Opgave Computeralgebra, week 6

Eerst komt er een lange inleiding (ten dele van wat op college behandeld is). Tot slot volgt de opgave.

Neem $n > 0$ geheel. Laat $\omega := e^{2\pi i/n}$. Dan is ω een *primitieve n-de machts wortel van 1*, d.w.z. dat $\omega^n = 1$, maar $\omega^k \neq 1$ als $0 < k < n$. Terzijde: we hadden ook $\omega := e^{2\pi im/n}$ met $0 < m < n$ en m en n co-priem kunnen nemen. Zo hadden we juist alle primitieve n-de machts wortels van 1 in $\mathbb{C}$ verkregen.

De *discrete Fourier-transformatie* (DFT) is de transformatie die een polynoom

$$f(x) = f_0 + f_1 x + \cdots + f_{n-1}x^{n-1} \in \mathbb{C}[x] \pmod{x^n - 1}$$

stuurt naar een polynoom

$$g(y) := \sum_{j=0}^{n-1} f(\omega^j) y^j \in \mathbb{C}[y] \pmod{y^n - 1}.$$

De *inverse discrete Fourier-transformatie* stuurt een polynoom

$$g(y) = g_0 + g_1 y + \cdots + g_{n-1}y^{n-1} \in \mathbb{C}[y] \pmod{y^n - 1}$$

naar een polynoom

$$\begin{aligned} h(x) :=& n^{-1} \sum_{k=0}^{n-1} g(\omega^{-k}) x^k \in \mathbb{C}[x] \pmod{x^n - 1} \\ =& n^{-1} \sum_{k=0}^{n-1} g(\omega^{n-k}) x^k \in \mathbb{C}[x] \pmod{x^n - 1} \end{aligned}$$

(de tweede som vermijdt negatieve machten van ω, wat geschikter is voor de computeralgebra). Als je begint met $f(x)$, daaruit de DFT $g(y)$ berekent en daaruit weer de inverse DFT $h(x)$ dan zal moeten gelden dat $h(x) = f(x)$. In plaats van te werken met de polynomen $f(x)$, $g(y)$ en $h(x)$ kun je ook werken met de coëfficiëntenrijen

$$\{f_0, f_1, \ldots, f_{n-1}\}, \quad \{g_0, g_1, \ldots, g_{n-1}\}, \quad \{h_0, h_1, \ldots, h_{n-1}\},$$

Als je begint met een polynoom $f(x)$ met gehele of rationale coefficiënten, dus als je in $\mathbb{Q}[x]$ werkt, dan zullen ω en de machten ω^k over het algemeen niet in $\mathbb{Q}$ zitten. Alleen $\omega^0 = 1$ en $\omega^{n/2} = -1$ (als n even) zitten in $\mathbb{Q}$. Doorgaans voldoen de machten ω^k wel aan bepaalde homogene lineaire relaties met gehele coëfficiënten. Er geldt bijv. altijd dat

$$1 + \omega + \omega^2 + \cdots + \omega^{n-1} = 0.$$

Als n een priemgetal is, dan is dit de enige lineaire relatie. Maar bijv. voor $n = 6$ hebben we ook de lineaire relaties

$$1 + \omega^3 = 0, \quad 1 + \omega^2 + \omega^4 = 0,$$

en geldt dus ook $1-\omega+\omega^2=0$ (de GCD van deze twee polynomen in ω). In feite kan er bewezen worden dat voor een polynoom $p(z)\in\mathbb{Q}[z]$ geldt dat $p(\omega)=0$ (voor $\omega=e^{2\pi i/6}$) dan en slechts dan als $p(z)=q(z)\,(1-z+z^2)$ voor een zeker polynoom $q(z)$. We noemen $\Phi_6(z):=1-z+z^2$ het *6de cyclotomische polynoom*. De graad van $\Phi_6(z)$ is 2. Het is niet toevallig dat deze graad gelijk is aan $\phi(6)$ (het aantal getallen k met $0<k\leq n=6$ dat co-priem is met $n=6$, nl. de getallen 1 en 5).

Voor algemene n geldt het volgende (zie §14.10 in het boek). Neem $\omega=e^{2\pi i/n}$. Dan is er een uniek polynoom $\Phi_n(z)$ met kopterm 1 en coëfficiënten in $\mathbb{Z}$ zo dat voor elk polynoom $p(z)\in\mathbb{Q}[z]$ geldt dat $p(\omega)=0$ desda $p(z)\equiv 0 \pmod{\Phi_n(z)}$. Het polynoom $\Phi_n(z)$ heet het *n-de cyclotomische polynoom*. Verder heeft $\Phi_n(z)$ graad $\phi(n)$, waarbij $\phi(n)$ de *totiënt-functie van Euler* is: het aantal getallen >0 en $\leq n$ dat co-priem is met n. In Mathematica krijgen we $\Phi_n(z)$ met het commando `Cyclotomic[n,z]` en $\phi(n)$ met het commando `EulerPhi[n]`. Een formule voor $\Phi_n(z)$ (niet zo geschikt voor berekeningen) is:

$$\Phi_n(z)=\prod_{i\leq j\leq n;\ (j,n)=1}(z-\omega^j).$$

Deze formule laat duidelijk zien dat $\Phi_n(z)$ graad $\phi(n)$ heeft.

Voor een implementatie van de DFT in een computeralgebra-systeem kunnen we, bij gegeven n, beginnen met een polynoom $f(x)$ met coëfficiënten in $\mathbb{Z}$ of $\mathbb{Q}$, en kunnenn we vervolgens de DFT $g(y)$ uitrekenen zonder ω te specificeren, maar door $g(y)$ te bekijken als polynoom in ω modulo $\Phi_n(\omega)$. Als je in Mathematica bijv. $\Phi_n(\omega)$ hebt aangeduid met Φ dan moet je op de verkregen DFT $g(y)$ nog ter vereenvoudiging loslaten het commando `PolynomialMod[g,Φ]`. Dan krijg je een polynoom in y en ω dat van graad $<\phi(n)$ in ω is.

Formulering van de opgave

1. Schrijf in Mathematica een procedure die voor gegeven n de DFT uitrekent van een polynoom $f(x)$ van graad $<n$ met rationale coëfficiënten (of zo je wilt de DFT van een rijtje $\{f_0,f_1,\ldots,f_{n-1}\}$ van rationale getallen). Werk met onbepaalde ω en neem het antwoord modulo $\Phi_n(\omega)$.
2. Schrijf een procedure die de inverse DFT uitrekent van een polynoom $g(y)$ met coëfficiënten in $\mathbb{Q}[\omega] \pmod{\Phi_n(\omega)}$.
3. Test voor verschillende n en voor verschillende invoer $f(x)$ (ook met random verkregen gehele coëfficiënten) dat de inverse DFT van de DFT van $f(x)$ weer $f(x)$ teruggeeft. Test dit ook als $f(x)$ zelf al coëfficiënten heeft die polynomen met (random verkregen) gehele coëfficiënten in ω zijn van graad $<\phi(n)$.
4. (eventueel) Neem $n=2^k$ en schrijf een procedure met een FFT-versie van de DFT. Vergelijk in testvorbeelden de uitkomst van de DFT met die van de FFT, ook wat timing betreft.