $(H(P), M(P))$ weergegeven voor alle polynomen met graad ≤ 6 en $M(P) < 2$. De dichtheid van de punten dichtbij de x-as is bij $H(P) = 1$ en $H(P) = 2$ aanzienlijk hoger dan bij grotere waarden voor H. Er is geen enkele polynoom gevonden met $H(P) > 11$ en $M(P) < 2$.
We zijn ervan uitgegaan dat alle zesdegraadspolynomen waarvan de coëfficiënten voldoen aan $a_k < 2\binom{6}{k}$ kandidaat zijn voor een lage $M(P)$-waarde. Daarom moeten polynomen van een hoogte tot $2\binom{6}{3} = 40$ worden nagegaan, terwijl de grafiek een sterkere afschatting laat zien: de grootste coëfficiënt is kleiner dan of gelijk aan 11.
Als we willen zoeken naar polynomen met lage maat dan suggereert de grafiek dat we ons voor het rekengemak kunnen beperken tot polynomen met kleine $H(P)$.
In figuur 3 is de maat van alle irreducibele zelf-reciproke polynomen van hoogte 1 en $M(P) < 2$ weergegeven als functie van de graad. Er zijn geen polynomen van oneven graad gevonden, want die zijn reducibel. Zo'n polynoom is namelijk te schrijven als:

$$P(x) = x^{2k+1} + a_{2k}x^{2k} + \cdots + a_k x^k + a_k x^{k-1} + \cdots + a_{2k}x + 1.$$

Elke coëfficiënt a_j komt voor bij zowel een even als een oneven macht van x, dus

$$P(-1) = -1 + a_{2k} + \cdots + a_k - a_k + \cdots - a_{2k} + 1 = 0$$

en dan is $x + 1$ een deler van $P(x)$. Met een vergelijkbaar argument wordt duidelijk dat $x-1$ een deler van is van $P(x)$ als $P(x) = -\hat{P}(x)$ en $P(x)$ van oneven graad is. De waarden van $M(P)$ kleiner dan $M(x^3 + x^2 - 1) = 1,32...$ die voorkomen bij polynomen van oneven graad n moeten dus ook voorkomen bij polynomen van graad $n - 1$.
Wat nog meer opvalt in figuur 3 is dat de dichtheid van de getekende punten hoger wordt naarmate de graad groter is. Het aantal polynomen met lage maat stijgt met de graad. Tabel 7.1 toont het aantal $A(n)$ irreducibele zelfreciproke polynomen van even graad n tot en met 30 en maat $0 < M(P) < 1,3$.



FIGUUR 2. Voor elke polynoom van graad ≤ 6 met $1 < M(P) < 2$ is hier het punt $(H(P), M(P))$ getekend.

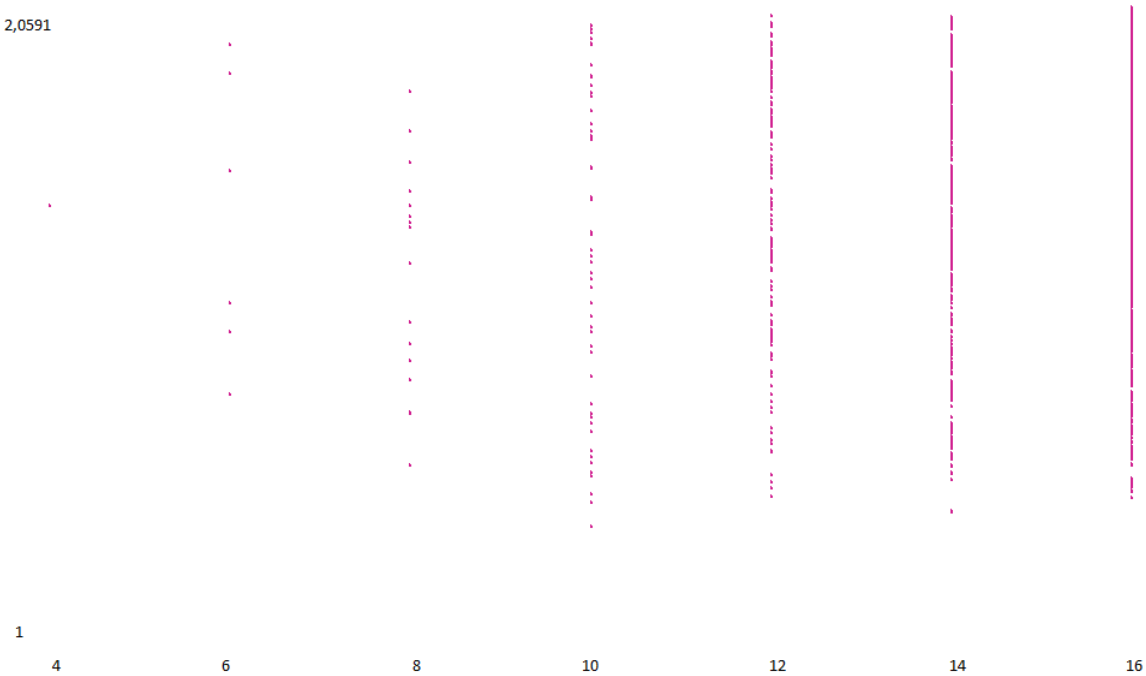
n	6	8	10	12	14	16	18	20	22	24	26	28	30
$A(n)$	0	2	14	8	22	28	40	72	90	88	108	114	148
$A'(n)$	0	2	14	8	22	26	40	58	90	80	108	92	134

Tabel 7.1: Deze tabel toont het aantal irreducibele polynomen van even graad n met $P(x) = \hat{P}(x)$ en $1 < M(P) < 1,3$.

In lemma 1.4 werd al opgemerkt dat polynomen van de vorm $P(x^k)$ dezelfde maat hebben als $P(x)$. Elke tiendegraadspolynoom $P(x)$ definiëert bijvoorbeeld de polynoom $Q(x) = P(x^2)$ van graad 20 waarvoor geldt $M(P) = M(Q)$. Dit gegeven garandeert het bestaan van polynomen van hoge graad en lage maat, maar geeft geen nieuwe waarden voor $M(P)$. We definiëren het gecorrigeerde aantal $A'(n)$ als:

$$A'(n) = A(n) - \sum_{k|n} A(k)$$

waarbij de som gaat over de delers $k \neq n$ van n. Dit aantal wordt weergegeven in tabel 7.1. Er lijkt nog steeds een stijging te zijn, precies zoals de verdichting van punten in figuur 3 al suggereert voor lagere



FIGUUR 3. Voor elke irreducibele polynoom van graad ≤ 16 met $P(x) = \hat{P}(x)$, coëfficiënten 0 en ± 1 en $M(P) < 2$ is het punt $(\text{graad}(P), M(P))$ getekend.

graden (tot 16).
De correctie $A'(n)$ van $A(n)$ sluit niet uit dat er alsnog polynomen worden meegeteld die een maat hebben die al wordt bereikt door een andere polynoom van lagere graad. In [2] worden nog enkele manieren toegelicht waarop de maten van verschillende polynomen kunnen samenvallen.

8. Reducibele polynomen

In het eerste hoofdstuk werd opgemerkt dat

$$M(P) = M(Q_1)M(Q_2)$$

als $P(x)$ een product is van de factoren $Q_1(x)$ en $Q_2(x)$. Als beide factoren niet-cyclotomisch zijn dan is $M(P)$ groter dan of gelijk aan een product van ten minste twee waarden uit (31). Dit leidt tot de volgende stelling.

Stelling 8.1. Laat $P(x)$ een polynoom van graad n zijn met $P(0) \neq 0$. Als

$$M(P) < \min_{k<n}\{M_k M_{n-k}\} \tag{32}$$

dan zijn alle factoren $Q(x)$ van $P(x)$ met $Q \neq P$ cyclotomisch.

In het bijzonder zijn de polynomen die voldoen aan (32) en niet deelbaar zijn door een cyclotomische factor irreducibel.

Voorbeeld 8.2. We maken een afschatting voor $M(P)$ van de achtstegraadspolynoom

$$P(x) = x^8 + 2x^7 + 2x^6 + 3x^5 + 3x^4 + 3x^3 + 2x^2 + 2x + 1.$$

Hiervoor gebruiken we dezelfde methode als in voorbeeld 5.3. Laat $P_k(x)$ de polynoom zijn met als nulpunten de 2^k-de macht van de nulpunten van $P(x)$. De recursieve formule

$$P_{k+1}(x) = P_k(\sqrt{x})P_k(-\sqrt{x})$$

levert de volgende reeks polynomen:

$$\begin{aligned}
P_1(x) &= x^8 - 2x^6 - 5x^5 - 7x^4 - 5x^3 - 2x^2 + 1 \\
P_2(x) &= x^8 - 4x^7 - 10x^6 - x^5 + 9x^4 - x^3 - 10x^2 - 4x + 1 \\
P_3(x) &= x^8 - 36x^7 + 110x^6 - 209x^5 + 249x^4 - 209x^3 + 110x^2 - 36x + 1 \\
P_4(x) &= x^8 - 1076x^7 - 2450x^6 - 3729x^5 - 3751x^4 - 3729x^3 - 2450x^2 - 1076x + 1
\end{aligned}$$

Voor $1 \leq k \leq 4$ gaan we na dat voor elke coëfficiënt $a_j^{(k)}$ van $P_k(x)$ geldt:

$$|a_j^{(k)}| \leq \binom{8}{j} 1{,}4^{2^k}.$$

Volgens (25) geldt dan:

$$M(P) \leq 1{,}4 \cdot 2^{\frac{8}{24}} = 1{,}664... \tag{33}$$

Als $P(x)$ een product van niet-cyclotomische polynomen is, dan moet gelden:

$$M(P) \geq \min_{k<n}\{M_k M_{n-k}\} = (1,32471...)^2 = 1,75485...$$

De afschatting van vergelijking (33) laat zien dat dit niet het geval is. Daarom zijn alle factoren van $P(x)$ cyclotomisch.

9. Substitutie van x^2

In hoofdstuk 7 zijn we ervan uitgegaan dat $P(x^n)$ irreducibel is als $P(x)$ irreducibel is. Dit is niet altijd het geval. Er komen irreducibele polynomen voor waarvoor geldt dat $P(x^2)$ reducibel is. Een voorbeeld hiervan wordt verderop in dit hoofdstuk gegeven.

Lemma 9.1. Als $P(x)$ een irreducibele polynoom is van graad n en $P(x^2)$ is reducibel, dan hebben de factoren van $P(x^2)$ graad n.

Bewijs: De graad van $P(x^2)$ is gelijk aan $2n$. Laat α een nulpunt zijn van $P(x^2)$. Dan is de minimumpolynoom $f_{\mathbb{Q}}^{\alpha}$ een deler van $P(x^2)$. We schrijven de lichaamsuitbreidingen over $\mathbb{Q}$ als:

$$\mathbb{Q} \subset \mathbb{Q}[\alpha^2] \subset \mathbb{Q}[\alpha].$$

De graad van de uitbreiding $\mathbb{Q}[\alpha^2]$ over $\mathbb{Q}$ is gelijk aan graad$(P) = n$, want $P(x)$ is irreducibel en $P(\alpha^2) = 0$. Er volgt dat n een deler moet zijn van de graad van de uitbreiding $\mathbb{Q}[\alpha]$ over $\mathbb{Q}$. Bovendien is deze graad kleiner dan graad$(P(x^2)) = 2n$, omdat $P(x^2)$ reducibel is en α als nulpunt heeft. Dan moet deze graad wel n zijn:

$$[\mathbb{Q}[\alpha] : \mathbb{Q}] = graad(f_{\mathbb{Q}}^{\alpha}) = graad(P) = n.$$

☺

Voorbeeld 9.2. De polynoom $P(x) = x^2 - 3x + 1$ is irreducibel. De nulpunten α^2 en β^2 worden gegeven door:

$$\alpha^2 = \frac{3}{2} + \frac{1}{2}\sqrt{5}, \beta^2 = \frac{3}{2} - \frac{1}{2}\sqrt{5}.$$

De 4 nulpunten van $P(x^2)$ zijn $\pm\alpha$ en $\pm\beta$. We merken op dat:

$$\alpha^2 = \frac{1}{4}(6 + 2\sqrt{5}) = \frac{1}{2^2}(1 + \sqrt{5})^2,$$

dus de nulpunten worden gegeven door $\{\pm\frac{1}{2} \pm \frac{1}{2}\sqrt{5}\}$. Dan is $\alpha := \frac{1}{2} + \frac{1}{2}\sqrt{5}$ een nulpunt van $P(x^2)$ en te schrijven als:

$$\alpha = -1 + \alpha^2.$$

Dit betekent dat $\alpha \in \mathbb{Q}[\alpha^2]$. Voor de graad van de minimumpolynoom geldt dan:

$$graad(f_{\mathbb{Q}}^{\alpha}) = graad(f_{\mathbb{Q}}^{\alpha^2}) = 2.$$

De polynoom $P(x^2)$ heeft α als nulpunt en wordt dus gedeeld door $f_{\mathbb{Q}}^{\alpha}$. Deze heeft een graad kleiner dan 4 en daarom is $P(x^2)$ reducibel, met de ontbinding:

$$P(x^2) = f_{\mathbb{Q}}^{\alpha}(x) f_{\mathbb{Q}}^{\gamma}(x)$$

waarbij γ een van de andere nulpunten van $P(x^2)$ is: $\gamma \in \{-\alpha, \beta, -\beta\}$ en $f_{\mathbb{Q}}^{\gamma} \neq f_{\mathbb{Q}}^{\alpha}$. Als $f_{\mathbb{Q}}^{\gamma}(-\alpha) \neq 0$ dan moet $-\alpha$ een nulpunt zijn van $f_{\mathbb{Q}}^{\alpha}$ en is deze te schrijven als:

$$f_{\mathbb{Q}}^{\alpha}(x) = (x - \alpha)(x + \alpha) = x^2 - \alpha^2.$$

Dit kan niet want $\alpha^2 \notin \mathbb{Z}$. Daarom moet gelden dat $f_{\mathbb{Q}}^{\gamma}(-\alpha) = 0$ en dus:

$$P(x^2) = f_{\mathbb{Q}}^{\alpha}(x) f_{\mathbb{Q}}^{-\alpha}(x) = f_{\mathbb{Q}}^{\alpha}(x) f_{\mathbb{Q}}^{\alpha}(-x).$$

Het bovenstaande voorbeeld laat zien dat $P(x^2)$ ontbindt als product van een $Q(x) \in \mathbb{Z}[X]$ met $Q(-x)$. Dit is in het algemeen waar.

Lemma 9.3. Als $P(x)$ irreducibel is en $g(x) := P(x^2)$ reducibel, dan $g(x) = \pm Q(x)Q(-x)$ voor een $Q(x) \in \mathbb{Z}[X]$.

Bewijs: Als $P(x) = x$, dan is het lemma triviaal. We nemen verder aan dat $P(x) \neq x$ en dus $P(0) \neq 0$. Laat $Q(x)$ een irreducibele deler zijn van $g(x)$. Omdat $g(x) = g(-x)$ moet ook $Q(-x)$ een deler zijn van $g(x)$. Als $Q(x) = \pm Q(-x)$ dan $Q(0) = \pm Q(0) \neq 0$ dus $Q(x) = Q(-x)$. Dat betekent dat $Q(x) = \tilde{Q}(x^2)$ voor een $\tilde{Q}(x) \in \mathbb{Z}[X]$. Hetzelfde geldt voor de andere deler $R(x)$, dus:

$$P(x^2) = \tilde{Q}(x^2)\tilde{R}(x^2).$$

Dan $P(x) = \tilde{Q}(x)\tilde{R}(x)$ en is $P(x)$ dus niet irreducibel. Het moet dus zo zijn dat $Q(x) \neq \pm Q(-x)$. De polynomen $Q(x)$ en $Q(-x)$ hebben beide graad n en zijn beide delers van de $2n$-degraadspolynoom $P(x^2)$, dus $P(x^2) = \pm Q(x)Q(-x)$. ☺

Een toepassing van lemma 9.3 en lemma 1.4 wordt geformuleerd in de volgende stelling.

Stelling 9.4. Als $P(x)$ irreducibel is en graad n heeft en $P(x^2)$ reducibel, dan is er een n-degraadspolynoom $Q(x)$ waarvoor geldt:

$$M(Q) = \sqrt{M(P)} \tag{34}$$

Bewijs: Uit lemma 9.3 volgt direct dat:

$$M(P(x^2)) = M(f^\alpha_{\mathbb{Q}}(x) f^\alpha_{\mathbb{Q}}(-x)) = M(f^\alpha_{\mathbb{Q}})^2,$$

waarbij $f^\alpha_{\mathbb{Q}}$ graad n heeft. En dus:

$$M(f^\alpha_{\mathbb{Q}}) = \sqrt{M(P(x^2))} = \sqrt{M(P)}.$$

☺

Als $P(x)$ niet-cyclotomisch is, dan $\sqrt{M(P)} < M(P)$.

Voorbeeld 9.5. De polynoom

$$P(x) = x^{14} - x^{13} + x^9 - x^8 - x^7 - x^6 + x^5 - x + 1$$

is irreducibel en heeft $M(P) = 1,7105\ldots$. De polynoom die wordt gedefiniëerd door $P(x^2)$ is reducibel en kan geschreven worden als $P(x^2) = Q(x)Q(-x)$, waarbij:

$$Q(x) = x^{14} - x^{13} + x^9 - x^8 + x^7 - x^6 + x^5 - x + 1.$$

Omdat $M(P) = M(Q)^2$, geldt:

$$M(Q) = \sqrt{1,7105\ldots} = 1,3078\ldots.$$

Het voorbeeld hierboven laat zien dat voor sommige polynomen de substitutie $x = x^2$ een methode is om een polynoom van dezelfde graad en lagere Mahler-maat te vinden. Hieronder geven we een voorbeeld van een irreducibele polynoom $P(x)$ waarvoor ook $P(x^2)$ irreducibel is, maar $P(x^3)$ reducibel.

Voorbeeld 9.6. De irreducibele 16-degraadspolynoom waarvan de coëfficiënten worden gegeven door de vector:

$$p = [1, -1, 1, 2, 0, 1, 2, 1, 2, 1, 2, 1, 0, 2, 1, -1, 1],$$

heeft $M(P) = 1,9438\ldots$. De substitutie $x = x^3$ levert een reducibele polynoom van graad 48 die een product is van $Q_1(x)$ van graad 16 en $Q_2(x)$ van graad 32. Voor de Mahler-maat van $Q_1(x)$ geldt:

$$M(Q_1) = M(P)^{\frac{1}{3}} = 1,2480\ldots,$$

en voor $Q_2(x)$:

$$M(Q_2) = M(P)^{\frac{2}{3}} = 1,5575\ldots.$$

10. Conclusie

In hoofdstuk 5 hebben we een methode gegeven om voor een vaste graad een ondergrens > 1 van $M(P)$ te vinden. Deze methode is nog verbeterd met behulp van een algoritme uit [2] en het resultaat van Smyth over niet-reciproke polynomen, dat besproken is in hoofdstuk 6. We hebben de ondergrenzen van $M(P)$ tot en met graad 10 gevonden. Deze ondergrenzen zijn in overeenstemming met de resultaten uit [2]. In hoofdstuk 8 en 9 zijn enkele gevolgen en toepassingen besproken.

Referenties

[1] K. Mahler *An application of Jensen's formula to polynomials*, Mathematika, **7** (1960), 98-100.

[2] D.W. Boyd *Reciprocal Polynomials Having Small Measure*, Mathematics of Computation, **35** 152 (1980), 1361-1377.

[3] R. Breusch *On the distribution of the roots of polynomials with integral coefficients*, Proceedings of the Am. Math. Soc. **2** 6 (1951), 939-941.

[4] B. van Geemen, H.W. Lenstra, F. Oort, J. Top *Algebraische structuren*, collegedictaat, Johann Bernouilli Instituut (2014).

[5] C.J. Smyth *On the product of the conjugates outside the unit circle of an algebraic integer*, Lond. Math. Soc. **3** (1971), 169-175.

[6] P. Borwein, E. Dobrowolski, M.J. Mossinghoff *Lehmer's problem for polynomials with odd coefficients*, Ann. of Math. **166** (2007), 347-366.

[7] E. Dobrowolski *On a question of Lehmer and the number of irreducible factors of a polynomial* Acta. Arit. **34** (1979), 391-401.

[8] P.A. Damianou *Monic Polynomials in $\mathbb{Z}[x]$ with roots in the unit disk*, Am. Math. Monthly **108** (2001), 253-257.

11. Appendix

In deze appendix wordt de programmacode voor GP/PARI gegeven die gebruikt is voor hoofdstuk 7. De functie M geeft de Mahler-maat voor een polynoom p. De functie $g6b(w1, W, d)$ geeft alle irreducibele polynomen met coëfficiënten $\{0, -1, 1\}$ waarvoor geldt: $M(P) < W$, $P(x) = \hat{P}(x)$ en graad$(p) = d$. Hierin is het argument $w1$ het aantal iteraties van het algoritme dat besproken is in hoofdstuk 5. Dit algoritme is in de functie $g3$ verwerkt. De functie $g12(w1, W, n)$ geeft alle irreducibele polynomen van graad n waarvoor geldt: $P(x) = \hat{P}(x)$ en $M(P) < W$. Ten slotte worden de functies $g7$ en $g7b$ gebruikt voor de constructie van zelf-reciproke polynomen.

```
M(p)={my(r,k);r=polroots(p);return(prod(k=1,length(r),max(1,
   abs(r[k]))))};
```

```
g3(k,M,c)= {n=length(c);b=c;for(m=1,k,for(i=0,n-1,q=min(i,(n
    -1)-i); if(i==n-1,s=0,s=sum(l=1,q,(-1)^(l+i)*c[1+i-l]*c[1+i
    +l]));b[i+1]=(-1)^(i)*c[i+1]^2+2*s;r=binomial(n-1,i)*M^(2^m
    );if(abs(b[i+1])>r,return(0)));c=b;);return(1)};
g4(y)={n=length(y);p=sum(k=1,n,y[k]*x^(n-k));return(p)};

g6b(w1,W,d)={d1=floor(d/2);d1=d1+1;for(k=3^(d1-1),3^(d1),c=
    digits(k,3);c=c-vector(length(c),x,1);if(d%2==0,c3=g7(c),c3
    =g7b(c));if(c3[1]==1,z=g3(w1,W,c3);if(z==1,p=g4(c3);y=M(p);
    if(y>1&&y<W&&polisirreducible(p),print(p);print(y)))))}

g7(v)={v1=Vecrev(v);v2=v1[2..length(v1)];w1=concat(v,v2);
    return(w1)}
g7b(v)={v1=Vecrev(v);w1=concat(v,v1);return(w1)}

g11(c,b)={s=sum(l=1,length(c),c[l]*b^(length(c)-l));return(s)}
g12(w1,W,n)={l=floor((n-1)/2);if(n%2==0,l=l+1);b1=2*floor(W*
    binomial(n,floor(n/2)));a=vector(l);for(l1=1,l,a[l1]=floor
    (-W*binomial(n,l1)));a2=-1*a;a=floor(a+W*binomial(n,floor(n
    /2))*vector(l,x,1));a2=floor(a2+W*binomial(n,floor(n/2))
    *vector(l,x,1));m1=floor(g11(a,b1));m2=floor(g11(a2,b1));
    for(k=m1,m2,c=digits(floor(k),floor(b1));c=c-vector(length(
    c),x,floor(b1/2));if(n%2==1,c=g7b(c),c=g7(c));c=concat(1,c)
    ;c=concat(c,1);t=1;j=2;while(j<l&&t==1,if(c[j]>binomial(n,j
    )*W,t=0);j=j+1);if(t==1,z=g3(w1,W,c);if(z==1,p=g4(c);y=M(p)
    ;if(y>1,print(p);print(y)))))}

addhelp(M,"<p>_mahlermaat_van_p")
addhelp(g3,"<k_M_c>_boyd_alg_voor_c")
addhelp(g4,"<y>_coeff-vector_naar_polynoom")
addhelp(g6b,"<w1_W_d1>
    _alle__reciproke_irreducibele_pol_met_coeff_-1
    _0_1_met_mahlermaat_kleiner_dan_W")
addhelp(g7,"<v>_coeff-vector_naar_reciproke_voor_even_graad")
addhelp(g7b,"<v>_g7_voor_oneven_graad")
addhelp(g12,"<w1_W_n>_alle_positieve_recip_pol_met_mahlermaat_
    <W_voor_gr_n")
```