Coëfficiënten van cyclotomische polynomen

Joris Luijsterburg
Studentnummer: 0314137

Maart 2009

Bachelorscriptie
Onder begeleiding van *Dr. W. Bosma*
Wiskunde
Faculteit der Natuurwetenschappen, Wiskunde en Informatica
Radboud Universiteit Nijmegen

Inhoudsopgave

1 Inleiding

De reden dat cyclotomische polynomen het onderwerp zijn geworden van mijn bachelorscriptie is eenvoudig. Cyclotomische polynomen hebben een aantal leuke eigenschappen. Polynomen ogenschijnlijk in $\mathbb{C}[x]$, die toch in $\mathbb{Z}[x]$ zitten. Misschien niet heel verwonderlijk, maar dat de eerste 104 allemaal uitsluitend coëfficiënten in $\{-1, 0, 1\}$ blijken te hebben is wel verbazend te noemen. En waarom nummer 105 niet? het blijkt dat het vooral interessant is om naar ternaire cyclotomische polynomen te kijken. Dit zijn de cyclotomische polynomen met als nummer een product van drie verschillende priemgetallen. Ternaire polynomen zijn namelijk de makkelijkste cyclotomische polynomen waar het gedrag van de coëfficiënten nog niet geheel bekend is. Het onderzoek naar deze ternaire polynomen is dan ook nog steeds actueel.
In deze scriptie wordt duidelijk gemaakt waarom tot de ternaire polynomen alles al bekend is, en wordt een familie aangewezen van ternaire cyclotomische polynomen waarvan de coëfficiënten in $\{-1, 0, 1\}$ zitten. De actualiteit van het onderzoek naar dit onderwerp blijkt uit het feit dat pas in 2007 in een publicatie[1] deze familie werd aangewezen. Tot nu toe is dit de enige bekende ternaire familie met die eigenschappen.

2 Cyclotomische polynomen in $\mathbb{Z}[x]$

Voordat we de definitie van een cyclotomisch polynoom opschrijven, moeten we wat werk verrichten.

Definitie 1. Een n-de machts eenheidswortel is een getal $\zeta_n \in \mathbb{C}$ zodat $\zeta_n^n = 1$. Een eenheidswortel is primitief als er geen macht k is met $k < n$ en $\zeta_n^k = 1$.

Als ζ_n een primitieve eenheidswortel is, dan is ζ_n^i ook een n-de machts eenheidswortel voor elke $i \in \mathbb{Z}$. Stel $\text{ggd}(i, n) = 1$, en $\zeta_n^{ik} = 1$ voor zekere $k \in \mathbb{Z}$. Omdat ζ_n orde n heeft, is $ik = ln$ voor zekere $l \in \mathbb{Z}$. Maar $\text{ggd}(i, n) = 1$, dus k is een veelvoud van n.
Omdat ζ_n primitief is en er n n-de machts eenheidswortels zijn, zijn ze allemaal te schrijven als ζ_n^k voor zekere $k \in \mathbb{Z}$. Als je een l neemt met $\text{ggd}(l, n) > 1$, dan is ζ_n^l een $\frac{n}{\text{ggd}(l,n)}$-de machts eenheidswortel, en dus geen primitieve n-de machts eenheidswortel. Dus zijn alle primitieve n-de machts eenheidswortels te schrijven als ζ_n^i met $\text{ggd}(n, i) = 1$. hieruit volgt:

Stelling 2. Zij ζ_n een primitieve n-de machts eenheidswortel, dan geldt voor elke $\zeta \in \mathbb{C}$:
ζ is een primitieve n-de machts eenheidswortel $\Leftrightarrow$ er is een $i \in \mathbb{Z}$ met $\text{ggd}(i, n) = 1$ en $\zeta_n^i = \zeta$

Met dit gereedschap kunnen we nu makkelijk de belangrijkste definitie van deze scriptie opschrijven.

Definitie 3. Zij ζ_n een primitieve n-de machts eenheidswortel. Het cyclotomisch polynoom $\Phi_n(x)$ is nu als volgt gedefinieerd:

$$\Phi_n(x) = \prod_{1 \le i \le n | ggd(i,n)=1} (x - \zeta_n^i)$$

het maakt in deze definitie niet uit welke ζ_n je kiest, omdat het uiteindelijke product alle primitieve eenheidswortels bevat.

Definitie 4. De Eulerindicator van een getal, aangeduid met $\phi(n)$ geeft aan hoeveel getallen i er zijn met de eigenschappen $0 < i \le n$ en $\text{ggd}(i, n) = 1$.

Gevolg 5. *De graad van het Polynoom Φ_n is gelijk aan $\phi(n)$*

Stelling 6. Als $n = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$ dan

$$\phi(n) = (p-1)p_1^{k_1-1}(p_2-1)p_2^{k_2-1} \dots (p_m-1)p_m^{k_m-1}$$

Bewijs. Als $n = p^k$ met p priem en $k > 0$ een natuurlijk getal, dan hebben precies alle veelvouden van p een ggd met p^k van meer dan 1. Er zijn precies p^{k-1} veelvouden van p kleiner of gelijk aan p^k. Er zijn dus $p^k - p^{k-1}$ getallen met ggd 1. Er geldt dus: $\phi(p^k) = (p-1)p^{k-1}$.

Stel we hebben een x, c en a zodat $x \equiv c \mod a$

$$\begin{aligned} & \text{ggd}(c,a) \neq 1 \\ \Leftrightarrow\ & \exists p > 1 \text{ met } p|\text{ggd}(c,a) \\ \Leftrightarrow\ & \exists p > 1, m, l, k \in \mathbb{N} \text{ zodat } x = ma + c = mlp + kp \\ \Leftrightarrow\ & \exists p \text{ met } p|\text{ggd}(x,a) \\ \Leftrightarrow\ & \text{ggd}(x,a) \neq 1 \end{aligned}$$

Dus $\text{ggd}(c,a) = 1 \Leftrightarrow \text{ggd}(x,a) = 1$. Nu zegt de Chinese reststelling dat als $\text{ggd}(a,b) = 1$ dan is er voor elke c en d een unieke x zodat $x \equiv c \mod a$ en $x \equiv d \mod b$. Als we nu alle paren (c,d) bekijken met $\text{ggd}(c,a) = 1$ en $\text{ggd}(d,b) = 1$, dan krijgen we $\mod ab$ precies alle getallen x met $\text{ggd}(x,a) = 1$. Er zijn precies $\phi(a)\phi(b)$ van die paren (c,d). Dus geldt $\phi(ab) = \phi(a)\phi(b)$. Nu volgt:

$$\begin{aligned} \phi(n) &= \phi(p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}) \\ &= \phi(p_1^{k_1})\phi(p_2^{k_2}) \dots \phi(p_m^{k_m}) \\ &= (p_1 - 1)p_1^{k_1 - 1}(p_2 - 1)p_2^{k_2 - 1} \dots (p_m - 1)p_m^{k_m - 1} \end{aligned}$$

□

Stelling 7. Voor alle $n \in \mathbb{N}$ geldt:

$$x^n - 1 = \prod_{d, d|n} \Phi_d$$

Bewijs. Alle n-de machts eenheidswortels vormen samen een cyclische groep van orde n. In die groep zijn precies $\phi(n)$ primitieve eenheidswortels. Als ζ_n niet primitief is, is er een $e < n$ zodat $\zeta_n^e = 1$. Van alle e's die deze eigenschap hebben is er een kleinste e', dus is ζ_n een primitieve e'-ste machts eenheidswortel. Dan brengt ζ_n een cyclische groep voort. Deze groep is een ondergroep van C_n, dus heeft hij orde een deler van n. Dus voor elke n-demachts eenheidswortel ζ is er een $d|n$ zodat $\zeta^d = 1$. Verder is elke primitieve $d-$demachts eenheidswortel met $d|n$ ook een n-demachts eenheidswortel. □

Gevolg 8. $n = \sum_{d|n} \phi(d)$

We kunnen nu zeer makkelijk Φ_p opschrijven als p een priemgetal is. Want de enige delers die p dan heeft zijn p en 1. Dus:

$$\Phi_p = \frac{x^p - 1}{\Phi_1} = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x^1 + 1 \tag{1}$$

Stelling 9. Voor alle $n \in \mathbb{N}$ met $n > 1$ geldt:

$$\Phi_n(x) = x^{\phi(n)}\Phi_n(x^{-1})$$

Bewijs. Als ζ_n een nulpunt is van $\Phi_n(x)$, dan is $\zeta_n^{n-1} = \zeta_n^{-1}$ dat ook, want $\text{ggd}(n, n-1) = 1$. Omdat ζ_n een nulpunt is van $\Phi_n(x)$, is ζ_n^{-1} een nulpunt van $\Phi_n(\frac{1}{x})$. Net zo is ζ_n een nulpunt van $\Phi_n(\frac{1}{x})$. En dus ook van $x^n\Phi_n(\frac{1}{x})$. Dit geldt voor alle nulpunten.Verder zijn alle Φ_n monisch. Als nu ook voor alle Φ_n met $n > 1$ de coëfficiënt van x^0 gelijk is aan 1 zijn we klaar.
Voor elke ζ_n nulpunt van Φ_n is er een ζ_n^{n-1} die ook nulpunt is van Φ_n. De coëfficiënt van x^0 is precies $\prod_{1\leq i\leq\phi(n)} -a_i$ met a_i de nulpunten van Φ_n. Omdat $\zeta_n\zeta_n^{n-1} = 1$ is de coëfficiënt 1. Tenzij $\zeta_n = \zeta_n^{n-1}$, maar dat kan alleen als $n = 2$. Voor $n = 2$ klopt de stelling: $\Phi_2 = x + 1$. □

Definitie 10. We noemen een polynoom in $\mathbb{Z}[x]$ primitief als er geen geheel getal groter dan 1 is dat alle coëfficiénten deelt.

Stelling 11. Als f en g beide primitief zijn in $\mathbb{Z}[x]$, dan is fg dat ook.

Bewijs. Stel f en g zijn primitief, maar fg niet. Dan is er een priemgetal p dat alle coëfficiënten van fg deelt. Als je nu het homomorfisme bekijkt $\psi : \mathbb{Z}[x] \rightarrowtail \mathbb{Z}/_p[x]$, dan geldt $0 = \psi(fg) = \psi(f)\psi(g) \neq 0$. Tegenspraak, dus is fg primitief. □

Stelling 12. Lemma van Gauss:
Als f monisch in $\mathbb{Z}[x]$ en g en h monisch in $\mathbb{Q}[x]$, dan

$$f = gh \Rightarrow g, h \in \mathbb{Z}[x]$$

Bewijs. We nemen u en v in $\mathbb{Z}$ zodat ug en vh primitief $\in \mathbb{Z}[x]$. Dit kan altijd. Stel je ug is niet primitief, dan deel je door de ggd van alle coëfficiënten. Maar omdat g monisch is, is die ggd een deler van u. Dus kun je een u' vinden met de goede eigenschappen. Dan is $ugvh$ primitief, dus is uvf primitief. Maar $f \in \mathbb{Z}[x]$ was al monisch, dus primitief. Dus u en v moeten 1 of -1 zijn. Maar ug en $vh \in \mathbb{Z}[x]$, dus ook g en $h \in \mathbb{Z}[x]$ □

Stelling 13. Voor alle $n \in \mathbb{N}$ geldt:
De coëfficiënten van Φ_n zitten in $\mathbb{Z}$.

Bewijs. Het bewijs gaat met inductie. Stel dat het waar is voor alle $d < n$. Dan $x^n - 1 = \Phi_n(x)K(x)$ met $K(x) = \prod_{d,d|n,d\neq n} \Phi_d \in \mathbb{Z}[x]$. Neem nu

$$\begin{aligned} \Phi_n &= b_d x^d + b_{d-1}x^{d-1} + \ldots + b_1 x + b_0 \\ K(x) &= a_e x^e + a_{e-1}x^{e-1} + \ldots + a_1 x + a_0 \\ X^n - 1 &= z_n x^n + z_{n-1}x^{n-1} + \ldots + z_1 x + z_0 \end{aligned}$$

Nu geldt $z_i = \sum_{0 \leq k \leq i} a_k b_{i-k}$. Stel nu dat voor alle $m < M$ geldt dat $b_m \in \mathbb{Q}$. We weten al dat $a_i \in \mathbb{Z}$. verder weten we ook dat $z_M \in \mathbb{Z}$. Dan is $a_0 b_M$ te schrijven als som van elementen uit $\mathbb{Q}$. Omdat a_0 geheel is zit b_M ook in $\mathbb{Q}$. Verder weten we dat $b_0 a_0 = -1$, dus $b_0 = \frac{-1}{a_0}$. Dus zitten alle b_i in $\mathbb{Q}$. Dan moet Φ_n dus in $\mathbb{Q}[x]$ zitten. Uit het Lemma van Gauss (stelling 12) volgt nu dat Φ_n in $\mathbb{Z}[x]$ zit. Rest nog te zeggen dat $\Phi_1 = x - 1 \in \mathbb{Z}[x]$ □

Er geldt zelfs dat Φ_n irreducibel is in $\mathbb{Z}[x]$. Φ_n zou ook gedefinieerd kunnen worden als het minimumpolynoom van een primitieve n-de machts wortel. Bewijzen doe ik deze bewering niet.

3 Platte cyclotomische polynomen

Als je cyclotomische polynomen gaat uitrekenen blijkt dat alle polynomen tot en met nummer 104 alleen maar $1, 0$ of -1 als coëfficiënt hebben. Het $105-$de polynoom blijkt een min twee te hebben op plek 8 ($-2x^7$). Waarom juist hier een min twee voorkomt en niet eerder, probeer ik te verklaren, alsmede probeer ik andere verbanden te zoeken tussen de coëfficiënten en het gekozen nummer van het polynoom. Mijn onderzoek richt zich op cyclotomische polynomen van de vorm Φ_{pqr} waarbij p, q en r drie verschillende priemgetallen zijn, met $2 < p < q < r$. Ook belangrijk is het aanwijzen van families van zogeheten platte cyclotomische polynomen. Een plat polynoom is een polynoom waar de coëfficiënten van in $\{-1, 0, 1\}$ zitten.

Stelling 14. Als $n = p * q$ met p en q twee verschillende priemgetallen, dan is Φ_n plat.

Bewijs. Volgens stelling 7 geldt

$$\Phi_{pq} = \frac{(x^{pq} - 1)}{(x - 1)\Phi_p\Phi_q} \tag{2}$$

Als we dit vermenigvuldigen met $(x - 1)/(x - 1)$ krijgen we

$$\Phi_{pq} = \frac{(x^{pq} - 1)(x - 1)}{(x^p - 1)(x^q - 1)}$$

Nu schrijven we de noemer om in een product van twee machtreeksen, en herschrijven we de teller zodat we krijgen:

$$\Phi_{pq} = (x^{pq+1} - x^{pq} - x + 1)(\sum_{m=0}^{\infty} x^{mp})(\sum_{m=0}^{\infty} x^{mq})$$

We weten dat de graad van Φ_{pq} gelijk is aan $\phi(pq) < pq$, dus als we de coëfficiënten van Φ_{pq} gaan bekijken, hoeven we ons geen zorgen te maken om machten groter of gelijk aan pq. De uitdrukking waar we dus naar kijken is

$$(-x + 1)(\sum_{m=0}^{q-1} x^{mp})(\sum_{m=0}^{p-1} x^{mq})$$

De enige manier waarop er in het eindproduct een coëfficiënt a met $|a| \geq 2$ kan komen te staan is als er k, l, k' en l' zijn met $k \neq k'$ en $l \neq l'$, en $kp+lq = k'p+l'q$. Maar als dat zo is dan geldt:

$$\begin{aligned} k'p - kp &= lq - l'q \\ (k' - k)p &= (l - l')q \end{aligned}$$

Zodat $q|(k - k')$. We kunnen zonder verlies van generaliteit aannemen dat $k' > k$, dus $k' = k+qm$ met $m > 0$ en dus $k'p+l'q = kp+pqm+l'q \geq pq > \phi(pq)$. Maar dan zou $k'p + l'q = kp + lq$ wegvallen, en dus coëfficiënt 0 hebben.

□

Stelling 15. Als n oneven is dan geldt:

$$\Phi_{2n}(x) = (-1)^{\phi(n)}\Phi_n(-x)$$

Bewijs. Bekijk voor oneven $n > 1$ een primitieve n-de eenheidswortel en noem hem ζ_n. Dan $(-\zeta_n)^{2n} = 1$. Stel er is een b zodat $0 < b < n$ en $(-\zeta_n)^b = 1$. Dan zijn er twee mogelijkheden. Of b is even, en in dat geval geldt $\zeta_n^b = 1$, wat tegen de aanname is dat ζ_n primitief is. Als b oneven is, geldt $\zeta_n^{2b} = 1$. Maar als $2b > n$, dan geldt ook $\zeta_n^{2b-n} = 1$. Maar $2b < 2n$, dus $2b - n < n$. Nu is er weer een tegenspraak met het feit dat ζ_n primitief is. Als $2b - n = n$, was niet $b < n$, en als $2b < n$, dan was er ook een tegenspraak. Nu is dus voor elke primitieve n-demachts eenheidswortel ϕ, $-\phi$ een primitieve $2n-$demachts eenheidswortel. Omdat n oneven is $\phi(2n) = \phi(2)\phi(n) = 1\phi(n)$, dus hebben we alle $2n$-de machts primitieve eenheidswortels. Verder geldt dat Φ_n voor alle n monisch is. Dus als $\Phi_n(x) = (x - \alpha_1)(x - \alpha_2)\dots(x - \alpha_{\phi(n)})$ dan

$$\begin{aligned}\Phi_{2n}(x) &= (x + \alpha_1)(x + \alpha_2)\dots(x + \alpha_{\phi(n)}) \\ &= (-1)^{\phi(n)}(-x - \alpha_1)(-x - \alpha_2)\dots(-x - \alpha_{\phi(n)}) \\ &= (-1)^{\phi(n)}\Phi_n(-x)\end{aligned}$$

□

Stelling 16.

$$\begin{aligned}\Phi_{pn}(x) &= \Phi_n(x^p) \text{ als } p|n. \\ &= \frac{\Phi_n(x^p)}{\Phi_n(x)} \text{ als } p \not| n\end{aligned} \tag{3}$$

Bewijs. Stel $p|n$, dan geldt voor elk nulpunt α van $\Phi_n(x^p)$ dat $\alpha^{pn} = 1$, en dat als $\beta = \alpha^p$, dat β een primitieve n-de machts eenheidswortel is. Stel nu $\alpha^k = 1$. Stel $p \not| k$. Dan is voor zekere $m, m' \in \mathbb{N}$en primitieve n-de machts eenheidswortel β:

$$\alpha^k = 1 \Rightarrow (\alpha^k)^p = (\alpha^p)^k = 1 \Rightarrow \beta^k = 1 \Rightarrow k = nm = pm'$$

tegenspraak, dus $p|k$. Nu geldt voor zekere $m \in \mathbb{N}$ en primitieve n-de machts eenheidswortel β:

$$\alpha^k = 1 \Rightarrow \beta^{k/p} = 1 \Rightarrow k/p = nm \Leftrightarrow k = pnm$$

Dit gaat al goed voor $m = 1$, dus is α een primitieve pn-de machts eenheidswortel en we hebben er $p\phi(n)$ verschillende. De graad van $\Phi_{pn}(x)$ is $\phi(pn)$. Maar

$p|n \Rightarrow \phi(pn) = p\phi(n)$. Dus is de bovenste gelijkheid van stelling 16 bewezen.
Stel nu dat $p \not| n$. Nu geldt wederom voor elk nulpunt α van $\Phi(x^p)$ dat $\alpha^{pn} = 1$. Omdat $p \not| n$ en p priem geldt $\text{ggd}(p, n) = 1$. Dus voor alle primitieve n-de machts eenheidswortel ζ_n geldt dat ζ_n^p dat ook is. Als je i laat lopen van 1 tot n krijg je alle n-de machts eenheidswortels. Als je ζ_n^{pi} laat lopen dus ook. Als $\text{ggd}(i, n) = 1$ dan heb je precies alle primitieve. Dus is elke primitieve n-de machts eenheidswortel een nulpunt van $\Phi_n(x^p)$. Dus $\Phi_n(x)|\Phi_n(x^p)$. Voor de overige nulpunten van $\Phi(x^p)$ geldt $\alpha^n \neq 1$, en α^p is een primitieve n-de machts eenheidswortel.
Pak nu de kleinste k waarvoor geldt $\alpha^k = 1$. Omdat α in een cyclysche groep van orde n zit moet k een deler van pn zijn. Stel nu $p \not| k$. Dan $k \not| p$ omdat p priem is. Dus $k|n$. Maar dan $\alpha^n = 1$. tegenspraak. Dus $p|k$. Nu geldt weer voor zekere $m \in \mathbb{N}$ en primitieve n-de machts eenheidswortel β:

$$\alpha^k = 1 \Rightarrow \beta^{k/p} = 1 \Rightarrow k/p = nm \Leftrightarrow k = pnm$$

Wederom doet $k = pn$ het al. Dus α is een primitieve n-de machts eeheidswortel. Er zijn er $p\phi(n) - \phi(n) = (p-1)\phi(n)\phi(pn)$. Dus hebben we ze allemaal. Dus geldt dat $\Phi_n(x^p) = \Phi_n(x)\phi_{np}(x)$ □

Φ_3, Φ_6 en Φ_{18} bijvoorbeeld zijn nu gemakkelijk uit te rekenen:

$$\begin{aligned}
\Phi_3(x) &= x^2 + x + 1 \\
\Phi_6(x) &= \Phi_{2*3}(x) = (-1)^{\phi(3)}\Phi_3(-x) = (-1)^2(x^2 - x + 1) = x^2 - x + 1 \\
\Phi_{18}(x) &= \Phi_{6*3}(x) = \Phi_6(x^3) = x^6 - x^3 + 1
\end{aligned}$$

We hebben nu een aantal stellingen om families van platte cyclotomische polynomen aan te wijzen. Als n een primgetal is, of een product van twee priemgetallen is Φ_n plat. Als Φ_n plat is, en n oneven, dan is Φ_{2n} ook plat. En als Φ_n plat is, en $p|n$ dan is Φ_{pn} ook plat. Dus, voor elke p, q priem, en $k, l, m \in \mathbb{N}$ geldt dat als $n = 2^k p^l q^m$, dan is Φ_n plat. $105 = 3 * 5 * 7$ is het kleinste getal dat niet van deze vorm is. En gelijk gaat het mis, er komt $-2x^7$ in voor. Drie verschillende priemgetallen zijn overigens geen garantie dat Φ_{pqr} niet plat is. Φ_{3*7*11} is namelijk wel plat. Sterker nog, er is zelfs een oneindige platte ternaire cyclotomische familie aan te wijzen Waarbij n een product is van drie verschillende priemgetallen.

4 Platte ternaire cyclotomische polynomen

We gaan nu zien hoe het komt dat de -2 in Φ_{105} voorkomt. Voordat we daaraan beginnen, schrijven we even wat om. Volgens stelling 7 geldt voor $n = pqr$:

$$x^n - 1 = \Phi_n \Phi_{pq} \Phi_{pr} \Phi_{qr} \Phi_p \Phi_q \Phi_r \Phi_1$$

Vul (1) en (2) hier in:

$$x^{pqr} - 1 = \frac{\Phi_n (x^{pq} - 1)(x^{pr} - 1)(x^{qr} - 1)(x - 1)}{(x^p - 1)(x^q - 1)(x^r - 1)}$$

Zodat

$$\Phi_{pqr} = \frac{(x^{pqr} - 1)(x^p - 1)(x^q - 1)(x^r - 1)}{(x^{pq} - 1)(x^{pr} - 1)(x^{qr} - 1)(x - 1)} \tag{4}$$

In het algemeen geldt dat $\frac{1}{1-x} = \sum_{n=1}^{\infty} x^n$ als formele machtreeks, zodat de onderste helft van (4) kan worden herschreven als:

$$\sum_{n=0}^{\infty} x^n \sum_{n=0}^{\infty} x^{pqn} \sum_{n=0}^{\infty} x^{prn} \sum_{n=0}^{\infty} x^{qrn} \tag{5}$$

Er zijn precies $\phi(pqr)$ wortels van Φ_{pqr}, zodat de graad van het polynoom $\phi(pqr) = (p-1)(q-1)(r-1)$ wordt. Als je de bovenste helft van (4) uitwerkt blijken alle machten groter of gelijk aan pqr dus weg te vallen na vermenigvuldiging met de machtreeksen. wat overblijft is dit:

$$-x^{p+q+r} + x^{q+r} + x^{p+r} + x^{p+q} - x^r - x^q - x^p + 1 \tag{6}$$

het is voldoende om naar deze termen in combinatie met de machtreeksen te kijken, bij het onderzoeken van de coëfficiënten van Φ_{pqr}.

Als we kijken naar de $m-$de coëfficiënt van een polynoom zien we dus dat het alleen belangrijk is om te kijken naar welke van de machten in (6) kleiner zijn dan m, en of m groter of kleiner is dan alle veelvouden van pq, pr en qr. Voor $m < p$ kun je alleen maar x^m krijgen door 1 in (6) te vermenigvuldigen met x^m in (5). Deze kun je alleen krijgen uit de eerste machtreeks. Dus alle

coëfficiënten zijn 1.
Als $p \leq m < q$ komt x^p in het spel. Omdat x^p ook nog steeds kleiner is dan x^{pq}(net als x^q overigens), en er in (6) voor x^p een -1 staat, komt de coëfficiënt op 0 uit. Als x^q in het spel komt, als $q \leq m <\min(p+q, r)$, wordt de coëfficiënt -1. Als $p + q > r$ is x^r de eerste macht waar weer iets verandert, en wel naar een -2 toe. Als we kijken naar Φ_{105}, dan zien we dat $3 + 5 = 8 > 7$, zodat de coëfficiënt -2 wordt.

Als je dit nog verder gaat uitwerken kun je een formule maken voor de coëfficiënt van een willekeurige macht, laten we zeggen ax^m. Een algemene formule kan dan als volgt gemaakt worden: Definiëer:

$$\begin{aligned} f(x,y) &= \max(\lfloor\frac{x-y}{qr}\rfloor, 0) + \max(\lfloor\frac{x-y}{pr}\rfloor, 0) + \\ &\quad \max(\lfloor\frac{x-y}{pq}\rfloor, 0) + \min(\max(x-y+1, 0), 1)) \end{aligned}$$

Nu hoort bij ax^m de formule:

$$\begin{aligned} a(m) &= f(m,0) - f(m,p) - f(m,q) - f(m,r) \\ &\quad + f(m,p+q) + f(m,p+r) + f(m,q+r) - f(m,p+q+r) \end{aligned}$$

Deze manier van coëfficiënten berekenen is niet erg handig als je het hele polynoom uit wil rekenen, maar voor het berekenen van precies de m-de coëfficiënt is deze methode vrij snel.
Met magma heb ik een hele hoop cyclotomische polynomen uitgerekend, en gezocht of ik de coëfficiënten van Φ_{pqr}kon linken aan p, q en r. Na een tijdje kwam ik op het volgende vermoeden. Ik heb het vervolgens nagerekend, en kwam er op uit dat de kleinste 8373 gevallen correct zijn. Het bleek dan ook te bewijzen te zijn.

Stelling 17. Als $n = pqr$ met p en q priem en $r = 2kpq \pm 1$ voor zekere $k \in \mathbb{N}$, dan geldt:

$$r = \text{priem} \Rightarrow \Phi_{pqr} \text{ is plat.}$$

Bewijs. Volgens stelling 16 geldt de volgende gelijkheid, die ik daarna uitwerk

met behulp van stelling 7:

$$\begin{aligned}
\Phi_{pqr}(x) &= \frac{\Phi_{pq}(x^r)}{\Phi_{pq}(x)} \\
&= \frac{\Phi_{pq}(x^r)\Phi_p(x)\Phi_q(x)(x-1)}{x^{pq}-1} \\
&= \Phi_{pq}(x^r)(x^{p-1}+x^{p-2}+\ldots+x+1)(x^q-1)\sum_{i=0}^{\infty}x^{pq} \\
&= \Phi_{pq}(x^r)g(x)\sum_{i=0}^{\infty}x^{pq}
\end{aligned}$$

Met $g(x) = (x^{q+p-1} + x^{q+p-2} + \ldots + x^q - x^{p-1} - \ldots - x - 1)$.
Nu is $\Phi_{pq}(x)$ plat, dus $\Phi_{pq}(x^r)$ ook. En omdat de hoogste macht in $g(x)$ kleiner is dan r, is $\Phi_{pq}(x^r)g(x)$ ook plat. Stel, er is een coëfficiënt groter dan 1 of kleiner dan -1. Die is te krijgen dan en slechts dan als er in $\Phi_{pq}(x^r)g(x)$ twee machten voorkomen die precies een pq-voud schelen. Er moeten dus m, m', a en $a' \in \mathbb{N}$ zijn, met m en $m' \leq \phi(pq)$, a en $a' \in \{0, \ldots, p-1\}$ of a en $a' \in \{q, \ldots, q(p-1)\}$ zodat $pq|mr + a - m'r - a'$.

$$\begin{aligned}
& pq|mr + a - m'r - a' \\
\Leftrightarrow\ & pq|(m-m')r + (a-a') \\
\Leftrightarrow\ & pq|(m-m)(2kpq \pm 1) + (a-a') \\
\Leftrightarrow\ & pq| \pm (m-m) + (a-a')
\end{aligned}$$

In alle gevallen is $|a - a'| \leq p - 1$. Maar om op een pq-voud uit te komen moet $|m - m'| \geq pq - (p - 1)$. Nu moet gelden:

$$pq - p - q + 1 = \phi(pq) \geq |m - m'| \geq pq - p + 1 > pq - p - q + 1$$

En er is een tegenspraak. Dus $\Phi_{pqr}(x)$ is plat.

□

De andere kant op is de stelling overigens niet waar. Als $p, q, r = 3, 7, 11$, zijn ook alle coëfficiënten 1, 0 en min 1. Als je jezelf niet beperkt tot $n = p*q*r$, kun je met behulp van deze stelling en stelling 16 nog meer oneindige families maken door n te vermenigvuldigen met $2^k p^l q^m r^j$ voor willekeurige $j, k, l, m \in \mathbb{N}$.

Referenties

[1] Nathan Kaplan, Flat cyclotomic polynomials of order three *journal of number theory, vol. 127, number 1, 2007, 0022-314X, DOI: 10.1016/j.jnt.2007.01.008*