Irreducibele polynomen

Peter Koymans Student nummer: 0748876
p.h.koymans@student.tue.nl

Begeleid door
Aart Blokhuis

12 augustus 2013

Inhoudsopgave

1 Inleiding

In dit bachelorproject kijken we naar irreducibele polynomen in $\mathbb{Q}[X]$. We zullen uitgaan van basiskennis in algebra, voornamelijk in ringen. Eerst zullen we beginnen met een aantal definities in hoofdstuk 2. Daarna zijn we klaar om het lemma van Gauss te bewijzen in hoofdstuk 3. Dit lemma zal de basis vormen voor verdere studie naar irreducibele polynomen. In essentie vertelt dit lemma ons dat we net zo goed kunnen kijken naar irreducibele polynomen in $\mathbb{Z}[X]$.

Vanuit dit startpunt zijn we in staat om verschillende criteria te bewijzen voor irreducibiliteit in $\mathbb{Z}[X]$. Vanwege het lemma van Gauss kunnen we deze resultaten direct overdragen naar $\mathbb{Q}[X]$. In hoofdstuk 4 bespreken we simpele testen voor irreducibiliteit. In hoofdstuk 5 zullen we kijken naar reductie modulo p. We gaan vervolgens verder met het criterium van Eisenstein in hoofdstuk 6, het criterium van Perron in hoofdstuk 7 en het criterium van Cohn in hoofdstuk 8. Waar mogelijk zullen we ook kijken of het criterium noodzakelijk is voor irreducibiliteit.

Tenslotte kijken we nog naar verschillende toepassingen, waarbij we veel materiaal uit [3] gebruiken. In hoofdstuk 9 kijken we naar toepassingen van het criterium van Eisenstein, in hoofdstuk 10 gebruiken we algebraïsche getaltheorie om irreducibiliteit aan te tonen en in hoofdstuk 11 kijken we naar toepassingen van het criterium van Perron. Alle overige toepassingen staan in hoofdstuk 12.

2 Basiskennis

Het materiaal in dit en het volgende hoofdstuk is grotendeels gebaseerd op [1]. We werken in commutatieve ringen R met 1. We noemen een element $a \in R$ een eenheid als er een $b \in R$ is met $ab = 1$. Natuurlijk geldt dat b uniek is. Stel immers dat er $c \in R$ is met $ac = 1$. Er volgt dat

$$c = cab = acb = b.$$

We schrijven daarom $b = a^{-1}$. We zijn nu klaar om reducibele elementen te definiëren. Laat daartoe $a, b, c \in R$. Als we kunnen schrijven $a = bc$, dan zeggen we dat b en c factoren zijn van a. We zullen ook zeggen dat b een deler is van a en schrijven

$$b \mid a.$$

Als $a = bc$ waar noch b noch c een eenheid is, dan noemen we b en c echte factoren. In dit geval zeggen we dat a reducibel is. Merk op dat we inderdaad moeten eisen dat b en c geen eenheden zijn. Er geldt namelijk altijd

$$a = b(b^{-1}a).$$

Tenslotte kunnen we irreducibele elementen definiëren. Hierbij moeten we echter wel voorzichtig zijn. Immers, laat $a \in R$ een eenheid zijn. We zullen zien dat een eenheid geen echte factoren kan hebben. Stel immers maar $a = bc$ voor $a, b, c \in R$. Er volgt dan dat

$$1 = aa^{-1} = bca^{-1}.$$

We zien dus dat b en c ook eenheden zijn. We introduceren het begrip irreducibiliteit daarom alleen maar voor elementen $a \in R$, die geen eenheid zijn. We zeggen dus dat een niet eenheid $a \in R$ irreducibel is als het geen echte factoren heeft. Als laatste introduceren we nog het begrip domein. We noemen R een domein als voor alle $a, b \in R$ geldt

$$ab = 0 \Rightarrow a = 0 \vee b = 0.$$

Een domein wordt ook wel een integriteitsgebied genoemd. We zijn nu klaar voor de volgende volgende stelling.

Stelling 2.1 Laat R een domein zijn. Dan zijn de eenheden in $R[X]$ precies de polynomen $p(X) = c$ waar c een eenheid is in R.
Bewijs Als $p(X) = c$ met c een eenheid in R, dan is het duidelijk dat p een eenheid is in $R[X]$. Andersom, laat $p \in R[X]$ een eenheid zijn. Dit betekent dat er een $q \in R[X]$ is zodanig dat

$$pq = 1.$$

Schrijf nu $p(X) = p_n X^n + \cdots + p_0$ met $p_n \neq 0$ en $q(X) = q_m X^m + \cdots + q_0$ met $q_m \neq 0$. De coëfficiënt voor X^{n+m} is dan $p_n q_m$. Aangezien R een domein is, volgt dat $p_n q_m \neq 0$. Maar dan kan $pq = 1$ alleen als $n = 0$ en $m = 0$. We zien dus dat

$$p_0 q_0 = 1.$$

Dus we concluderen dat $p(X) = p_0$ met p_0 een eenheid in R, zoals we moesten bewijzen. □

De eenheden in $\mathbb{Z}$ en $\mathbb{Q}$ kunnen we eenvoudig vinden. Natuurlijk geldt dat $x \in \mathbb{Z}$ is een eenheid dan en slechts dan als $x = 1$ of $x = -1$. Op vergelijkbare wijze zien we dat $x \in \mathbb{Q}$ een eenheid is dan en slechts dan als $x \neq 0$. Dit vatten we samen in gevolg 2.2.

Gevolg 2.2 De eenheden in $\mathbb{Z}[X]$ zijn de polynomen $p(X) = c$ met $c = 1$ of $c = -1$. De eenheden in $\mathbb{Q}[X]$ zijn de polynomen $p(X) = c$ met $c \neq 0$.

3 Lemma van Gauss

In dit hoofdstuk bewijzen we het lemma van Gauss in verschillende vormen. We beginnen met de klassieke versie.

Stelling 3.1 Laat $p \in \mathbb{Z}[X]$ en $q, r \in \mathbb{Q}[X]$. Als $p = qr$, dan is er een $\lambda \in \mathbb{Q}$ met $\lambda \neq 0$ zodanig dat $\lambda q \in \mathbb{Z}[X]$ en $\lambda^{-1} r \in \mathbb{Z}[X]$.
Bewijs Kies $m \in \mathbb{Z}$ zodanig dat $q' = mq \in \mathbb{Z}[X]$ en $n \in \mathbb{Z}$ zodanig dat $r' = nr \in \mathbb{Z}[X]$. Hierbij eisen we bovendien dat $m \neq 0$ en $n \neq 0$. We zien dan dat:

$$mnp = q'r'.$$

Schrijf nu even $a = mn \in \mathbb{Z}$. Dan staat er

$$ap = q'r'.$$

Het doel is nu om aan te tonen dat $d \mid a$ (in $\mathbb{Z}$) impliceert dat $d \mid q'$ of $d \mid r'$ (in $\mathbb{Z}[X]$) voor d priem. Dit zullen we doen in lemma 3.2. Op deze manier kunnen we blijven uitdelen totdat

$$p = q''r''$$

met $q'' \in \mathbb{Z}[X]$ en $r'' \in \mathbb{Z}[X]$ (opmerking: dit kan natuurlijk alleen als $a \neq 0$, maar dit geldt vanwege de keuze van m en n). Hierbij hebben we alleen maar gedeeld en vermenigvuldigd met getallen in $\mathbb{Z}$. Er volgt dus dat $q'' = \lambda q$ en $r'' = \mu r$ met $\lambda, \mu \in \mathbb{Q}$. Uit $p = qr$ kunnen we dan tenslotte concluderen dat $\mu = \lambda^{-1}$, waarmee het bewijs voltooid is. □

Lemma 3.2 Laat $p, q, r \in \mathbb{Z}[X]$ en $a \in \mathbb{Z}$. Stel bovendien dat $ap = qr$ en laat d een priemgetal zijn met $d \mid a$ in $\mathbb{Z}$. Dan geldt dat $d \mid q$ of $d \mid r$ in $\mathbb{Z}[X]$: hier vatten we d dus op als polynoom.
Bewijs Merk op dat $a \mid qr$ voor $a \in \mathbb{Z}$. Dit betekent dat alle coëfficiënten van qr een veelvoud zijn van a. Aangezien $d \mid a$, geldt dus dat alle coëfficiënten van qr een veelvoud zijn van d. We moeten bewijzen dat $d \mid q$ of $d \mid r$, oftewel dat d alle coëfficiënten van q deelt of alle coëfficiënten van r. We schrijven

$$q(X) = \sum_{k=0}^{n} q_k X^k$$

$$r(X) = \sum_{k=0}^{m} r_k X^k.$$

Er volgt dat

$$qr(X) = \sum_{k=0}^{n+m} \sum_{a+b=k} q_a r_b X^k.$$

Hierbij definiëren dat $q_a = 0$ als $a > n$ en $r_b = 0$ als $b > m$. Onze aanname komt dus neer op

$$d \mid \sum_{a+b=k} q_a r_b \tag{1}$$

voor alle natuurlijke k. Bekijk nu de bewering $P(a, b)$

$$(\forall x : 0 \leq x \leq a : d \mid q_x) \vee (\forall y : 0 \leq y \leq b : d \mid r_y)$$

We zullen dit bewijzen voor alle natuurlijke a en b met inductie op $a + b$. De stelling is simpelweg $P(n, m)$, zodat de stelling hiermee onmiddellijk volgt. De inductiebasis is dus $a + b = 0$, kortom $a = b = 0$. We moeten $P(0, 0)$ bewijzen, oftewel

$$d \mid q_0 \vee d \mid r_0.$$

Echter onze aanname in (1) voor $k = 0$ geeft

$$d \mid \sum_{a+b=0} q_a r_b = q_0 r_0.$$

En aangezien d priem is, volgt de inductiebasis. Stel nu dat het waar is voor alle natuurlijke a en b met $a + b$ vast. We moeten het nu bewijzen voor $P(e, f)$ met $e + f = a + b + 1$. Echter, per inductiehypothese geldt $P(e - 1, f)$ en $P(e, f - 1)$. We mogen dus vanwege de inductiehypothese aannemen dat

$$(\forall x : 0 \leq x \leq e - 1 : d \mid q_x) \wedge (\forall y : 0 \leq y \leq f - 1 : d \mid r_y). \tag{2}$$

Immers, anders volgt triviaal $P(e, f)$. Bekijk nu onze aanname in (1) voor $k = e + f$. Dit geeft (let op, $a + b$ in deze som is slechts een variabele voor de sommatie)

$$d \mid \sum_{a+b=k} q_a r_b. \tag{3}$$

En als we nu (2) en (3) combineren, krijgen we dat

$$d \mid q_e r_f.$$

Aangezien d priem is, volgt dus

$$d \mid q_e \vee d \mid r_f. \tag{4}$$

Combineren van (2) en (4) bewijst $P(e, f)$. Daarmee is de inductie voltooid. □

In het bewijs van lemma 3.2 moet men nog oppassen voor het geval dat $e = 0$ of $f = 0$. Dan kunnen we namelijk $P(e-1, f)$ en $P(e, f-1)$ niet concluderen uit de inductiehypothese. Gelukkig zijn $P(-1, f)$ en $P(e, -1)$ echter triviaal waar, zodat dit geen probleem vormt.

Voordat we dit hoofdstuk afsluiten, zullen we het lemma van Gauss opnieuw formuleren in een voor ons nuttigere vorm. Zij daartoe $p \in \mathbb{Q}[X]$ een willekeurig polynoom. We weten al dat er een $n \in \mathbb{Z}$ is met $n \neq 0$ zodat $np \in \mathbb{Z}[X]$. Als alle coëfficiënten van np vervolgens een gemeenschappelijke deler hebben, kunnen we de gemeenschappelijke delers uitdelen. Hierdoor krijgen we een polynoom $p' \in \mathbb{Z}[X]$ met $p' = qp$ voor zekere $q \in \mathbb{Q}$ met $q \neq 0$, waarbij bovendien geldt dat de grootste gemene deler van alle coëfficiënten 1 is. Nu beweren we dat p irreducibel is in $\mathbb{Q}[X]$ dan en slechts dan als p' irreducibel is in $\mathbb{Z}[X]$.

Hiertoe moeten we terug naar de resultaten in hoofdstuk 2. We merken eerst op dat cp irreducibel is als c een eenheid is en p irreducibel is. Vanwege gevolg 2.2 geldt dus dat p irreducibel is in $\mathbb{Q}[X]$ dan en slechts dan als p' irreducibel is in $\mathbb{Q}[X]$. We zouden nu graag concluderen dat irreducibiliteit van p' in $\mathbb{Q}[X]$ irreducibiliteit van p' in $\mathbb{Z}[X]$ impliceert. Dit lijkt triviaal, maar de eenheden in $\mathbb{Z}[X]$ zijn onverwachts anders dan in $\mathbb{Q}[X]$. Bekijk bijvoorbeeld het polynoom

$$q(X) = 3X^2 + 3X + 3.$$

In $\mathbb{Q}[X]$ is dit polynoom irreducibel, in $\mathbb{Z}[X]$ heeft dit polynoom echter de deler $r(X) = 3$. Dit wordt veroorzaakt door het feit dat $r(X) = 3$ geen eenheid is in $\mathbb{Z}[X]$, maar wel in $\mathbb{Q}[X]$. Dus, het zou nog kunnen dat p' een deler heeft van de vorm $s(X) = c$ met c geen eenheid in $\mathbb{Z}$. Om deze reden is de eis dat de grootste gemene deler van alle coëfficiënten 1 is zo belangrijk: dit sluit namelijk delers van de vorm $s(X) = c$ met c geen eenheid in $\mathbb{Z}$ uit.

Tenslotte moeten we nog concluderen dat irreducibiliteit van p' in $\mathbb{Z}[X]$ irreducibiliteit van p' in $\mathbb{Q}[X]$ impliceert. Echter, dit volgt onmiddellijk uit stelling 3.1. Dit betekent dat we vanaf nu alleen maar irreducibiliteit in $\mathbb{Z}[X]$ hoeven te bekijken. Het is eenvoudig om de resultaten dan over te dragen naar $\mathbb{Q}[X]$.

4 Eenvoudige testen voor irreducibiliteit

In dit hoofdstuk bespreken we verschillende eenvoudige testen voor irreducibiliteit. We beginnen met zogenaamde shifts, zoals geformuleerd in stelling 4.1.

Stelling 4.1 Laat $f \in \mathbb{Z}[X]$ en $a \in \mathbb{Z}$. Dan geldt

$$f(X) \text{ irreducibel } \Leftrightarrow f(X+a) \text{ irreducibel.}$$

Bewijs We bewijzen eerst de implicatie van links naar rechts. De implicatie van rechts naar links gaat dan analoog. Stel dus dat $f(X)$ irreducibel is en stel bovendien dat

$$f(X+a) = g(X)h(X).$$

We moeten bewijzen dat $g(X)$ of $h(X)$ een eenheid is. Echter, we weten dat

$$f(X) = g(X-a)h(X-a).$$

Aangezien $f(X)$ irreducibel is, volgt dat $g(X-a)$ of $h(X-a)$ een eenheid is. Als $g(X-a)$ een eenheid is, dan volgt $g(X-a) = 1$ of $g(X-a) = -1$ vanwege gevolg 2.2. We concluderen dat respectievelijk $g(X) = 1$ of $g(X) = -1$, zodat $g(X)$ een eenheid is. Als $h(X-a)$ een eenheid is, dan volgt eveneens $h(X-a) = 1$ of $h(X-a) = -1$ vanwege gevolg 2.2. Weer kunnen we concluderen dat respectievelijk $h(X) = 1$ of $h(X) = -1$, zodat $h(X)$ een eenheid is. □

Ook kunnen we het polynoom omkeren.

Stelling 4.2 Laat $f \in \mathbb{Z}[X]$ en schrijf $n = \deg f$. Als $f(0) \neq 0$, dan geldt

$$f(X) \text{ irreducibel } \Leftrightarrow X^n f(\frac{1}{X}) \text{ irreducibel.}$$

Bewijs Uit de aanname $f(0) \neq 0$ volgt dat $f(X)$ en $X^n f(\frac{1}{X})$ dezelfde graad hebben. Met behulp van gevolg 2.2 is het nu eenvoudig om te bewijzen dat

$$f(X) \text{ eenheid } \Leftrightarrow X^n f(\frac{1}{X}) \text{ eenheid.}$$

We moeten nu nog bewijzen dat

$$f(X) \text{ reducibel } \Leftrightarrow X^n f(\frac{1}{X}) \text{ reducibel.}$$

Stel dus dat $f(X)$ reducibel is. Dit betekent dat

$$f(X) = g(X)h(X),$$

waarbij $g(X)$ en $h(X)$ geen eenheden zijn. Schrijf $k = \deg g$ en $l = \deg h$. Dan geldt $k+l = n$, zodat

$$X^n f(\frac{1}{X}) = X^n g(\frac{1}{X})h(\frac{1}{X}) = X^k g(\frac{1}{X})X^l h(\frac{1}{X}).$$

Aangezien $g(X)$ en $h(X)$ geen eenheden zijn, zijn ook $X^k g(\frac{1}{X})$ en $X^l h(\frac{1}{X})$ geen eenheden. We concluderen dat $X^n f(\frac{1}{X})$ reducibel is. De implicatie van rechts naar links gaat analoog. □

Ook is het eenvoudig om te testen op lineaire factoren. Deze stelling is makkelijker te formuleren in $\mathbb{Q}[X]$ en staat ook wel bekend als de rational root theorem.

Stelling 4.3 Laat $f \in \mathbb{Q}[X]$ met gehele coëfficiënten. Laat bovendien $c \in \mathbb{Q}$ en schrijf $c = \frac{p}{q}$ met $\text{ggd}(p, q) = 1$. Als $X - c \mid f$, dan geldt $p \mid a_0$ en $q \mid a_n$.
Bewijs Het is een bekende stelling dat

$$X - c \mid f \Leftrightarrow f(c) = 0.$$

Stel dus dat $f(c) = 0$ en schrijf

$$f(X) = \sum_{k=0}^{n} a_k X^k$$

met $a_i \in \mathbb{Z}$. Uitwerken van $f(c) = 0$ geeft

$$f(c) = \sum_{k=0}^{n} a_k c^k = \sum_{k=0}^{n} a_k \frac{p^k}{q^k} = 0. \qquad (*)$$

We zullen eerst bewijzen dat $p \mid a_0$. Hiertoe herschrijven we (*) tot

$$\sum_{k=0}^{n} a_k \frac{p^k q^{n-k}}{q^n} = 0.$$

Maar dit impliceert dat

$$\sum_{k=0}^{n} a_k p^k q^{n-k} = 0.$$

Dit herschrijven we weer tot

$$a_0 q^n = -\sum_{k=1}^{n} a_k p^k q^{n-k} = -p \sum_{k=1}^{n} a_k p^{k-1} q^{n-k}.$$

Merk op dat $\sum_{k=1}^{n} a_k p^{k-1} q^{n-k} \in \mathbb{Z}$, zodat $p \mid a_0 q^n$. Aangezien $\text{ggd}(p, q) = 1$, concluderen we dat $p \mid a_0$. Resteert te bewijzen dat $q \mid a_n$. We gaan hiervoor weer uit van (*). Vermenigvuldigen met q^{n-1} en herschrijven van (*) geeft dan

$$a_n \frac{p^n}{q} = -\sum_{k=0}^{n-1} a_k p^k q^{n-k-1}.$$

Merk nu op dat $-\sum_{k=0}^{n-1} a_k p^k q^{n-k-1} \in \mathbb{Z}$, zodat $a_n \frac{p^n}{q} \in \mathbb{Z}$. Er volgt dus $q \mid a_n p^n$. Aangezien $\text{ggd}(p, q) = 1$, concluderen we dat $q \mid a_n$. □

Het elegante aan stelling 4.3 is dat het ons in staat stelt om alle lineaire factoren te vinden in eindige tijd. We zullen nu stelling 4.4 bewijzen. Deze stelling legt een verband tussen irreducibele polynomen en priemgetallen. Hoewel deze stelling zelf niet bijzonder interessant

is, zal het wel aanleiding zijn om een aantal bijzonder interessante stellingen te bekijken. Een van deze stellingen is het criterium van Cohn, dat we in hoofdstuk 8 zullen bespreken.

Stelling 4.4 Laat $f \in \mathbb{Z}[X]$. Stel dat er oneindig veel $x \in \mathbb{Z}$ zijn zodat $f(x)$ priem is. Dan is f irreducibel.
Bewijs Stel dat we f kunnen schrijven als

$$f = gh$$

voor $g, h \in \mathbb{Z}[X]$. Ons doel zal zijn om nu te bewijzen dat g of h een eenheid is in $\mathbb{Z}[X]$. Fixeer een $x \in \mathbb{Z}$ zodat $f(x)$ priem is. Er volgt dat

$$f(x) = g(x)h(x).$$

We concluderen dat $g(x) = 1$, $g(x) = -1$, $h(x) = 1$ of $h(x) = -1$. Vanwege het ladenprincipe volgt nu dat er

1. of oneindig veel $x \in \mathbb{Z}$ zijn zodat $g(x) = 1$;
2. of oneindig veel $x \in \mathbb{Z}$ zijn zodat $g(x) = -1$;
3. of oneindig veel $x \in \mathbb{Z}$ zijn zodat $h(x) = 1$;
4. of oneindig veel $x \in \mathbb{Z}$ zijn zodat $h(x) = -1$.

Maar dan volgt respectievelijk $g = 1$, $g = -1$, $h = 1$ of $h = -1$. Vanwege gevolg 2.2 concluderen we nu dat g of h eenheden zijn in $\mathbb{Z}[X]$. □

Een interessante vraag is nu: stel dat $f \in \mathbb{Z}[X]$ irreducibel is. Zijn er dan oneindig veel $x \in \mathbb{Z}$ zodat $f(x)$ priem is? Deze vraag is vrij eenvoudig te beantwoorden. Bekijk bijvoorbeeld maar

$$f(X) = X^2 + X + 4.$$

Het is niet moeilijk om te zien dat f irreducibel is, maar $2 \mid f(x)$ voor alle $x \in \mathbb{Z}$. We zullen de vraag daarom opnieuw formuleren als: stel dat $f \in \mathbb{Z}[X]$ irreducibel is met graad groter dan 1. Stel bovendien dat $\text{ggd}(f(1), f(2), \ldots) = 1$. Het Bunyakovsky vermoeden zegt dan dat er oneindig veel $x \in \mathbb{Z}$ zijn zodat $f(x)$ priem is. Dit vermoeden werd al geformuleerd in 1857, maar is nog steeds niet bewezen. We weten wel dat deze bewering waar is als f graad 1 heeft. Dit is de stelling van Dirichlet over priemgetallen in rekenkundige rijen.

Als laatste zullen we nog kijken naar dubbele nulpunten. Daartoe moeten we natuurlijk eerst definiëren wat een dubbel nulpunt is. Laat nu $f \in \mathbb{C}[X]$ en $\alpha \in \mathbb{C}$. We zeggen dat α een dubbel nulpunt is als

$$(X - \alpha)^2 \mid f.$$

Merk op dat dan zeker

$$X - \alpha \mid f$$

waaruit volgt dat $f(\alpha) = 0$. Verder definiëren we nog de afgeleide als een afbeelding van $\mathbb{C}[X] \to \mathbb{C}[X]$, zodat het beeld van

$$f(X) = \sum_{k=0}^{n} a_k X^k$$

gelijk is aan

$$f'(X) = \sum_{k=1}^{n} k a_k X^{k-1} = \sum_{k=0}^{n-1} (k+1) a_{k+1} X^k.$$

Merk op dat we de afgeleide ook kunnen beschouwen als een afbeelding $\mathbb{Z}[X] \to \mathbb{Z}[X]$ of $\mathbb{Q}[X] \to \mathbb{Q}[X]$. De gebruikelijke regels voor differentiëren blijven geldig. In het bijzonder geldt dat

$$(fg)' = f'g + fg'.$$

We hebben nu de volgende stelling.

Stelling 4.5 Laat $f \in \mathbb{C}[X]$. Dan geldt

$$\alpha \in \mathbb{C} \text{ is een dubbel nulpunt } \Leftrightarrow f(\alpha) = 0 \wedge f'(\alpha) = 0.$$

Bewijs Stel dat $\alpha \in \mathbb{C}$ een dubbel nulpunt is. Dit betekent per definitie dat

$$(X - \alpha)^2 \mid f.$$

Dus we kunnen schrijven $f(X) = (X - \alpha)^2 g(X)$ voor zekere $g \in \mathbb{C}[X]$. Het is duidelijk dat $f(\alpha) = 0$. Verder vinden we dat

$$f'(X) = (X - \alpha)^2 g'(X) + 2(X - \alpha) g(X)$$

zodat ook $f'(\alpha) = 0$. Dit voltooit de implicatie van links naar rechts. Stel dus nu dat $f(\alpha) = 0$ en $f'(\alpha) = 0$. Er volgt dat

$$X - \alpha \mid f.$$

Dus we kunnen schrijven $f(X) = (X - \alpha) g(X)$ voor zekere $g \in \mathbb{C}[X]$. Differentiëren geeft nu

$$f'(X) = (X - \alpha) g'(X) + g(X).$$

Invullen van $X = \alpha$ geeft

$$f'(\alpha) = (\alpha - \alpha) g'(\alpha) + g(\alpha) = g(\alpha).$$

Aangezien $f'(\alpha) = 0$, concluderen we dat $g(\alpha) = 0$. Maar dan geldt dat

$$X - \alpha \mid g$$

oftewel $g(X) = (X - \alpha) h(X)$ voor zekere $h \in \mathbb{C}[X]$. We concluderen dat

$$f(X) = (X - \alpha)^2 h(X)$$

en daarmee dat

$$(X - \alpha)^2 \mid f.$$

Dus α is een dubbel nulpunt, waarmee het bewijs is voltooid. □

We hebben nu een simpele methode om alle dubbele nulpunten van een polynoom $f \in \mathbb{C}[X]$ uit te delen. Dit kunnen we namelijk doen door $\gcd(f, f')$ te berekenen. Merk op dat dit ook werkt als $f \in \mathbb{Q}[X]$. Dan geldt immers ook $f' \in \mathbb{Q}[X]$. We voeren eerst de berekening van

ggd(f, f') uit in $\mathbb{C}[X]$. Echter, elke stap in deze berekening kunnen we ook uitvoeren in $\mathbb{Q}[X]$. Er volgt dus dat ggd$(f, f') \in \mathbb{Q}[X]$. Het is belangrijk om te beseffen dat dit niet onmiddellijk volgt uit $f, f' \in \mathbb{Q}[X]$, aangezien we ggd(f, f') in principe in $\mathbb{C}[X]$ berekenen. We concluderen dus dat we alle dubbele nulpunten van een polynoom $f \in \mathbb{Q}[X]$ kunnen uitdelen. Tenslotte zullen we nog kijken naar twee belangrijke lemma's.

Lemma 4.6 Laat $a, b \in \mathbb{Z}$ en laat bovendien $n \in \mathbb{Z}$ met $n \geq 0$. Dan geldt

$$a - b \mid a^n - b^n.$$

Bewijs 1 Fixeer $b \in \mathbb{Z}$ en bekijk het polynoom

$$f(X) = X^n - b^n.$$

Merk op dat $f(b) = 0$, waaruit volgt dat

$$X - b \mid X^n - b^n.$$

Maar dan geldt voor alle $a \in \mathbb{Z}$

$$a - b \mid a^n - b^n.$$

Dit voltooit het bewijs. □

Bewijs 2 We hebben de volgende factorisatie voor alle $a, b \in \mathbb{Z}$ en $n \in \mathbb{Z}$ met $n \geq 0$

$$a^n - b^n = (a - b) \cdot (\sum_{i=0}^{n-1} a^i b^{n-i-1}).$$

Hieruit concluderen we dat

$$a - b \mid a^n - b^n,$$

waarmee het bewijs is voltooid. □

Het is opvallend dat in beide bewijzen polynomen een belangrijke rol spelen. In bewijs 1 is deze rol duidelijk. Echter, in bewijs 2 is dit iets subtieler. In feite berust het tweede bewijs op een gedeeltelijke factorisatie van het polynoom $f(X, Y) = X^n - Y^n$ in $\mathbb{Z}[X, Y]$. We zijn nu in staat om lemma 4.7 te bewijzen. Dit is een elegante generalisatie van lemma 4.6 voor polynomen.

Lemma 4.7 Laat $a, b \in \mathbb{Z}$ en laat bovendien $f \in \mathbb{Z}[X]$. Dan geldt

$$a - b \mid f(a) - f(b).$$

Bewijs Schrijf f als

$$f(X) = \sum_{i=0}^{n} c_i X^i$$

met $c_i \in \mathbb{Z}$ voor $i = 0, \cdots, n$. Dan geldt

$$f(a) - f(b) = \sum_{i=0}^{n} c_i a^i - \sum_{i=0}^{n} c_i b^i = \sum_{i=0}^{n} c_i (a^i - b^i).$$

Vanwege lemma 4.6 weten we dat $a - b \mid a^i - b^i$ voor $i = 0, \cdots, n$. Hieruit volgt dat

$$a - b \mid \sum_{i=0}^{n} c_i(a^i - b^i) = f(a) - f(b),$$

wat we moesten bewijzen. □

5 Reductie modulo p

Laat $f, g, h \in \mathbb{Z}[X]$. Stel dat

$$f = gh$$

waar g en h echte factoren zijn. Dit betekent dus dat f reducibel is. Het idee is nu om dit over te dragen naar $\mathbb{Z}/p\mathbb{Z}[X]$ voor een priemgetal p. Natuurlijk geldt ook in $\mathbb{Z}/p\mathbb{Z}[X]$ dat

$$f = gh.$$

Als g en h nog steeds echte factoren zijn, dan volgt meteen dat f reducibel is in $\mathbb{Z}/p\mathbb{Z}[X]$. Het voordeel van $\mathbb{Z}/p\mathbb{Z}[X]$ is natuurlijk dat er maar eindig veel mogelijkheden zijn voor elke coëfficient. Dit geeft ons een nieuwe mogelijkheid om irreducibiliteit aan te tonen.

Eerst moeten we echter onze notatie wat uitbreiden. Bekijk daartoe het natuurlijke homomorfisme $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$. Dit kunnen we natuurlijk uitbreiden tot een homomorfisme $\mathbb{Z}[X] \to \mathbb{Z}/p\mathbb{Z}[X]$. Als $f \in \mathbb{Z}[X]$, dan geven we met $\hat{f} \in \mathbb{Z}/p\mathbb{Z}[X]$ het beeld aan van f onder dit homomorfisme. Nu kunnen we de volgende stelling bewijzen.

Stelling 5.1 Laat $f \in \mathbb{Z}[X]$ en stel dat $\hat{f} \in \mathbb{Z}/p\mathbb{Z}[X]$ irreducibel is in $\mathbb{Z}/p\mathbb{Z}[X]$ voor een zeker priemgetal p. Als de graad van f gelijk is aan de graad van $\hat{f}$, dan is f irreducibel op constante factoren na.
Bewijs Het is duidelijk dat f geen eenheid kan zijn. Immers, als f een eenheid is, dan is ook $\hat{f}$ een eenheid. Stel dus dat f reducibel is met niet constante factoren. Dit betekent dat er $g, h \in \mathbb{Z}[X]$ zijn met

$$f = gh;$$

$$\deg g \geq 1;$$

$$\deg h \geq 1.$$

Er volgt nu in $\mathbb{Z}/p\mathbb{Z}[X]$ dat

$$\hat{f} = \hat{g}\hat{h}.$$

Aangezien $\deg \hat{f} = \deg f$, volgt er dat $\deg \hat{g} = \deg g \geq 1$ en $\deg \hat{h} = \deg h \geq 1$. Maar dan kunnen $\hat{g}$ en $\hat{h}$ geen eenheden zijn. Dit betekent dat $\hat{f}$ reducibel is in $\mathbb{Z}/p\mathbb{Z}[X]$. Dit is de gezochte tegenspraak. □

Het is goed om ons nu af te vragen of het omgekeerde ook geldt. Stel dus dat $f \in \mathbb{Z}[X]$ irreducibel is. Is er dan een priemgetal p zodat $\hat{f} \in \mathbb{Z}/p\mathbb{Z}[X]$ irreducibel is? Het verrassende antwoord is nee, zoals de volgende stelling laat zien. Deze stelling wordt in [2] zonder bewijs genoemd. We zullen hierbij intensief gebruik maken van kwadraatresten.

Stelling 5.2 Laat $f(X) = X^4 + 6X^2 + 1 \in \mathbb{Z}[X]$ en laat p een priemgetal zijn. Dan gelden de volgende eigenschappen

1. f is irreducibel in $\mathbb{Z}[X]$;
2. $\hat{f}$ is reducibel in $\mathbb{Z}/p\mathbb{Z}[X]$.

Bewijs De eerste eigenschap is eenvoudig na te gaan. We zullen ons daarom richten op de tweede eigenschap. We zullen bewijzen dat

$$\hat{f}(X) = X^4 + 6X^2 + 1 = (X^2 + aX + b)(X^2 + cX + d)$$

in $\mathbb{Z}/p\mathbb{Z}[X]$ voor zekere $a, b, c, d \in \mathbb{Z}/p\mathbb{Z}[X]$. Dit is equivalent met het volgende systeem vergelijkingen

$$\begin{aligned} a + c &\equiv 0 \mod p \\ ac + b + d &\equiv 6 \mod p \\ ad + bc &\equiv 0 \mod p \\ bd &\equiv 1 \mod p. \end{aligned}$$

We onderscheiden nu drie gevallen afhankelijk van p.

1. $p = 2$: in dit geval voldoet $a = c = 0$ en $b = d = 1$.

2. $p = 4k + 1$: we weten dat -1 een kwadraatrest is. Bovendien weten we dat 4 een kwadraatrest is. We concluderen dat -4 een kwadraatrest is. Kies a nu zodanig dat

   $$a^2 \equiv -4 \mod p.$$

   Kies verder $c = -a$ en $b = d = 1$. Dan hebben we inderdaad een oplossing van het systeem vergelijkingen.

3. $p = 4k + 3$: we weten dat -1 geen kwadraatrest is. Daarom geldt dat -8 of 8 een kwadraatrest moet zijn. Immers, het product van twee niet kwadraatresten is een kwadraatrest. Als -8 een kwadraatrest is, kies a dan zodanig dat

   $$a^2 \equiv -8 \mod p.$$

   Kies verder $c = -a$ en $b = d = -1$. Dit geeft weer een oplossing van het systeem vergelijkingen. Als 8 een kwadraatrest is, kies b dan zodanig dat

   $$(b - 3)^2 \equiv 8 \mod p.$$

   Kies verder $a = c = 0$ en $d = 6 - b$. Ook dit is een oplossing van het systeem vergelijkingen. Hiermee is het bewijs voltooid. □

6 Criterium van Eisenstein

We zullen in dit hoofdstuk het criterium van Eisenstein bewijzen. Dit criterium zullen we vervolgens toepassen in een concreet voorbeeld. Tenslotte zullen we aantonen dat het criterium van Eisenstein alleen een voldoende voorwaarde is voor irreducibiliteit. We beginnen dus met het criterium van Eisenstein, zoals geformuleerd in stelling 6.1.

Stelling 6.1 Laat $f \in \mathbb{Z}[X]$ en schrijf

$$f(X) = \sum_{k=0}^{m} a_k X^k.$$

Stel dat er een priemgetal p is met de volgende drie eigenschappen

1. $p \nmid a_m$;
2. $p \mid a_i$ voor $i = 0, 1, \cdots, m-1$;
3. $p^2 \nmid a_0$.

Dan is f irreducibel in $\mathbb{Q}[X]$. Vanwege de theorie in hoofdstuk 3 kunnen we dit ook formuleren als: f is irreducibel in $\mathbb{Z}[X]$ op mogelijke constante factoren na.
Bewijs We zullen de tweede bewering bewijzen, oftewel f is irreducibel in $\mathbb{Z}[X]$ op mogelijke constante factoren na. Stel daartoe dat $f = gh$ met $g, h \in \mathbb{Z}[X]$, waar

$$g(X) = \sum_{k=0}^{r} b_k X_k$$

en

$$h(X) = \sum_{k=0}^{s} c_k X_k.$$

We mogen aannemen dat $r \geq 1$ en $s \geq 1$. Immers, f mag wel constante factoren hebben. Het idee is nu om de gelijkheid $f = gh$ in $\mathbb{Z}[X]$ te beschouwen als een gelijkheid $f = gh$ in $\mathbb{Z}/p\mathbb{Z}[X]$. Aangezien $p \mid a_i$ voor $i = 0, 1, \cdots, m-1$, staat er dus

$$a_m X^m = g(X)h(X)$$

in $\mathbb{Z}/p\mathbb{Z}[X]$. Merk nu op dat $\mathbb{Z}/p\mathbb{Z}[X]$ unieke factorisatie heeft in irreducibele polynomen. Hieruit volgt dat $g(X) = b_r X^r$ en $h(X) = c_s X^s$ met $b_r c_s = a_m$ in $\mathbb{Z}/p\mathbb{Z}[X]$. Aangezien $r \geq 1$ en $s \geq 1$, concluderen we dat $p \mid b_0$ en $p \mid c_0$. Dit impliceert echter dat $p^2 \mid b_0 c_0 = a_0$, wat een tegenspraak is met de derde eigenschap. □

Als we het bewijs opnieuw lezen, is het goed om te beseffen dat $p \nmid a_m$ inderdaad wordt gebruikt. Anders zou de factorisatie in irreducibele polynomen

$$a_m X^m = a_m X \cdot X \cdot \cdots \cdot X$$

namelijk niet kloppen. Deze factorisatie wordt gebruikt om te concluderen dat $g(X) = b_r X^r$ en $h(X) = c_s X^s$.

Er is ook een andere manier om het criterium van Eisenstein te bewijzen. Daartoe kijken we naar zogenaamde Newton polygonen. Met behulp van Newton polygonen is het ook mogelijk om verschillende generalisaties van het criterium van Eisenstein te bewijzen.

Laat p een priemgetal zijn en laat $n \in \mathbb{Z}$ met $n \neq 0$. We definiëren $\nu_p(n)$ als de grootste j zodanig dat $p^j \mid n$. Verder definiëren we nog $\nu_p(0) = \infty$. Laat $f \in \mathbb{Z}[X]$ en schrijf

$$f(X) = \sum_{j=0}^{m} a_j X^j.$$

We nemen aan dat $a_0 \neq 0$ en $a_m \neq 0$. We bekijken de verzameling

$$S = \{(0, \nu(a_m)), (1, \nu(a_{m-1})), \ldots, (m, \nu(a_0)).$$

De onderkant van het convexe omhulsel van S geeft interessante informatie over f. Merk op dat de onderkant van het convexe omhulsel van S een polygonaal pad is. Het dusdanig gevormde polygonale pad heet het Newton polygoon van f ten opzichte van p. Laat $l_1, \ldots, l_k$ de lijnstukken zijn van dit pad, waarbij k minimaal is. Als we de hellingen van $l_1, \ldots, l_k$ berekenen, krijgen we een strikt stijgende rij getallen. Nu geldt de volgende stelling, ook wel bekend als de stelling van Dumas.

Laat p een priemgetal zijn en laat $g, h \in \mathbb{Z}[X]$. Stel dat $g(0)h(0) \neq 0$. Laat u de leidende coëfficiënt van $g(X)h(X)$ zijn en laat $\nu_p(u) = t$. Het Newton polygoon van $g(X)h(X)$ ten opzichte van p kan worden gemaakt door een polygonaal pad vanuit $(0, t)$ te construeren en lijnstukken van het Newton polygoon van $g(X)$ of $h(X)$ ten opzichte van p te gebruiken. Hierbij moet elk lijnstuk precies één keer worden gebruikt. Merk op dat de hellingen van de lijnstukken een strikt stijgende rij getallen moeten vormen. Dit legt het Newton polygoon van $g(X)h(X)$ vast, zie ook appendix A.

Het is nu bijna triviaal om de stelling van Eisenstein te bewijzen. Stel dat $f \in \mathbb{Z}[X]$ voldoet aan de voorwaarden in stelling 6.1. Dan is het Newton polygoon van f het lijnstuk van $(0, 1)$ naar $(m, 0)$. Stel nu dat $f = gh$ voor zekere $g, h \in \mathbb{Z}[X]$ zodanig dat $\deg g > 0$ en $\deg h > 0$. Als we de stelling van Dumas gebruiken, zien we dat $g(X)$ of $h(X)$ een lijnstuk met helling $\frac{-1}{m}$ moet hebben. Maar hieruit volgt dat $\deg g = m$ of $\deg h = m$, tegenspraak.

We zijn nu klaar om het criterium van Eisenstein toe te passen: we zullen bewijzen dat de cyclotomische polynomen irreducibel zijn voor priemgetallen p. Dit feit is belangrijk bij de bestudering van cyclotomische lichamen. Het criterium van Eisenstein is oorspronkelijk bewezen voor deze toepassing. Eerst hebben we het volgende lemma nodig.

Lemma 6.2 Laat p een priemgetal zijn. Bekijk nu de binomiaalcoëfficiënt

$$\binom{p}{i}$$

voor $0 < i < p$. Dan geldt

$$p \mid \binom{p}{i}.$$

Bewijs Laat $0 < i < p$. Het is triviaal dat

$$p \mid p! = i! \cdot (p - i)! \cdot \binom{p}{i}.$$

Omdat p een priemgetal is, mogen we daarom concluderen dat

$$p \mid i! \vee p \mid (p-i)! \vee p \mid \binom{p}{i}.$$

Aangezien $p \nmid i!$ en $p \nmid (p-i)!$ voor $0 < i < p$, volgt het gevraagde. □

Gevolg 6.3 Laat p een priemgetal zijn. Dan is het polynoom

$$f(X) = \sum_{k=0}^{p-1} X^k.$$

irreducibel.
Bewijs Als eerste merken we op dat het criterium van Eisenstein niet direct is toe te passen op $f(X)$. We zien dus dat het criterium van Eisenstein slechts een voldoende voorwaarde is en geen noodzakelijke voorwaarde voor irreducibiliteit. Het idee is nu om het criterium van Eisenstein toe te passen op $f(X+1)$. Vanwege stelling 4.1 volgt dan de irreducibiliteit van $f(X)$. Er geldt

$$f(X) = \sum_{k=0}^{p-1} X^k = \frac{X^p - 1}{X - 1}$$

zodat

$$f(X+1) = \frac{(X+1)^p - 1}{(X+1) - 1} = \frac{(X+1)^p - 1}{X}.$$

Dit werken we vervolgens uit met het binomium van Newton

$$f(X+1) = \frac{\sum_{k=0}^{p} \binom{p}{k} X^k - 1}{X} = \frac{\sum_{k=1}^{p} \binom{p}{k} X^k}{X} = \sum_{k=1}^{p} \binom{p}{k} X^{k-1} = \sum_{k=0}^{p-1} \binom{p}{k+1} X^k.$$

Nu verifiëren we de condities van stelling 6.1. Er geldt dat

1. $p \nmid a_{p-1}$, aangezien $a_{p-1} = \binom{p}{p-1+1} = 1$;
2. $p \mid a_i$ voor $i = 0, 1, \cdots, p-2$ vanwege lemma 6.2;
3. $p^2 \nmid a_0$, aangezien $a_0 = \binom{p}{0+1} = p$.

Dus er is voldaan aan alle voorwaarden voor het criterium van Eisenstein. Dit voltooit het bewijs. □

We hebben gezien dat stelling 6.1 geen noodzakelijke voorwaarde is voor irreducibiliteit. Echter, in gevolg 6.3 zagen we ook dat combineren van stelling 4.1 en stelling 6.1 een mogelijke oplossing hiervoor kan zijn. Laat dus $f(X) \in \mathbb{Z}[X]$ irreducibel. Is er dan een $a \in \mathbb{Z}$ zodat we het criterium van Eisenstein kunnen toepassen op $f(X+a)$? Het antwoord is helaas nee. Bekijk maar $f(X) = X^2 + 4 \in \mathbb{Z}[X]$. Het is duidelijk dat $f(X)$ irreducibel is. Laat $a \in \mathbb{Z}$ en bekijk

$$f(X+a) = (X+a)^2 + 4 = X^2 + 2aX + a^2 + 4.$$

Zij $p \in \mathbb{Z}$ nu een priemgetal met $p \mid 2a$ en $p \mid a^2 + 4$: dit betekent dus dat p voldoet aan de tweede voorwaarde in het criterium van Eisenstein. We bewijzen dat $p = 2$. Uit $p \mid 2a$ volgt immers

$$p \mid 2 \vee p \mid a.$$

Als $p \mid 2$, dan zijn we klaar. Stel dus maar dat $p \mid a$. Als we dit combineren met $p \mid a^2 + 4$, dan krijgen we

$$p \mid a^2 + 4 - a \cdot a = 4.$$

Opnieuw volgt dat $p = 2$. Uit $2 \mid a^2 + 4$ volgt dat a even moet zijn. Echter, dan geldt

$$2^2 \mid a^2 + 4.$$

Er is dus niet voldaan aan de derde voorwaarde in het criterium van Eisenstein. Desalniettemin is het criterium van Eisenstein zeer nuttig. Dit zullen we nog een keer laten zien in stelling 6.4, waarin we verschillende technieken zullen combineren.

Stelling 6.4 Laat $n \in \mathbb{Z}$ met $n > 0$ en bekijk het polynoom

$$f(X) = X^n + 1.$$

Dan is f irreducibel dan en slechts dan als $n = 2^k$ voor zekere $k \in \mathbb{Z}$ met $k \geq 0$.
Bewijs We bewijzen eerst de implicatie van links naar rechts. Het is makkelijker om de contrapositie te bewijzen. Laat daartoe p een oneven priemgetal zijn en stel dat $p \mid n$. Het doel is nu om te bewijzen dat f reducibel is. Vanwege lemma 4.6 weten we dat

$$X - Y \mid X^l - Y^l$$

voor alle $l \in \mathbb{Z}$ met $l \geq 0$. Merk op dat we hier deling in $\mathbb{Z}[X, Y]$ bedoelen. Eerst substitueren we $Y = -1$. We concluderen voor oneven l dat

$$X + 1 \mid X^l + 1.$$

Voor X substitueren we $X^{\frac{n}{p}}$ en voor Y substitueren we $Y^{\frac{n}{p}}$. Dit geeft voor oneven l dat

$$X^{\frac{n}{p}} + 1 \mid X^{\frac{n}{p}l} + 1.$$

Aangezien p oneven is, kunnen we $l = p$ kiezen. Dit geeft ons

$$X^{\frac{n}{p}} + 1 \mid X^n + 1.$$

Dit bewijst dat f reducibel is. We gaan nu de implicatie van rechts naar links bewijzen. Laat dus $n = 2^k$ voor zekere $k \in \mathbb{Z}$ met $k \geq 0$. We bewijzen dat $f(X + 1)$ irreducibel is. Uit stelling 4.1 volgt dan dat f irreducibel is. Eerst laten we $k = 0$. Dan volgt natuurlijk $n = 1$: in dit geval is de stelling triviaal. Laat dus $k > 0$ en laat $i \in \mathbb{Z}$ met $0 < i < n$. Bekijk nu de identiteit

$$\binom{n}{i} = \frac{n}{i}\binom{n-1}{i-1}.$$

Merk op dat n in totaal k factoren 2 bevat. Aangezien i niet meer dan $k - 1$ factoren 2 kan bevatten, volgt hieruit dat

$$2 \mid \binom{n}{i}.$$

We weten dat

$$f(X+1) = (X+1)^n + 1 = 1 + \sum_{i=0}^{n} \binom{n}{i} X^i.$$

We zien dus dat $2 \nmid a_n = \binom{n}{n} = 1$ en $2 \mid a_i = \binom{n}{i}$ voor $0 < i < n$. Tenslotte zien we dat $a_0 = 1 + \binom{n}{0} = 2$, zodat $2 \mid a_0$ en $2^2 \nmid a_0$. We kunnen dus het criterium van Eisenstein toepassen met $p = 2$. □

In stelling 6.4 gebruikten we dat

$$\binom{n}{i} = \frac{n}{i}\binom{n-1}{i-1}$$

voor $0 < i < n$. Deze identiteit kan ook worden gebruikt om een alternatief bewijs te geven voor lemma 6.2.

De implicatie van rechts naar links in stelling 6.4 kan ook worden bewezen met behulp van de theorie uit 5. Voor $k = 0$ is het triviaal, stel dus $k > 0$. We weten dat

$$X^{2^k} + 1 = (X+1)^{2^k}$$

in $\mathbb{Z}/2\mathbb{Z}[X]$. Een echte ontbinding van $X^{2^k} + 1$ moet er dus uitzien als

$$((X+1)^a + 2f(X))((X+1)^b + 2g(X)) = X^{2^k} + 1$$

met $a, b > 0$ en $f, g \in \mathbb{Z}[X]$. Invullen van -1 geeft nu

$$4f(-1)g(-1) = 2$$

en dit kan niet. Dit idee komt nog een keer terug in hoofdstuk 10.

7 Criterium van Perron

Voordat we het criterium van Perron formuleren, zullen we eerst een lemma bewijzen. Dit lemma vertelt ons iets over de complexe nulpunten van polynomen, wat weer kan worden gebruikt om irreducibiliteit aan te tonen. Het bewijs is gebaseerd op [3].

Lemma 7.1 Laat $f \in \mathbb{Z}[X]$ monisch en schrijf

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0.$$

Stel nu dat

$$|a_{n-1}| > 1 + |a_{n-2}| + \cdots + |a_1| + |a_0|.$$

Dan is er precies één nulpunt α van f zodanig dat $|\alpha| > 1$ en voor alle andere $n-1$ nulpunten van f geldt $|\alpha| < 1$.
Bewijs We mogen aannemen dat $a_0 \neq 0$, aangezien we factoren van de vorm X^k kunnen uitdelen. We zullen eerst bewijzen dat er geen nulpunt α van f is met $|\alpha| = 1$. Stel immers maar dat er een nulpunt α van f is met $|\alpha| = 1$. Dan geldt

$$-a_{n-1}\alpha^{n-1} = \alpha^n + a_{n-2}\alpha^{n-2} + \cdots + a_1\alpha + a_0.$$

Hieruit volgt dat

$$\begin{aligned} |a_{n-1}| = |a_{n-1}\alpha^{n-1}| &= |\alpha^n + a_{n-2}\alpha^{n-2} + \cdots + a_1\alpha + a_0| \\ &\leq |\alpha^n| + |a_{n-2}\alpha^{n-2}| + \cdots + |a_1\alpha| + |a_0| \\ &= 1 + |a_{n-2}| + \cdots + |a_1| + |a_0|. \end{aligned}$$

Dit is in tegenspraak met de veronderstelde ongelijkheid. We concluderen dat geen nulpunt van f op de eenheidscirkel kan liggen. Schrijf nu $\alpha_1, \alpha_2, \ldots, \alpha_n$ voor de nulpunten van f. Merk op dat $|\alpha_1\alpha_2 \cdots \alpha_n| = |a_0|$, waaruit volgt dat er minstens één nulpunt is met absolute waarde groter dan 1. Stel dat $|\alpha_1| > 1$ en laat

$$g(X) = X^{n-1} + b_{n-2}X^{n-2} + \cdots + b_1X + b_0$$

het polynoom zijn met wortels $\alpha_2, \alpha_3, \ldots, \alpha_n$. Dan geldt

$$f(X) = (X-\alpha_1)g(X) = X^n + (b_{n-2}-\alpha_1)X^{n-1} + (b_{n-3}-b_{n-2}\alpha_1)X^{n-2} + \cdots + (b_0 - b_1\alpha_1)X - b_0\alpha_1.$$

We concluderen dat $a_0 = -b_0\alpha_1$ en $a_k = b_{k-1} - b_k\alpha_1$ voor alle $1 \leq k \leq n-1$, waar we afspreken dat $b_{n-1} = 1$. Dan volgt

$$\begin{aligned} |b_{n-2} - \alpha_1| = |a_{n-1}| &> 1 + |a_{n-2}| + \cdots + |a_1| + |a_0| \\ &= 1 + |b_{n-3} - b_{n-2}\alpha_1| + \cdots + |b_0 - b_1\alpha_1| + |b_0\alpha_1| \\ &\geq 1 + |b_{n-2}||\alpha_1| - |b_{n-3}| + |b_{n-3}||\alpha_1| - |b_{n-4}| + \cdots + |b_1||\alpha_1| - |b_0| + |b_0||\alpha_1| \\ &= 1 + |b_{n-2}| + (|\alpha_1| - 1)(|b_{n-2}| + |b_{n-3}| + \cdots + |b_1| + |b_0|). \end{aligned}$$

Uit $|b_{n-2} - \alpha_1| \leq |b_{n-2}| + |\alpha_1|$ volgt

$$|b_{n-2}| + |\alpha_1| > 1 + |b_{n-2}| + (|\alpha_1| - 1)(|b_{n-2}| + |b_{n-3}| + \cdots + |b_1| + |b_0|).$$

En dus

$$|b_{n-2}| + |b_{n-3}| + \cdots + |b_1| + |b_0| < 1.$$

We concluderen dat voor alle complexe getallen α met $|\alpha| \geq 1$ wel moet gelden dat

$$\begin{aligned} |g(\alpha)| &= |\alpha^{n-1} + b_{n-2}\alpha^{n-2} + b_{n-3}\alpha^{n-3} + \cdots + b_1\alpha + b_0| \\ &\geq |\alpha^{n-1}| - |b_{n-2}\alpha^{n-2}| - |b_{n-3}\alpha^{n-3}| - \cdots - |b_1\alpha| - |b_0| \\ &\geq |\alpha|^{n-1} - |\alpha|^{n-1}(|b_{n-2}| + |b_{n-3}| + \cdots + |b_1| + |b_0|) \\ &= |\alpha|^{n-1}(1 - |b_{n-2}| - |b_{n-3}| - \cdots - |b_1| - |b_0|) \\ &> 0. \end{aligned}$$

We concluderen dat α geen nulpunt kan zijn. Kortom, alle nulpunten van g liggen binnen de eenheidscirkel. Dit voltooit het bewijs. □

Het is nu eenvoudig om het criterium van Perron te bewijzen. Dit gaat als volgt.

Stelling 7.2 Laat $f \in \mathbb{Z}[X]$ monisch en schrijf

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0.$$

Stel nu dat

$$|a_{n-1}| > 1 + |a_{n-2}| + \cdots + |a_1| + |a_0|.$$

Als bovendien geldt $a_0 \neq 0$, dan is f irreducibel.
Bewijs Stel dat er $g, h \in \mathbb{Z}[X]$ zijn zodanig dat $f = gh$. Uit lemma 7.1 volgt dat er precies één nulpunt α van f is zodanig dat $|\alpha| \geq 1$. Hieruit volgt dat ofwel alle nulpunten van g binnen de eenheidscirkel liggen ofwel alle nulpunten van h binnen de eenheidscirkel liggen. Zonder verlies van algemeenheid nemen we aan dat alle nulpunten van g binnen de eenheidscirkel liggen. Laat $\alpha_1, \cdots \alpha_k$ de nulpunten van g zijn. Dan geldt dus $|\alpha_1|, \ldots, |\alpha_k| < 1$.

Merk nu op dat $a_0 \neq 0$ impliceert dat $g(0) \neq 0$. Bovendien weten we dat

$$|g(0)| = |\alpha_1 \cdots \alpha_k| < 1$$

voor $k \geq 1$. Dit is in tegenspraak met $g(0) \in \mathbb{Z}$. Resteert nog het geval $k = 0$. Dit impliceert dat g constant is. Uit het feit dat f monisch is, volgt dan tenslotte dat $g(X) = 1$ of $g(X) = -1$. We concluderen dat f irreducibel is. □

Een alternatief bewijs voor het criterium van Perron gebruikt de stelling van Rouché. Dit is een bekende stelling uit de complexe analyse. We zullen de stelling hier niet bewijzen, maar wel noemen.

Stelling 7.3 Laat f en g analytische functies zijn op en binnen een Jordan-kromme C. Stel dat $|f(z)| > |g(z)|$ voor alle z op C. Dan hebben f en $f+g$ hetzelfde aantal nulpunten binnen C.

Tenslotte maken we nog twee opmerkingen. Ten eerste moeten we in stelling 7.3 rekening houden met de multipliciteit van het nulpunt: een dubbel nulpunt telt minstens twee keer. Ten tweede merken we nog op dat polynomen analytische functies zijn.

8 Criterium van Cohn

We beginnen met het klassieke criterium van Cohn. Dit criterium legt een interessant verband tussen priemgetallen en irreducibele polynomen. Het bewijs van dit criterium komt uit [2]. Vervolgens kijken we naar verschillende generalisaties.

Stelling 8.1 Zij p een priemgetal en schrijf p in basis 10 als

$$p = a_n 10^n + a_{n-1}10^{n-1} + \cdots + a_0.$$

Dit betekent dus dat $0 \leq a_i < 10$ voor $i = 0, \cdots, n$. Dan is het polynoom

$$f(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_0$$

irreducibel in $\mathbb{Z}[X]$.
Bewijs Zie stelling 8.3. □

Het is niet moeilijk om stelling 8.1 te generaliseren voor willekeurige basis b. Dit zullen we doen in stelling 8.3. We zullen beginnen met een voorbereidend lemma.

Lemma 8.2 Laat $f(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_0$ met $f \in \mathbb{Z}[X]$. Stel bovendien dat $a_n \geq 1$, $a_{n-1} \geq 0$ en $|a_i| \leq H$ voor $i = 0, 1, \cdots, n-2$, waar H een positieve constante is. Laat α een complex nulpunt van f zijn. Dan geldt $\Re(\alpha) \leq 0$ of $|\alpha| < \frac{1+\sqrt{1+4H}}{2}$.
Bewijs We bewijzen de contrapositie. Stel dus dat $\Re(\alpha) > 0$ en $|\alpha| \geq \frac{1+\sqrt{1+4H}}{2}$. We moeten bewijzen dat α geen complex nulpunt van f kan zijn. De omgekeerde driehoeksongelijkheid vertelt ons dat

$$|x - y| \geq ||x| - |y||.$$

We concluderen dat

$$|x - y| \geq |x| - |y|$$

en daarmee dat

$$|x + y| \geq |x| - |y|.$$

Bekijk nu

$$|\frac{f(\alpha)}{\alpha^n}| \geq |a_n + \frac{a_{n-1}}{\alpha}| - |\frac{a_{n-2}}{\alpha^2} + \cdots + \frac{a_0}{\alpha^n}| \geq |a_n + \frac{a_{n-1}}{\alpha}| - H(\frac{1}{|\alpha|^2} + \cdots + \frac{1}{|\alpha|^n}).$$

Uit $|\alpha| \geq \frac{1+\sqrt{1+4H}}{2}$ volgt in het bijzonder dat $|\alpha| > 1$. We kunnen de meetkundige reeks dus afschatten

$$H(\frac{1}{|\alpha|^2} + \cdots + \frac{1}{|\alpha|^n}) > \frac{H}{|\alpha|^2 - |\alpha|}.$$

Verder geldt natuurlijk dat

$$|a_n + \frac{a_{n-1}}{\alpha}| \geq \Re(a_n + \frac{a_{n-1}}{\alpha}) = \Re(a_n) + \Re(\frac{a_{n-1}}{\alpha}) \geq 1 + \Re(\frac{a_{n-1}}{\alpha}).$$

Uit $\Re(\alpha) > 0$ volgt dat $\Re(\frac{a_{n-1}}{\alpha}) \geq 0$. We concluderen dat

$$|a_n + \frac{a_{n-1}}{\alpha}| \geq 1.$$

Als we dit combineren, dan krijgen we

$$|\frac{f(\alpha)}{\alpha^n}| > 1 - \frac{H}{|\alpha|^2 - |\alpha|} = \frac{|\alpha|^2 - |\alpha| - H}{|\alpha|^2 - |\alpha|}.$$

Uit $|\alpha| \geq \frac{1+\sqrt{1+4H}}{2}$ volgt dan dat $|\alpha|^2 - |\alpha| - H \geq 0$, zodat

$$|\frac{f(\alpha)}{\alpha^n}| > 0.$$

Dit laat zien dat α geen nulpunt kan zijn. □

We zijn nu klaar om de generalisatie van de stelling van Cohn te bewijzen voor willekeurige basis b. We zullen aannemen dat $b > 2$. De stelling is ook waar voor $b = 2$, maar dit is iets moeilijker om te bewijzen.

Stelling 8.3 Laat $b > 2$ en laat p een priemgetal zijn. Schrijf p in basis b als

$$p = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_0.$$

Dit betekent dus dat $0 \leq a_i < b$ voor $i = 0, \cdots, n$. Dan is het polynoom

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0$$

irreducibel in $\mathbb{Z}[X]$.
Bewijs Het is niet moeilijk om te bewijzen dat f geen constante factoren kan hebben, zie ook de discussie na stelling 8.4. Stel dus dat

$$f = gh,$$

waar g en h niet constante polynomen in $\mathbb{Z}[X]$ zijn. Merk op dat $f(b) = p$, zodat $g(b) = \pm 1$ of $h(b) = \pm 1$. Zonder verlies van algemeenheid mogen we aannemen dat $g(b) = \pm 1$. Schrijf nu

$$g(X) = c \prod_{i=0}^{m} (X - \alpha_i),$$

waar $c \in \mathbb{Z}$ met $c \neq 0$. Merk op dat $0 < m < n$ en dat elke α_i een nulpunt van f is. Laat α een nulpunt van f zijn. Uit lemma 8.2 volgt dat $\Re(\alpha) \leq 0$ of $|\alpha| < \frac{1+\sqrt{1+4(b-1)}}{2}$. Het doel is om eerst te bewijzen dat $|b - \alpha| > 1$. Vervolgens leiden we dan een tegenspraak af met $g(b) = \pm 1$. Uit $\Re(\alpha) \leq 0$ concluderen we meteen dat $|b - \alpha| > 1$. Stel daarom dat $|\alpha| < \frac{1+\sqrt{1+4(b-1)}}{2}$. Als we kunnen bewijzen dat

$$\frac{1 + \sqrt{1 + 4(b-1)}}{2} \leq b - 1,$$

dan mogen we concluderen dat

$$|\alpha| < b - 1.$$

Daaruit volgt dan

$$|b - \alpha| \geq ||b| - |\alpha|| \geq |b| - |\alpha| = b - |\alpha| > 1.$$

We zullen daarom bewijzen dat

$$\frac{1+\sqrt{1+4(b-1)}}{2} \leq b-1.$$

Merk op dat

$$1+4(b-1) \leq (2b-3)^2$$

voor $b \geq 3$, waaruit we de vorige ongelijkheid direct kunnen afleiden. We concluderen dat $|b-\alpha| > 1$. Daaruit volgt echter dat $|g(b)| > 1$, aangezien het product $c\prod_{i=0}^{m}(X-\alpha_i)$ niet leeg is. Dit is een tegenspraak. □

We zullen de volgende generalisatie als deg $f = 2$ bewijzen voor het criterium van Cohn.

Stelling 8.4 Laat $f \in \mathbb{Z}[X]$ met deg $f = 2$. Schrijf nu

$$f(X) = aX^2 + bX + c.$$

Laat bovendien $a > 0$, $b \geq 0$ en $c \geq 0$. Stel nu dat f reducibel is in $\mathbb{Q}[X]$. Dan is $f(g) = ag^2 + bg + c$ niet priem voor $g > 1$. Bovendien kan $f(1) = a + b + c$ alleen priem zijn als $a + b$ priem is en $c = 0$.
Bewijs We zullen de laatste twee uitspraken tegelijkertijd bewijzen. Laat daartoe $g > 0$ en stel dat $f(g)$ priem is. Dit betekent dus dat

$$ag^2 + bg + c = p$$

voor een zeker priemgetal $p \in \mathbb{Z}$. Merk op dat f reducibel is in $\mathbb{Q}[X]$ dan en slechts dan als

$$D = b^2 - 4ac$$

een kwadraat is. We kunnen dus schrijven

$$b^2 - 4ac = d^2$$

voor zekere $d \in \mathbb{Z}$, waarbij we bovendien mogen aannemen dat $d \geq 0$. We gaan nu $ag^2+bg+c = p$ omschrijven tot

$$bg = p - ag^2 - c.$$

We willen natuurlijk gebruiken dat $b^2 - 4ac = d^2$. Als we $bg = p - ag^2 - c$ kwadrateren, krijgen we

$$(bg)^2 = (p - ag^2 - c)^2 = p^2 - 2p(ag^2 + c) + (ag^2 + c)^2.$$

Nu trekken we $4acg^2$ af van beide kanten. Merk op dat de linkerkant dan simpelweg d^2g^2 is:

$$d^2g^2 = (bg)^2 - 4acg^2 = p^2 - 2p(ag^2 + c) + (ag^2 + c)^2 - 4acg^2 = p^2 - 2p(ag^2 + c) + (ag^2 - c)^2.$$

Hieruit volgt dat

$$d^2g^2 - (ag^2 - c)^2 = p^2 - 2p(ag^2 + c)$$

oftewel dat

$$p \mid d^2g^2 - (ag^2 - c)^2 = (dg - (ag^2 - c))(dg + (ag^2 - c)).$$

We concluderen dat

$$p \mid dg - ag^2 + c \vee p \mid dg + ag^2 - c.$$

Het doel is nu om te bewijzen dat

$$-p \leq dg - ag^2 + c \leq p$$

en analoog

$$-p \leq dg + ag^2 - c \leq p.$$

Merk op dat $b^2 - 4ac = d^2$, zodat $d^2 \leq b^2$. Hieruit volgt dat $d \leq b$, aangezien d en b positief zijn. We concluderen nu dat

$$|dg - ag^2 + c| \leq |dg| + | - ag^2| + |c| = dg + ag^2 + c \leq bg + ag^2 + c = p. \qquad (*)$$

Analoog zien we in dat

$$|dg + ag^2 - c| \leq |dg| + |ag^2| + | - c| = dg + ag^2 + c \leq bg + ag^2 + c = p. \qquad (**)$$

Dit geeft ons zes mogelijke gevallen. Het doel is om te bewijzen dat $c = 0$. Als we gelijkheid hebben in (*) of (**), dan moet in het bijzonder gelden dat $b = d$. Maar dan volgt $4ac = 0$, zodat $c = 0$. Dus resteren er nog maar twee gevallen, namelijk

$$0 = dg - ag^2 + c$$

en

$$0 = dg + ag^2 - c.$$

Merk op dat in beide gevallen volgt dat

$$p^2 - 2p(ag^2 + c) = 0.$$

Maar dan moet wel gelden dat

$$p = 2(ag^2 + c).$$

Aangezien p priem is, concluderen we dat $ag^2 + c = 1$. Uit $ag^2 \geq 1$ volgt dan dat $c = 0$. We kunnen f dus schrijven als

$$f(X) = aX^2 + bX.$$

Er volgt dat

$$f(g) = ag^2 + bg = p.$$

Als $g > 1$, dan zien we dat $g \mid p$ met $g \neq p$. Dit is natuurlijk een tegenspraak. Als $g = 1$, dan zien we dat $a + b = p$. Dit voltooit het bewijs. □

In stelling 8.4 keken we naar reducibiliteit in $\mathbb{Q}[X]$. Het is niet moeilijk om nu te bewijzen dat f zoals in stelling 8.4 ook reducibel is in $\mathbb{Z}[X]$. In dit geval moeten we nog rekening houden met delers van de vorm $h(X) = d$ met d geen eenheid in $\mathbb{Z}$. Het is echter niet moeilijk om in te zien dat een dergelijke deler niet kan bestaan. Immers we zien dat dan in het bijzonder $d \mid f(g) = p$. Aangezien d geen eenheid is, volgt dat $d = p$ of $d = -p$. Merk bovendien op dat $d \mid a$, maar dan moet wel $a = p$ en $b = c = 0$. We concluderen dat $g = 1$ en dit een bijzonder geval is van de uitzonderingen in stelling 8.4. We zullen nu kijken naar het geval

dat $\deg f = 3$. We nemen aan dat f monisch is.

Stelling 8.5 Laat $f \in \mathbb{Z}[X]$ met $\deg f = 3$ en f monisch. Schrijf nu

$$f(X) = X^3 + aX^2 + bX + c.$$

Laat bovendien $a \geq 0$, $b \geq 0$ en $c \geq 0$. Stel nu dat f reducibel is in $\mathbb{Q}[X]$. Dan is $f(g) = g^3 + ag^2 + bg + c$ niet priem voor $g > 1$. Bovendien kan $f(1) = 1 + a + b + c$ alleen priem zijn als $1 + a + b$ priem is en $c = 0$, of als $a = b = 0$ en $c = 1$.
Bewijs We weten dat f reducibel is. Aangezien $\deg f = 3$, volgt hieruit dat f een lineaire factor heeft. Dit betekent dat $f(\alpha) = 0$ voor zekere $\alpha \in \mathbb{Q}$. We passen nu stelling 4.3 toe. Uit het feit dat f monisch is, volgt dan $\alpha \in \mathbb{Z}$. Merk op dat $\alpha \leq 0$. Stel nu dat $f(g) = g^3 + ag^2 + bg + c$ priem is, kortom

$$f(g) = g^3 + ag^2 + bg + c = p$$

voor een priemgetal $p \in \mathbb{Z}$. We gebruiken nu lemma 4.7, waaruit volgt dat

$$x - y \mid f(x) - f(y)$$

voor alle $x, y \in \mathbb{Z}$. We kiezen $x = g$ en $y = \alpha$ en verkrijgen

$$g - \alpha \mid f(g) - f(\alpha) = p - 0 = p.$$

We weten dat $g - \alpha \geq 1$, zodat $g - \alpha = 1$ of $g - \alpha = p$. Als $g - \alpha = 1$, dan volgt $g = 1$ en $\alpha = 0$. Uit $\alpha = 0$ volgt dan $c = 0$, waaruit de stelling volgt. Resteert nog het geval $g - \alpha = p$, oftewel $\alpha = g - p$. Uitwerken van $f(\alpha) = 0$ geeft dan

$$0 = f(\alpha) = f(g - p) = (g - p)^3 + a(g - p)^2 + b(g - p) + c = 0.$$

Dit kunnen we verder herschrijven tot

$$g^3 - 3pg^2 + 3p^2g - p^3 + ag^2 - 2agp + ap^2 + bg - bp + c = 0.$$

We gebruiken nu dat $g^3 + ag^2 + bg + c = p$, waaruit volgt dat

$$p - 3pg^2 + 3p^2g - p^3 - 2agp + ap^2 - bp = 0.$$

Natuurlijk kunnen we de factor p uitdelen. Dan verkrijgen we

$$1 - 3g^2 + 3pg - p^2 - 2ag + ap - b = 0.$$

Tenslotte herschrijven we dit tot

$$p(3g - p + a) = 3g^2 + 2ag + b - 1.$$

Hieruit concluderen we dat

$$p \mid 3g^2 + 2ag + b - 1.$$

Merk op dat $3g^2 + 2ag + b - 1 \geq 3 + 2a + b - 1 > 0$. We gaan nu bewijzen dat

$$3g^2 + 2ag + b - 1 \leq 2p,$$

waarbij gelijkheid alleen kan optreden als $g = 1$ en $c = 0$. Merk daartoe op dat $2p = 2g^3 + 2ag^2 + 2bg + 2c$ en verder dat

$$3g^2 - 1 \leq 2g^3,$$

$$2ag \leq 2ag^2,$$

$$b \leq 2bg,$$

$$0 \leq 2c.$$

Optellen van deze vier ongelijkheden geeft inderdaad de gevraagde ongelijkheid. Bovendien kan in de eerste en vierde ongelijkheid alleen gelijkheid optreden als respectievelijk $g = 1$ en $c = 0$. Als $g = 1$ en $c = 0$, dan volgt de stelling. We mogen dus aannemen dat $3g^2+2ag+b-1 < 2p$. Mar dan volgt meteen dat $3g^2 + 2ag + b - 1 = p$. Maar dit kan alleen als

$$3g - p + a = 1.$$

Maar dit kunnen we herschrijven tot

$$3g + a - 1 = p.$$

Merk op dat dus

$$3g^2 + 2ag + b = 3g + a.$$

Dit kan alleen als $g = 1$, $a = 0$ en $b = 0$. Hieruit volgt dat $f(X) = X^3 + c^3 = (X + c)(X^2 - cX + c^2)$. Het is dus voldoende om nu nog te bewijzen dat $c = 0$ of $c = 1$. Uit $f(1) = p$ volgt echter dat

$$(1 + c)(1^2 - c + c^2) = p.$$

Als $c > 1$, dan weten we dat $1 + c > 1$ en $1 - c + c^2 > 1$. Dit geeft een tegenspraak, dus moeten we wel hebben dat $c = 0$ of $c = 1$. Dit voltooit het bewijs. □

Als we het bewijs van stelling 8.5 bekijken, kunnen we een aantal opmerkingen maken. Ten eerste kunnen we de aanname dat f reducibel is in $\mathbb{Q}[X]$ vervangen door de aanname dat f reducibel is in $\mathbb{Z}[X]$. Dit hebben we ook al gezien na stelling 8.4. Het bewijs hiervan gaat dan ook volledig analoog. Ten tweede is de aanname dat f monisch is enigszins vreemd. Deze aanname is inderdaad niet nodig. Dit zien we in stelling 8.6.

Stelling 8.6 Laat $f \in \mathbb{Z}[X]$ met $\deg f = 3$. Schrijf nu

$$f(X) = aX^3 + bX^2 + cX + d.$$

Laat bovendien $a > 0$, $b \geq 0$, $c \geq 0$ en $d \geq 0$. Stel nu dat f reducibel is in $\mathbb{Q}[X]$. Dan is $f(g) = ag^3 + bg^2 + cg + d$ niet priem voor $g > 1$. Bovendien kan $f(1) = a + b + c + d$ alleen priem zijn als $a + b + c$ priem is en $d = 0$, of als $a = 1$, $b = c = 0$ en $d = 1$.
Bewijs We weten dat f reducibel is. Aangezien $\deg f = 3$, volgt hieruit dat f een lineaire factor heeft. Laat $g(X) = uX - v$ deze lineaire factor zijn met $u, v \in \mathbb{Z}$. Dit betekent dus dat $f(\frac{v}{u}) = 0$. We mogen aannemen dat $\text{ggd}(u, v) = 1$, $u > 0$ en $v \leq 0$. We bekijken weer $f(g) - f(\frac{v}{u})$

$$p = f(g) - f(\frac{v}{u}) = a(g^3 - \frac{v^3}{u^3}) + b(g^2 - \frac{v^2}{u^2}) + c(g - \frac{v}{u}) = (g - \frac{v}{u})(a(g^2 + \frac{v}{u}g + \frac{v^2}{u^2}) + b(g + \frac{v}{u}) + c).$$

Vermenigvuldigen met u^3 geeft dan

$$pu^3 = (gu - v)(a(g^2u^2 + guv + v^2) + b(gu^2 + vu) + cu^2).$$

Laat q nu een priemgetal zijn. Stel dat $q \mid u^3$ en $q \mid gu - v$. Aangezien q priem is, concluderen we dat $q \mid u$. Maar dan volgt meteen dat $q \mid v$. Dit is een tegenspraak met $\text{ggd}(u, v) = 1$. We hebben nu bewezen dat een dergelijke q niet kan bestaan. Dit betekent dat $\text{ggd}(u^3, gu - v) = 1$. Dan moet wel gelden dat $gu - v \mid p$. Merk bovendien op dat $gu - v \geq 0$. Stel eerst dat $gu - v = 1$, waaruit volgt dat $g = 1$, $u = 1$ en $v = 0$. We concluderen dat $d = 0$. In dit geval geldt de stelling dus. Stel nu dat $gu - v = p$. Hieruit volgt dat $\frac{v}{u} = g - \frac{p}{u}$. Uitwerken van $f(\frac{v}{u}) = 0$ geeft dan

$$0 = a(g-\frac{p}{u})^3+b(g-\frac{p}{u})^2+c(g-\frac{p}{u})+d = ag^3+bg^2+cg+d-3ag^2\frac{p}{u}+3ag\frac{p^2}{u^2}-a\frac{p^3}{u^3}-2bg\frac{p}{u}+b\frac{p^2}{u^2}-c\frac{p}{u}.$$

We gebruiken eerst dat $ag^3 + bg^2 + cg + d = p$. Vervolgens delen we door p

$$0 = 1 - 3a\frac{g^2}{u} + 3ag\frac{p}{u^2} - a\frac{p^2}{u^3} - 2b\frac{g}{u} + b\frac{p}{u^2} - \frac{c}{u}.$$

Na vermenigvuldiging met u^3 kunnen we dit herschrijven tot

$$p(3agu - ap + bu) = (3ag^2 + 2bg + c - u)u^2.$$

Uit stelling 4.3 volgt dat $u \mid a$. In het bijzonder geldt dat $u \leq a$. Als $a \geq p$, dan volgt de stelling onmiddellijk. We mogen dus aannemen dat $u < p$. Dit geeft dan

$$p \mid 3ag^2 + 2bg + c - u.$$

We kunnen nu net zoals in stelling 8.5 bewijzen dat $p = 3ag^2 + 2bg + c - u$. Hieruit volgt dat

$$u^2 = 3agu - ap + bu.$$

Dit kunnen we omschrijven tot

$$ap = 3agu + bu - u^2.$$

We gebruiken nu dat $p = 3ag^2 + 2bg + c - u$

$$a(3ag^2 + 2bg + c - u) = 3agu + bu - u^2.$$

Merk op dat

$$a(3ag^2 - u) \geq a(3ag - u) \geq u(3ag - u) = 3agu - u^2.$$

$$a(2bg) \geq bu.$$

$$a(c) \geq 0.$$

Optellen van deze drie ongelijkheden geeft

$$a(3ag^2 + 2bg + c - u) \geq 3agu + bu - u^2.$$

Gelijkheid kan alleen optreden als $b = c = 0$, $g = 1$ en $u = a$. Dit geeft tenslotte dat $p = ag^3 + bg^2 + cg + d = a + d$ en $p = 3ag^2 + 2bg + c - u = 2a$. We concluderen dat $a = d$ en daarmee dat $p = 2a$. Dit forceert $a = 1$ en dus $d = 1$. Bij elkaar geeft dit $a = 1$, $b = c = 0$ en $d = 1$, waarmee het bewijs voltooid is. □

9 Toepassingen van Eisenstein

In dit hoofdstuk bekijken we verschillende toepassingen van het criterium van Eisenstein. We zullen zien dat het criterium van Eisenstein gebruikt kan worden om problemen op te lossen, die op het eerste gezicht niets met irreducibiliteit te maken hebben. Een goed voorbeeld is toepassing 9.1.

Toepassing 9.1 Bepaal alle paren van polynomen $f, g \in \mathbb{Z}[X]$ zodanig dat

$$f(g(X)) = X^{2007} + 2X + 1.$$

Oplossing Laat $f, g \in \mathbb{Z}[X]$ zijn zodanig dat

$$f(g(X)) = X^{2007} + 2X + 1.$$

Differentiëren geeft dan

$$g'(X)f'(g(X)) = 2007X^{2006} + 2.$$

We zullen nu bewijzen dat het polynoom

$$2007X^{2006} + 2$$

irreducibel is. Dit volgt direct uit het criterium van Eisenstein, stelling 6.1, met $p = 2$. We onderscheiden nu vier gevallen.

1. Stel dat
$$g'(X) = 1.$$
Hieruit volgt dat
$$g(X) = X + c$$
voor een zekere $c \in \mathbb{Z}$. We krijgen dus
$$f(X + c) = X^{2007} + 2X + 1.$$
We concluderen daarom dat
$$f(X) = (X - c)^{2007} + 2(X - c) + 1.$$
Het is eenvoudig na te gaan dat deze oplossing ook voldoet.

2. Stel dat
$$g'(X) = -1.$$
Hieruit volgt dat
$$g(X) = -X + c$$
voor een zekere $c \in \mathbb{Z}$. We krijgen dus
$$f(-X + c) = X^{2007} + 2X + 1.$$
We concluderen daarom dat
$$f(X) = (-X + c)^{2007} + 2(-X + c) + 1.$$
Het is eenvoudig na te gaan dat deze oplossing ook voldoet.

3. Stel dat
$$f'(g(X)) = 1.$$
Hieruit volgt dat
$$f'(X) = 1$$
en dus
$$f(X) = X + c$$
voor een zekere $c \in \mathbb{Z}$. We krijgen dus
$$g(X) + c = X^{2007} + 2X + 1.$$
We concluderen daarom dat
$$g(X) = X^{2007} + 2X + 1 - c.$$
Het is eenvoudig na te gaan dat deze oplossing ook voldoet.

4. Stel dat
$$f'(g(X)) = -1.$$
Hieruit volgt dat
$$f'(X) = -1$$
en dus
$$f(X) = -X + c$$
voor een zekere $c \in \mathbb{Z}$. We krijgen dus
$$-g(X) + c = X^{2007} + 2X + 1.$$
We concluderen daarom dat
$$g(X) = -X^{2007} - 2X - 1 + c.$$
Het is eenvoudig na te gaan dat deze oplossing ook voldoet.

Hiermee hebben we alle oplossingen gevonden. □

Merk op dat toepassing 9.1 eenvoudig is te generaliseren. We gebruiken eigenlijk alleen dat het polynoom
$$X^{2007} + 2X + 1$$
een primitieve is van een irreducibel polynoom. Voor de tweede toepassing gebruiken we een generalisatie van het criterium van Eisenstein. Eerst zullen we deze generalisatie formuleren in stelling 9.2.

Stelling 9.2 Laat $f \in \mathbb{Z}[X]$ en schrijf
$$f(X) = \sum_{k=0}^{m} a_k X^k.$$
Stel dat er een priemgetal p is met de volgende drie eigenschappen

1. $p \nmid a_k$;
2. $p \mid a_i$ voor $i = 0, 1, \cdots, k-1$;
3. $p^2 \nmid a_0$.

Dan heeft f een irreducibele factor van graad minstens k.
Bewijs Dit kan op precies dezelfde manier worden bewezen als het criterium van Eisenstein, zie stelling 6.1. Ook kan de stelling van Dumas worden gebruikt, zie hoofdstuk 6 en appendix A. □

Nu zijn we klaar voor de laatste toepassing, die sterk lijkt op gevolg 6.3.

Toepassing 9.3 Laat p een priemgetal zijn. Dan is het polynoom

$$f(X) = \sum_{i=0}^{p-1} (p-i)X^i$$

irreducibel.
Oplossing Voor $p = 2$ is het triviaal. We nemen dus aan dat $p > 2$. We bewijzen dat het polynoom

$$g(X) = \sum_{i=0}^{p-1} (i+1)X^i$$

irreducibel is. Dit mag vanwege stelling 4.2. Definieer nu

$$h(X) = \sum_{i=0}^{p} X^i = \frac{X^{p+1}-1}{X-1}.$$

Merk op dat $g(X) = h'(X)$, zodat

$$g(X) = \frac{(X-1)(p+1)X^p - (X^{p+1}-1)}{(X-1)^2} = \frac{pX^{p+1} - (p+1)X^p + 1}{(X-1)^2}.$$

We bewijzen nu dat $g(X+1)$ irreducibel is. Het gevraagde volgt dan uit stelling 4.1. Er geldt

$$\begin{aligned} g(X+1) &= \frac{p(X+1)^{p+1} - (p+1)(X+1)^p + 1}{X^2} \\ &= \sum_{i=2}^{p+1} p\binom{p+1}{i} X^{i-2} - \sum_{i=2}^{p} (p+1)\binom{p}{i} X^{i-2}. \end{aligned} \tag{5}$$

We passen nu stelling 9.2 toe met $k = p-2$. Merk op dat

$$a_k = p\binom{p+1}{p} - (p+1)\binom{p}{p} = p(p+1) - (p+1) = p^2 - 1,$$

zodat $p \nmid a_k$. Merk verder op dat

$$a_0 = p\binom{p+1}{2} - (p+1)\binom{p}{2} = \frac{p^2(p+1)}{2} - \frac{(p-1)p(p+1)}{2} = \frac{p+1}{2}p,$$

zodat $p \mid a_0$ en $p^2 \nmid a_0$. Hier gebruiken we dat $p > 2$. Laat nu $0 < i < k$. Tenslotte geldt nog

$$a_i = p\binom{p+1}{i+2} - (p+1)\binom{p}{i+2}$$

Uit lemma 6.2 volgt nu dat $p \mid a_i$. We concluderen dat $g(X+1)$ een irreducibele factor heeft van graad minstens $p-2$. Het is triviaal om na te gaan dat $g(X+1)$ geen constante factoren heeft. Aangezien de graad van $g(X+1)$ gelijk is aan $p-1$, kan $g(X+1)$ dus alleen reducibel zijn als $g(X+1)$ een lineaire factor heeft. Met behulp van stelling 4.3 kunnen we echter eenvoudig inzien dat $g(X)$ en dus ook $g(X+1)$ geen lineaire factoren kan hebben. □

10 Toepassingen van algebraïsche getaltheorie

In dit hoofdstuk zullen we irreducibiliteit van polynomen bewijzen met behulp van algebraïsche getaltheorie. We nemen aan dat de lezer bekend is met algebraïsche getaltheorie.

Toepassing 10.1 Laat p een priemgetal zijn en laat $a \in \mathbb{Z}$ zodanig dat $p \nmid a$. Dan is het polynoom

$$f(X) = X^p - X - a$$

irreducibel in $\mathbb{Z}/p\mathbb{Z}[X]$.
Oplossing Stel dat

$$f(X) = g(X)h(X)$$

voor zekere $g, h \in \mathbb{Z}/p\mathbb{Z}[X]$ met $\deg g < p$ en $\deg h < p$. Laat α een nulpunt zijn van f in een lichaamsuitbreiding van $\mathbb{Z}/p\mathbb{Z}[X]$. Zonder verlies van algemeenheid mogen we aannemen dat $g(\alpha) = 0$. Dan geldt

$$\begin{aligned} 0 &= g(\alpha) \\ &= g(\alpha)^p \\ &= g(\alpha^p) \\ &= g(\alpha + a). \end{aligned}$$

We concluderen dat $\alpha + a$ ook een nulpunt van g is. Maar dan zijn $\alpha, \alpha + a, \ldots, \alpha + (p-1)a$ verschillende nulpunten van g. Dit is een tegenspraak met $\deg g < p$. □

In de volgende toepassing zien we een mooie combinatie van reductie modulo p en algebraïsche getaltheorie.

Toepassing 10.2 Laat $n \in \mathbb{Z}_{\geq 0}$. Dan is het polynoom

$$f(X) = (X^2 + X)^{2^n} + 1$$

irreducibel.
Oplossing 1 Laat $\hat{f}$ de reductie van f modulo 2 zijn. Dan geldt

$$\hat{f}(X) = (X^2 + X)^{2^n} + 1 = (X^2 + X + 1)^{2^n}.$$

Stel nu dat $f(X) = g(X)h(X)$ met $\deg g > 0$ en $\deg h > 0$. Dan moet wel gelden dat

$$\hat{g}(X) = (X^2 + X + 1)^a$$

en

$$\hat{h}(X) = (X^2 + X + 1)^b,$$

waar $a + b = 2^n$, $a > 0$ en $b > 0$. We concluderen dat

$$g(X) = (X^2 + X + 1)^a + 2g_1(X)$$

en

$$h(X) = (X^2 + X + 1)^b + 2h_1(X)$$

voor zekere $g_1, h_1 \in \mathbb{Z}[X]$. Laat ω een oplossing zijn van

$$\omega^2 + \omega + 1 = 0.$$

Invullen van ω in $f(X) = g(X)h(X)$ geeft nu

$$2 = 4g_1(\omega)h_1(\omega)$$

oftewel

$$\frac{1}{2} = g_1(\omega)h_1(\omega).$$

Hieruit volgt echter dat $\frac{1}{2}$ een element is van $\mathbb{Z}[\omega]$. Dit is de gezochte tegenspraak. □

Oplossing 2 Voor $n = 0$ is het triviaal. We zullen dus aannemen dat $n > 0$. Definieer ξ als

$$\xi^{2^n} = -1$$

en definieer η als

$$\eta^2 + \eta = \xi.$$

We willen bewijzen dat

$$[\mathbb{Q}(\eta) : \mathbb{Q}] = 2^{n+1}.$$

Merk daartoe op dat

$$[\mathbb{Q}(\eta, \xi) : \mathbb{Q}(\eta)][\mathbb{Q}(\eta) : \mathbb{Q}] = [\mathbb{Q}(\eta, \xi) : \mathbb{Q}] = [\mathbb{Q}(\eta, \xi) : \mathbb{Q}(\xi)][\mathbb{Q}(\xi) : \mathbb{Q}].$$

Uit $\eta^2 + \eta = \xi$ concluderen we dat

$$[\mathbb{Q}(\eta, \xi) : \mathbb{Q}(\eta)] = 1.$$

In stelling 6.4 hebben we bewezen dat het polynoom $X^{2^n} + 1$ irreducibel is, zodat

$$[\mathbb{Q}(\xi) : \mathbb{Q}] = 2^n.$$

Resteert nog te bewijzen dat

$$[\mathbb{Q}(\eta, \xi) : \mathbb{Q}(\xi)] = 2.$$

Het is dus voldoende om te bewijzen dat het polynoom

$$X^2 + X - \xi$$

irreducibel is in $\mathbb{Q}(\xi)$. We zullen daartoe bewijzen dat dit polynoom geen nulpunten kan hebben in $\mathbb{Q}(\xi)$. Stel maar dat

$$X^2 + X - \xi = 0.$$

Dit impliceert dat

$$(2X + 1)^2 = 1 + 4\xi.$$

We nemen nu aan beide kanten de norm. Merk op dat

$$N(1 + 4\xi) = (1 + 4\xi)(1 + 4\xi^3) \cdots (1 + 4\xi^{2^{n+1}-1}).$$

Als we nu gebruiken dat

$$X^{2^n} + 1 = (X - \xi)(X - \xi^3) \cdots (X - \xi^{2^{n+1}-1}),$$

vinden we dat

$$X^{2^n} + 4^{2^n} = (X - 4\xi)(X - 4\xi^3) \cdots (X - 4\xi^{2^{n+1}-1}).$$

Invullen van -1 geeft dan

$$N(1 + 4\xi) = 1 + 4^{2^n}.$$

Schrijf nu

$$N(2X + 1) = y \in \mathbb{Q},$$

dan

$$y^2 = 1 + 4^{2^n}.$$

Merk op dat $1 + 4^{2^n} \in \mathbb{Z}$, zodat ook $y \in \mathbb{Z}$. Tenslotte merken we nog op dat 4^{2^n} een kwadraat is, maar dan moet wel gelden dat

$$4^{2^n} = 0.$$

Dit is de gezochte tegenspraak. □

Tenslotte merken we nog op dat uit het irreducibel zijn van

$$(X^2 + X)^{2^n} + 1$$

het irreducibel zijn van

$$X^{2^n} + 1$$

onmiddellijk volgt. Hiermee is de implicatie van rechts naar links in stelling 6.4 dus opnieuw bewezen.

11 Toepassingen van Perron

In dit hoofdstuk bekijken we verschillende toepassingen van het criterium van Perron. We zullen beginnen met een probleem uit de IMO van 1993.

Toepassing 11.1 Laat

$$f(X) = X^n + 5X^{n-1} + 3,$$

waar $n > 1$ een geheel getal is. Bewijs dat f irreducibel is.
Oplossing Dit volgt onmiddellijk uit stelling 7.2. □

Het zal echter vaak voorkomen dat het criterium van Perron niet direct kan worden toegepast. In dit geval is het soms mogelijk om de ideeën in het bewijs te gebruiken. De volgende twee toepassingen zijn goede voorbeelden hiervan.

Toepassing 11.2 Laat $a_1 \geq a_2 \geq \cdots \geq a_n > 0$ positieve gehele getallen zijn. Dan is het polynoom

$$f(X) = X^n - a_1X^{n-1} - a_2X^{n-2} - \cdots - a_n$$

irreducibel.
Oplossing Voor $n = 1$ is het triviaal. We zullen dus aannemen dat $n > 1$. We bekijken

$$(X-1)f(X) = X^{n+1} + (-1-a_1)X^n + (a_1-a_2)X^{n-1} + \cdots + a_n.$$

Schrijf nu

$$g(X) = (X-1)f(X) = \sum_{i=0}^{n+1} b_iX^i.$$

Dan weten we dat $b_0 = a_n$, $b_i = a_{n-i} - a_{n-i+1}$ voor $0 < i < n$, $b_n = -1 - a_1$ en $b_{n+1} = 1$. Merk op dat

$$|b_n| = 1 + |b_{n-1}| + \cdots + |b_1| + |b_0|.$$

We kunnen dus 'bijna' het criterium van Perron toepassen op $g(X)$. Door het bewijs van lemma 7.1 te volgen vinden we dat:

1. Precies één (enkelvoudig) nulpunt van $g(X)$ ligt op de eenheidscirkel, dit is het nulpunt $\alpha = 1$;

2. Precies één (enkelvoudig) nulpunt van $g(X)$ ligt buiten de eenheidscirkel;

3. Alle andere nulpunten van $g(X)$ liggen binnen de eenheidscirkel.

Als we nu het bewijs van stelling 7.2 volgen, zien we dat $f(X)$ irreducibel is. □

De laatste toepassing lijkt sterk op de vorige toepassing.

Toepassing 11.3 Laat $a \in \mathbb{Z}$ zodanig dat $a \neq 0$ en laat $n \in \mathbb{Z}$ zodanig dat $n \geq 3$. Dan is het polynoom

$$f(X) = X^n + aX^{n-1} + aX^{n-2} + \cdots + aX - 1$$

irreducibel.
Oplossing We bekijken

$$(X-1)f(X) = X^{n+1} + (a-1)X^n - (a+1)X + 1.$$

Als $a < 0$, dan geldt

$$|a-1| = 1 + |a+1| + 1.$$

We gebruiken nu het argument in Toepassing 11.2 om te bewijzen dat $f(X)$ irreducibel is. Als $a > 0$, bekijk dan het reciproke polynoom van $(X-1)f(X)$, oftewel

$$X^{n+1} - (a+1)X^n + (a-1)X + 1.$$

Het is vanwege stelling 4.2 voldoende om te bewijzen dat dit polynoom irreducibel is. In dit geval geldt

$$|a+1| = 1 + |a-1| + 1.$$

Dus ook hier kunnen we het argument in Toepassing 11.2 gebruiken. □

12 Miscellanea

In dit hoofdstuk bekijken we verschillende toepassingen. We beginnen met een handige stelling, waarmee we een groot aantal problemen kunnen oplossen.

Stelling 12.1 Laat $f \in \mathbb{Z}[X]$ en schrijf

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0.$$

Stel dat $|a_0|$ priem is en stel dat

$$|a_0| > |a_1| + |a_2| + \cdots + |a_n|.$$

Dan is f irreducibel.
Bewijs Laat α een complex nulpunt van f zijn. Stel dat $|\alpha| \leq 1$, dan

$$|a_0| = |a_1\alpha + \cdots + a_n\alpha^n| \leq |a_1| + \cdots + |a_n|.$$

Dit is in tegenspraak met de gegeven ongelijkheid. Dus alle nulpunten van f voldoen aan $|\alpha| > 1$. Stel nu dat $f(X) = g(X)h(X)$ met $g(X)$ en $h(X)$ geen eenheden. Merk op dat zowel $g(X)$ als $h(X)$ dan niet constant kan zijn. Er geldt

$$a_0 = f(0) = g(0)h(0).$$

Aangezien $|a_0|$ priem is, concluderen we dat $|g(0)| = 1$ of $|h(0)| = 1$. Stel zonder verlies van algemeenheid dat $|g(0)| = 1$ en laat b de kopcoëfficiënt van g zijn. Als $\alpha_1, \alpha_2, \ldots, \alpha_k$ de wortels van g zijn, dan hebben we

$$|\alpha_1\alpha_2 \cdots \alpha_k| = \frac{1}{|b|} \leq 1.$$

Echter, $\alpha_1, \alpha_2, \ldots, \alpha_k$ zijn ook nulpunten van f, zodat $|\alpha_i| > 1$ voor alle $i = 1, \ldots, k$. Tenslotte merken we nog op dat $g(X)$ niet constant is, zodat het bovenstaande product niet leeg is. Dit is een tegenspraak. □

De volgende twee problemen zijn nu triviaal.

Toepassing 12.2 Laat $f \in \mathbb{Z}[X]$. Bestaat er altijd een positief geheel getal k zodanig dat $f(X) - k$ irreducibel is?
Oplossing Ja, zie stelling 12.1. □

Toepassing 12.3 Bestaat er een rij $a_0, a_1, a_2, \ldots$ in $\mathbb{N}$ zodanig dat voor alle $i \neq j$ geldt dat $\gcd(a_i, a_j) = 1$ en voor alle n geldt dat het polynoom $\sum_{i=0}^{n} a_i X^i$ irreducibel is in $\mathbb{Z}[X]$?
Oplossing Ja, zie stelling 12.1. □

We bekijken nu een niet-triviale toepassing van stelling 12.1.

Toepassing 12.4 Laat n een positief geheel getal zijn en laat $A_1, A_2, \ldots A_k$ een partitie zijn van de verzameling positieve gehele getallen. Bewijs dat er een $i \in \{1, 2, \ldots, k\}$ is zodanig dat er oneindig veel irreducibele polynomen zijn van graad n met coëfficiënten verschillende

elementen in A_i.
Oplossing We kiezen i zodanig dat A_i oneindig veel priemgetallen bevat. Laat $p_1, \ldots, p_n$ de kleinste priemgetallen zijn in A_i. Bekijk nu de familie van polynomen

$$f_c(X) = c + \sum_{i=1}^{n} p_i X^i,$$

waarbij c nog nader te bepalen is. Merk op dat er oneindig veel priemgetallen p in A_i zijn zodanig dat

$$p > \sum_{i=1}^{n} p_i.$$

Uit stelling 12.1 volgt dan dat $f_p(X)$ irreducibel is en dus aan alle eigenschappen in de stelling voldoet. □

We kijken tenslotte nog naar een bekende stelling, oorspronkelijk bewezen door Selmer. We volgen het sterk vereenvoudigde bewijs van Shoumin Liu uit [4].

Stelling 12.5 Laat $n \in \mathbb{N}$ zodanig dat $n \geq 2$. Dan is het polynoom

$$f_n(X) = X^n - X - 1$$

irreducibel.
Bewijs Laat $f(X) \in \mathbb{Z}[X]$ monisch zijn zodanig dat de constante term niet nul is. Laat dan $x_1, \ldots, x_n$ de wortels van $f(X)$ zijn met multipliciteiten. Definieer nu

$$S(f) = \sum (x_i - \frac{1}{x_i}).$$

Merk op dat S een rationale combinatie van de elementair symmetrische functies σ_1, σ_{n-1} en σ_n is. We concluderen dat $S(f) \in \mathbb{Q}$. Bovendien geldt dat $S(f) \in \mathbb{Z}$ als de constante term van $f(X)$ 1 of -1 is. Stel nu dat $f(X) = g(X)h(X)$ met $g(X), h(X) \in \mathbb{Z}[X]$. Dan geldt

$$S(f) = S(g) + S(h).$$

Als $f(X)$ constante term 1 of -1 heeft, dan geldt dat ook voor $g(X)$ en $h(X)$. In dit geval geldt dus $S(f), S(g), S(h) \in \mathbb{Z}$. Laat nu $n \geq 3$ en schrijf $f_n(X)$ als volgt

$$f_n(X) = \prod_{i=1}^{n} (X - x_i) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0,$$

waar $a_{n-1} = 0$, $a_1 = -1$ en $a_0 = -1$. Nu geldt

$$S(f_n) = \sum (x_i - \frac{1}{x_i}) = \sum x_i - \sum \frac{1}{x_i} = -a_{n-1} - \sum \frac{x_1 \cdots x_{i-1} x_{i+1} \cdots x_n}{x_1 \cdots x_n} = 0 + \frac{a_1}{a_0} = 1.$$

Laat x_i een wortel zijn van f_n, dan

$$x_i + 1 = x_i^n, \quad \overline{x_i} + 1 = \overline{x_i}^n.$$

En dus

$$(x_i + 1)(\overline{x_i} + 1) = x_i^n \overline{x_i}^n,$$

waaruit volgt dat

$$x_i + 1 + \overline{x_i} = x_i^n \overline{x_i}^n - x_i \overline{x_i} = \begin{cases} \geq 0, & |x_i| \geq 1 \\ \leq 0, & |x_i| \leq 1. \end{cases}$$

We concluderen dat

$$(x_i + 1 + \overline{x_i})(1 - \frac{1}{x_i \overline{x_i}}) \geq 0,$$

oftewel

$$x_i - x_i^{-1} + \overline{x_i} - \overline{x_i}^{-1} = (x_i + \overline{x_i})(1 - \frac{1}{x_i \overline{x_i}}) \geq \frac{1}{x_i \overline{x_i}} - 1.$$

Dus voor elke factor g van f_n geldt

$$S(g) = \sum (x_i - \frac{1}{x_i}) \geq \frac{1}{2} \sum (\frac{1}{|x_i|^2} - 1).$$

De som is over alle wortels van g. Echter, voor het product van diezelfde wortels geldt

$$\prod \frac{1}{|x_i|^2} = 1.$$

Uit de rekenkundig-meetkundig gemiddelde ongelijkheid (met gelijkheid alleen als $|x_i| = 1$ voor alle i) volgt nu dat $S(g) \geq 0$. Dus elke factorisatie van f_n leidt tot de partitie

$$1 = 0 + 1.$$

Maar dan moet wel gelden dat

$$1 = |x| = |x + 1| = |x^n|.$$

Dit kan alleen als $x = e^{\pm \frac{2\pi i}{3}}$. De enige mogelijke factor van f_n met $S(g) = 0$ is dus $g(X) = X^2 + X + 1$. Het is niet moeilijk om na te gaan dat $X^2 + X + 1$ geen factor van f_n is, waarmee het bewijs voltooid is. □

13 Literatuurlijst

1 L. N. Stewart en D. O. Tall, Algebraic Number Theory, Chapman and Hall, 1979.
2 M. Ram Murty, Prime Numbers and Irreducible Polynomials, http://www.mast.queensu.ca/~murty/monthly.pdf.
3 Yufei Zhao, Integer Polynomials, http://yufeizhao.com/olympiad/intpoly.pdf.
4 Shoumin Liu, Trinomials and exponential Diophantine equations, http://www.math.leidenuniv.nl/scripties/Liu2Master.pdf.

A Newton polygonen

Deze appendix bestaat uit twee delen. In het eerste deel zullen we de nodige meetkundige theorie bespreken. We zullen vervolgens met behulp van deze meetkundige theorie een bewijs geven van de stelling van Dumas.

Laat $A, B \subseteq \mathbb{R}^2$, dan definiëren we de Minkowski som van A en B als

$$A + B = \{a + b \mid a \in A, b \in B\}.$$

Hier bedoelen we met $a+b$ componentsgewijze optelling van de twee vectoren. De Minkowski som heeft een aantal mooie eigenschappen. Laat $A, B, C \subseteq \mathbb{R}^2$, dan geldt

$$A + B = B + A$$

en

$$(A + B) + C = A + (B + C).$$

Laat l nu een lijnstuk zijn. We zullen aannemen dat l niet verticaal loopt. We zullen het punt met de kleinste x-coördinaat het beginpunt noemen van het lijnstuk en het punt met de grootste x-coördinaat het eindpunt noemen van het lijnstuk. We definiëren het gebied $G(l) \subseteq \mathbb{R}^2$ als volgt: transleer l zodanig dat het beginpunt in de oorsprong komt te liggen. Nu is $G(l)$ het gebied op of boven het lijnstuk l.

Laat $l_1, l_2, \ldots, l_k$ de lijnen van een Newton polygoon zijn, zodanig dat de hellingen stijgend zijn. Laat P het beginpunt van l_1 zijn. Met N noteren het gebied in $\mathbb{R}^2$ op of boven het Newton polygoon. Dan geldt

$$N = \{P\} + G(l_1) + G(l_2) + \ldots + G(l_k).$$

Als we terugdenken aan de stelling van Dumas, dan wordt het Newton polygoon van $f = gh$ geconstrueerd door de lijnstukken van g en h in de juiste volgorde achter elkaar te zetten. Dit zullen we nu de lijnstukken-som noemen. Laat N, M en O het gebied op of boven het Newton polygoon van respectievelijk f, g en h zijn. Met behulp van de bovenstaande observatie is het niet moeilijk om in te zien dat

$$M + O$$

precies correspondeert met de lijnstukken-som van g en h. Het is daarom voldoende om te bewijzen dat

$$N = M + O.$$

Daartoe bewijzen we eerst dat

$$(i, \nu(f_i)) \in M + O,$$

waar

$$f_i = \sum_{a=0}^{i} g_a h_{i-a}.$$

Merk daartoe op dat

$$\nu(f_i) = \nu(\sum_{a=0}^{i} g_a h_{i-a}) \geq \min_{0 \leq a \leq i} \nu(g_a) + \nu(h_{i-a}).$$

Nu geldt voor alle gehele $0 \leq a \leq i$ dat $(a, \nu(g_a)) \in M$ en $(i-a, \nu(h_{i-a})) \in O$, zodat

$$(i, \nu(g_a) + \nu(h_{i-a})) \in M + O.$$

Omdat dit geldt voor alle gehele $0 \leq a \leq i$, concluderen we dat

$$(i, \min_{0 \leq a \leq i} \nu(g_a) + \nu(h_{i-a})) \in M + O$$

en dus

$$(i, \nu(f_i)) \in M + O.$$

We mogen nu concluderen dat $M + O$ zeker N bevat. Om het bewijs te voltooien, hebben we de notie van halfruimte nodig. Een verzameling H is een halfruimte als het van de volgende vorm is voor zekere $n \in \mathbb{R}^2$ en $a \in \mathbb{R}$

$$H_{n,a} = \{x \in \mathbb{R}^2 \mid x \cdot n \leq a\},$$

waar $x \cdot n$ het inproduct is. Laat A nu een convexe verzameling zijn. We noemen $x \in \mathbb{R}^2$ een knoop van A als er een halfruimte H is met

$$A \cap H = \{x\}.$$

We kunnen nu het bewijs eenvoudig afmaken. Merk op dat M en O convexe verzamelingen zijn. Laat x een knoop van M zijn met bijbehorende halfruimte $H_{n,a}$ en laat y een knoop van O zijn met bijbehorende halfruimte $H'_{n',a'}$. Nu geldt het volgende: als $n = n'$, dan is $x + y$ een knoop van $M + O$ met bijbehorende halfruimte $H_{n,a} + H'_{n',a'}$. Het is niet moeilijk om na te gaan dat alle knopen van $M + O$ op precies deze manier ontstaan. Het is dus voldoende om te bewijzen dat $x + y \in N$.

Schrijf daartoe $x = (i, \nu(g_i))$ en $y = (j, \nu(h_j))$. Dan geldt

$$\nu(f_{i+j}) = \nu(\sum_{a=0}^{i+j} g_a h_{i+j-a}).$$

We willen bewijzen dat

$$\nu(f_{i+j}) = \nu(g_i) + \nu(h_j).$$

Laat nu $s \neq 0$ en bekijk $g_{i-s}h_{j+s}$. Merk op dat de rand van zowel $H_{n,a}$ als $H'_{n',a'}$ een lijn is. Deze twee lijnen hebben dezelfde richtingscoëfficiënt r. Nu geldt

$$\nu(g_{i-s}) > \nu(g_i) - sr$$

en

$$\nu(h_{j+s}) > \nu(h_j) + sr.$$

Hieruit kunnen we inderdaad concluderen dat

$$\nu(f_{i+j}) = \nu(g_i) + \nu(h_j),$$

waarmee het bewijs voltooid is.