

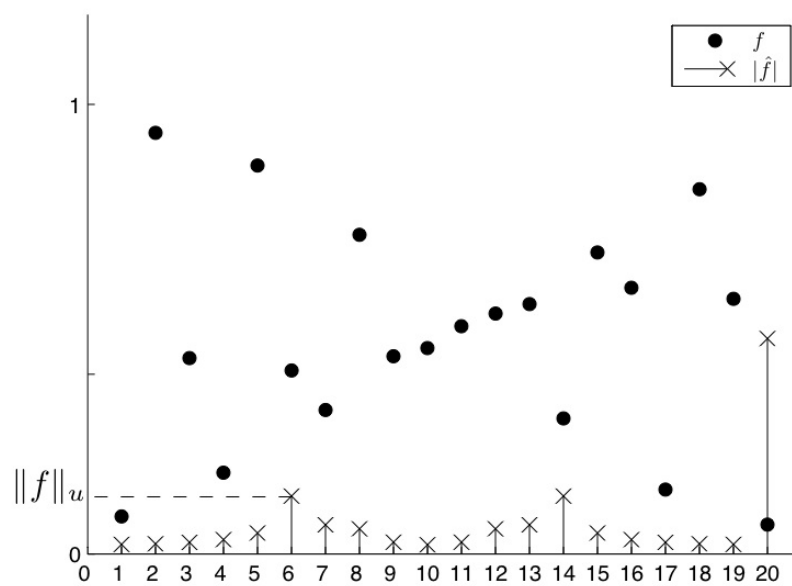
Eindige Fourier-Analyse in de Additieve Combinatoriek

Sam van Gool

22 juni 2007

Bachelorscriptie

Begeleiding: prof. dr. T. H. Koornwinder



KdV Instituut voor wiskunde
Faculteit der Natuurwetenschappen, Wiskunde en Informatica
Universiteit van Amsterdam



Samenvatting

De stelling van Szemerédi zegt dat verzamelingen met een positieve bovendichtheid voor iedere $k \geq 3$ een rekenkundig rijtje van lengte k bevatten.

In dit verslag bestuderen en vergelijken we twee bewijzen van deze stelling voor het geval $k = 3$ zoals gegeven door Tao en Vu in het boek Additive Combinatorics en door Roth in zijn artikel uit 1953.

Voor dit doel gebruiken we de technieken die Fourier-analyse op eindige groepen geeft om problemen uit het rijke vakgebied van de Additieve Combinatoriek aan te pakken.

Abstract

According to Szemerédi's theorem, sets of positive upper density contain an arithmetic progression of length k for every $k \geq 3$.

In this report, we study and compare two proofs of this theorem in the case $k = 3$ as given by Tao and Vu in the book Additive Combinatorics and by Roth in his article from 1953.

To achieve this goal, we use techniques from Fourier analysis on finite groups to tackle problems from the rich field of Additive Combinatorics.

Gegevens

Titel: Eindige Fourier-Analyse in de Additieve Combinatoriek

Auteur(s): Sam van Gool, sgool@science.uva.nl, 0468177

Website: <http://student.science.uva.nl/~sgool/>

Begeleider: prof. dr. T. H. Koornwinder

Tweede beoordelaar: dr. D. C. Gijswijt

Einddatum: 22 juni 2007

Korteweg de Vries Instituut voor Wiskunde

Universiteit van Amsterdam

Plantage Muidersgracht 24, 1018 TV Amsterdam

<http://www.science.uva.nl/math>

Afbeelding voorzijde: Een voorbeeld van een redelijk uniforme functie f op \mathbb{Z}_{20} met de absolute waarde van de Fourier-getransformeerde $|\hat{f}|$ en lineaire afwijking $\|f\|_u$.

Inhoudsopgave

Inleiding	3
1 Eindige Fourier-analyse: technieken	5
1.1 Fouriertransformatie	6
1.2 Convolutie	12
1.3 Lineaire afwijking	14
1.4 Uniforme verzamelingen optellen	19
2 De stelling van Szemerédi	23
2.1 Formulering met behulp van r_k	24
2.2 Equivalentie van formuleringen	25
3 Het bewijs van Tao voor $k = 3$	29
3.1 De Λ_3 -operator	29
3.2 Niet-uniformiteit in \mathcal{A}_3 -verzamelingen	32
3.3 Dichtheidstoename bij niet-uniforme functies	35
3.4 Dichtheidstoename bij \mathcal{A}_3 -verzamelingen	38
3.5 $o(N)$ schatting voor r_3	40
3.6 $O(N/\log \log N)$ schatting voor r_3	40
3.6.1 Bewijs uit het ongerijmde	40
3.6.2 Bewijs met behulp van iteratie	42
4 Het bewijs van Roth voor $k = 3$	47
4.1 Enkele eigenschappen van de functie a	47
4.2 Een functionele ongelijkheid voor $a(m)$	48
4.3 De schatting voor $a(m)$	57
Nawoord	61
Spelen met Verzamelingen (populaire samenvatting)	63
Bibliografie	67

Inleiding

Οἱ πρῶτοι ἀριθμοὶ πλείους εἰσὶ παντὸς τοῦ προτεθέντος πλήθους πρώτων ἀριθμῶν.

“Er zijn meer priemgetallen dan iedere vooraf genoemde hoeveelheid priemgetallen.”
(Euclides: Elementen [1], Propositie 9.20)

Rond 300 voor Christus was Alexandrijns wiskundige Euclides de eerste die, in bovenstaande bewoordingen, de oneindigheid van priemgetallen beschreef. Hiermee opende hij de deur tot het rijke vakgebied van de getaltheorie, dat ook 23 eeuwen later nog aanleiding geeft tot talrijke publicaties.

In 2004 bewezen Ben Green en Terence Tao een vermoeden over de structuur van priemgetallen dat al lange tijd bestond en sindsdien bekend staat als de stelling van Green-Tao [3]:

Stelling 0.1 (Green, Tao, 2004). *Voor iedere $k \geq 3$ bestaat er een rekenkundig rijtje priemgetallen van lengte k .*

Het bewijs van deze stelling omvat 56 pagina’s harde wiskunde en bleek al in een vroeg stadium van mijn onderzoek te hoog gegrepen als doel voor mijn Bachelorscriptie, door de vele verschillende technieken en vakgebieden die in het bewijs van Green en Tao samenkwamen.

Een belangrijk ingrediënt in de oplossing van veel problemen uit het vakgebied van de Additieve Combinatoriek, waar ook de stelling van Green-Tao toe behoort, blijkt Eindige Fourier-analyse te zijn.

Op het eerste gezicht is dat misschien verrassend, omdat we veelal gewend zijn Fourier-analyse op functies, niet op eindige verzamelingen toe te passen, maar de principes van Fourier-analyse van functies $f : \mathbb{R}/\mathbb{Z} \rightarrow \mathbb{C}$ zijn, zoals in Hoofdstuk 1 van deze scriptie zal blijken, ook toe te passen op functies $f : Z \rightarrow \mathbb{C}$, waarin Z een willekeurige eindige abelse groep mag zijn.

Na de technieken van de eindige Fourier-analyse besproken te hebben, zullen we als grote toepassing de stelling van Szemerédi voor het geval $k = 3$ bekijken. De stelling van Szemerédi zegt dat verzamelingen die ‘dicht genoeg’ liggen in de natuurlijke getallen altijd rekenkundige rijtjes van lengte k bevatten, voor iedere k . De precieze formulering van Szemerédi en een equivalente, voor onze doelen bruikbaarere formulering worden in Hoofdstuk 2 besproken.

De stelling van Szemerédi blijkt helaas geen directe uitspraak over priemgetallen te doen: de verzameling van priemgetallen is niet ‘dicht genoeg’ in de zin van Szemerédi’s stelling, die hij in 1975 al bewees. Het heeft sindsdien nog bijna 30 jaar geduurd tot Green en Tao er gezamenlijk in slaagden een bewijs van de stelling van Szemerédi zó aan te passen dat het ook voor de priemgetallen bruikbaar werd.

We leggen ons in deze scriptie toe op het geval $k = 3$ van van de stelling van Szemerédi en behandelen hiervoor twee bewijzen, in Hoofdstuk 3 beginnend met het bewijs zoals Tao en Vu dat geven in [8], waarin het begrip Lineaire afwijking (dat al in Hoofdstuk 1 zal worden geïntroduceerd) een belangrijke rol zal spelen.

Het oorspronkelijke bewijs van Roth zal ten slotte in Hoofdstuk 4 besproken worden. Ook van dit bewijs zou men kunnen zeggen dat er Fourier-analyse in gebruikt wordt, maar dan wel op een nogal ‘verborgen’ manier die Roth in zijn oorspronkelijke artikel uit 1953 [4] niet expliciet maakte. In Hoofdstuk 4 bespreken we het bewijs van Roth en proberen we bovendien door het gebruik van Tao’s moderne notatie dit verband met Fourier-analyse enigszins te verduidelijken.

Het onderscheid tussen inleiding en voorwoord is voor mijn gevoel altijd enigszins kunstmatig. In een Voorwoord bedankt een auteur doorgaans zijn begeleiders, inspiratiebronnen en dierbaren voor hun steun tijdens zijn onderzoek, maar naar mijn idee (en eigen leeservaring) slaan lezers het Voorwoord, wanneer het als aparte sectie gepresenteerd wordt, vaak over.

Om dit te voorkomen bedank ik hier nu, plotseling, onverwachts, aan het eind van mijn inleiding, graag een aantal mensen: mijn begeleider Tom Koornwinder voor zijn aanstekelijke enthousiasme, grote hulp en mailtjes met hints en aanwijzingen, zelfs na middernacht; mijn tweede beoordelaar Dion Gijswijt voor zijn kritiek op mijn presentatie en op dit stuk; Vincent van der Noort voor een gesprek op een winteravond dat mij uiteindelijk tot dit onderwerp bracht; Chris van Dorp voor de kopjes koffie en de geruststelling dat eenieder die zijn scriptie schrijft het er af en toe wel even mee gehad heeft; mijn ouders en zussen/-jes, voor al het andere.

Sam van Gool
Amsterdam, juni 2007

Hoofdstuk 1

Eindige Fourier-analyse: technieken

Zowel in de door Terence Tao gevolgde werkwijze bij het bewijzen van de stelling van Green-Tao (Stelling 0.1) als in eenvoudiger resultaten uit de additieve getaltheorie (zoals bijvoorbeeld Gevolg 1.37) kunnen de klassieke principes van de Fourier-analyse worden toegepast op eindige abelse groepen.

In ons geval zal de eindige abelse groep waarop Fourier-analyse toegepast wordt altijd een groep van de vorm $\mathbb{Z}_N := \mathbb{Z}/N\mathbb{Z}$ zijn, maar dat is niet noodzakelijk; zelfs het abels-zijn van een groep is niet essentieel voor de theorie. In het vervolg zullen we wel steeds eisen dat de eindige groep in kwestie abels is, ter versimpeling, en omdat het laten vallen van deze eis niet veel nieuwe informatie oplevert.

Er zijn mijns inziens twee grote voordelen aan het gebruik van Fourier-analyse in het geval van eindige groepen:

- Veel van de stellingen en technieken uit de Fourier-analyse blijken in het eindige geval zeer eenvoudig te bewijzen, vooral omdat er geen sprake meer is van convergentie-kwesties: iedere som die je kunt tegenkomen is eindig en convergeert dus.
- De eindige Fourier-analyse biedt een goed startpunt voor het visualiseren van de vaak nogal abstracte getaltheoretische vragen. We zullen meerdere malen zien dat met behulp van Fourier-analyse een ogenschijnlijk zeer gecompliceerde vraag over een bepaalde eigenschap van getallen met behulp van Fourier-analyse kan worden gereduceerd tot een (mogelijk nog altijd gecompliceerde, maar in ieder geval in bekende, heldere termen formuleerbare) vraag naar een orde-schatting voor een bepaalde Fourier-getransformeerde of daarmee geassocieerde norm.

Het eerste punt zal direct in dit hoofdstuk geïllustreerd worden door een demonstratie van de kracht van de technieken uit de Fourier-analyse, door in Sectie 1.4 een probleem over het *optellen van verzamelingen* (zie bijvoorbeeld ook [5]) op te lossen.

Het tweede punt zal in latere hoofdstukken duidelijk worden, als we zien hoe Tao in zijn bewijs van de stelling van Szemerédi voor het geval $k = 3$ ook Fourier-analyse (en dan vooral het later in dit hoofdstuk te introduceren begrip *lineaire afwijking*) gebruikt.

1.1 Fouriertransformatie

Voor een functie $f : \mathbb{R}/\mathbb{Z} \rightarrow \mathbb{C}$ kan de Fourier-getransformeerde $\widehat{f}(n)$ voor een bepaalde frequentie n gedefinieerd worden als het L^2 -inproduct van f met een karakter-functie $e_n : \theta \mapsto e^{2\pi i n \theta}$.

Door naar de karakterfuncties van een eindige abelse groep Z te kijken en in het inproduct de verwachting in plaats van de integraal te nemen kunnen we ook voor functies $f : Z \rightarrow \mathbb{C}$ een Fourier-getransformeerde definiëren.

Om de definitie van de karakters op Z precies te maken, leggen we eerst een niet-gedegeneerde symmetrische bilineaire vorm op de groep Z . Een niet-gedegeneerde symmetrische bilineaire vorm kan gezien worden als een functie die aan twee elementen uit Z hun ‘gezamenlijke hoek’, een element uit \mathbb{R}/\mathbb{Z} , toekent.

Definitie 1.1. Laat Z een eindige abelse groep zijn. Een functie $\cdot : Z \times Z \rightarrow \mathbb{R}/\mathbb{Z}$ die een paar $(x, \xi) \in Z \times Z$ naar $x \cdot \xi$ stuurt heet een **niet-gedegeneerde symmetrische bilineaire vorm** als zij aan de volgende eigenschappen voldoet:

1. $\forall \xi_1, \xi_2, x \in Z : (\xi_1 + \xi_2) \cdot x = \xi_1 \cdot x + \xi_2 \cdot x$, en
 $\forall \xi, x_1, x_2 \in Z : \xi \cdot (x_1 + x_2) = \xi \cdot x_1 + \xi \cdot x_2$ (bilineair);
2. $\forall \xi \in Z \setminus \{0\} : \exists x \in Z : \xi \cdot x \neq 0$, en
 $\forall x \in Z \setminus \{0\} : \exists \xi \in Z : \xi \cdot x \neq 0$ (niet-gedegeneerd);
3. $\forall x, \xi \in Z : x \cdot \xi = \xi \cdot x$ (symmetrisch).

Voorbeeld 1.2. Als $Z = \mathbb{Z}_N$ dan kunnen we definiëren

$$(\xi + N\mathbb{Z}, x + N\mathbb{Z}) \mapsto \frac{\xi x}{N} + \mathbb{Z}.$$

Claim. Dit is een goed gedefinieerde niet-gedegeneerde symmetrische bilineaire vorm.

Bewijs. Om in te zien dat \cdot goed gedefinieerd is, laat $x \in \mathbb{Z}_N$ willekeurig. Als $\xi, \xi' \in \mathbb{Z}$, met $\xi' \equiv \xi \pmod{N}$, dan geldt

$$\xi' \cdot x = \frac{(\xi + rN)x}{N} \pmod{\mathbb{Z}} = \frac{\xi x}{N} + rx \pmod{\mathbb{Z}} = \frac{\xi x}{N} \pmod{\mathbb{Z}} = \xi \cdot x,$$

dus de waarde hangt niet af van de keuze van de representanten (het bewijs voor de tweede coördinaat is analoog).

De symmetrie volgt direct uit de commutativiteit van de normale vermenigvuldiging op \mathbb{Z} .

Als $\xi_1, \xi_2, x \in \mathbb{Z}_N$ dan geldt

$$(\xi_1 + \xi_2) \cdot x = \frac{\xi_1 x + \xi_2 x}{N} \pmod{\mathbb{Z}} = \frac{\xi_1 x}{N} \pmod{\mathbb{Z}} + \frac{\xi_2 x}{N} \pmod{\mathbb{Z}} = \xi_1 \cdot x + \xi_2 \cdot x,$$

dus de vorm is bilineair (uit symmetrie-overwegingen).
 Als $\xi \in \mathbb{Z}_N \setminus \{0\}$, dan geldt voor $x := 1$ dat

$$\xi \cdot x = \frac{\xi}{N} \bmod \mathbb{Z} \neq 0,$$

dus de vorm is niet-gedegeneerd. □

Voor de meetkundige interpretatie en ook op veel andere plaatsen in deze scriptie gebruiken we de volgende definitie.

Definitie 1.3. Voor alle $\theta \in \mathbb{C}$ definiëren we:

$$e(\theta) := e^{2\pi i \theta}.$$

Uit Voorbeeld 1.2 en Definitie 1.3 is met behulp van eenvoudige complexe analyse duidelijk waarom de vorm als ‘gezamenlijke hoek’ geïnterpreteerd kan worden: met behulp van Definitie 1.3 identificeren we \mathbb{R}/\mathbb{Z} met de eenheidscirkel. Als we vervolgens \mathbb{Z}_N inbedden in de eenheidscirkel via de afbeelding $n \mapsto e^{2\pi i n/N}$, dan komt $\xi \cdot x$ overeen met het punt waar we terecht komen als we x keer de hoek bij ξ over de eenheidscirkel lopen.

Met behulp van Voorbeeld 1.2 en de structuurstelling voor eindige abelse groepen kunnen we nu bewijzen dat iedere eindige abelse groep een niet-gedegeneerde symmetrische bilineaire vorm heeft.

Stelling 1.4. *Voor iedere eindige abelse groep Z bestaat er minstens één niet-gedegeneerde symmetrische bilineaire vorm.*

Bewijs. Dankzij de structuurstelling voor eindige groepen (zie bijvoorbeeld 4.1.1 in [6]) weten we dat $Z = \mathbb{Z}_{N_1} \times \cdots \times \mathbb{Z}_{N_k}$ voor zekere juist gekozen N_1, \dots, N_k .

We schrijven dus $x \in Z$ als $x = (x_1, \dots, x_k)$ en definiëren vervolgens $\xi \cdot x := (\xi_1 \cdot x_1, \dots, \xi_k \cdot x_k)$, waar we voor de vormen op de \mathbb{Z}_{N_i} de vormen uit Voorbeeld 1.2 nemen.

Het is eenvoudig na te gaan dat de zo verkregen afbeelding \cdot op Z niet-gedegeneerd, symmetrisch en bilineair is (alle eigenschappen worden direct overgeërfd van de eigenschappen van \cdot op \mathbb{Z}_N). □

We nemen vanaf nu steeds aan dat Z een abelse groep met een niet-gedegeneerde symmetrische bilineaire vorm \cdot is.

Definitie 1.5. Een **karakter** ξ van Z is een homomorfisme $\xi : Z \rightarrow \mathbb{R}/\mathbb{Z}$, dat wil zeggen $\xi(x + y) = \xi(x) + \xi(y)$ voor alle $x, y \in Z$.

Definitie 1.6. Voor iedere $\xi \in Z$ definiëren we e_ξ als de functie

$$e_\xi(x) := e(\xi \cdot x),$$

waar we $\xi \cdot x \in \mathbb{R}/\mathbb{Z}$ kunnen opvatten als element van \mathbb{C} .

Stelling 1.7. *De karakters van Z zijn precies de functies e_ξ voor $\xi \in Z$.*

Bewijs. Zie bijvoorbeeld [7]. □

Voor we daadwerkelijk een aantal technieken van Fourier-analyse kunnen toepassen op eindige abelse groepen voeren we nog enige notatie in die afkomstig is uit de kansrekening. Tao gebruikt deze notatie in zijn boek [8] voortdurend.

Een voordeel van deze notatie is dat termen als ‘verwachting’ en ‘kans’ misschien hanterbaarder zijn dan ‘som’ en ‘quotient’. Een nadeel is dat het op het eerste gezicht door de kans-notatie kan lijken alsof er ook sprake is van onzekerheid. Dit is geenszins het geval, zoals uit de definitie zal blijken.

Definitie 1.8. We definiëren voor iedere deelverzameling $A \subseteq Z$ de **indicatorfunctie**

$$1_A(x) := \begin{cases} 1 & \text{als } x \in A; \\ 0 & \text{anders.} \end{cases}$$

We zullen voor $\xi \in Z$ ook de notatie 1_ξ gebruiken als we eigenlijk $1_{\{\xi\}}$ bedoelen.

Voor een functie $f : Z \rightarrow \mathbb{C}$ definiëren we de **verwachting** van f als volgt:

$$\mathbf{E}_Z(f) = \mathbf{E}_{x \in Z} f(x) := \frac{1}{|Z|} \sum_{x \in Z} f(x).$$

Voor een deelverzameling $A \subseteq Z$ definiëren we de **kans** of **dichtheid** van A in Z :

$$\mathbf{P}_Z(A) = \mathbf{P}_{x \in Z}(x \in A) := \frac{|A|}{|Z|} = \mathbf{E}_Z(1_A).$$

De cruciale eigenschap om Fourier-analyse te laten werken is dat de karakters orthogonaal zijn, in de volgende zin:

Lemma 1.9 (Orthogonaliteitseigenschappen). *Voor alle $\xi, \xi', x, x' \in Z$ gelden de volgende twee eigenschappen:*

$$\mathbf{E}_{x \in Z} e_\xi(x) \overline{e_{\xi'}(x)} = 1_\xi(\xi'); \tag{1.1}$$

$$\sum_{\xi \in Z} e_\xi(x) \overline{e_\xi(x')} = |Z| 1_x(x'). \tag{1.2}$$

Bewijs. De cruciale stap van het bewijs is de eenvoudige berekening:

$$\begin{aligned} \mathbf{E}_{x \in Z} e_\xi(x) \overline{e_{\xi'}(x)} &= \mathbf{E}_{x \in Z} e(\xi \cdot x) e(-\xi' \cdot x) \\ &= \frac{1}{|Z|} \sum_{x \in Z} e((\xi - \xi') \cdot x), \end{aligned}$$

zodat als $\xi - \xi' = 0$ ten duidelijkste geldt dat de linkerzijde van (1.1) gelijk is aan 1.

Als $\xi - \xi' \neq 0$ dan bestaat er een $h \in Z$ zodat $(\xi - \xi') \cdot h \neq 0$, omdat \cdot niet-gedegeneerd is. Er geldt dus ook dat $e((\xi - \xi') \cdot h) \neq 1$.

Anderzijds zien we door over te gaan op een nieuwe sommatievariabele $y := x + h$ het volgende:

$$\begin{aligned} \frac{1}{|Z|} \sum_{x \in Z} e((\xi - \xi') \cdot x) &= \frac{1}{|Z|} \sum_{y \in Z} e((\xi - \xi') \cdot y) \\ &= \frac{1}{|Z|} e((\xi - \xi') \cdot h) \sum_{x \in Z} e((\xi - \xi') \cdot x), \end{aligned}$$

dus er geldt

$$(1 - e((\xi - \xi') \cdot h)) \mathbf{E}_{x \in Z} e((\xi - \xi') \cdot x) = 0.$$

Omdat we al zagen dat $e((\xi - \xi') \cdot h) \neq 1$ moet dus gelden dat

$$\mathbf{E}_{x \in Z} e((\xi - \xi') \cdot x) = 0,$$

waarmee (1.1) ook bewezen is als $\xi - \xi' \neq 0$.

Uit het feit dat \cdot symmetrisch is en de definitie van \mathbf{E} volgt nu uit (1.1) ook direct (1.2). \square

We kunnen met behulp van dit orthogonaliteitslemma de karakters zien als basis van de ruimte van functies op Z , zoals ook in de klassieke Fourier-analyse van functies die op een interval in \mathbb{R} gedefinieerd zijn.

Definitie 1.10. We noteren met $\mathbb{C}^Z := \{f : Z \rightarrow \mathbb{C}\}$ de ruimte van alle functies van Z naar \mathbb{C} .

\mathbb{C}^Z wordt een vectorruimte over \mathbb{C} met de optelling van functies gedefinieerd door $(f + g)(x) := f(x) + g(x)$ en scalarvermenigvuldiging $(cf)(x) := cf(x)$.

\mathbb{C}^Z wordt zelfs een algebra door de vermenigvuldiging van functies elementsgewijs door vermenigvuldiging in \mathbb{C} te definiëren: $(fg)(x) := f(x)g(x)$.

Op \mathbb{C}^Z leggen we een inproduct door te definiëren:

$$\langle f, g \rangle_{\mathbb{C}^Z} := \mathbf{E}_Z(f\bar{g}).$$

Lemma 1.11. \mathbb{C}^Z is een Hilbertruimte en $\langle e_\xi \mid \xi \in Z \rangle$ is een basis voor \mathbb{C}^Z .

Bewijs. Merk op dat de dimensie van \mathbb{C}^Z precies $|Z|$ is. We zien dit bijvoorbeeld in door het isomorfisme van vectorruimten $\phi : \mathbb{C}^Z \rightarrow \mathbb{C}^{|Z|}$ gedefinieerd door

$$f \mapsto (f(z_1), \dots, f(z_{|Z|})),$$

waar $\{z_i\}_{i=1}^{|Z|}$ iedere willekeurige ordening van de elementen van Z kan zijn.

Vanwege Lemma 1.9 is $\langle e_\xi \mid \xi \in Z \rangle$ een orthonormaal systeem ten opzichte van het inproduct op \mathbb{C}^Z . Omdat verder $|\{e_\xi \mid \xi \in Z\}| = |Z| = \dim \mathbb{C}^Z$ geldt dat $\langle e_\xi \mid \xi \in Z \rangle$ een basis voor \mathbb{C}^Z is.

Ten slotte is \mathbb{C}^Z volledig omdat het een eindig-dimensionale ruimte is. \square

We kunnen nu elementen uit \mathbb{C}^Z uitschrijven ten opzichte van deze basis. De coëfficiënten die we zo verkrijgen zullen we noteren met \widehat{f} , zodat \widehat{f} ook een functie op Z wordt. Deze functie noemen we de Fourier-getransformeerde van f .

Definitie 1.12. Laat $f \in \mathbb{C}^Z$. We definiëren de **Fourier-getransformeerde** \widehat{f} van f voor $\xi \in Z$ als volgt:

$$\widehat{f}(\xi) := \langle f, e_\xi \rangle_{\mathbb{C}^Z} = \mathbf{E}_{x \in Z} f(x) \overline{e(\xi \cdot x)}.$$

$\widehat{f}(\xi)$ heet de **Fourier-coëfficiënt** van f op **frequentie** ξ .

Fourier-transformatie respecteert de bewerkingen van de vectorruimte \mathbb{C}^Z :

Lemma 1.13. Voor alle $f, g \in \mathbb{C}^Z$ en $c \in \mathbb{C}$ geldt:

$$\widehat{f + g} = \widehat{f} + \widehat{g},$$

$$\widehat{cf} = c\widehat{f}.$$

Uit het feit dat $\langle e_\xi \mid \xi \in Z \rangle$ een basis voor \mathbb{C}^Z vormt kunnen we nu direct een aantal krachtige identiteiten afleiden.

Stelling 1.14 (Fourier-inversie). Laat $f \in \mathbb{C}^Z$. Dan geldt

$$f = \sum_{\xi \in Z} \widehat{f}(\xi) e_\xi. \quad (1.3)$$

Bewijs. Zij $x \in Z$. Uit de definitie van \widehat{f} en Lemma 1.9 volgt nu:

$$\begin{aligned} \sum_{\xi \in Z} \widehat{f}(\xi) e_\xi(x) &= \sum_{\xi \in Z} \mathbf{E}_{x' \in Z} f(x') \overline{e(\xi \cdot x')} e(\xi \cdot x) \\ &= \mathbf{E}_{x' \in Z} f(x') \sum_{\xi \in Z} \overline{e(\xi \cdot x')} e(\xi \cdot x) \\ &= \mathbf{E}_{x' \in Z} f(x') |Z| 1_x(x') \\ &= f(x). \end{aligned}$$

□

Gevolg 1.15. Fouriertransformatie is een lineaire bijectieve afbeelding van de ruimte \mathbb{C}^Z op zichzelf.

Bewijs. Laat $\psi : \mathbb{C}^Z \rightarrow \mathbb{C}^Z$ de afbeelding gedefinieerd door $\psi(f) := \widehat{f}$.

Uit Lemma 1.13 zien we direct dat ψ de optelling en scalar-vermenigvuldiging van \mathbb{C}^Z respecteert.

Uit Stelling 1.14 zien we dat een functie f volledig vastligt door zijn Fourier-coëfficiënten: $f = g \Leftrightarrow \widehat{f} = \widehat{g}$, dus ψ is injectief.

ψ is dus een injectieve lineaire afbeelding van \mathbb{C}^Z op zichzelf. Omdat \mathbb{C}^Z eindig-dimensionaal is, volgt nu uit lineaire algebra direct dat ψ ook surjectief is, waarmee het gestelde bewezen is.

□

Stelling 1.16 (Plancherel). *Laat $f, g \in \mathbb{C}^Z$. Dan geldt*

$$\langle f, g \rangle_{\mathbb{C}^Z} = \sum_{\xi \in Z} \widehat{f}(\xi) \widehat{g}(\xi). \quad (1.4)$$

Bewijs. We schrijven f uit als in (1.3) en gebruiken de definities van het inproduct en de Fourier-getransformeerde:

$$\begin{aligned} \langle f, g \rangle_{\mathbb{C}^Z} &= \mathbf{E}_{x \in Z} \left(\sum_{\xi \in Z} \widehat{f}(\xi) e_{\xi}(x) \right) \overline{g(x)} \\ &= \sum_{\xi \in Z} \widehat{f}(\xi) \left(\mathbf{E}_{x \in Z} g(x) \overline{e_{\xi}(x)} \right) \\ &= \sum_{\xi \in Z} \widehat{f}(\xi) \widehat{g}(\xi), \end{aligned}$$

waarmee (1.4) bewezen is. □

Stelling 1.17 (Parseval). *Laat $f \in \mathbb{C}^Z$. Dan geldt*

$$\mathbf{E}_Z(|f|^2) = \sum_{\xi \in Z} |\widehat{f}(\xi)|^2. \quad (1.5)$$

Bewijs. Merk op dat

$$\mathbf{E}_Z(|f|^2) = \mathbf{E}_Z f(x) \overline{f(x)} = \langle f, f \rangle_{\mathbb{C}^Z},$$

zodat (1.5) direct volgt uit (1.4) met $f = g$. □

Opmerking. De Fourier-coëfficiënt van f bij de frequentie $\xi = 0$ vervult een speciale rol:

$$\widehat{f}(0) = \langle f, 1 \rangle_{\mathbb{C}^Z} = \mathbf{E}_Z(f).$$

Voor ondergroepen van Z ziet de Fourier-getransformeerde er zeer regelmatig uit: zij is gelijk aan een genormeerde indicatorfunctie van het orthogonale complement van de ondergroep. Eerst definiëren we dit orthogonale complement.

Definitie 1.18. Voor een deelverzameling $S \subseteq Z$ definiëren we het **orthogonale complement** S^{\perp} als volgt:

$$S^{\perp} := \{\xi \in Z : \xi \cdot x = 0 \quad \forall x \in S\}.$$

Opmerking. Voor iedere deelverzameling S is S^{\perp} een ondergroep. Er geldt immers $0 \in S^{\perp}$. Uit de lineariteit van \cdot volgt dat als $\xi, \eta \in S$, dan ook $(\xi + \eta) \cdot x = \xi \cdot x + \eta \cdot x = 0 + 0 = 0$, dus $\xi + \eta \in S$ en zo ook $-\xi \in S$.

Lemma 1.19. *Laat G een ondergroep van Z zijn. Dan geldt:*

$$\widehat{1}_G = \mathbf{P}_Z(G)1_{G^\perp}. \quad (1.6)$$

Bewijs. Laat $\xi \in Z$ willekeurig.

Als $\xi \in G^\perp$ dan geldt $\xi \cdot x = 0$ dus ook $e(\xi \cdot x) = 1$ voor alle $x \in G$. We kunnen dus berekenen:

$$\widehat{1}_G(\xi) = \mathbf{E}_{x \in Z} 1_G(x) \overline{e(\xi \cdot x)} = \frac{1}{|Z|} \sum_{x \in G} 1 = \mathbf{P}_Z(G).$$

Als echter $\xi \notin G^\perp$, dan weten we dat er een $h \in G$ bestaat zo dat $\xi \cdot h \neq 0$, dus ook $e(\xi \cdot h) \neq 1$. We gebruiken nu eenzelfde argument als in het bewijs van Lemma 1.9, omdat we uit het feit dat G een ondergroep is en $h \in G$ weten dat we als we sommeren over $x \in G$, ook mogen sommeren over $x + h \in G$:

$$\widehat{1}_G(\xi) = \frac{1}{|Z|} \sum_{x \in G} \overline{e(\xi \cdot x)} = \frac{1}{|Z|} \sum_{x \in G} \overline{e(\xi \cdot (x + h))} = \overline{e(\xi \cdot h)} \frac{1}{|Z|} \sum_{x \in G} \overline{e(\xi \cdot x)} = \overline{e(\xi \cdot h)} \widehat{1}_G(\xi),$$

waaruit we concluderen dat $\widehat{1}_G(\xi) = 0$, waarmee het lemma bewezen is. \square

Uit dit lemma volgt onmiddellijk een eenvoudige groepen-theoretische stelling over de relatie tussen ondergroepen en hun orthogonale complement:

Gevolg 1.20. *Laat $G \subseteq Z$ een ondergroep zijn. Dan geldt*

$$|G||G^\perp| = |Z|.$$

Bewijs. We passen (1.5) toe op 1_G en met behulp van Lemma 1.19 vinden we:

$$\begin{aligned} \mathbf{P}_Z(G) &= \mathbf{E}_Z(|1_G|^2) = \sum_{\xi \in Z} |\widehat{1}_G(\xi)|^2 \\ &= \sum_{\xi \in Z} |\mathbf{P}_Z(G)1_{G^\perp}(\xi)|^2 \\ &= \mathbf{P}_Z(G)^2 |G^\perp|, \end{aligned}$$

waaruit het gestelde volgt met de definitie van $\mathbf{P}_Z(G)$. \square

1.2 Convolutie

Een belangrijke fundamentele operatie op functies in \mathbb{C}^Z is de convolutie. Met behulp van deze operatie zal het mogelijk blijken de technieken van de eindige Fourier-analyse te verbinden aan het zuiver combinatorische concept ‘optellen van verzamelingen’.

Definitie 1.21. Laat $f, g \in \mathbb{C}^Z$. De **convolutie** $f * g$ van f en g is de functie $Z \rightarrow \mathbb{C}$ gedefinieerd door

$$(f * g)(x) = \mathbf{E}_{y \in Z} f(x - y)g(y) = \mathbf{E}_{y \in Z} f(y)g(x - y).$$

Definitie 1.22. Laat $A, B \subseteq Z$ deelverzamelingen. We definiëren de **somverzameling** van A en B als

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

Op dezelfde manier definiëren we de **verschilverzameling**

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

We noteren voor $b \in B$ ook $A \pm b$ als we eigenlijk $A \pm \{b\}$ bedoelen en noemen een verzameling van de vorm $A \pm b$ een **getransleerde** van A .

Om het verband tussen somverzamelingen en convolutie in te zien hebben we nog het begrip drager nodig:

Definitie 1.23. Voor een functie $f \in \mathbb{C}^Z$ definiëren we de **drager** (support) van f als de verzameling

$$\text{supp}(f) := \{x \in Z : f(x) \neq 0\}.$$

Het belang van het begrip convolutie voor somverzamelingen ligt besloten in identiteiten uit het volgende lemma.

Lemma 1.24. *Laat $A, B \subseteq Z$ deelverzamelingen zijn. Dan geldt*

$$(1_A * 1_B)(x) = \mathbf{P}_Z(A \cap (x - B)), \tag{1.7}$$

en in het bijzonder

$$\text{supp}(1_A * 1_B) = A + B. \tag{1.8}$$

Bewijs. Merk eerst op dat $x - y \in B \Leftrightarrow y \in x - B$.

We zien nu uit de definitie van convolutie en dichtheid dat voor alle $x \in Z$ geldt

$$\begin{aligned} (1_A * 1_B)(x) &= \mathbf{E}_{y \in Z} 1_A(y)1_B(x - y) \\ &= \mathbf{E}_{y \in Z} 1_A(y)1_{x - B}(y) \\ &= \mathbf{E}_{y \in Z} 1_{A \cap (x - B)}(y) = \mathbf{P}_Z(A \cap (x - B)). \end{aligned}$$

Om (1.8) in te zien merken we eerst op dat

$$x \in A + B \Leftrightarrow \exists b \in B : x - b \in A \Leftrightarrow A \cap (x - B) \neq \emptyset,$$

dus $\mathbf{P}_Z(A \cap (x - B)) \neq 0 \Leftrightarrow x \in A + B$. Vanwege (1.7) en de definitie van drager geldt nu dus (1.8). \square

Om de Fourier-technieken uit de vorige sectie hiervoor te kunnen gebruiken, bewijzen we ten slotte dat de Fourier-getransformeerde zich netjes gedraagt voor convoluties van functies.

Propositie 1.25. *Laat $f, g \in \mathbb{C}^Z$. Dan geldt*

$$\widehat{f * g} = \widehat{f} \widehat{g}. \quad (1.9)$$

Bewijs. Het bewijs bestaat uit het invullen van de definities van convolutie en de Fourier-getransformeerde en een variabelen-transformatie $z := x + y$:

$$\begin{aligned} \widehat{f}(\xi)\widehat{g}(\xi) &= \mathbf{E}_{x \in Z} f(x) \overline{e(\xi \cdot x)} \mathbf{E}_{y \in Z} g(y) \overline{e(\xi \cdot y)} \\ &= \mathbf{E}_{x \in Z} \mathbf{E}_{y \in Z} f(x) g(y) \overline{e(\xi \cdot (x + y))} \\ &= \mathbf{E}_{z \in Z} \mathbf{E}_{x \in Z} f(x) g(z - x) \overline{e(\xi \cdot z)} \\ &= \mathbf{E}_{z \in Z} (f * g)(z) \overline{e(\xi \cdot z)} \\ &= \widehat{f * g}(\xi). \end{aligned}$$

□

1.3 Lineaire afwijking

Met behulp van de Fourier-analyse op eindige groepen zoals in dit hoofdstuk behandeld is, kunnen we nu een nieuwe semi-norm op \mathbb{C}^Z leggen: de lineaire afwijking.

Grof gezegd geeft de lineaire afwijking van een functie aan hoe ‘willekeurig’ of ‘uniform’ een functie is: een lage lineaire afwijking impliceert een hoge mate van willekeur. Functies met een lage lineaire afwijking hebben geen opvallend hoge Fourier-coëfficiënten op bepaalde frequenties, maar bezitten een zekere mate van uniformiteit.

De lineaire afwijking van *indicatorfuncties* is voor ons in het bijzonder interessant, omdat we hiermee ook aan de deelverzamelingen van de groep Z een getal kunnen verbinden dat de ‘uniformiteit’ van de verzameling voorstelt, zodat we uiteindelijk weer terug zullen kunnen keren naar onze oorspronkelijke combinatorische vragen.

We geven eerst de definitie en illustreren daarna het begrip lineaire afwijking aan de hand van een aantal elementaire eigenschappen en voorbeelden.

Definitie 1.26. Voor $f \in \mathbb{C}^Z$ definiëren we de **lineaire afwijking** (Eng: linear bias) van f door

$$\|f\|_u := \sup_{\xi \in Z \setminus \{0\}} |\widehat{f}(\xi)|.$$

Als $A \subseteq Z$ een deelverzameling is noteren we de **lineaire afwijking van A** met $\|A\|_u$, deze is gedefinieerd als de lineaire afwijking van de bijbehorende indicatorfunctie 1_A :

$$\|A\|_u := \|1_A\|_u = \sup_{\xi \in Z \setminus \{0\}} |\widehat{1_A}(\xi)|.$$

Voor $\alpha \geq 0$ heet een verzameling A α -**uniform** als $\|A\|_u \leq \alpha$.

Propositie 1.27. $\|\cdot\|_u$ is een semi-norm op \mathbb{C}^Z .

Bewijs. We gebruiken dat Fourier-transformatie een lineaire afbeelding is (Lemma 1.13).

Voor iedere $f, g \in \mathbb{C}^Z$, $\xi \in Z \setminus \{0\}$ geldt nu:

$$|\widehat{f+g}(\xi)| = |\widehat{f}(\xi) + \widehat{g}(\xi)| \leq |\widehat{f}(\xi)| + |\widehat{g}(\xi)| \leq \|f\|_u + \|g\|_u,$$

dus het supremum aan de linkerkant nemen geeft dat

$$\|f+g\|_u \leq \|f\|_u + \|g\|_u, \tag{1.10}$$

de driehoeksongelijkheid voor $\|\cdot\|_u$ geldt.

Uit het feit dat $\widehat{cf}(\xi) = c\widehat{f}(\xi)$ volgt ook direct dat

$$\|cf\|_u = |c|\|f\|_u,$$

waarmee de eisen voor een semi-norm bewezen zijn. \square

Allereerst vragen we ons af wanneer de semi-norm op \mathbb{C}^Z de waarde nul aanneemt: welke functies hebben helemaal geen lineaire afwijking? De volgende propositie geeft hierover uitsluitel.

Propositie 1.28. Een functie $f \in \mathbb{C}^Z$ heeft lineaire afwijking 0 dan en slechts dan als $f \equiv C$ voor zekere $C \in \mathbb{C}$.

Bewijs. Laat $f \in \mathbb{C}^Z$.

Als $f \equiv C$ voor zekere $C \in \mathbb{C}$, dan geldt wegens Lemma 1.9 toegepast op $\xi = 0$ voor iedere $\xi' \in Z \setminus \{0\}$:

$$\widehat{f}(\xi') = \mathbf{E}_{x \in Z} \overline{C e_{\xi'}(x)} = C \mathbf{E}_{x \in Z} \overline{e_{\xi'}(x)} = 0.$$

Voor de andere richting, stel dat $\|f\|_u = 0$. Dan geldt dus $\widehat{f}(\xi) = 0$ voor alle $\xi \in Z \setminus \{0\}$. Dus door (1.3) toe te passen op de functie f vinden we voor iedere $x \in Z$:

$$f(x) = \sum_{\xi \in Z} \widehat{f}(\xi) e_{\xi}(x) = \widehat{f}(0) e_0(x) = \widehat{f}(0),$$

dus f is een constante functie. \square

Gevolg 1.29. In iedere groep Z zijn \emptyset en Z de 0-uniforme verzamelingen.

Bewijs. Merk op dat $1_Z \equiv 1$ en $1_\emptyset \equiv 0$. Vanwege Propositie 1.28 zijn Z en \emptyset dus 0-uniforme verzamelingen.

Andere deelverzamelingen in Z hebben altijd een niet-constante indicatorfunctie en dus kan de lineaire afwijking van deze verzamelingen wegens Propositie 1.28 niet gelijk aan nul zijn. \square

Opmerking. Uit Propositie 1.28 zien we dat de semi-norm $\|\cdot\|_u$ een norm wordt door \mathbb{C}^Z uit te delen naar de constante functies.

Uit de driehoeksongelijkheid voor de lineaire afwijking van functies volgt ook een driehoeksongelijkheid voor de lineaire afwijking van disjuncte deelverzamelingen van Z .

Propositie 1.30. *Als A, B disjuncte deelverzamelingen van Z zijn geldt*

$$\|A \cup B\|_u \leq \|A\|_u + \|B\|_u.$$

Bewijs. Omdat $A \cap B = \emptyset$ geldt $1_{A \cup B} = 1_A + 1_B$. Uit de definitie $\|A\|_u := \|1_A\|_u$ en de driehoeksongelijkheid (1.10) volgt het gestelde nu. \square

Verder is de lineaire afwijking van deelverzamelingen invariant onder translatie, complement en spiegeling om 0, zoals blijkt uit de volgende propositie.

Propositie 1.31. *Laat $A \subseteq Z$ en $h \in Z$. Dan geldt:*

$$\|A\|_u = \|A + h\|_u = \|Z \setminus A\|_u = \|-A\|_u.$$

Bewijs. Laat $\xi \in Z \setminus \{0\}$ zo dat $\|A\|_u = \widehat{1}_A(\xi)$.

We kunnen door over te gaan op een andere sommatievariabele $y := x - h$ zelfs aantonen dat $|\widehat{1}_A(\xi)| = |\widehat{1}_{A+h}(\xi)|$ voor alle $\xi \in Z$:

$$\begin{aligned} |\widehat{1}_{A+h}(\xi)| &= \left| \mathbf{E}_{x \in Z} 1_{A+h}(x) \overline{e(\xi \cdot x)} \right| \\ &= \left| \mathbf{E}_{x \in Z} 1_{A+h}(x-h) \overline{e(\xi \cdot (x-h))} \right| \\ &= \left| e(\xi \cdot h) \mathbf{E}_{x \in Z} 1_A(x) \overline{e(\xi \cdot x)} \right| \\ &= |\widehat{1}_A(\xi)|, \end{aligned}$$

dus nu volgt in het bijzonder dat $\|A\|_u = \|A + h\|_u$.

Omdat A en $Z \setminus A$ disjuncte deelverzamelingen van Z zijn die samen Z vormen geldt $1_A + 1_{Z \setminus A} = 1$. Omdat wegens Propositie 1.28 geldt $\widehat{1}(\xi) = 0$ als $\xi \neq 0$, volgt nu uit Lemma 1.13:

$$\widehat{1}_{Z \setminus A}(\xi) = \widehat{1}(\xi) - \widehat{1}_A(\xi) = -\widehat{1}_A(\xi),$$

zodat voor alle $\xi \in Z \setminus \{0\}$ geldt $|\widehat{1}_{Z \setminus A}(\xi)| = |\widehat{1}_A(\xi)|$, en dus weer in het bijzonder $\|A\|_u = \|Z \setminus A\|_u$.

Ten slotte volgt uit de eigenschap die voor alle complexe getallen $c \in \mathbb{C}$ geldt dat $|c| = |\bar{c}|$ en het overgaan op sommatievariabele $y := -x$ dat

$$\begin{aligned} |\widehat{1_{-A}}(\xi)| &= \left| \mathbf{E}_{x \in Z} 1_{A(-x)} \overline{e(\xi \cdot x)} \right| \\ &= \left| \mathbf{E}_{x \in Z} 1_A(x) \overline{e(\xi \cdot (-x))} \right| \\ &= \left| \overline{\mathbf{E}_{x \in Z} 1_A(x) e(\xi \cdot x)} \right| \\ &= |\widehat{1_A}(\xi)|, \end{aligned}$$

waaruit in het bijzonder $\|A\|_u = \|-A\|_u$ volgt. \square

Een verdere eigenschap van $\|A\|_u$ is dat deze hoogstens gelijk is aan $\mathbf{P}_Z(A)$, de dichtheid van A . Deze grens kan bereikt worden mits er een echte ondergroep G van Z is met A bevat in een getransleerde van G , zoals blijkt uit de volgende propositie.

Propositie 1.32. *Voor alle $A \subseteq Z$ geldt $\|A\|_u \leq \mathbf{P}_Z(A)$, met gelijkheid dan en slechts dan als $A \subseteq G + z$ voor zekere ondergroep $G \lesssim Z$ en $z \in Z$.*

Bewijs. De ongelijkheid volgt direct uit de definitie; laat immers $\xi \in Z \setminus \{0\}$ willekeurig, dan geldt:

$$|\widehat{1_A}(\xi)| = \frac{1}{|Z|} \left| \sum_{x \in Z} 1_A(x) \overline{e(\xi \cdot x)} \right| \leq \frac{1}{|Z|} \sum_{x \in Z} 1_A(x) |e(\xi \cdot x)| = \frac{|A|}{|Z|} = \mathbf{P}_Z(A),$$

dus ook $\|A\|_u = \sup_{\xi \in Z \setminus \{0\}} |\widehat{1_A}(\xi)| \leq \mathbf{P}_Z(A)$.

Laat nu, voor het bewijs van het tweede deel van de bewering, eerst $A \subseteq G + z$ voor zekere ondergroep $G \lesssim Z$ en $z \in Z$.

Neem $y \in A$ vast, dan is duidelijk $B := A + (-y)$ een deelverzameling van de ondergroep G .

Wegens Gevolg 1.20 geldt $|G^\perp| = \frac{|Z|}{|G|} > 1$ omdat $Z \neq G$, dus in het bijzonder geldt $G^\perp \setminus \{0\} \neq \emptyset$.

Laat dus $\xi \in G^\perp \setminus \{0\}$. In het bijzonder geldt voor iedere $x \in B \subseteq G$ dat $\xi \cdot x = 0$. We kunnen nu eerst $\widehat{1_B}$ als volgt berekenen:

$$|\widehat{1_B}(\xi)| = |\mathbf{E}_{x \in Z} 1_B(x) \overline{e(\xi \cdot x)}| = \mathbf{P}_Z(B),$$

dus we zien dat $\|B\|_u = \mathbf{P}_Z(B)$. Aangezien $\|A + (-y)\|_u = \|A\|_u$ wegens Propositie 1.31 en $|A + (-y)| = |A|$ geldt dus ook $\|A\|_u = \mathbf{P}_Z(A)$.

Voor de andere richting nemen we aan dat $A \subseteq Z$ met $\|A\|_u = \mathbf{P}_Z(A)$.

Als $A = \emptyset$ is het gestelde triviaal waar wanneer we voor de ondergroep $G := \{0\}$ en $z := 0$ nemen.

Als $A \neq \emptyset$, laat dan $z \in A$ en bekijk de verzameling $B := A + (-z)$. We zien dat $0 \in B$ en uit Propositie 1.31 dat $\|B\|_u = \|A\|_u$, terwijl uit de definitie van B volgt dat $\mathbf{P}_Z(B) = \mathbf{P}_Z(A)$.

Er bestaat omdat $\|B\|_u = \mathbf{P}_Z(B)$ een $\xi_0 \in Z \setminus \{0\}$ zo dat $|\widehat{1_B}(\xi_0)| = \mathbf{P}_Z(B)$.

Hieruit volgt door aan beide kanten met $|Z|$ te vermenigvuldigen en de definitie van $\widehat{1_B}$ in te vullen dat

$$\left| \sum_{x \in B} e(\xi_0 \cdot x) \right| = |B|.$$

Aan de linkerkant staat nu een som van $|B|$ complexe getallen die in absolute waarde allemaal gelijk aan 1 zijn. Omdat $0 \in B$ één van de termen is moet elk getal zelfs precies gelijk aan 1.

Stel namelijk dat er een $x_0 \in B$ zou bestaan waarvoor $e(\xi_0 \cdot x_0) \neq 1$, zodat ook geldt $|1 + e(\xi_0 \cdot x_0)| < 2$, dan zou gelden

$$|B| = \left| \sum_{x \in B} e(\xi_0 \cdot x) \right| \leq |1 + e(\xi_0 \cdot x_0)| + (|B| - 2) < 2 + (|B| - 2) = |B|,$$

een tegenspraak. Dus $e(\xi_0 \cdot x) = 1$ voor alle $x \in B$.

We definiëren nu $H := \langle \xi_0 \rangle$, de ondergroep voortgebracht door ξ_0 .

We kunnen een element uit H schrijven als $n\xi_0$ voor $n \in \mathbb{Z}$, waar de notatie $n\xi_0$ betekent: $\xi_0 + \dots + \xi_0$ (n keer) als $n \geq 0$ en $n\xi_0 := -n(-\xi_0)$ als $n < 0$.

Laat nu $G := H^\perp$. Het orthoplement van een verzameling is altijd een ondergroep van Z . Omdat $|H| > 1$ (want $\xi_0 \neq 0$) volgt uit Gevolg 1.20 dat $|G| < |Z|$, dus G is een echte ondergroep van Z .

Als nu $x \in B$ dan geldt $\xi \cdot x = 0$ voor alle $\xi \in H$ vanwege de lineariteit van \cdot en het feit dat $\xi_0 \cdot x = 0$ in combinatie met het feit dat iedere $\xi \in H$ een eindig aantal keer $\pm\xi_0$ is.

Dus we zien dat $A + (-z) = B \subseteq H^\perp = G$, dus $A \subseteq G + z$, zoals bewezen moest worden. \square

Voorbeeld 1.33. Laat $N > 1$ even zijn. In $Z = \mathbb{Z}_N$ hebben zowel de verzameling van (klassen van) even getallen E als de verzameling van (klassen van) oneven getallen $Z \setminus E$ lineaire afwijking $\mathbf{P}_Z(E)$, omdat E een ondergroep is.

Meer in het algemeen: als $(N, n) \neq 1$ dan is de verzameling $G := n\mathbb{Z}_N$ een echte ondergroep van \mathbb{Z}_N en hebben deelverzameling A van G en van de nevenklassen van G dus lineaire afwijking $\mathbf{P}_Z(A)$.

We hebben nu gezien hoe groot de lineaire afwijking van een verzameling kan worden. Aan de andere kant zijn verzamelingen van kleine lineaire afwijking te maken door willekeurige deelverzamelingen te nemen. We noemen voor de volledigheid het Lemma dat deze bewering ondersteunt, maar geven hiervan geen bewijs.

Hiertoe definiëren we eerst wat we verstaan onder een willekeurige deelverzameling.

Definitie 1.34. Laat A een eindige verzameling van cardinaliteit N .

Noteer $A := \{a_1, \dots, a_N\}$.

Voor $\tau \in [0, 1]$ definiëren we nu eerst N onafhankelijke stochasten X_1, \dots, X_N met voor elke i de volgende kansverdeling:

$$P(X_i = k) := \begin{cases} \tau & \text{als } k = 1; \\ 1 - \tau & \text{als } k = 0; \\ 0 & \text{anders.} \end{cases}$$

We definiëren nu de stochast \mathbf{B} als volgt:

$$\mathbf{B} := \{a_i : X_i = 1\}$$

\mathbf{B} heet de τ -willekeurige deelverzameling van A .

Het volgende lemma geeft het verband tussen de lineaire afwijking en de ‘willekeur’ van een verzameling: als een τ -willekeurige verzameling B wordt gekozen in een deelverzameling A in de omhullende groep Z , dan is de kans zeer klein dat de lineaire afwijking van B ‘groot’ is. De kans dat de lineaire afwijking van B , vergeleken met de lineaire afwijking van A , groter is dan een ondergrens ϵ neemt exponentieel af met ϵ .

Lemma 1.35. *Laat $A \subseteq Z$, $\tau \in [0, 1]$, $\sigma^2 := \frac{|A|\tau(1-\tau)}{|Z|^2}$ en \mathbf{B} de τ -willekeurige deelverzameling van A .*

Voor elke $\lambda > 0$ geldt

$$\mathbf{P}(\|\mathbf{B}\|_u - \tau\|A\|_u \geq \lambda\sigma) \leq 4|Z| \max(e^{-\lambda^2/8}, e^{-\lambda\sigma/2\sqrt{2}}).$$

Opmerking. De formulering van dit Lemma is de formulering zoals in [8] en is mogelijk gebaseerd op Lemma 14 in [2]. We noemen het hier slechts om ook het probabilistische aspect van de Additieve Combinatoriek, waar verder in deze scriptie niet op ingegaan wordt, toch even aan te stippen. Tao en Vu wijden aan dit aspect in [8] het gehele eerste hoofdstuk.

1.4 Uniforme verzamelingen optellen

In de laatste sectie van dit hoofdstuk bespreken we een eenvoudige toepassing van de in dit hoofdstuk beschreven technieken van eindige Fourier-analyse en het begrip lineaire afwijking.

De volgende stelling geeft een verband tussen de lineaire afwijking van deelverzamelingen A_1, \dots, A_n van Z en het aantal mogelijke schrijfwijzen van x als som van elementen $a_i \in A_i$. Hieruit verkrijgen we dan in het bijzonder een voldoende voorwaarde voor de lineaire afwijking van die verzamelingen om te kunnen concluderen dat $A_1 + \dots + A_n = Z$.

De lineaire afwijking blijkt niet te groot te mogen zijn: als de verzamelingen A_i uniform genoeg zijn, verkrijgen we na optelling de hele groep Z .

Stelling 1.36. *Laat $n \geq 3$ en laat A_1, \dots, A_n deelverzamelingen van een abelse groep Z .*

Voor $x \in Z$ noteren we met A_x het aantal manieren om x te schrijven als som van elementen $a_i \in A_i$, dus

$$A_x := |\{(a_1, \dots, a_n) \in A_1 \times \dots \times A_n : x = a_1 + \dots + a_n\}|.$$

Dan geldt voor iedere $x \in Z$:

$$A_x \geq \frac{|A_1| \cdots |A_n|}{|Z|} - |Z|^{n-2} \|A_1\|_u \cdots \|A_{n-2}\|_u \sqrt{|A_{n-1}| |A_n|}.$$

Opmerking. We kunnen de verzamelingen, die we in de rechterzijde van deze ongelijkheid (en in het vervolg) de rol van A_{n-1} en A_n laten spelen, vrij kiezen.

Gevolg 1.37. Laat $n \geq 3$ en laat A_1, \dots, A_n deelverzamelingen van een abelse groep Z en neem verder aan dat

$$\frac{\|A_1\|_u}{\mathbf{P}_Z(A_1)} \cdots \frac{\|A_{n-2}\|_u}{\mathbf{P}_Z(A_{n-2})} < \sqrt{\mathbf{P}_Z(A_{n-1}) \mathbf{P}_Z(A_n)}.$$

Dan geldt $A_1 + \dots + A_n = Z$.

Bewijs (Gevolg). Zij $x \in Z$. Met Stelling 1.36 vinden we:

$$A_x \geq \frac{|A_1| \cdots |A_n|}{|Z|} - |Z|^{n-2} \|A_1\|_u \cdots \|A_{n-2}\|_u \sqrt{|A_{n-1}| |A_n|} > \frac{|A_1| \cdots |A_n|}{|Z|} - \frac{|A_1| \cdots |A_n|}{|Z|}$$

vanwege de aanname over de lineaire afwijkingen van de A_i .

Dus $A_x > 0$, dus de verzameling $\{(a_1, \dots, a_n) \in A_1 \times \dots \times A_n : x = a_1 + \dots + a_n\}$ is niet leeg, dus $x \in A_1 + \dots + A_n$. \square

Bewijs (Stelling). We gebruiken de eigenschappen van de convolutie zoals in Sectie 1.2 ontwikkeld. Laat $f := 1_{A_1} * \dots * 1_{A_n}$.

$f(x)$ blijkt nu op een factor $|Z|^{1-n}$ na gelijk te zijn aan de kwantiteit A_x waar we in geïnteresseerd zijn. Om dit te bewijzen passen we inductie toe op Lemma 1.24. We leiden uit (1.7) af dat

$$(1_{A_1} * 1_{A_2})(x) = \mathbf{P}_Z(A_1 \cap (x - A_2)) = |Z|^{1-2} |\{(a_1, a_2) \in A_1 \times A_2 : x = a_1 + a_2\}|.$$

Stel nu dat we voor zekere $m \in (2, n]$ weten

$$(1_{A_1} * \dots * 1_{A_{m-1}})(x) = |Z|^{1-(m-1)} |\{(a_1, \dots, a_{m-1}) \in A_1 \times \dots \times A_{m-1} : x = a_1 + \dots + a_{m-1}\}|.$$

Uit de definitie van convolutie volgt nu

$$\begin{aligned} (1_{A_1} * \dots * 1_{A_m})(x) &= |Z|^{-1} \sum_{y \in Z} (1_{A_1} * \dots * 1_{A_{m-1}})(y) 1_{A_m}(x - y) \\ &= |Z|^{1-m} \sum_{y \in Z} |\{(a_1, \dots, a_{m-1}) \in A_1 \times \dots \times A_{m-1} : y = a_1 + \dots + a_{m-1}\}| 1_{A_m}(x - y) \\ &= |Z|^{1-m} |\{(a_1, \dots, a_m) \in A_1 \times \dots \times A_m : x = a_1 + \dots + a_m\}|. \end{aligned}$$

Dus er geldt

$$f(x) = |Z|^{1-n} A_x. \quad (1.11)$$

Uit (1.9) vinden we verder dat geldt:

$$\widehat{f} = \widehat{1_{A_1}} \cdots \widehat{1_{A_n}}.$$

Met behulp van het feit dat f reëel is en de Fourier-inversie formule (1.3) zien we

$$f(x) = \operatorname{Re} f(x) = \operatorname{Re} \sum_{\xi \in Z} \widehat{1_{A_1}}(\xi) \cdots \widehat{1_{A_n}}(\xi) e(x \cdot \xi). \quad (1.12)$$

Merk op dat uit de ongelijkheden $|\operatorname{Re} z| \leq |z|$ (Pythagoras) en de driehoeksongelijkheid volgt:

$$\begin{aligned} \operatorname{Re} \sum_{\xi \in Z \setminus \{0\}} \widehat{1_{A_1}}(\xi) \cdots \widehat{1_{A_n}}(\xi) e(x \cdot \xi) &\geq - \left| \sum_{\xi \in Z \setminus \{0\}} \widehat{1_{A_1}}(\xi) \cdots \widehat{1_{A_n}}(\xi) e(x \cdot \xi) \right| \\ &\geq - \sum_{\xi \in Z \setminus \{0\}} |\widehat{1_{A_1}}(\xi)| \cdots |\widehat{1_{A_n}}(\xi)| \end{aligned}$$

Als we nu de frequentie 0 isoleren en deze afchatting gebruiken in (1.12) vinden we

$$f(x) \geq \widehat{1_{A_1}}(0) \cdots \widehat{1_{A_n}}(0) - \sum_{\xi \in Z \setminus \{0\}} |\widehat{1_{A_1}}(\xi)| \cdots |\widehat{1_{A_n}}(\xi)|.$$

Voor de eerste term aan de rechterzijde gebruiken we dat $\widehat{1_A}(0) = \mathbf{E}_Z(1_A) = \mathbf{P}_Z(A)$ voor elke verzameling A en voor de tweede term gebruiken we de definitie van lineaire afwijking om tot een afchatting voor de eerste $n-2$ Fourier-coëfficiënten te komen, zodat we krijgen:

$$f(x) \geq \mathbf{P}_Z(A_1) \cdots \mathbf{P}_Z(A_n) - \|A_1\|_u \cdots \|A_{n-2}\|_u \sum_{\xi \in Z} |\widehat{1_{A_{n-1}}}(\xi)| |\widehat{1_{A_n}}(\xi)|.$$

Merk op dat vanwege de ongelijkheid van Cauchy-Schwartz en de Parseval-identiteit (1.5) geldt

$$\begin{aligned} \sum_{\xi \in Z} |\widehat{1_{A_{n-1}}}(\xi)| |\widehat{1_{A_n}}(\xi)| &\leq \sum_{\xi \in Z} |\widehat{1_{A_{n-1}}}(\xi)|^2 \sum_{\xi \in Z} |\widehat{1_{A_n}}(\xi)|^2 \\ &= \mathbf{E}_Z(|1_{A_{n-1}}|^2) \mathbf{E}_Z(|1_{A_n}|^2) = \mathbf{P}_Z(A_{n-1}) \mathbf{P}_Z(A_n). \end{aligned}$$

We concluderen dus

$$f(x) \geq \mathbf{P}_Z(A_1) \cdots \mathbf{P}_Z(A_n) - \|A_1\|_u \cdots \|A_{n-2}\|_u \mathbf{P}_Z(A_{n-1}) \mathbf{P}_Z(A_n),$$

en door hierin (1.11) in te vullen en aan beide zijden te vermenigvuldigen met $|Z|^{n-1}$ vinden we

$$A_x \geq |Z|^{n-1} (\mathbf{P}_Z(A_1) \cdots \mathbf{P}_Z(A_n) - \|A_1\|_u \cdots \|A_{n-2}\|_u \mathbf{P}_Z(A_{n-1}) \mathbf{P}_Z(A_n)),$$

waaruit na invullen van de definitie van \mathbf{P}_Z het gestelde volgt.

□

Hoofdstuk 2

De stelling van Szemerédi

Een voorbeeld waarop de technieken van eindige Fourier-analyse kunnen worden toegepast is de stelling van Szemerédi over rekenkundige rijtjes van willekeurige lengte in een gegeven deelverzameling $A \subset \mathbb{N} := \{1, 2, 3, \dots\}$.

De stelling van Szemerédi geeft een voldoende voorwaarde, namelijk dat A een ‘positieve bovendichtheid’ heeft, op grond waarvan men mag concluderen dat in de verzameling rekenkundige rijtjes van willekeurige lengte voorkomen.

De voorwaarde van positieve bovendichtheid blijkt overigens niet noodzakelijk te zijn. Hoewel de priemgetallen bovendichtheid gelijk aan nul hebben (een resultaat dat al sinds Euler bekend is), bewezen Ben Green en Terence Tao in 2004 dat de priemgetallen rekenkundige rijtjes van willekeurige lengte bevatten [3].

Voor de stelling van Szemerédi bestaan meerdere, equivalente, formuleringen. In dit hoofdstuk geven we er twee, van één formulering is intuïtief direct duidelijk wat zij betekent, van de ander is dit misschien minder duidelijk, maar deze formulering blijkt wel vaak handiger om mee te werken.

Eerst moeten we weten wat ‘bovendichtheid’ betekent: intuïtief is $\bar{\sigma}(A)$ een maat voor de ‘kans’ dat een willekeurig natuurlijk getal in de verzameling A zit. Ook maken we de term ‘rekenkundig rijtje’ precies en sluiten daarmee direct ook een trivialiteit uit.

Definitie 2.1. Laat $A \subset \mathbb{N}$ een verzameling natuurlijke getallen zijn. Dan is de **bovendichtheid** van A gedefinieerd als

$$\bar{\sigma}(A) := \limsup_{n \rightarrow \infty} \frac{|A \cap [0, n]|}{n}.$$

Definitie 2.2. Een **rekenkundig rijtje** van lengte k is een deelverzameling $P \subseteq \mathbb{Z}$ zo dat $|P| = k$ en er vaste $a \in \mathbb{Z}, b \in \mathbb{Z} \setminus \{0\}$ bestaan zo dat iedere $p \in P$ geschreven kan worden als $p = a + bj$ voor zekere $j \in \{1, \dots, k\}$.

We noteren in dit geval ook wel $P = a + b \cdot [1, k]$.

Stelling 2.3 (Szemerédi). *Laat A een deelverzameling van de positieve gehele getallen zijn met positieve bovendichtheid, $\bar{\sigma}(A) > 0$.*

Dan bevat A voor iedere $k > 0$ een rekenkundig rijtje van lengte k .

2.1 Formulering met behulp van r_k

Er bestaat een equivalente, kwantitatieve formulering voor Stelling 2.3, die vaak handiger blijkt om mee te werken. Hiervoor definiëren we eerst een constante die meet hoe groot een verzameling *zonder* rekenkundige rijtjes van lengte k kan worden.

Definitie 2.4 (Erdős-Turán constante). Laat P een eindige deelverzameling van een additieve groep zijn en laat $k \geq 1$.

We noemen een verzameling $A \subset P$ een \mathcal{A}_k -**verzameling** in P als A geen rekenkundige rijtjes van lengte k bevat.

We noteren met $r_k(P) := \max\{|A| : A \subset P \text{ een } \mathcal{A}_k\text{-verzameling}\}$.

We bekijken nu eerst twee eenvoudige eigenschappen van de functie r_k .

Lemma 2.5 (Herschalinglemma). *Laat $k \geq 1$, $N \in \mathbb{N}$ en P een rekenkundig rijtje in \mathbb{Z} van lengte N zijn. Dan geldt*

$$r_k([1, N]) = r_k(P).$$

Met andere woorden, de maximale grootte van een \mathcal{A}_k -deelverzameling van P hangt alleen af van $|P|$.

Bewijs. Schrijf $P = a \cdot [1, N] + b$ voor $a \in \mathbb{N}$ en $b \in \mathbb{Z}$.

Laat $A \subset [1, N]$ een \mathcal{A}_k -verzameling zijn met $|A| = r_k([1, N])$.

De verzameling $A' := a \cdot A + b$ is een deelverzameling van P . Stel dat $(au_1 + b, \dots, au_k + b)$ een rekenkundig rijtje van lengte k is in A' , dan geldt voor iedere $1 < i < k$:

$$u_i - u_{i-1} = \frac{1}{a}((au_i + b) - (au_{i-1} + b)) = \frac{1}{a}((au_{i+1} + b) - (au_i + b)) = u_{i+1} - u_i,$$

dus (u_1, \dots, u_k) is een rekenkundig rijtje van lengte k in A , maar omdat A een \mathcal{A}_k -verzameling is kan dat alleen als het een triviaal rijtje is, dat wil zeggen $u_i = u_1$ voor alle $1 < i \leq k$.

Dus ook $(au_1 + b, \dots, au_k + b)$ is een triviaal rijtje, dus A' is een \mathcal{A}_k -verzameling.

Hiermee is bewezen dat $r_k(P) \leq r_k([1, N])$.

Als we beginnen met een maximale \mathcal{A}_k -verzameling $A' \subset P$ dan vinden we op analoge wijze met hierboven dat de verzameling $A := \frac{1}{a}(A' - b)$ een \mathcal{A}_k -verzameling in $[1, N]$ is, zodat ook geldt $r_k([1, N]) \leq r_k(P)$. Hiermee is het lemma bewezen. \square

Opmerking. We noteren op grond van bovenstaand lemma $r_k(N) := r_k([1, N])$.

Lemma 2.6 (Monotonie). *Laat $k \geq 1$, $m, n \in \mathbb{N}$ met $m \leq n$. Dan geldt*

$$r_k(m) \leq r_k(n).$$

Bewijs. Laat A een \mathcal{A}_k -verzameling in $[1, m]$ van maximale grootte, dus $|A| = r_k(m)$.

Omdat $m \leq n$ is A ook een deelverzameling van $[1, n]$ en aangezien A een \mathcal{A}_k -verzameling is geldt:

$$r_k(m) = |A| \leq r_k(n),$$

wat bewezen moest worden. \square

We zijn nu klaar om met behulp van r_k een tweede, kwantitatieve formulering van de stelling van Szemerédi te geven.

Stelling 2.7 (Szemerédi, tweede formulering). *Laat $k \geq 1$ en $N \geq 1$. Dan geldt*

$$\lim_{N \rightarrow \infty} \frac{r_k(N)}{N} = 0. \quad (2.1)$$

2.2 Equivalentie van formuleringen

De twee formuleringen Stelling 2.3 en Stelling 2.7 zijn, zoals aangekondigd, equivalent:

Propositie 2.8. *Stelling 2.3 \iff Stelling 2.7*

Bewijs. Neem Stelling 2.7 aan. Laat A een deelverzameling van de positieve gehele getallen zijn met $\bar{\sigma}(A) > 0$. Laat verder $k \geq 1$ willekeurig.

We tonen aan dat A een rekenkundig rijtje van lengte k bevat.

Uit (2.1) volgt omdat $\bar{\sigma}(A) > 0$ dat er een N_k bestaat zodat voor alle $N \geq N_k$ geldt:

$$\frac{r_k(N)}{N} < \frac{\bar{\sigma}(A)}{2}.$$

Uit Definitie 2.1 van $\bar{\sigma}(A)$ volgt dat

$$\sup_{N \geq N_k} \frac{|A \cap [0, N]|}{N} \geq \bar{\sigma}(A).$$

Kies nu een $N^* \geq N_k$ zodat $\frac{|A \cap [0, N^*]|}{N^*} \geq \frac{\bar{\sigma}(A)}{2}$, dan geldt

$$\frac{|A \cap [0, N^*]|}{N^*} \geq \frac{\bar{\sigma}(A)}{2} > \frac{r_k(N^*)}{N^*},$$

dus $|A \cap [0, N^*]| > r_k([1, N^*])$, dus $A \cap [0, N^*]$ is een deelverzameling van $[1, N^*]$ met meer elementen dan $r_k(N^*)$, dus bevat $A \cap [0, N^*]$ per definitie een rekenkundig rijtje van lengte k . Dit is tevens een rekenkundig rijtje van lengte k in A , waarvan het bestaan bewezen moest worden.

Neem voor de andere richting Stelling 2.3 aan en laat $k \geq 1$, $N \geq 1$. Stel, om een tegenstelling te krijgen, dat (2.1) niet geldt, dus

$$\limsup_{N \rightarrow \infty} \frac{r_k(N)}{N} > 0. \quad (2.2)$$

Omdat voor $k = 1$ en $k = 2$ uit de definitie van r_k volgt dat $r_1(N) \equiv 0$ en $r_2(N) \equiv 1$, kan (2.2) dan zeker niet gelden. We mogen dus aannemen dat $k \geq 3$.

We construeren nu een verzameling met positieve bovendichtheid die geen willekeurig lange rekenkundige rijtjes kan bevatten.

Vanwege de aanname (2.2) bestaat er een $\epsilon > 0$ zodat $\limsup_{N \rightarrow \infty} \frac{r_k(N)}{N} > 2\epsilon$. Hieruit volgt dat er een rij $\{N_j\}_{j=0}^\infty$ bestaat zodat

$$\frac{r_k([1, N_j])}{N_j} > 2\epsilon \quad (2.3)$$

voor elke j .

Nu bestaat wegens de definitie van r_k voor iedere $j \geq 0$ een deelverzameling $B_j \subseteq [1, N_j]$ zodat B_j geen rekenkundig rijtje van lengte k bevat en $|B_j| > 2\epsilon N_j$.

We definiëren een rij $\{m_j\}_{j=0}^\infty$ door $m_0 := N_0$ en $m_j := N_j + 2m_{j-1}$ en maken nu een nieuwe verzameling A die bestaat uit kopieën van de B_j , maar steeds met een ruimte $2m_j$ tussen B_j en B_{j+1} , om te voorkomen dat er in A nieuwe rekenkundige rijtjes ontstaan.

Definieer nu $A_0 = B_0$ en voor elke $j > 0$ de verzameling $A_j := B_j + 2m_{j-1}$, een translatie van de verzameling B_j . Laat vervolgens de verzameling $A := \bigcup_{j=0}^\infty A_j$.

A bestaat uit achter elkaar geplakte kopieën van de verzamelingen B_j . Tussen elk van deze kopieën zit een tussenruimte van grootte min $A_{j+1} - \max A_j$. Uit de definitie van A_j , B_j en m_j leiden we nu af dat voor elke j geldt:

$$\begin{aligned} \min A_{j+1} &\geq 1 + 2m_j, \\ \max A_j &\leq N_j + 2m_{j-1} = m_j, \\ \min A_{j+1} - \max A_j &\geq 1 - N_j + 2(m_j - m_{j-1}) \\ &= 1 - N_j + 2(N_j + m_{j-1}) \\ &= N_j + 2m_{j-1} + 1 > \max A_j. \end{aligned}$$

De ruimte tussen A_{j+1} en $\bigcup_{i=1}^j A_i$ is dus altijd strikt groter dan $\max A_j$. Een eventueel rekenkundig rijtje van lengte groter dan 2 dat elementen uit kopieën van verschillende B_j 's bevat is dus onmogelijk. Verder bevat per aanname geen van de B_j 's een rekenkundig rijtje, dus A bevat geen rekenkundig rijtje.

We tonen nu aan dat A positieve bovendichtheid heeft. Merk op dat

$$A \cap [1, m_j] = \bigcup_{i=0}^j A_i,$$

omdat $\max A_k \geq 1 + 2m_k > m_j$ als $k > j$ en $\min A_i \leq m_j$ als $i \leq j$. Omdat de A_i paarsgewijs disjuncte verzamelingen zijn, geldt

$$\left| \bigcup_{i=0}^j A_i \right| = \sum_{i=0}^j |A_i| \quad (2.4)$$

We kunnen nu de bovendichtheid van A van onderen afschatten met behulp van het feit

dat $|A_i| = |B_i| > 2\epsilon N_i$ en (2.4):

$$\begin{aligned} \frac{|A \cap [1, m_j]|}{m_j} &= \frac{\left| \bigcup_{i=0}^j A_i \right|}{m_j} \\ &= \frac{\sum_{i=0}^j |A_i|}{m_j} \\ &> \frac{\sum_{i=0}^j 2\epsilon N_i}{m_j} \\ &\geq \epsilon, \end{aligned}$$

waar we in de laatste stap opmerken dat uit de definitie van m_j volgt dat $\sum_{i=0}^j 2N_i \geq m_j$.

De m_j vormen dus een deelrij van de natuurlijke getallen waarvoor de fractie getallen in A altijd groter of gelijk aan ϵ is. Er geldt dus $\bar{\sigma}(A) \geq \epsilon > 0$, wat de gewenste tegenspraak oplevert. \square

In de volgende twee hoofdstukken zullen we nu twee mogelijke bewijzen van de stelling van Szemerédi (de tweede formulering) bespreken.

Hoofdstuk 3

Het bewijs van Tao voor $k = 3$

De stelling van Szemerédi (Stelling 2.3) is voor het geval $k = 3$ te bewijzen met behulp van het feit dat \mathcal{A}_3 -verzamelingen een bepaalde mate van *niet-uniformiteit* bezitten (Propositie 3.7): de *lineaire afwijking* (Definitie 1.26) van de indicator-functie van dergelijke verzamelingen blijkt $\Omega(\delta^2)$ te zijn, waar δ de dichtheid van de verzameling is.

Voor een functie met een bepaalde mate van niet-uniformiteit (i.e. een ‘hoge’ lineaire afwijking) blijkt altijd een deelverzameling van haar drager te vinden te zijn waarop de functie nog altijd een hoge mate van niet-uniformiteit heeft (Lemma 3.10).

Door deze twee ingrediënten samen te voegen vinden we dat we in een \mathcal{A}_3 -verzameling altijd een \mathcal{A}_3 -deelverzameling met hogere dichtheid kunnen vinden (Gevolg 3.11).

Met behulp van Gevolg 3.11 zien we vervolgens redelijk eenvoudig met een bewijs uit het ongerijmde in dat $r_3(N) = o(N)$ (Gevolg 3.14). Dit is de tweede formulering van de stelling van Szemerédi (Stelling 2.7) voor $k = 3$. In Propositie 2.8 is de equivalentie van deze formuleringen bewezen en daarmee is dan ook Stelling 2.3 voor $k = 3$ bewezen.

Uit Gevolg 3.11 kunnen we echter ook de sterkere bewering $r_3(N) = O(\frac{N}{\log \log N})$ afleiden. Voor deze bewering (Stelling 3.16) zullen twee bewijzen gegeven worden: het eerste bewijs (Sectie 3.6.1) is een bewijs uit het ongerijmde. Het tweede bewijs (Sectie 3.6.2) gebruikt een iteratie-argument, waaruit duidelijker wordt waar de $\log \log N$ in de schatting vandaan komt.

3.1 De Λ_3 -operator

Definitie 3.1. We definiëren een trilineaire operator Λ_3 op de ruimte van functies van een groep Z naar \mathbb{C} door:

$$\Lambda_3(f, g, h) := \mathbf{E}_{x, r \in Z} f(x)g(x+r)h(x+2r).$$

Lemma 3.2. *Laat p priem, $Z = \mathbb{Z}_p$ en $A \subset Z$ een \mathcal{A}_3 -deelverzameling. Dan geldt:*

$$\Lambda_3(1_A, 1_A, 1_A) = \frac{|A|}{p^2}.$$

Bewijs. Omdat A geen rekenkundige rijtjes van lengte 3 bevat, zijn de enige elementen in $A \times A \times A$ van de vorm $(x, x+r, x+2r)$ de ‘triviale’ rijtjes van de vorm (x, x, x) met $x \in A$ willekeurig. Van deze rijtjes bestaan er precies $|A|$, dus uit de definitie van Λ_3 op \mathbb{Z}_p volgt dan direct het gestelde. \square

Voor het bewijs van het volgende lemma en vervolgens ook voor Propositie 3.7, zullen we de volgende eigenschap van de priemgetallen nodig hebben:

Stelling 3.3 (Bertrand’s Postulaat). *Laat n een natuurlijk getal. Er bestaat een priemgetal p tussen n en $2n$.*

Lemma 3.4. *Laat $N \geq 1$ en p een priemgetal zo dat $2N \leq p \leq 4N$. In de groep $Z = \mathbb{Z}_p$ geldt:*

$$\Lambda_3(1_{[1,N]}, 1_{[1,N]}, 1_{[1,N]}) > \frac{1}{100}.$$

Bewijs. Merk op dat er werkelijk een p als in de formulering van het lemma bestaat wegens Bertrand’s Postulaat.

We kunnen $\Lambda_3(1_{[1,N]}, 1_{[1,N]}, 1_{[1,N]})$ afschatten door op te merken dat voor alle $0 \leq r \leq N/3$ en $1 \leq x \leq N-2r$ geldt dat $(x, x+r, x+2r)$ een element is van $[1, N] \times [1, N] \times [1, N]$. Hieruit volgt met behulp van de niet-negativiteit van de functie $1_{[1,N]}$ en de aanname dat $p \leq 4N$:

$$\begin{aligned} \Lambda_3(1_{[1,N]}, 1_{[1,N]}, 1_{[1,N]}) &= \frac{1}{p^2} \sum_{r \in \mathbb{Z}_p} \sum_{x \in \mathbb{Z}_p} 1_{[1,N]}(x) 1_{[1,N]}(x+r) 1_{[1,N]}(x+2r) \\ &\geq \frac{1}{16N^2} \sum_{0 \leq r \leq N/3} \sum_{1 \leq x \leq N-2r} 1 \\ &= \frac{1}{16N^2} \frac{2N}{3} \left(\frac{N}{3} + 1 \right) \geq \frac{1}{16N^2} \frac{2N}{3} \frac{N}{3} = \frac{1}{72}, \end{aligned}$$

waarmee het lemma bewezen is. \square

Opmerking. De afchatting in dit bewijs van Lemma 3.4 is erg grof. Door $r \in [0, \lfloor N/2 \rfloor]$ te nemen zou de afchatting verscherpt kunnen worden, maar dat is voor onze doeleinden verder niet nodig.

Een lemma dat we vaak zullen gebruiken staat in de combinatoriek ook bekend als het duiventil-principe en werkt goed voor eindige sommen. Hoewel het bewijs heel simpel is, blijkt het argument in veel situaties toepasbaar.

Lemma 3.5 (Duiventil-principe). *Laat $n \geq 1$ en a_1, \dots, a_n complexe getallen. Stel dat voor zekere $M > 0$ geldt:*

$$\left| \sum_{i=1}^n a_i \right| \geq M.$$

Dan is er een $1 \leq j \leq N$ zo dat $|a_j| \geq \frac{M}{n}$.

Bewijs. Stel, om een tegenspraak te krijgen, dat voor alle $i = 1, \dots, n$ zou gelden $|a_i| < \frac{M}{n}$. Met behulp van de driehoeksongelijkheid vinden we dan de eenvoudige afchatting:

$$\left| \sum_{i=1}^n a_i \right| \leq \sum_{i=1}^n |a_i| < n \frac{M}{n} = M,$$

hetgeen de aanname dat $|\sum_{i=1}^n a_i| \geq M$ tegenspreekt. \square

In de volgende cruciale propositie zien we hoe we de Λ_3 -operator kunnen schrijven als som van Fourier-coëfficiënten. Hiervoor gebruiken we de eindige Fourier-analyse zoals in Hoofdstuk 1 besproken is.

Propositie 3.6. *Laat Z een groep van oneven orde en $f, g, h : Z \rightarrow \mathbb{C}$ willekeurige functies. Dan geldt de gelijkheid*

$$\Lambda_3(f, g, h) = \sum_{\xi \in Z} \widehat{f}(\xi) \widehat{g}(-2\xi) \widehat{h}(\xi). \quad (3.1)$$

Bewijs. Met behulp van Fourier-inversie (Stelling 1.14) kunnen we f, g en h ontbinden op de basis van karakters $\langle e_\xi \rangle_{\xi \in Z}$:

$$f = \sum_{\xi_1} \widehat{f}(\xi_1) e_{\xi_1}; \quad g = \sum_{\xi_2} \widehat{g}(\xi_2) e_{\xi_2}; \quad h = \sum_{\xi_3} \widehat{h}(\xi_3) e_{\xi_3}.$$

Hieruit zien we met behulp van de lineariteit van de Λ_3 -operator:

$$\begin{aligned} \Lambda_3(f, g, h) &= \Lambda_3 \left(\sum_{\xi_1} \widehat{f}(\xi_1) e_{\xi_1}, \sum_{\xi_2} \widehat{g}(\xi_2) e_{\xi_2}, \sum_{\xi_3} \widehat{h}(\xi_3) e_{\xi_3} \right) \\ &= \sum_{\xi_1, \xi_2, \xi_3 \in Z} \widehat{f}(\xi_1) \widehat{g}(\xi_2) \widehat{h}(\xi_3) \Lambda_3(e_{\xi_1}, e_{\xi_2}, e_{\xi_3}). \end{aligned} \quad (3.2)$$

We willen nu $\Lambda_3(e_{\xi_1}, e_{\xi_2}, e_{\xi_3})$ berekenen. Hiervoor gebruiken we de definitie van Λ_3 met de substitutie $y := x + r$, Lemma 1.9 en de definitie van $e(\theta)$:

$$\begin{aligned}
\Lambda_3(e_{\xi_1}, e_{\xi_2}, e_{\xi_3}) &= \frac{1}{|Z|^2} \sum_{y \in Z} \sum_{r \in Z} e_{\xi_1}(y-r) e_{\xi_2}(y) e_{\xi_3}(y+r) \\
&= \frac{1}{|Z|^2} \sum_{y \in Z} e_{\xi_1}(y) e_{\xi_2}(y) e_{\xi_3}(y) \sum_{r \in Z} e_{\xi_3}(r) \overline{e_{\xi_1}(r)} \\
&= \frac{1}{|Z|} \sum_{y \in Z} e_{\xi_1}^2(y) e_{\xi_2} 1_{\{\xi_3 = \xi_1\}} \\
&= \frac{1}{|Z|} \sum_{y \in Z} e_{\xi_2} \overline{e_{-2\xi_1}(y)} 1_{\{\xi_3 = \xi_1\}} \\
&= 1_{\{\xi_2 = -2\xi_1\}} 1_{\{\xi_3 = \xi_1\}}.
\end{aligned}$$

Als we dit invullen in (3.2) zien we dat

$$\begin{aligned}
\Lambda_3(f, g, h) &= \sum_{\xi_1, \xi_2, \xi_3 \in Z} \widehat{f}(\xi_1) \widehat{g}(\xi_2) \widehat{h}(\xi_3) 1_{\{\xi_2 = -2\xi_1\}} 1_{\{\xi_3 = \xi_1\}} \\
&= \sum_{\xi \in Z} \widehat{f}(\xi) \widehat{g}(-2\xi) \widehat{h}(\xi),
\end{aligned}$$

waarmee het gestelde bewezen is. □

3.2 Niet-uniformiteit in \mathcal{A}_3 -verzamelingen

Met behulp van de Λ_3 -operator kunnen we nu een uitspraak doen over de uniformiteit van \mathcal{A}_3 -verzamelingen. Verzamelingen zonder rekenkundige rijtjes van lengte 3 blijken namelijk altijd een niet-uniform deel te bezitten: de indicatorfunctie van een \mathcal{A}_3 -verzameling van dichtheid δ kan altijd opgedeeld worden in een uniform en een niet-uniform deel, op zo'n manier dat het niet-uniforme deel een lineaire afwijking van minstens $\Omega(\delta^2)$ heeft.

Propositie 3.7 (Geen rijtjes impliceert niet-uniformiteit). *Laat P een rekenkundig rijtje van gehele getallen en laat $A \subset P$ een \mathcal{A}_3 -deelverzameling.*

Schrijf $\delta := \frac{|A|}{|P|}$ en veronderstel $|P| \geq \frac{100}{\delta^2}$.

Dan bestaan er $\xi \in \mathbb{R}/\mathbb{Z}$ en $c > 0$ (onafhankelijk van δ) zodanig dat

$$|\mathbf{E}_{n \in P}(1_A(n) - \delta)e(n\xi)| \geq c\delta^2. \quad (3.3)$$

Bewijs. Als we schrijven $N := |P|$ mogen we na eventuele herschaling aannemen dat $P = [1, N]$. Laat p een priemgetal in $[2N, 4N]$ zijn. (We kunnen zo een p weer kiezen dankzij het postulaat van Bertrand.)

We splitsen de functie 1_A op in een ‘uniform’ deel $f_{U^\perp}(x) := \delta 1_{[1,N]}$ en een ‘niet-uniform’ deel $f_U(x) := 1_A(x) - f_{U^\perp}(x)$.

We willen uiteindelijk een geschikte ξ kiezen om $\widehat{f_U}(\xi)$ van onderen af te schatten, waaruit we dan de gewenste afchatting (3.3) gemakkelijk kunnen afleiden.

Om in te zien dat dit mogelijk is, gebruiken we dat we $\Lambda_3(1_A, 1_A, 1_A)$ kunnen afschatten met Lemma 3.2 en dat we $\Lambda_3(1_A, 1_A, 1_A)$ door de opsplitsing $1_A = f_U + f_{U^\perp}$ kunnen schrijven als som van acht termen, als volgt:

$$\begin{aligned}
\Lambda_3(1_A, 1_A, 1_A) &= \Lambda_3(f_U + f_{U^\perp}, f_U + f_{U^\perp}, f_U + f_{U^\perp}) \\
&= \Lambda_3(f_U, f_U + f_{U^\perp}, f_U + f_{U^\perp}) + \Lambda_3(f_{U^\perp}, f_U + f_{U^\perp}, f_U + f_{U^\perp}) \\
&= (\dots) \\
&= \sum_{x \in \{U, U^\perp\}} \sum_{y \in \{U, U^\perp\}} \sum_{z \in \{U, U^\perp\}} \Lambda_3(f_x, f_y, f_z). \tag{3.4}
\end{aligned}$$

De laatste term in deze som, $\Lambda_3(f_{U^\perp}, f_{U^\perp}, f_{U^\perp})$, kunnen we met Lemma 3.4 en de lineariteit van de Λ_3 -operator van onderen afschatten door:

$$\Lambda_3(f_{U^\perp}, f_{U^\perp}, f_{U^\perp}) = \delta^3 \Lambda_3(1_{[1,N]}, 1_{[1,N]}, 1_{[1,N]}) \geq \frac{\delta^3}{100}. \tag{3.5}$$

Uit Lemma 3.2 en de aanname $N = |P| \geq \frac{100}{\delta^2}$ weten we verder dat:

$$\Lambda_3(1_A, 1_A, 1_A) = \frac{|A|}{p^2} \leq \frac{\delta |P|}{4N^2} = \frac{\delta}{4N} \leq \frac{\delta^3}{400}. \tag{3.6}$$

Door nu (3.5) en (3.6) te combineren vinden we dat

$$|\Lambda_3(1_A, 1_A, 1_A) - \Lambda_3(f_{U^\perp}, f_{U^\perp}, f_{U^\perp})| \geq \frac{3\delta^3}{400}.$$

We weten nu dankzij Lemma 3.5 dat een van de eerste zeven termen in de schrijfwijze (3.4) van $\Lambda_3(1_A, 1_A, 1_A)$ minstens $\frac{3}{2800}\delta^3$ is.

In plaats van zeven gevallen te onderscheiden, nemen we aan dat de eerste term voldoet, dus

$$|\Lambda_3(f_U, f_U, f_U)| \geq \frac{3}{2800}\delta^3.$$

De enige essentiële informatie over de term die aan deze afchatting voldoet is immers dat er minstens één f_U in staat. Voor de andere zes termen gaat het bewijs op vergelijkbare wijze verder.

Met behulp van Propositie 3.6 en de driehoeksongelijkheid zien we nu dat

$$\sum_{\xi \in \mathbb{Z}_p} |\widehat{f_U}(\xi)|^2 |\widehat{f_U}(-2\xi)| \geq \left| \sum_{\xi \in \mathbb{Z}_p} \widehat{f_U}(\xi)^2 \widehat{f_U}(-2\xi) \right| \quad (3.7)$$

$$= |\Lambda_3(f_U, f_U, f_U)| \geq \frac{3}{2800} \delta^3. \quad (3.8)$$

Uit deze afchatting willen we nu een grote waarde voor $\widehat{f_U}(-2\xi)$ vinden, door te laten zien dat $\sum_{\xi \in \mathbb{Z}_p} |\widehat{f_U}(\xi)|^2$ niet zo groot kan worden.

Hiervoor gebruiken we de Plancherel-identiteit, (1.4):

$$\begin{aligned} \sum_{\xi \in \mathbb{Z}_p} |\widehat{f_U}(\xi)|^2 &= \frac{1}{p} \sum_{x \in \mathbb{Z}_p} |f_U(x)|^2 \\ &= \frac{1}{p} \sum_{x \in \mathbb{Z}_p} |1_A(x) - \delta 1_{[1, N]}(x)|^2 \\ &\leq \frac{1}{p} (|A| + \delta^2 |P|) \leq 2\delta, \end{aligned}$$

waar de laatste stap volgt uit de triviale ongelijkheden $\delta^2 \leq \delta$ en $p > |P|$.

We kunnen nu het maximum van $|\widehat{f_U}(-2\xi)|$ van onderen afschatten, als volgt:

$$\begin{aligned} 2\delta \max_{\xi \in \mathbb{Z}_p} |\widehat{f_U}(-2\xi)| &\geq \sum_{\xi \in \mathbb{Z}_p} |\widehat{f_U}(\xi)|^2 \max_{\xi \in \mathbb{Z}_p} |\widehat{f_U}(-2\xi)| \\ &\geq \sum_{\xi \in \mathbb{Z}_p} |\widehat{f_U}(\xi)|^2 |\widehat{f_U}(-2\xi)| \\ &\geq \frac{3}{2800} \delta^3, \end{aligned}$$

waaruit in het bijzonder blijkt dat er een $\xi_0 \in \mathbb{Z}_p$ en $c := \frac{3}{5600}$ bestaat zo dat $|\widehat{f_U}(-2\xi_0)| \geq \frac{3}{5600} \delta^2$.

Nu voldoet $\xi := \frac{2\xi_0}{p}$, wanneer opgevat als element van \mathbb{R}/\mathbb{Z} , aan de gewenste afchatting, wanneer we de definities van $e(\theta)$ en $\widehat{f_U}$ gebruiken:

$$\begin{aligned} |\mathbf{E}_{n \in P} (1_A(n) - \delta) e(n\xi)| &= |\mathbf{E}_{n \in \mathbb{Z}_p} (1_A(n) - \delta 1_{[1, N]}(n)) e\left(\frac{-2n\xi_0}{p}\right)| \\ &= |\widehat{f_U}(-2\xi_0)| \geq c\delta^2. \end{aligned}$$

□

3.3 Dichtheidstoename bij niet-uniforme functies

In de vorige sectie zagen we dat voor (indicatorfuncties van) \mathcal{A}_3 -verzamelingen met dichtheid δ een ondergrens $\Omega(\delta^2)$ bestaat voor hun lineaire afwijking. Functies met een eindige drager en een van onderen begrensde lineaire afwijking hebben de handige eigenschap dat er altijd een deelverzameling van de drager bestaat waarop de verwachting van de functie van onderen begrensd is.

De bestaande ondergrens voor de lineaire afwijking moet wel met een factor 8 verkleind worden om tot een ondergrens voor de verwachting van de functie op een kleinere drager te komen, maar in ruil daarvoor is de nieuwe drager nog steeds redelijk groot: $\Omega(\sigma^2\sqrt{N})$, als de oorspronkelijke drager grootte N had.

Omdat de verwachting van een indicatorfunctie gelijk is aan de dichtheid van de verzameling zal in de volgende sectie blijken dat we deze eigenschap goed kunnen gebruiken voor de indicatorfuncties van \mathcal{A}_3 -verzamelingen, waarvan we in de vorige sectie al zagen dat ze een van onderen begrensde lineaire afwijking hebben.

Voor de volgende stap in het bewijs hebben we een definitie en een klassieke stelling van Kronecker (1884) nodig:

Definitie 3.8. Voor $x \in \mathbb{R}$ definiëren we $\|x\|_{\mathbb{R}/\mathbb{Z}}$, de **\mathbb{R}/\mathbb{Z} -norm van x** , als de kleinste afstand van x tot een geheel getal. Verder noteren we de **entier** van $y \in \mathbb{R}$ als volgt:

$$\lfloor y \rfloor := \max\{n \in \mathbb{Z} : n \leq y\}.$$

Merk op dat $x = \lfloor x \rfloor + \|x\|_{\mathbb{R}/\mathbb{Z}} + 1_{\|x\|_{\mathbb{R}/\mathbb{Z}} > \frac{1}{2}}(x)(1 - 2\|x\|_{\mathbb{R}/\mathbb{Z}})$, dus $x = z \pm \|x\|_{\mathbb{R}/\mathbb{Z}}$ voor zekere $z \in \mathbb{Z}$.

Lemma 3.9 (Kronecker Approximatie Lemma). *Laat $\alpha \in \mathbb{R}$ en $0 < \theta < 1$. Dan geldt voor elke $N > 0$ zo dat $N\theta \geq 1$ dat er een geheel getal $0 < n < N$ bestaat zo dat $\|n\alpha\|_{\mathbb{R}/\mathbb{Z}} \leq \theta$.*

Bewijs. Laat $R := \{\|n\alpha\|_{\mathbb{R}/\mathbb{Z}} \mid 0 \leq n < N\} \subset [0, 1)$ en laat $(r_i)_{i=0}^{N-1}$ een lineaire ordening van R , dus $0 = r_0 \leq r_1 \leq \dots \leq r_{N-1}$ en definieer $r_N := 1$. De collectie intervallen $\{[r_i, r_{i+1}]\}_{i=0}^{N-1}$ is een partitie het interval $[0, 1]$, zodat geldt:

$$\sum_{i=0}^{N-1} |r_{i+1} - r_i| = 1. \tag{3.9}$$

Merk nu op dat als $|r_{i+1} - r_i| > \frac{1}{N}$ voor iedere $0 \leq i < N$, dan zou

$$\sum_{i=0}^{N-1} |r_{i+1} - r_i| > N \frac{1}{N} = 1,$$

hetgeen (3.9) zou tegenspreken.

Er bestaat dus een $0 \leq i < N$ zo dat

$$|r_{i+1} - r_i| \leq \frac{1}{N} \leq \theta$$

We kunnen voor geschikte $0 \leq m_1, m_2 < N$ met $m_1 \neq m_2$ schrijven:

$$|r_{i+1} - r_i| = \left| \|m_1\alpha\|_{\mathbb{R}/\mathbb{Z}} - \|m_2\alpha\|_{\mathbb{R}/\mathbb{Z}} \right| = \left| \|m_1 - m_2\alpha\|_{\mathbb{R}/\mathbb{Z}} \right|,$$

dus voor $n := |m_1 - m_2|$ geldt nu dat $\|n\alpha\|_{\mathbb{R}/\mathbb{Z}} \leq \theta$.

□

Lemma 3.10 (Niet-uniformiteit impliceert dichtheidstoename). *Laat $f : \mathbb{Z} \rightarrow [-1, 1]$ een functie met de eigenschappen:*

1. $P := \text{supp}(f)$ is een rekenkundige rij,
2. $\sum_n f(n) = 0$,
3. Voor zekere $\xi \in \mathbb{R}/\mathbb{Z}$ en $\sigma > 0$ geldt

$$|\mathbf{E}_{n \in P} f(n) e(n\xi)| \geq \sigma.$$

Dan bestaan er een rekenkundige rij $P' \subset P$ en $c' > 0$ zo dat

1. $|P'| \geq c'\sigma^2|P|^{1/2}$,
2. $|\mathbf{E}_{n \in P'} f(n)| \geq \frac{\sigma}{8}$.

Bewijs. We mogen opnieuw aannemen dat $P = [1, N]$. Verder kiezen we $\xi \in \mathbb{R}/\mathbb{Z}$ zo dat aanname 3 geldt en noteren we $g(m) := f(m)e(m\xi)$, zodat we aanname 3 kunnen schrijven als:

$$\left| \sum_{m=1}^N g(m) \right| \geq \sigma N. \quad (3.10)$$

Vanwege Lemma 3.9 bestaat er een geheel getal $r \leq N^{\frac{1}{2}}$ zodanig dat $\|r\xi\|_{\mathbb{R}/\mathbb{Z}} \leq N^{-\frac{1}{2}}$. We kunnen schrijven $r\xi = a \pm \|r\xi\|_{\mathbb{R}/\mathbb{Z}}$ voor zekere $a \in \mathbb{Z}$.

Definieer $P_0 := [1, \sigma N^{\frac{1}{2}}/100] \cdot r$. Merk op, als $x \in P_0$, dan $x = rt$ voor een geheel getal $1 \leq t \leq \sigma N^{\frac{1}{2}}/100$, dus $\pi x \xi = \pi t(a \pm \|r\xi\|_{\mathbb{R}/\mathbb{Z}})$, zodat de volgende afchatting geldt:

$$|e(-x\xi) - 1| = |e^{-i\pi x\xi} - e^{i\pi x\xi}| = |2 \sin(\pi t \|r\xi\|_{\mathbb{R}/\mathbb{Z}})| \leq 2\pi \frac{\sigma N^{\frac{1}{2}}}{100} N^{-\frac{1}{2}} \leq \frac{\sigma}{10}. \quad (3.11)$$

We kunnen nu eerst de som over $n \in (-N, N]$ van de verwachtingen op P_0 van de functie $f(n+x)e(n\xi)$ van onderen afschatten en vervolgens weer het Duiventil-principe (Lemma 3.5) gebruiken om een n_0 te vinden waarvoor we de verwachting op P_0 van $f(n_0+x)e(n\xi)$ kunnen afschatten.

Uit (3.11) leiden we af dat:

$$\begin{aligned} \left| \sum_{n=-N+1}^N \mathbf{E}_{x \in P_0} g(n+x)(e(-x\xi) - 1) \right| &= \sum_{n=-N+1}^N \mathbf{E}_{x \in P_0} |f(n+x)e(n\xi)(e(-x\xi) - 1)| \\ &\leq \sum_{n=-N+1}^N 1 \cdot \frac{\sigma}{10} \leq \frac{\sigma N}{2}. \end{aligned} \quad (3.12)$$

Anderzijds geldt ook dat:

$$\begin{aligned} \left| \mathbf{E}_{x \in P_0} \sum_{n=-N+1}^N g(n+x) \right| &= \left| \mathbf{E}_{x \in P_0} \sum_{m=1}^N g(m) \right| \\ &= \left| \sum_{m=1}^N g(m) \right| \\ &\geq \sigma N, \end{aligned} \quad (3.13)$$

waar we (3.10) gebruiken, alsmede het feit dat $\text{supp}(f) = \text{supp}(g) = [1, N]$.

Uit (3.12) en (3.13) vinden we nu met de driehoeksongelijkheid een ondergrens voor de som over $n \in (-N, N]$ van verwachtingen van $f(n+x)e(n\xi)$ als x de verzameling P_0 doorloopt:

$$\begin{aligned} \left| \sum_{n=-N+1}^N \mathbf{E}_{x \in P_0} f(n+x)e(n\xi) \right| &= \left| \sum_{n=-N+1}^N \mathbf{E}_{x \in P_0} g(n+x)e(-x\xi) \right| \\ &\geq \left| \sum_{n=-N+1}^N \mathbf{E}_{x \in P_0} g(n+x) \cdot 1 \right| - \left| \sum_{n=-N+1}^N \mathbf{E}_{x \in P_0} g(n+x)(e(-x\xi) - 1) \right| \\ &\geq \sigma N - \frac{\sigma N}{2} \geq \frac{\sigma N}{2}. \end{aligned} \quad (3.14)$$

In het bijzonder geldt dus voor zekere $\theta \in \mathbb{R}/\mathbb{Z}$ dat

$$\text{Re} \sum_{n=-N+1}^N \mathbf{E}_{x \in P_0} f(n+x)e(n\xi + \theta) \geq \frac{\sigma N}{2}.$$

Omdat we aangenomen hebben dat $\sum_n f(n) = 0$ mogen we in deze ongelijkheid ook $\sum_{n=-N+1}^N \mathbf{E}_{x \in P_0} f(n+x)$ optellen en omdat f reëelwaardig is, kunnen we de ongelijkheid dan ook schrijven als:

$$\sum_{n=-N+1}^N \mathbf{E}_{x \in P_0} f(n+x) \operatorname{Re}(1 + e(n\xi + \theta)) \geq \frac{\sigma N}{2}.$$

Vanwege het Duiventil-principe bestaat er nu een $n_0 \in (-N, N)$ zo dat

$$\mathbf{E}_{x \in P_0} f(n_0 + x) \operatorname{Re}(1 + e(n_0\xi + \theta)) \geq \frac{\sigma}{4}.$$

Als we nu $P' := (n_0 + P_0) \cap P$ nemen, zien we dat

$$\mathbf{E}_{x \in P'} f(x) = \mathbf{E}_{x \in P_0} f(n_0 + x) \geq \mathbf{E}_{x \in P_0} f(n_0 + x) \operatorname{Re}(1 + e(n_0\xi + \theta)) \cdot \frac{1}{2} \geq \frac{\sigma}{8},$$

waar we gebruiken dat $\frac{1}{2} \operatorname{Re}(1 + e^{2\pi i \eta}) \leq 1$ voor alle η .

In het bijzonder geldt, omdat $f \leq 1$ en $\operatorname{supp}(f) = P$ (dus $f \cdot 1_P = f$), dat

$$|P'| = |P_0| \mathbf{E}_{x \in P_0} 1_P(n_0 + x) \geq |P_0| \mathbf{E}_{x \in P'} f(x) \geq \frac{\sigma |P_0|}{8},$$

en omdat $|P_0| = \lceil \sigma N^{\frac{1}{2}} / 100 \rceil \geq \frac{1}{2} \sigma N^{\frac{1}{2}} / 100$ geldt nu voor $c' := \frac{1}{1600}$ dat

$$|P'| \geq c' \sigma^2 |P|^{\frac{1}{2}},$$

zoals te bewijzen was. □

3.4 Dichtheidstoename bij \mathcal{A}_3 -verzamelingen

We kunnen nu de vruchten plukken van Sectie 3.2 en Sectie 3.3, door de resultaten uit Propositie 3.7 en Lemma 3.10 te combineren tot Gevolg 3.11.

Met dit gevolg zien we dat we voor een \mathcal{A}_3 -deelverzameling A van een rekenkundig rijtje P met een bepaalde dichtheid δ altijd een redelijk grote deelrij $P' \subset P$ kunnen vinden waarop de \mathcal{A}_3 -verzameling een nog grotere dichtheid heeft. Dat P' ‘redelijk groot’ is, is belangrijk: we sluiten hiermee bijvoorbeeld de triviale oplossing uit waarbij we voor P' slechts 2 elementen uit A nemen om vervolgens te beweren dat A in P' dichtheid 1 heeft.

Maar er is meer: P' blijkt zó groot gekozen te kunnen worden, dat we door slim terugredeneren uiteindelijk zullen kunnen bewijzen dat de oorspronkelijke dichtheid δ van A in P niet al te groot kan zijn geweest: anders zou de dichtheid van A uiteindelijk, na herhaald toepassen van Gevolg 3.11 zo groot worden dat A plotseling geen \mathcal{A}_3 -verzameling meer zou kunnen zijn. Dit argument zullen we in de volgende secties precies maken.

Gevolg 3.11 (Geen rijtjes impliceert dichtheidstoename). *Laat P een rekenkundig rijtje van gehele getallen en laat $A \subset P$ een \mathcal{A}_3 -deelverzameling.*

Schrijf $\delta := \frac{|A|}{|P|}$ en veronderstel $|P| \geq \frac{100}{\delta^2}$.

Dan bestaan er een rekenkundige rij $P' \subset P$ en $c_1, c_2 > 0$ onafhankelijk van P en A zo dat

1. $|P'| \geq c_1 \delta^4 |P|^{1/2}$,
2. $\frac{|A \cap P'|}{|P'|} \geq \frac{|A|}{|P|} + c_2 \delta^2$.

Bewijs. Definieer $f(n) := (1_A(n) - \delta)1_P(n)$. Vanwege Propositie 3.7 bestaan er $\xi \in \mathbb{R}/\mathbb{Z}$ en $c > 0$ zodanig dat

$$|\mathbf{E}_{n \in P} f(n) e(n\xi)| \geq c\delta^2.$$

Er geldt $P = \text{supp}(f)$ per definitie van f en $\sum_{n \in P} f(n) = |A| - |P|\delta = 0$. We kunnen dus uit Lemma 3.10 concluderen dat er een rekenkundige rij $P' \subset P$ en $c' > 0$ bestaan zo dat

1. $|P'| \geq c' c^2 \delta^4 |P|^{1/2}$,
2. $|\mathbf{E}_{n \in P'} f(n)| \geq \frac{c\delta^2}{8}$.

Door $c_1 := c' c^2$ te stellen vinden we de eerste gewenste ongelijkheid.

Voor de tweede ongelijkheid vullen we de definitie van f in en gebruiken we dat $1_P \equiv 1$ op P' :

$$\begin{aligned} |\mathbf{E}_{n \in P'} f(n)| &= |\mathbf{E}_{n \in P'} (1_A(n) - \delta)| \\ &= \frac{|A \cap P'|}{|P'|} - \frac{|A|}{|P|} \geq \frac{c\delta^2}{8}. \end{aligned}$$

Als we dus $c_2 := \frac{c}{8}$ nemen volgt nu de tweede te bewijzen ongelijkheid direct. □

Definitie 3.12. Het blijkt in het vervolg handig te zijn de functie $a(N)$ als volgt te definiëren:

$$a(N) := \frac{r_3(P)}{N}$$

waar P een willekeurige rekenkundige rij van lengte N is. Het is duidelijk dat de waarde van r_3 niet afhangt van de keuze van P .

Deze definitie maakt het mogelijk om Gevolg 3.11 geheel te formuleren als een eigenschap van de functie a . Hierbij is het oorspronkelijke probleem, dat combinatorisch/getaltheoretisch van aard was, wordt hiermee gereduceerd tot een analytisch probleem: het aantonen van een ongelijkheid voor een functie die aan bepaalde eigenschappen voldoet.

Gevolg 3.13. *Er bestaan $c_1, c_2 > 0$ zo dat voor de functie $a : \mathbb{N} \rightarrow [0, 1]$ geldt:*

Voor iedere N met $a(N) \geq \frac{10}{\sqrt{N}}$ bestaat er een $N' < N$ zo dat

1. $N' \geq c_1 a^4(N) N^{1/2}$,

$$2. a(N') \geq a(N) + c_2 a^2(N).$$

Bewijs. Kies c_1 en c_2 zo dat Gevolg 3.11 geldt.

Zij $N \in \mathbb{N}$ zo dat $a(N) \geq \frac{10}{\sqrt{N}}$. Laat $P := [1, N]$ en $A \subset P$ een \mathcal{A}_3 -deelverzameling met $|A| = r_3(N)$.

Als we nu schrijven $\delta = \frac{|A|}{|P|} = a(N)$ dan zien we uit de aanname over $a(N)$ dat $|P| \geq \frac{100}{\delta^2}$. Gevolg 3.11 geeft nu een rekenkundige rij $P' \subset P$.

Als we stellen $N' := |P'|$ dan volgt het gestelde direct uit Gevolg 3.11 en het feit dat $A \cap P'$ een \mathcal{A}_3 -verzameling in P' is en dus $a(N') = \frac{r_3([1, N'])}{N'} = \frac{r_3(P')}{|P'|} \geq \frac{|A \cap P'|}{|P'|}$. \square

3.5 $o(N)$ schatting voor r_3

Gevolg 3.14. Voor elke $\epsilon > 0$ bestaat er $N_0 \in \mathbb{N}$ zo dat voor alle $N \geq N_0$ geldt:

$$r_3(N) \leq \epsilon N.$$

Bewijs. We kunnen aantonen dat $\lim_{N \rightarrow \infty} a(N) = 0$, hetgeen equivalent is met het gestelde.

Stel immers dat $\limsup_{N \rightarrow \infty} a(N) = a > 0$.

Kies nu M_1 en M_2 zo dat $\frac{10}{\sqrt{N}} < \frac{a}{2}$ voor alle $N > M_1$ en $a(N) > \frac{a}{2}$ voor alle $N > M_2$.

Er bestaat vanwege de aanname over $\limsup_{N \rightarrow \infty} a(N)$ een strikt stijgende rij natuurlijke getallen $(N_k)_{k=0}^\infty$ zo dat $N_0 > \max\{M_1, M_2\}$ en $\lim_{k \rightarrow \infty} a(N_k) = a$.

Elke N_k voldoet nu aan de voorwaarde van Gevolg 3.13: $a(N_k) > \frac{a}{2} > \frac{10}{\sqrt{N_k}}$.

Er bestaat dus voor elke k een $N'_k < N_k$ zo dat

1. $N' \geq c_1 a^4(N) N^{1/2}$,
2. $a(N') \geq a(N) + c_2 a^2(N)$.

De rij getallen $(N'_k)_{k=0}^\infty$ gaat dus naar oneindig vanwege de eerste ongelijkheid, en vanwege de tweede ongelijkheid gecombineerd met het feit dat $a(N) > \frac{a}{2}$ geldt $\limsup_{k \rightarrow \infty} a(N'_k) \geq \lim_{k \rightarrow \infty} a(N_k) + \frac{c_2 a^2}{4} > a$, hetgeen de aanname dat $a = \limsup_{N \rightarrow \infty} a(N)$ tegenspreekt. \square

3.6 $O(N/\log \log N)$ schatting voor r_3

3.6.1 Bewijs uit het ongerijmde

Lemma 3.15. Voor $\alpha > 1$ en $N \geq e^{e^\alpha}$ is de functie

$$N \mapsto \frac{\log \log N}{N^{1/\alpha}}$$

dalend.

Bewijs. De afgeleide naar N van de functie is gelijk aan

$$N^{-\frac{\alpha+1}{\alpha}} \left(\frac{1}{\log N} - \frac{1}{\alpha} \log \log N \right).$$

Merk nu op dat $\frac{1}{\log N} < 1 < \frac{1}{\alpha} \log \log N$ voor alle $N \geq e^{e^\alpha}$, dus de afgeleide is daar negatief, dus de functie dalend. \square

Stelling 3.16. *Er bestaat een $C > 0$ zo dat voor alle $N \geq 3$ geldt:*

$$r_3(N) \leq C \frac{N}{\log \log N}.$$

Bewijs. Stel dat het gestelde niet waar is.

Kies $c_1, c_2 > 0$ zo dat Gevolg 3.13 geldt. Kies vervolgens $N_0 \geq \max\{10^4, c_1^{-4}, e^{4(c_2^{-1}+1)}, e^{e^{16}}\}$.

Uit de ontkenning van de stelling toegepast op $C := \log \log N_0$ volgt nu dat er een N bestaat zodanig dat

$$a(N) > \frac{\log \log N_0}{\log \log N}.$$

Kies N nu zo klein mogelijk. Merk op dat $N > N_0$, omdat $N \leq N_0$ zou impliceren dat $a(N) > 1$, wat per definitie van $a(N)$ onmogelijk is.

Merk op dat $\frac{\log \log N}{N^{\frac{1}{2}}} < 1$ voor alle $N \geq e^{e^{16}}$ wegens Lemma 3.15, dus omdat verder geldt dat $\log \log N_0 \geq 16$ volgt hieruit dat $a(N) > \frac{10}{\sqrt{N}}$. Er bestaat dus wegens Gevolg 3.13 een $N' < N$ zodanig dat

1. $N' \geq c_1 a(N)^4 \sqrt{N}$,
2. $a(N') \geq a(N) + c_2 a(N)^2$.

Omdat N minimaal gekozen was kunnen we uit $N' < N$ concluderen dat

$$a(N') \leq \frac{\log \log N_0}{\log \log N'},$$

dit combineren met de tweede ongelijkheid over $a(N')$ geeft:

$$\frac{\log \log N_0}{\log \log N'} > \frac{\log \log N_0}{\log \log N} + c_2 \left(\frac{\log \log N_0}{\log \log N} \right)^2 \quad (3.15)$$

Anderzijds blijkt door de aanname over $a(N)$ in te vullen in de eerste ongelijkheid over N' hierboven en verder te gebruiken dat $\frac{N^{\frac{1}{4}}}{(\log \log N)^4} > \frac{N_0^{\frac{1}{4}}}{(\log \log N_0)^4}$ (uit Lemma 3.15):

$$\begin{aligned}
N' &\geq c_1 a(N)^4 \sqrt{N} \\
&> c_1 (\log \log N_0)^4 \frac{N^{\frac{1}{4}}}{(\log \log N)^4} N^{\frac{1}{4}} \\
&> c_1 N_0^{\frac{1}{4}} N^{\frac{1}{4}} \\
&\geq N^{\frac{1}{4}},
\end{aligned}$$

waar de laatste ongelijkheid volgt uit de aanname dat $N_0 \geq c_1^{-4}$. Dus $N' \geq N^{1/4}$.

Door dit gegeven te combineren met (3.15) en overal te delen door een factor $\log \log N_0$ krijgen we nu

$$\frac{1}{\log \log N^{\frac{1}{4}}} > \frac{1}{\log \log N} + \frac{c_2 \log \log N_0}{(\log \log N)^2},$$

Merk op dat $\log \log N^{\frac{1}{4}} = \log \log N - \log 4$, dus we kunnen deze ongelijkheid ook schrijven als

$$\frac{\log 4}{\log \log N - \log 4} > c_2 \frac{\log \log N_0}{\log \log N},$$

of te wel

$$\frac{\log \log N}{\log \log N - \log 4} > c_2 \frac{\log \log N_0}{\log 4}.$$

Door aan beide kanten inverses te nemen krijgen we nu

$$1 - \frac{\log 4}{\log \log N} < c_2^{-1} \frac{\log 4}{\log \log N_0},$$

en dus, omdat $N > N_0$, moet gelden dat

$$1 < \frac{(c_2^{-1} + 1) \log 4}{\log \log N_0},$$

maar dit geeft een tegenspraak met de aanname dat $N_0 \geq e^{4c_2^{-1}+1}$ (oftewel $\log \log N_0 \geq (c_2^{-1} + 1) \log 4$), waarmee het gestelde bewezen is. \square

3.6.2 Bewijs met behulp van iteratie

Een aanzienlijk korter bewijs voor Stelling 3.16 kan gevonden worden met behulp van een argument waarin Gevolg 3.11 geïtereerd wordt. Ook Roth maakte in zijn oorspronkelijke bewijs (zie Hoofdstuk 4) gebruik van een dergelijk argument.

Bewijs. Uit Gevolg 3.14 weten we dat voor zekere N_0 geldt dat $a(N) \leq e^{e^{-1}}$ voor alle $N \geq N_0$. Laat $N \in \mathbb{N}$ met $N \geq N_0$.

Stel dat A_0 een \mathcal{A}_3 -verzameling van maximale grootte in $P_0 := [1, N]$ van dichtheid $\delta_0 := \frac{|A_0|}{N} = a(N) \geq \frac{10}{\sqrt{N}}$ is. (Als voor alle N zou gelden dat $a(N) < \frac{10}{\sqrt{N}}$ waren we onmiddellijk klaar wegens Lemma 3.15.)

Wegens Gevolg 3.11 vinden we, bij een gegeven \mathcal{A}_3 -verzameling A_{n-1} in een rekenkundig rijtje P_{n-1} met $\delta_{n-1} := \frac{|A_{n-1}|}{|P_{n-1}|}$ zo dat $|P_{n-1}| \geq \frac{100}{\delta_{n-1}^2}$, een rekenkundig rijtje P_n en \mathcal{A}_3 -verzameling $A_n := A_{n-1} \cap P_n$ zo dat

$$|P_n| \geq c_1 \delta_n^4 |P_{n-1}|^{\frac{1}{2}}, \quad (3.16)$$

$$\delta_n \geq \delta_{n-1} + c_2 \delta_{n-1}^2. \quad (3.17)$$

Zonder verlies van algemeenheid mogen we hierin aannemen dat $c_1 \leq 1$, want als we uit Gevolg 3.11 een $c'_1 > 1$ zouden krijgen, dan zou (3.16) in het bijzonder waar zijn voor $c_1 := 1$. Uit (3.16) volgt in het bijzonder dat deze rij van verzamelingen afbreekt zodra $P_n < \frac{100}{\delta_n^2} \leq \frac{100}{\delta_0^2}$.

Anderzijds leiden we uit (3.17) af dat voor alle n geldt $\delta_n \geq \delta_0$ en verder:

$$\begin{aligned} \frac{1}{\delta_n} &\leq \frac{1}{\delta_{n-1}} \left(\frac{1}{1 + c_2 \delta_{n-1}} \right) \\ &= \frac{1}{\delta_{n-1}} - \frac{c_2}{1 + c_2 \delta_{n-1}} \\ &\leq \frac{1}{\delta_{n-1}} - c_3, \end{aligned} \quad (3.18)$$

waar $c_3 := \frac{c_2}{1+c_2} < 1$ en (3.18) geldt omdat $\delta_{n-1} \leq 1$ voor alle n .

Door de ongelijkheid (3.18) n keer toe te passen vinden we nu dat

$$\frac{1}{\delta_n} \leq \frac{1}{\delta_0} - c_3 n,$$

en dus krijgen we hieruit voor n de ongelijkheid:

$$n \leq \frac{1}{c_3} \left(\frac{1}{\delta_0} - \frac{1}{\delta_n} \right) < \frac{1}{c_3 \delta_0}. \quad (3.19)$$

Uit (3.16) en omdat $1 \geq \delta_n \geq \delta_0$ weten we dat $1 \leq \delta_n^{-8} \leq \delta_0^{-8}$, zien we dat

$$\begin{aligned} |P_{n-1}| &\leq \frac{1}{c_1^2} |P_n|^2 \delta_n^{-8} \\ &\leq \frac{1}{c_1^2} |P_n|^2 \delta_0^{-8} =: (R|P_n|)^2, \end{aligned} \quad (3.20)$$

waar we stellen $R := c_1^{-1}\delta_0^{-4} \geq 1$.

Als we de ongelijkheid (3.20) n keer toepassen vinden we dat

$$N = |P_0| \leq (R^2)^{2^n-1} |P_n|^{2^n} \leq (R^2 |P_n|)^{2^n}. \quad (3.21)$$

We kunnen nu gebruiken dat $|P_n| < \frac{100}{\delta_0^2}$ omdat de rij bij de n 'de term afbreekt. Verder weten we uit (3.19) dat $n < \frac{1}{c_3\delta_0}$, dus (omdat natuurlijk ook $|P_n| \geq 1$) geldt:

$$N \leq (R^2 |P_n|)^{2^n} \leq \left(\frac{100}{c_1^2 \delta_0^{10}} \right)^{2^{\frac{1}{c_3\delta_0}}}.$$

Een logaritme nemen aan beide kanten geeft:

$$\begin{aligned} \log N &\leq 2^{\frac{1}{c_3\delta_0}} \log \left(\frac{100}{c_1^2 \delta_0^{10}} \right) \\ &= \exp \left(\frac{\log 2}{c_3\delta_0} + \log \log \left(\frac{100}{c_1^2 \delta_0^{10}} \right) \right). \end{aligned} \quad (3.22)$$

Laat nu $c_4 := 1 + \frac{\log 2}{c_3} + \log \log \frac{100}{c_1^2} + \log 10$. Merk op dat zeker geldt $c_4 > 0$ omdat de eerste term en de derde term zeker positief zijn, en omdat $c_1 < 1$ is ook de tweede term positief.

Merk op dat geldt

$$\frac{\log \log e^e}{e^e} < 1.$$

Per aanname geldt $\delta_0 = a(N) < e^{e^{-1}}$ en dus $\frac{1}{\delta_0} \geq e^{e^1}$. Vanwege Lemma 3.15, toegepast op $\alpha = 1$ en als variabele $\frac{1}{\delta_0}$ geldt nu:

$$\begin{aligned} \log \log \frac{1}{\delta_0} &< \frac{1}{\delta_0} = \left(c_4 - \frac{\log 2}{c_3} - \log \log \frac{100}{c_1^2} - \log 10 \right) \delta_0^{-1} \\ &\leq \left(c_4 - \frac{\log 2}{c_3} \right) \delta_0^{-1} - \log \log \left(\frac{100}{c_1^2} \right) - \log 10, \end{aligned} \quad (3.23)$$

waar de laatste ongelijkheid volgt uit $\delta_0 \leq 1$, dus $-\delta_0^{-1} \leq -1$.

$$\begin{aligned} \frac{\log 2}{c_3\delta_0} + \log \log \left(\frac{100}{c_1^2 \delta_0^{10}} \right) &= \frac{\log 2}{c_3\delta_0} + \log \left(\log \left(\frac{100}{c_1^2} \right) + 10 \log \left(\frac{1}{\delta_0} \right) \right) \\ &\leq \frac{\log 2}{c_3\delta_0} + \log \log \left(\frac{100}{c_1^2} \right) + \log 10 + \log \log \left(\frac{1}{\delta_0} \right), \end{aligned} \quad (3.24)$$

waar de laatste ongelijkheid volgt uit het feit dat $\log(A + B) \leq \log(A) + \log(B)$ voor $A, B > 2$.

Door nu (3.23) in te vullen in (3.24) vinden we uiteindelijk dat

$$\frac{\log 2}{c_3 \delta_0} + \log \log \left(\frac{100}{c_1^2 \delta_0^{10}} \right) \leq c_4 \delta_0^{-1},$$

en door dit terug in te vullen in (3.22) dat:

$$\log N \leq \exp(c_4 \delta_0^{-1})$$

Aan beide kanten nog een laatste logaritme nemen geeft nu dat

$$\delta_0 = a(N) \leq \frac{c_4}{\log \log N}.$$

Hiermee is het gestelde bewezen voor $N \geq N_0$. Als we nu verder nog definiëren $c_5 := \max\{a(N) \log \log N : 3 \leq N < N_0\}$, dan kunnen we voor $C := \max\{c_4, c_5\}$ het gestelde concluderen.

□

Hoofdstuk 4

Het bewijs van Roth voor $k = 3$

In het vorige hoofdstuk hebben we gezien hoe met behulp van eindige Fourier-analyse en het concept lineaire afwijking de stelling van Szemerédi voor het geval $k = 3$ bewezen kan worden.

Met een uitbreiding van deze methode, waarin de norm $\|\cdot\|_u$ voor de lineaire afwijking vervangen wordt door een hogere orde norm (de zogenaamde Gowers uniformity norm), kan de stelling van Szemerédi uiteindelijk ook voor $k > 3$ bewezen worden.

Toen Roth echter in 1952 voor het eerst de stelling van Szemerédi voor het geval $k = 3$ bewees, gebruikte hij hiervoor niet expliciet het krachtige gereedschap van de eindige Fourier-analyse, maar gaf een bewijs dat meer elementair van aard was, met als essentiële stap de *cirkelmethode van Hardy en Littlewood*, die Tao in zijn bewijs niet meer nodig had.

In dit hoofdstuk zullen we de bewijsmethode van Roth beschrijven, maar wel in de moderne terminologie van verwachtingen en indicatorfuncties, die in Roth's oorspronkelijke artikel uit 1952 geheel niet voorkwamen.

Hiervoor noteren we als volgt de Fourier-getransformeerde van functies in $\mathbb{C}^{\mathbb{Z}}$ met eindige drager, ook voor niet-gehele frequenties:

Definitie 4.1. Als $f : \mathbb{Z} \rightarrow \mathbb{C}$ een functie met eindige drager is, noteer dan $A := \text{supp}(f)$. We definiëren voor $\alpha \in \mathbb{R}$

$$\alpha \cdot n := \frac{\alpha n}{|A|} \bmod \mathbb{Z},$$

$$\widehat{f}(\alpha) := \mathbf{E}_{n \in A} f(n) \overline{e(\alpha \cdot n)},$$

de Fourier-getransformeerde van f bij frequentie α .

4.1 Enkele eigenschappen van de functie a

Lemma 4.2 (Multiplicatieve monotonie). *Voor de functie $a : \mathbb{N} \rightarrow [0, 1]$ gelden voor alle $x, y \in \mathbb{N}$ de volgende ongelijkheden:*

$$a(xy) \leq a(y), \tag{4.1}$$

$$a(x) \leq (1 + yx^{-1})a(y). \quad (4.2)$$

Bewijs. Laat $x, y \in \mathbb{N}$.

Als $A \subset [1, x+y]$ een \mathcal{A}_3 -verzameling is, dan zijn $A_x := A \cap [1, x]$ en $A_y := A \cap [x+1, x+y]$ ook \mathcal{A}_3 -verzamelingen, dus er geldt $|A_x| \leq r_3(x)$ en (wegens Lemma 2.5) $|A_y| \leq r_3(y)$.

Hieruit concluderen we omdat $|A| = |A_x| + |A_y|$ de driehoeksongelijkheid voor r_3 :

$$r_3(x+y) \leq r_3(x) + r_3(y).$$

Door de driehoeksongelijkheid $x-1$ keer toe te passen zien we hieruit ook dat

$$r_3(xy) = r_3((x-1)y + y) \leq r_3((x-1)y) + r_3(y) \leq \dots \leq xr_3(y). \quad (4.3)$$

In deze ongelijkheid kunnen we aan beide zijden delen door xy zodat we krijgen:

$$\frac{r_3(xy)}{xy} \leq \frac{r_3(y)}{y},$$

waarmee (4.1) bewezen is.

Door x met rest te delen door y zien we dat voor zekere $0 \leq b < y$ geldt:

$$x = \lfloor \frac{x}{y} \rfloor y + b \leq \left(\lfloor \frac{x}{y} \rfloor + 1 \right) y,$$

dus omdat r_3 een stijgende functie is (Lemma 2.6) geldt dankzij (4.3):

$$r_3(x) \leq r_3\left(\left(\lfloor \frac{x}{y} \rfloor + 1\right)y\right) \leq \left(\lfloor \frac{x}{y} \rfloor + 1\right)r_3(y) \leq \frac{x+y}{y}r_3(y)$$

Aan beide kanten delen door x geeft nu:

$$\frac{r_3(x)}{x} \leq \frac{x+y}{x} \frac{r_3(y)}{y} = (1 + yx^{-1}) \frac{r_3(y)}{y},$$

waaruit met de definitie van de functie a nu (4.2) volgt. \square

4.2 Een functionele ongelijkheid voor $a(m)$

Om tot een functionele ongelijkheid van $a(m)$ te komen benaderen we de Fouriercoëfficiënt van een indicatorfunctie met de Fouriercoëfficiënt van de functie die constant gelijk is aan $a(m)$, waarna we kunnen gebruiken dat we de Fouriercoëfficiënt van de constante functie expliciet kunnen uitdrukken in $a(m)$.

Lemma 4.3. *De functie $e(\theta) := e^{2\pi i\theta}$ heeft de volgende eigenschappen:*

1. Voor iedere $\alpha \in \mathbb{R}, N \in \mathbb{N}$ geldt:

$$\left| \sum_{k=1}^N e(\alpha k) \right| \leq \frac{1}{2\|\alpha\|_{\mathbb{R}/\mathbb{Z}}}. \quad (4.4)$$

2. Voor iedere $p \in \mathbb{N}$, $h \in \mathbb{Z}$ geldt zelfs:

$$\sum_{k=1}^p e\left(\frac{hk}{p}\right) = 1_{\{1\}}(p). \quad (4.5)$$

3. Voor iedere $t \in \mathbb{Z}$, $\eta \in \mathbb{R}$ geldt:

$$\int_{-\eta}^{1-\eta} e(\alpha t) d\alpha = 1_{\{0\}}(t). \quad (4.6)$$

4. Voor iedere $\alpha \in \mathbb{R}$ geldt:

$$|e(\alpha) - 1| \leq 2\pi|\alpha|. \quad (4.7)$$

Bewijs. We gebruiken de formule voor de som van een afbrekende meetkundige reeks: als $r \in \mathbb{C} \setminus \{1\}$ en $N \in \mathbb{N}$ geldt:

$$\sum_{k=1}^N r^k = \frac{r^{N+1} - r}{r - 1}.$$

Om (4.4) in te zien passen we deze formule toe met $r = e^{2\pi i\alpha}$:

$$\begin{aligned} \sum_{k=1}^N e(\alpha k) &= \sum_{k=1}^N (e^{2\pi i\alpha})^k \\ &= \frac{e^{2\pi i\alpha(N+1)} - e^{2\pi i\alpha}}{e^{2\pi i\alpha} - 1}. \end{aligned} \quad (4.8)$$

Uit de identiteit $|e^{2\pi i\alpha} - 1| = 2 \sin |\pi\alpha|$ en de afschatting $|e(\theta) - e(\rho)| \leq 2$ volgt nu dat

$$\left| \sum_{k=1}^N e(\alpha k) \right| \leq \frac{2}{2 \sin |\pi\alpha|}. \quad (4.9)$$

We kunnen voor zekere $a \in \mathbb{Z}$ schrijven $\alpha = a \pm \|\alpha\|_{\mathbb{R}/\mathbb{Z}}$, zodat $\sin |\pi\alpha| = \sin \pi \|\alpha\|_{\mathbb{R}/\mathbb{Z}} \geq 2\|\alpha\|_{\mathbb{R}/\mathbb{Z}}$. Door dit in te vullen in (4.9) volgt nu (4.4).

Omdat $e(h) = 1$ is (4.5) direct waar voor $p = 1$. Als $p > 1$ zien we met behulp van (4.8) ook (4.5) direct in als we $N = p$ en $\alpha = \frac{h}{p}$ invullen en gebruiken dat $e(h) = 1$, terwijl $e(\frac{h}{p}) \neq 1$ omdat $p > 1$:

$$\sum_{k=1}^p e\left(\frac{hk}{p}\right) = e^{\frac{2\pi ih}{p}} \frac{e^{2\pi ih} - 1}{e^{\frac{2\pi ih}{p}} - 1} = 0.$$

Als $t = 0$, dan is de integraal in de linkerzijde van (4.6) gelijk aan de lengte van het interval $[-\eta, 1 - \eta]$, dat is 1.

Stel nu $t \in \mathbb{Z}$ en $t \neq 0$. Door te gebruiken dat $e(t) = 1$ kunnen we de integraal expliciet berekenen:

$$\begin{aligned} \int_{-\eta}^{1-\eta} e(\alpha t) d\alpha &= \frac{1}{2\pi it} (e^{2\pi it(1-\eta)} - e^{-2\pi it\eta}) \\ &= \frac{1}{2\pi it} (e^{-2\pi it\eta} - e^{-2\pi it\eta}) = 0, \end{aligned}$$

waarmee ook (4.6) bewezen is.

Door wederom de identiteit $|e^{2\pi i\alpha} - 1| = 2 \sin |\pi\alpha|$ te gebruiken samen met de ongelijkheid $\sin x \leq x$ vinden we uiteindelijk ook (4.7). \square

Met behulp van deze eigenschappen voor de functie $e(\theta)$ en de eigenschappen van de functie $a(m)$ die al in de vorige sectie bewezen zijn, kunnen we nu een functionele ongelijkheid afleiden voor de functie $a(m)$. Dit bewijs komt overeen met sectie 4 in [4] en beslaat het grootste deel van dit hoofdstuk.

We formuleren eerst de ongelijkheid waarop we uiteindelijk met behulp van een lange integraal-afschatting zullen uitkomen. De cruciale stap hierin blijkt Propositie 4.6 te zijn. Deze Propositie, die in [4] in sectie 3 bewezen wordt, doet in de nieuwe notatie die hieronder gegeven is sterk denken aan Tao's Propositie 3.7.

Stelling 4.4. *Er bestaat een $c_1 > 0$ zo dat voor iedere even $m \in \mathbb{N}$ en $\delta > \frac{4}{m^4}$ de volgende ongelijkheid geldt:*

$$a^2(m) < c_1 (a(m)\delta + a^2(m)\delta^2 + (\delta^{-1}a(m) + 1)(a(m) - a(m^4) + m^{-1})). \quad (4.10)$$

Bewijs. Laat $m \in \mathbb{N}$ even en $N := \frac{m^4}{2}$.

Laat $A_2 \subset [1, 2N]$ een \mathcal{A}_3 -verzameling van maximale grootte, zodat $|A_2| = r_3(2N)$.

Laat E de verzameling van even getallen zijn en laat $A_1 := \frac{1}{2}(A_2 \cap E)$.

Het zal later van pas komen om enkele grove schattingen van de grootte van de verzamelingen A_r te hebben.

Merk hiertoe eerst op dat

$$|A_2| = r_3(2N) = 2Na(2N) \quad (4.11)$$

$$\leq 2Na(m) \quad (4.12)$$

waar de laatste ongelijkheid (4.12) direct volgt uit (4.1) omdat $2N = m^4$.

Merk verder op dat A_1 een \mathcal{A}_3 -verzameling in $[1, N]$ is wegens hetzelfde herschalingsargument als dat in het bewijs van Lemma 2.5, zodat

$$\begin{aligned} |A_1| &\leq Na(N) \\ &\leq Na(m), \end{aligned} \quad (4.13)$$

waar (4.13) weer volgt uit (4.1).

We zien dus dat voor $r = 1, 2$ geldt

$$|A_r| = O(Na(m)). \quad (4.14)$$

We kunnen $|A_1|$ ook van onderen afschatten door te bedenken dat uit de definitie van A_1 volgt dat $|A_1| = |A| - |A \cap O|$, waar O de verzameling van oneven getallen voorstelt. $A \cap O$ is een \mathcal{A}_3 -verzameling in $[1, 2N] \cap O$ en weer wegens Lemma 2.5 geldt dus $A \cap O \leq r_3(N)$, zodat

$$\begin{aligned} |A_1| &= |A| - |A \cap O| \geq 2Na(2N) - Na(N) \\ &\geq 2Na(2N) - Na(m), \end{aligned} \quad (4.15)$$

waar in de laatste stap wederom (4.1) gebruikt is.

Definieer de constante functie $\delta_m^r(n) := a(m)$ voor $n \in [1, rN]$.

We bekijken nu voor $\alpha \in \mathbb{R}$, $r = 1, 2$ de volgende functies:

$$f_r(\alpha) := rN \widehat{1_{A_r}}(-rN\alpha) = rN \mathbf{E}_{n \in [1, rN]} 1_{A_r}(n) \overline{e(-rN\alpha \cdot n)} = \sum_{n=1}^{rN} 1_{A_r}(n) e(n\alpha) \quad (4.16)$$

$$F_r(\alpha) := rN \widehat{\delta_m^r}(-rN\alpha) = rN \mathbf{E}_{n \in [1, rN]} \delta_m^r(n) \overline{e(-rN\alpha \cdot n)} = \sum_{n=1}^{rN} a(m) e(n\alpha). \quad (4.17)$$

De schrijfwijze uiterst rechts is de schrijfwijze die Roth in zijn oorspronkelijke artikel hanteerde, hij maakte nog geen gebruik van de in Hoofdstuk 1 besproken Fourier-technieken.

We kunnen deze functies direct met de driehoeksongelijkheid op grove wijze van boven afschatten door $O(Na(m))$. Voor het afschatten van f_r gebruiken we verder nog (4.14):

$$|f_r(\alpha)| \leq \sum_{n=1}^{rN} 1_{A_r}(n) |e(n\alpha)| = |A_r| = O(Na(m)), \quad (4.18)$$

$$|F_r(\alpha)| \leq a(m) \sum_{n=1}^{rN} |e(n\alpha)| = a(m)rN = O(Na(m)). \quad (4.19)$$

Met behulp van (4.6) en (4.17) vinden we een identiteit tussen $a(m)$ en een integraal van functies F_r :

$$\begin{aligned} \int_{-\frac{1}{2}}^{\frac{1}{2}} F_2(\alpha) F_1^2(-\alpha) d\alpha &= a^3(m) \sum_{j=1}^{2N} \sum_{k=1}^N \sum_{l=1}^N \int_{-\frac{1}{2}}^{\frac{1}{2}} e(\alpha(j-k-l)) d\alpha \\ &= a^3(m) |\{(j, k, l) \in [1, 2N] \times [1, N] \times [1, N] : j = k + l\}| \\ &= N^2 a^3(m), \end{aligned} \quad (4.20)$$

waar de laatste stap volgt uit het eenvoudige feit dat met ieder paar $(k, l) \in [1, N] \times [1, N]$ precies 1 $j \in [1, 2N]$ zo dat $j = k + l$ correspondeert en er natuurlijk N^2 van zulke paren (k, l) bestaan.

Aan de andere kant kunnen we op analoge wijze een identiteit afleiden voor de functies f_r . Voor iedere $\eta \in \mathbb{R}$ geldt:

$$\begin{aligned} \int_{-\eta}^{1-\eta} f_2(\alpha) f_1^2(-\alpha) d\alpha &= \sum_{j=1}^{2N} \sum_{k=1}^N \sum_{l=1}^N 1_{A_2}(j) 1_{A_1}(k) 1_{A_1}(l) \int_{-\eta}^{1-\eta} e(\alpha(j-k-l)) d\alpha \\ &= |\{(j, k, l) \in A_2 \times A_1 \times A_1 : j = k + l\}| \\ &= |A_1|, \end{aligned}$$

waar de laatste gelijkheid volgt uit het feit dat A_2 een \mathcal{A}_3 -verzameling is:

Als immers $(j, k, l) \in A_2 \times A_1 \times A_1$ zo dat $j = k + l$, dan is $j - 2k = l - k = 2l - j$, dus $(2k, j, 2l)$ is dan een rekenkundig rijtje van lengte drie in A_2 . Omdat A_2 een \mathcal{A}_3 -verzameling is kan dit alleen maar een triviaal rijtje van lengte 3 zijn, dus $k = l$ en $j = 2k$ voor $k \in A_1$ willekeurig. Er zijn dus inderdaad precies $|A_1|$ van zulke drietallen $(j, k, l) \in A_2 \times A_1 \times A_1$.

Met (4.13) vinden we dus dat:

$$\int_{-\eta}^{1-\eta} f_2(\alpha) f_1^2(-\alpha) d\alpha \leq Na(m). \quad (4.21)$$

Een laatste identiteit geeft de exacte waarde van $|f_1|^2$ geïntegreerd over $[0, 1]$:

$$\int_0^1 |f_1(\alpha)|^2 d\alpha = \sum_{n=1}^N 1_{A_1}(n) \int_0^1 e(n\alpha) \overline{e(n\alpha)} d\alpha = |A_1| = O(Na(m)). \quad (4.22)$$

We willen nu graag de functies F_r en f_r met elkaar vergelijken, omdat we voor beiden een verband met $a(m)$ gevonden hebben. Juist voor $a(m)$ willen we uiteindelijk een ongelijkheid afleiden.

We zijn dus in eerste instantie geïnteresseerd in de grootheid

$$f_r(\alpha) - F_r(\alpha) = rN \mathbf{E}_{n \in [1, rN]} (1_{A_r}(n) - a(m)) e(n\alpha), \quad (4.23)$$

die we kunnen afschatten door $\alpha \in \mathbb{R}$ met behulp van onderstaand Lemma 4.5 te benaderen door een breuk met een niet al te grote noemer q :

Lemma 4.5. *Voor iedere $\alpha \in \mathbb{R}, M \in \mathbb{N}$ bestaan er $h \in \mathbb{Z}, q \in \mathbb{N}$ zo dat $(h, q) = 1$ en β zo dat*

$$\alpha = \frac{h}{q} + \beta$$

met $q \leq M^{\frac{1}{2}}$ en $q|\beta| \leq M^{-\frac{1}{2}}$.

Bewijs. Uit het Kronecker Approximatielemma (Lemma 3.9) volgt dat er $0 < q < M^{\frac{1}{2}}$ bestaat zodat $\|q\alpha\|_{\mathbb{R}/\mathbb{Z}} \leq M^{-\frac{1}{2}}$. Er zijn nu twee mogelijkheden:

1. $q\alpha = \lfloor q\alpha \rfloor + \|q\alpha\|_{\mathbb{R}/\mathbb{Z}}$. Dan stellen we $h = \lfloor q\alpha \rfloor$.
2. $q\alpha = \lfloor q\alpha \rfloor + 1 - \|q\alpha\|_{\mathbb{R}/\mathbb{Z}}$. Dan stellen we $h = \lfloor q\alpha \rfloor + 1$.

In beide gevallen volgt het gestelde nu door te stellen $\beta := \alpha - \frac{h}{q}$, want $q|\beta| = |q\alpha - h| = \|q\alpha\|_{\mathbb{R}/\mathbb{Z}} \leq M^{-\frac{1}{2}}$. Merk op dat we mogen eisen dat $(h, q) = 1$ door de breuk $\frac{h}{q}$ zo ver mogelijk te vereenvoudigen. \square

Met behulp van de volgende propositie kunnen we nu een afchatting voor $f_r - F_r$ maken.

Propositie 4.6. *Laat $M \in \mathbb{N}$ en A een \mathcal{A}_3 -verzameling in $[1, M]$ zijn.*

Laat $\alpha \in \mathbb{R}$ willekeurig en $h \in \mathbb{Z}$, $q \in \mathbb{N}$, $\beta \in \mathbb{R}$ zoals in Lemma 4.5.

Dan geldt voor elke $m < M$:

$$|\mathbf{E}_{n \in [1, M]}(1_A(n) - a(m)1_{\{1\}}(q))e(n\alpha)| < a(m) - \frac{|A|}{M} + O(mM^{-\frac{1}{2}}). \quad (4.24)$$

Bewijs. We noteren

$$S := \sum_{n=1}^M 1_A(n)e(n\alpha),$$

$$S' := a(m)q^{-1} \left(\sum_{r=1}^q e\left(\frac{rh}{q}\right) \right) \left(\sum_{t=1}^M e(\beta t) \right).$$

Merk op dat uit (4.5) volgt dat $S' = 0$ als $q > 1$. Als $q = 1$ geldt dat $\alpha - \beta$ geheel is, dus $e(\beta t) = e(\alpha t)$. Dus we kunnen S' dan als volgt herschrijven:

$$S' = a(m)e(h) \left(\sum_{t=1}^M e(\beta t) \right) = \sum_{n=1}^M a(m)e(n\alpha),$$

zodat we zien dat $\frac{1}{M}|S - S'|$ gelijk is aan de linkerkant van (4.24).

Anderzijds kunnen we S' zien als benadering van S .

We beginnen met op te merken dat er voor iedere $n \in [1, M]$ precies mq gehele getallen t (namelijk alle t in het interval $(n - mq, n]$) bestaan zo dat

$$t \leq n < t + mq,$$

en dat deze getallen t ook allen element zijn van $[1, M]$ als $n \geq mq$, zodat we voor $n \geq mq$ de volgende identiteit hebben:

$$\frac{1}{mq} \sum_{t=1}^M 1_{[t, t+mq)}(n) = 1.$$

We kunnen dus de som S als volgt opsplitsen naar congruentieklassen modulo q :

$$\begin{aligned}
|S| &\leq \left| \sum 1_{[mq, M]}(n) 1_A(n) e(n\alpha) \right| + \left| \sum 1_{[1, mq]} 1_A(n) e(n\alpha) \right| \\
&\leq \left| \sum_{r=1}^q \sum_{n \equiv r} 1_{[mq, M]}(n) 1_A(n) e(n\alpha) \right| + mq \\
&= \left| \frac{1}{mq} \sum_{r=1}^q \sum_{t=1}^M \sum_{n \equiv r} 1_{[t, t+mq)}(n) 1_{[mq, M]}(n) 1_A(n) e(n\alpha) \right| + O(mq). \tag{4.25}
\end{aligned}$$

Laat $n \in A' := A \cap [t, t + mq) \cap \{n \equiv r \pmod{q}\}$. n is te schrijven als $r + qj$ met $\frac{t-r}{q} \leq j < \frac{t-r}{q} + m$. Verder is $A' \subseteq A$, dus A' is een \mathcal{A}_3 -verzameling en bovendien is A' een deelverzameling van een rekenkundige rij van m elementen en heeft dus hoogstens cardinaliteit $r_3(m)$ wegens het herschalingslemma, Lemma 2.5. We definiëren $D(t, m, q, r) := r_3(m) - |A'| \geq 0$.

Voor $n \in A'$ met $n = r + qj$ en $n = t + i$ voor zekere $i, j \in \mathbb{Z}_{\geq 0}$ en $i < mq$ kunnen we berekenen

$$e(\alpha n) = e\left(\left(\frac{h}{q} + \beta\right)n\right) = e\left(\frac{hr}{q}\right) e(hj) e(\beta(t+i)) = e\left(\frac{hr}{q}\right) e(\beta t) e(\beta i),$$

zodat

$$|e(\alpha n) - e\left(\frac{hr}{q}\right) e(\beta t)| \leq |e(\beta i) - 1| \leq 2\pi|\beta|mq,$$

waar de laatste afchatting volgt uit $i < mq$ en de ongelijkheid (4.7).

We hebben nu dus gezien dat de term $e(n\alpha)$ in (4.25) afgeschat kan worden door $e\left(\frac{hr}{q}\right) e(\beta t) + O(mq|\beta|)$. Door dit met behulp van de definitie van D in (4.25) in te vullen vinden we dat

$$S = \frac{1}{mq} \sum_{r=1}^q \sum_{t=1}^M \left((A(m) - D(t, m, q, r)) e\left(\frac{hr}{q}\right) e(\beta t) + O(mq|\beta|) \right) + O(mq),$$

en dus, met de definitie van S' :

$$S = S' - \frac{1}{mq} \sum_{r=1}^q \sum_{t=1}^M \left(D(t, m, q, r) e\left(\frac{hr}{q}\right) e(\beta t) \right) + O(mq) + O(Mmq|\beta|) \tag{4.26}$$

en in het bijzonder voor $\beta = 0$ en $h = 0$:

$$|A| = a(m)M - \frac{1}{mq} \sum_{r=1}^q \sum_{t=1}^M D(t, m, q, r) + O(mq).$$

We zien dus dat de term $\frac{1}{mq} \sum_{r=1}^q \sum_{t=1}^M D(t, m, q, r)$ afgeschat kan worden door $|A| - a(m)M + O(mq)$ en met behulp van de aannames $q \leq M^{\frac{1}{2}}$ en $q|\beta| \leq M^{-\frac{1}{2}}$ zien we dus uit (4.26) dat

$$|S - S'| \leq |A| - a(m)M + O(mM^{\frac{1}{2}}),$$

waarna delen door M nu de rechterzijde van (4.24) oplevert. \square

We zijn nu klaar om de volgende schatting te bewijzen:

$$f_r(\alpha) - F_r(\alpha) = O(N(a(m) - a(2N)) + N^{\frac{3}{4}}) \quad (4.27)$$

(Merk op dat de uitdrukking binnenin het grote O -symbool niet-negatief is: $a(m) - a(2N) = a(m) - a(m^4) \geq 0$ wegens (4.1).)

Deze afschatting komt in de rest van het bewijs vaak voor. Ter afkorting zullen we in het vervolg noteren:

$$g(m, N) := N(a(m) - a(2N)) + N^{\frac{3}{4}}.$$

Door Propositie 4.6 toe te passen met $M = rN$ blijkt dat

$$\begin{aligned} rN \left| \mathbf{E}_{n \in [1, M]} (1_{A_r}(n) - a(m)1_{\{1\}}(q)) e(n\alpha) \right| &< rNa(m) - |A_r| + O(mN^{\frac{1}{2}}) \\ &\leq rNa(m) - |A_r| + O(N^{\frac{3}{4}}), \end{aligned} \quad (4.28)$$

waarin de laatste ongelijkheid volgt uit $m = (2N)^{\frac{1}{4}}$.

Uit (4.11) zien we dat $|A_2| = O(Na(2N))$. Voor $|A_1|$ hebben we in (4.15) afgeleid dat $|A_1| \geq 2Na(2N) - Na(m)$. Deze schattingen geven als $q = 1$ wegens (4.23) nu direct (4.27).

Als we uit Lemma 4.5 toegepast op $M = rN$ alleen maar een $q > 1$ kunnen krijgen, dan merken we op dat $\|\alpha\|_{\mathbb{R}/\mathbb{Z}} > (rN)^{-\frac{1}{2}}$, want zo niet, dan zou de keuze $h = \alpha - \|\alpha\|_{\mathbb{R}/\mathbb{Z}}$ en $q = 1$ voldoen.

Dankzij (4.4) weten we dat

$$|F_r(\alpha)| = a(m) \left| \sum_{n=1}^{rN} e(n\alpha) \right| \leq a(m) \frac{1}{2\|\alpha\|_{\mathbb{R}/\mathbb{Z}}}, \quad (4.29)$$

dus omdat nu $\|\alpha\|_{\mathbb{R}/\mathbb{Z}} > (rN)^{-\frac{1}{2}}$ geldt zeker dat $F_r(\alpha) = O(N^{\frac{3}{4}})$. Omdat de linkerzijde van (4.28) voor $q \neq 1$ gelijk is aan $f_r(\alpha)$ volgt met de driehoeksongelijkheid nu ook (4.27).

We noteren vanaf nu de integranden in (4.20) en (4.21) korter: $\mathbf{F}(\alpha) := F_2(\alpha)F_1^2(-\alpha)$ en $\mathbf{f}(\alpha) := f_2(\alpha)f_1^2(-\alpha)$.

Met een algebraïsch truukje kunnen we nu (4.27) ook gebruiken om het verschil van de integranden \mathbf{f} en \mathbf{F} af te schatten. Er geldt immers:

$$|f_2 f_1^2 - F_2 F_1^2| = |f_2(f_1^2 - F_1^2) + F_1^2(f_2 - F_2)| \leq |f_2(f_1 + F_1)(f_1 - F_1)| + |F_1^2(f_2 - F_2)|,$$

en door hier de schattingen (4.27), (4.18) en (4.19) te gebruiken zien we uiteindelijk dat

$$\mathbf{f} - \mathbf{F} = f_2(\alpha)f_1^2(-\alpha) - F_2(\alpha)F_1^2(-\alpha) = O((Na(m))^2g(m, N)) \quad (4.30)$$

Om de uiteindelijke ongelijkheid te bereiken moeten we van de integraal in (4.20), waarvan we de exacte uitkomst kennen, naar de integraal in (4.21) zien te komen.

Zij $\delta > \frac{4}{m^4}$. Kies $\eta := (N\delta)^{-1}$, dan geldt $0 < \eta = 2m^{-4}\delta^{-1} < \frac{1}{2}$.

We kunnen nu de integraal van \mathbf{F} als volgt afschatten door de integraal van \mathbf{f} plus resttermen:

$$\begin{aligned} \left| \int_{-\frac{1}{2}}^{\frac{1}{2}} \mathbf{F} d\alpha \right| &\leq \left| \int_{-\eta}^{\eta} \mathbf{F} d\alpha \right| + 2 \left| \int_{\eta}^{\frac{1}{2}} \mathbf{F} d\alpha \right| \\ &\leq \left| \int_{-\eta}^{\eta} \mathbf{f} d\alpha \right| + \left| \int_{-\eta}^{\eta} (\mathbf{f} - \mathbf{F}) d\alpha \right| + 2 \left| \int_{\eta}^{\frac{1}{2}} \mathbf{F} d\alpha \right| \\ &\leq \left| \int_{-\eta}^{1-\eta} \mathbf{f} d\alpha \right| + \left| \int_{\eta}^{1-\eta} \mathbf{f} d\alpha \right| + \int_{-\eta}^{\eta} |\mathbf{f} - \mathbf{F}| d\alpha + 2 \left| \int_{\eta}^{\frac{1}{2}} \mathbf{F} d\alpha \right| \end{aligned} \quad (4.31)$$

De eerste integraal in (4.31) is nu de integraal die we wilden hebben, terwijl de derde integraal zich laat afschatten met behulp van (4.30).

De tweede en de vierde integraal moeten nog voldoende scherp afgeschat worden. Voor het afschatten van de vierde integraal blijkt (4.29) voldoende:

$$2 \left| \int_{\eta}^{\frac{1}{2}} \mathbf{F} d\alpha \right| \leq 2a^3(m) \int_{\eta}^{\frac{1}{2}} \left(\frac{1}{2\alpha} \right)^3 d\alpha = 2a^3(m) \frac{1}{8} (\eta^{-2} - 4) = O(a^3(m)\eta^{-2})$$

De tweede integraal in (4.31) is ten slotte af te schatten door eerst te gebruiken dat vanwege (4.27) geldt $f_2 = F_2 + O(g(m, N))$, en $F_2 = O(a(m)\eta^{-1})$ vanwege (4.29) en de triviale ongelijkheid $\|\alpha\|_{\mathbb{R}/\mathbb{Z}} \geq \eta$ op het integratie-interval $[\eta, 1 - \eta]$.

Dus:

$$\begin{aligned} \left| \int_{\eta}^{1-\eta} \mathbf{f} d\alpha \right| &\leq \int_{\eta}^{1-\eta} |f_2(\alpha)| \cdot |f_1(-\alpha)|^2 d\alpha \\ &\leq O(a(m)\eta^{-1} + g(m, N)) \int_{\eta}^{1-\eta} |f_1(-\alpha)|^2 d\alpha \\ &= O(\{a(m)\eta^{-1} + g(m, N)\}Na(m)), \end{aligned}$$

waar de laatste ongelijkheid volgt uit (4.22).

Als we nu de afschattingen en aan de linkerkzijde de exact berekende integraal invullen in (4.31) vinden we:

$$\begin{aligned} N^2 a^3(m) &= \left| \int_{-\frac{1}{2}}^{\frac{1}{2}} \mathbf{F} d\alpha \right| \\ &\leq O(Na(m)) + O(\{a(m)\eta^{-1} + g(m, N)\}Na(m)) + O((Na(m))^2g(m, N)\eta) + O(a^3(m)\eta^{-2}) \end{aligned}$$

Na delen door $N^2a(m)$ en bij elkaar nemen van termen geeft dit:

$$\begin{aligned} a^2(m) &= O(N^{-1} + \{a(m)\eta^{-1} + g(m, N)\}N^{-1} + a(m)g(m, N)\eta + a^2(m)N^{-2}\eta^{-2}) \\ &= O(a(m)N^{-1}\eta^{-1} + a^2(m)N^{-2}\eta^{-2} + g(m, N)(N^{-1} + a(m)\eta) + N^{-1}) \\ &= O(a(m)N^{-1}\eta^{-1} + a^2(m)N^{-2}\eta^{-2} + (a(m) - a(2N) + N^{-\frac{1}{4}})(1 + Na(m)\eta)), \end{aligned}$$

waar in de laatste stap de term $O(N^{-1})$ wegvalt omdat $N^{-1} \leq N^{-\frac{1}{4}}$ voor alle N . Door hier nu $\eta = (N\delta)^{-1}$ en $2N = m^4$ in te vullen vinden we:

$$a^2(m) = O(a(m)\delta + a^2(m)\delta^2 + (a(m) - a(m^4) + 2^{\frac{1}{4}}m^{-1})(1 + \delta^{-1}a(m))),$$

waaruit de gestelde ongelijkheid (4.10) nu direct volgt. □

4.3 De schatting voor $a(m)$

Gevolg 4.7. Voor iedere $x \in \mathbb{N}$ definiëren we $m(x) := 2^{4^x}$, $b(x) := a(m(x))$. De functie $b(x)$ heeft de volgende eigenschappen:

1. $b(x)$ is een dalende functie.
2. Er bestaan $c_3, c_4 > 0$ zo dat voor iedere $x > c_4$ geldt

$$b^2(x) < c_3 (b(x) - b(x+1) + 2^{-4^x}). \quad (4.32)$$

3. Er bestaat een $c_5 > 0$ zo dat als $P > c_4$ en $2Pb(2P) > 4c_5$, dan geldt

$$2Pb(2P) < Pb(P). \quad (4.33)$$

4. Er bestaat een $c_6 > 0$ zo dat voor alle x geldt

$$b(x) \leq c_6 x^{-1}.$$

Bewijs. De eerste bewering, dat b een dalende functie is, kunnen we direct afleiden uit (4.1), aangezien $b(x+1) = a(2^{4^{x+1}}) = a((2^{4^x})^3 2^{4^x}) \leq a(2^{4^x}) = b(x)$.

Voor de tweede bewering leiden we eerst uit (4.10) en de feiten $m(x+1) = m^4(x)$ en m is even af dat

$$b^2(x) < c_1(b(x)\delta + b^2(x)\delta^2 + (\delta^{-1}b(x) + 1)(b(x) - b(x+1) + 2^{-4^x})) \quad (4.34)$$

als $\delta > \frac{4}{m^4(x)}$.

We mogen hierin aannemen dat $c_1 \geq 1$.

Verder stellen we nu $\delta := \frac{1}{2c_1}b(x)$. We merken op dat de triviale ongelijkheid $a(m(x)) \geq \frac{1}{m(x)}$ volgt uit de definitie van a en de opmerking dat een verzameling van 1 element altijd een \mathcal{A}_3 -verzameling is.

We zien nu voor $m(x) > (8c_1)^{\frac{1}{3}}$ dat

$$\delta = \frac{1}{2c_1}b(x) \geq \frac{1}{2c_1m(x)} > \frac{4}{m^4(x)},$$

en omdat $m(x)$ naar oneindig gaat kunnen we c_4 zo kiezen dat inderdaad geldt $\delta \geq \frac{4}{m^4(x)}$ als $x > c_4$.

We zien verder uit de ongelijkheid $b(x) \leq 1$ en het invullen van de definitie van δ dat:

$$c_1(b(x)\delta + b^2(x)\delta^2) = \frac{b^2(x)}{2} + \frac{b^4(x)}{4c_1} \leq \frac{3}{4}b^2(x).$$

Door dit gegeven en de definitie van δ in te vullen in (4.34) zien we nu dat aan (4.32) voldaan is wanneer we $c_3 := 4c_1(1 + 2c_1)$ kiezen:

$$\begin{aligned} b^2(x) &< \frac{3}{4}b^2(x) + c_1(2c_1 + 1)(b(x) - b(x+1) + 2^{-4^x}), \\ \frac{1}{4}b^2(x) &< c_1(2c_1 + 1)(b(x) - b(x+1) + 2^{-4^x}). \end{aligned}$$

Om nu de derde bewering te bewijzen gebruiken we de eerste twee. Vanwege het feit dat b een dalende functie is kunnen we b voor grote waarden van x met behulp van (4.32) als volgt als een telescopsom schrijven:

$$\begin{aligned} Pb^2(2P) &= \sum_{x=P}^{2P-1} b^2(2P) \leq \sum_{x=P}^{2P-1} b^2(x) \\ &< c_3 \sum_{x=P}^{2P-1} (b(x) - b(x+1) + 2^{-4^x}) \\ &= c_3(b(P) - b(2P)) + c_3 \sum_{x=P}^{2P-1} 2^{-4^x}. \end{aligned}$$

We houden hier dus een restterm over. Deze kunnen we als volgt (grof) afschatten:

$$\sum_{x=P}^{2P-1} 2^{-4^x} < P2^{-4^P} < \frac{4c_5}{2P},$$

waar we zeker een geschikte $c_5 \geq c_3$ kunnen kiezen, aangezien

$$\lim_{P \rightarrow \infty} \frac{P^2}{2^{4^P}} = 0.$$

We zien dus dat voor deze c_5 geldt

$$Pb^2(2P) < c_5(b(P) - b(2P) + \frac{4c_5}{2P}).$$

Als nu $P > c_4$ en $2Pb(2P) > 4c_5$, dan geldt door $2Pb(2P)$ te vermenigvuldigen met $\frac{2Pb(2P)}{4c_5} (> 1)$ dat

$$2Pb(2P) < \frac{1}{4c_5} 4P^2b^2(2P) < P(b(P) - b(2P) + \frac{4c_5}{2P}) < Pb(P),$$

aangezien dan ook $\frac{4c_5}{2P} - b(2P) < 0$. Hiermee is de derde eigenschap bewezen.

De vierde eigenschap leiden we nu af uit de derde eigenschap.

Laat $t_0 := \lceil \log_2 c_4 \rceil > 0$ en $t > t_0$ een willekeurig geheel getal, zodat $c_4 < 2^{t_0} < 2^t$.

Claim. Voor alle $t > t_0$ geldt dat

$$2^t b(2^t) \leq \max(4c_5, 2^{t_0} b(2^{t_0})).$$

Bewijs Claim. Stel immers van niet. Dan bestaat er een kleinste $t_1 > t_0$ waarvoor dit niet geldt. Voor deze t_1 geldt dat $2^{t_1} b(2^{t_1}) > 4c_5$, zodat (4.33) geeft dat

$$2^{t_1} b(2^{t_1}) < 2^{t_1-1} b(2^{t_1-1}),$$

maar omdat $2^{t_1} b(2^{t_1}) > \max(4c_5, 2^{t_0} b(2^{t_0}))$ per aanname zou nu ook moeten gelden dat $2^{t_1-1} b(2^{t_1-1}) > \max(4c_5, 2^{t_0} b(2^{t_0}))$, hetgeen de minimale keuze van t_1 tegenspreekt. \square

Laat nu $C := \max\{xb(x) : x \leq 2^{t_0}\}$ en $c_6 := 2 \max(4c_5, 2^{t_0} b(2^{t_0}), C)$.

Voor $x \leq 2^{t_0}$ is nu per definitie voldaan aan $b(x) \leq c_6 x^{-1}$.

Als $x > 2^{t_0}$ dan bestaat er een $t \geq t_0$ zo dat $x \in (2^t, 2^{t+1}]$, dus, omdat b een dalende functie is, geldt

$$b(x) \leq b(2^t) \leq 2^{-t} \max(4c_5, 2^{t_0} b(2^{t_0})) \leq c_6 x^{-1},$$

waarmee de laatste bewering ook bewezen is. \square

Stelling 4.8. *Er bestaat een $C > 0$ zo dat voor iedere $m \in \mathbb{N}$ geldt*

$$a(m) < \frac{C}{\log \log m}.$$

Bewijs. Laat $m \in \mathbb{N}$ willekeurig. Er bestaat voor een vaste $c_7 > 0$ een $x > c_7 \log \log m$ zo dat $m > 2^{4^x}$. Er geldt nu wegens (4.2) dat

$$a(m) \leq (1 + m^{-1} 2^{4^x}) a(2^{4^x}) < 2a(2^{4^x}) = 2b(x),$$

en aangezien in Gevolg 4.7 bewezen is dat $2b(x) \leq c_6 x^{-1}$ zien we nu dat geldt

$$a(m) < \frac{2c_6}{x} < \frac{2c_6}{c_7 \log \log m},$$

dus als we $C := \frac{2c_6}{c_7}$ stellen is het gestelde bewezen. \square

Nawoord

Bij gebrek aan een voorwoord eindig ik deze scriptie met een nawoord, waarin ik kort verwijs naar wat ik uiteindelijk niet in deze scriptie heb opgenomen, maar wel in mijn onderzoek tegen ben gekomen.

Het begrip **lineaire afwijking** (Definitie 1.26) geeft aanleiding voor veel vragen, waarvan in deze scriptie slechts een klein deel beantwoord is. Ik noem enkele vragen uit het overgebleven deel.

- Hoe klein kan de lineaire afwijking van een verzameling A worden als gegeven is dat $\mathbf{P}_Z(A) = \delta$ voor vaste δ ? Hoe kunnen verzamelingen geconstrueerd worden die deze ondergrens bereiken?
- Hebben willekeurige verzamelingen (in de zin van Definitie 1.34) altijd een kleine lineaire afwijking?
- Hoe verhoudt de lineaire afwijking zich tot de ‘Gowers uniformity norms’ die in het bewijs van de stelling van Green-Tao gebruikt worden?

De stelling van Szemerédi is in deze scriptie alleen bewezen voor het geval $k = 3$. Tao bespreekt in zijn boek ook de gevallen $k > 3$, maar waarschuwt hierbij dat dit allerlei extra technieken vereist. In mijn onderzoek heb ik ervoor gekozen niet het hele bewijs van de stelling van Szemerédi te proberen te doorgronden, maar liever naast het bewijs in [8] ook het oorspronkelijke bewijs van Roth voor het geval $k = 3$ zoals hij dat in 1953 publiceerde [4] te bekijken.

Wat betreft andere toepassingen van de Fourier-analyse: in de getaltheorie heb ik tijdens mijn onderzoek ook het bewijs van de stelling van Dirichlet in [7] bestudeerd, maar niet in mijn scriptie opgenomen.

Een voordeel van deze keuzes is dat ik in het uiteindelijke verslag genoeg ruimte had om de twee bewijzen met ieder hun eigen invalshoek te bespreken.

Tot slot rest nog de vraag: hoe zit het met rekenkundige rijtjes in priemgetallen? Van het bewijs van de stelling van Green-Tao hoop ik misschien ooit nog een beter beeld te kunnen krijgen, maar het zal mogelijk nog enige tijd duren alvorens ik hiertoe voldoende wiskundige achtergrond bezit.

Euclides noemt priemgetallen in het citaat dat in de inleiding is opgenomen $\pi\rho\tilde{\omega}\tau\omicron\iota\ \acute{\alpha}\rho\iota\theta\mu\omicron\iota$, letterlijk ‘eerste getallen’, een mooie benaming, maar in het licht van het bovenstaande zou de naam $\xi\sigma\chi\alpha\tau\omicron\iota\ \acute{\alpha}\rho\iota\theta\mu\omicron\iota$ ook niet hebben misstaan.

Spelen met Verzamelingen (Populaire Samenvatting)

De wiskundige inhoud van deze scriptie is het beste uit te leggen met een eenvoudig gokspelletje.

Het spel gaat als volgt: ik neem een verzameling getallen in gedachten (ik geef de verzameling ook een naam: ik noem hem A), maar ik vertel jou niets over de verzameling A . Jouw doel is er achter te komen of er 3 getallen in mijn verzameling A voorkomen die **even ver** van elkaar af liggen. Als jij gelijk hebt, win jij, anders win ik.

Ik kan bijvoorbeeld de verzameling van alle ‘natuurlijke’ getallen in gedachten nemen: mijn verzameling A kan $\{1, 2, 3, 4, \dots\}$ zijn. Daar liggen **wel** 3 getallen in die even ver van elkaar af liggen, bijvoorbeeld 1, 2 en 3, maar ook 7, 10 en 13 zijn drie getallen in mijn verzameling A die even ver van elkaar af liggen.

Ik zou ook alleen maar de verzameling van even getallen in gedachten kunnen nemen, de verzameling A is dan $\{2, 4, 6, 8, \dots\}$. Ook deze verzameling heeft zeker 3 getallen die even ver van elkaar af liggen, bijvoorbeeld 4, 6 en 8 of 200, 300 en 400. Het maakt dus niet uit hóe ver de getallen van elkaar af liggen, als ze maar **even ver** van elkaar af liggen.

Stel nu dat ik de verzameling $A = \{2, 4, 8, 16, 32, \dots\}$ in gedachten neem, alle machten van twee. Komen in deze verzameling 3 getallen voor die even ver van elkaar af liggen?

Het antwoord is nee. De getallen in de verzameling A komen namelijk steeds verder van elkaar af te liggen: tussen 2 en 4 ligt slechts 1 getal, maar tussen 4 en 8 al 3 en tussen 16 en 32 liggen 15 getallen in; het lukt dus nooit om 3 getallen in de verzameling A te vinden die even ver van elkaar af liggen.

Als we het spel op deze manier spelen, weet jij nog niets over de verzameling die ik in gedachten neem en kun je dus alleen maar gokken of er wel of niet 3 getallen in de verzameling A even ver van elkaar af liggen. Een verzameling waarin **helemaal geen** 3 getallen voorkomen die even ver van elkaar af liggen, heet in deze scriptie een \mathcal{A}_3 -verzameling. De verzameling van twee-machten, $A = \{2, 4, 8, 16, 32, \dots\}$, is dus een voorbeeld van een \mathcal{A}_3 -verzameling.

We versoepelen de regels van het spel enigszins: jij mag mij één vraag stellen over mijn verzameling A . Dingen die je me natuurlijk niet mag vragen zijn “Is A een \mathcal{A}_3 -verzameling?”, of “Noem de getallen op die in A voorkomen”, of een andere vraag waardoor je onmiddellijk zou winnen (en waardoor wiskundigen het spel ‘triviaal’ zouden noemen).

Je zou bijvoorbeeld wél kunnen vragen:

“Hoeveel getallen zitten er in de verzameling A ?”

Als het aantal getallen in A minder is dan 3 (misschien heb ik wel alleen maar $A = \{17, 900\}$ in gedachten genomen), dan weet je alvast zeker dat er nooit 3 getallen in A even ver van elkaar af liggen, omdat er niet eens 3 getallen in A zitten.

Aan de andere kant, als ik $A = \{1, 2, 7\}$ in gedachten had genomen, dan is mijn antwoord op jouw vraag “3”, maar dat antwoord helpt jou niet echt verder: je weet nog steeds niet zeker of er drie getallen in A voorkomen die even ver van elkaar af liggen.

Vraag. *Welke vraag kun je mij het beste stellen?*

In 1953 bedacht wiskundige Klaus Roth een goede vraag. De vraag zag er op de manier waarop Roth hem opschreef nogal ingewikkeld uit, maar het idee is ook te volgen zonder de lastige wiskundige techniek precies te begrijpen.

De vraag van Roth bestaat uit de volgende 4 stappen (stap 4 geeft de eigenlijke vraag, waarop ik antwoord (a) of (b) kan geven):

1. Kies een willekeurig ‘grensgetal’ N .
2. Tel hoeveel getallen uit de verzameling A onder dat grensgetal N liggen.
3. Deel dit aantal door het grensgetal N .
4. Als je het grensgetal N heel groot kiest, ligt de uitkomst van stap 3 dan (a) steeds dichterbij 0, of (b) altijd meer dan een vaste marge van 0 af?

Stel dat mijn verzameling A bestaat uit alle even getallen.

Als ik dan bijvoorbeeld als grensgetal $N = 11$ kies (stap 1), dan zijn er 5 even getallen tot en met N (stap 2), deel ik dit vervolgens door 11 (stap 3), dan krijg ik als uitkomst $\frac{5}{11} \approx \frac{1}{2}$.

Als ik $N = 20$ kies, dan zijn er 10 even getallen tot en met N . Ik bereken dan bij stap 3 $\frac{10}{20} = \frac{1}{2}$. Hoe groot ik het grensgetal N ook kies, ik zie dat ik **niet** steeds dichterbij 0 komen, maar bij stap 3 altijd een uitkomst krijg die zeker meer dan een vaste marge, bijvoorbeeld $\frac{1}{4}$ van 0 af ligt. In stap 4 hierboven is (b) dus waar.

Als mijn antwoord (b) is, dan is het **zeker** dat mijn verzameling A **geen** \mathcal{A}_3 -verzameling is: Klaus Roth kon in 1953 **bewijzen** dat een verzameling A die het antwoord (b) oplevert altijd 3 getallen moet bevatten die even ver van elkaar af liggen.

De wiskundige formulering van ‘ A levert antwoord (b) op’ is ‘ A heeft **positieve bovendichtheid**’. Roth’s vraag was dus:

Heeft A positieve bovendichtheid?

De stelling van Roth ondersteunt de bewering dat dit een goede vraag is:

Stelling (Roth, 1953). *Als A positieve bovendichtheid heeft, dan is A geen \mathcal{A}_3 -verzameling.*

Roth kon het spel dus winnen, als ik een verzameling met positieve bovendichtheid had gekozen. In deze scriptie worden twee verschillende manieren besproken om te bewijzen dat de stelling van Roth waar is.

Je kunt je nu afvragen of het omgekeerde ook waar is:

Vraag. *Als er 3 getallen in A zijn die even ver van elkaar af liggen, heeft A dan altijd positieve bovendichtheid?*

Het antwoord op deze vraag is helaas nee. De vraag van Roth is wel goed, maar als mijn antwoord bij stap 4 hierboven (a) is, dan kan het nog steeds gebeuren dat er in mijn verzameling A tóch drie getallen zijn die even ver van elkaar af liggen. Jij kunt dan, nadat je je ene vraag verspeeld hebt, niets anders doen dan gokken.

Een voorbeeld van een verzameling waarbij dit zou gebeuren is de verzameling van alle priemgetallen.

Een **priemgetal** is een getal dat je niet kunt delen zonder een rest over te houden (behalve wanneer je deelt door 1 of het getal zelf).

Het getal 5 is dus een priemgetal, want als je 5 probeert te delen door 2 of 4, dan houd je een rest van 1 over, of als je 5 probeert te delen door 3, dan houd je een rest van 2 over. Je kunt er zelf door proberen achterkomen dat 19 bijvoorbeeld ook een priemgetal is. (104239 trouwens ook, maar dat is wat moeilijker uit te rekenen.)

Maar 20 is bijvoorbeeld geen priemgetal, want als je 20 deelt door 10 houd je geen rest over.

De verzameling van priemgetallen begint met 2, 3, 5, 7, 11, 13, ... en gaat zo eindeloos door. Dat er oneindig veel priemgetallen zijn, werd voor het eerst opgeschreven door Euclides van Alexandrië. Euclides was in 300 voor Christus de eerste die een wiskundig werk (*“Elementen”*) schreef, dat onder andere over priemgetallen ging. Sindsdien vragen wiskundigen zich af hoeveel **structuur** er in de priemgetallen zit: zijn de priemgetallen net zo gestructureerd als bijvoorbeeld de even getallen?

Uit al dit onderzoek is onder andere gebleken dat het antwoord op de vraag van Roth ‘Nee’ is (in wiskundige termen: de priemgetallen hebben geen positieve bovendichtheid, maar bovendichtheid gelijk aan nul).

Toch zijn er 3 priemgetallen die even ver van elkaar af liggen: 3, 5 en 7 bijvoorbeeld. Als ik de priemgetallen in gedachten heb genomen, geeft mijn antwoord op de vraag van Roth jou dus onvoldoende informatie.

Er is tot nu toe nog niemand die een handige vraag heeft bedacht waarmee jij altijd helemaal zeker kunt zijn dat je het spel wint; hoewel je van verzamelingen met positieve bovendichtheid dus zeker weet dat er 3 getallen in voorkomen die even ver van elkaar af liggen, kun je van een verzameling met bovendichtheid 0 niet uitsluiten dat er tóch 3 getallen in voorkomen die even ver van elkaar af liggen.

Wel zijn er uitbreidingen voor het spel bedacht: je zou in plaats van 3 getallen die even ver van elkaar af liggen, ook kunnen kijken naar meer getallen, 4 of 5 of 2000, die allemaal even ver van elkaar af liggen.

Een verzameling waarin nooit k getallen voorkomen die even ver van elkaar af liggen heet een \mathcal{A}_k -verzameling. Jouw doel wordt nu er achter te komen of mijn verzameling A een \mathcal{A}_k -verzameling is.

In 1975 bewees Endre Szemerédi dat de vraag over positieve bovendichtheid ook werkt voor de andere spellen:

Stelling (Szemerédi, 1975). *Als A positieve bovendichtheid heeft, dan is A geen \mathcal{A}_k -verzameling.*

In 2004 bewezen Ben Green en Terence Tao dat de priemgetallen, die bovendichtheid nul hebben, toch nooit een \mathcal{A}_k -verzameling zijn, hoe groot k ook is: er zijn altijd nog k priemgetallen die even ver van elkaar af liggen.

Stelling (Green-Tao, 2004). *De verzameling van priemgetallen is geen \mathcal{A}_k -verzameling, voor iedere k .*

Als ik het spel zou spelen, zou ik dus altijd voor mijn verzameling A de verzameling van priemgetallen kunnen kiezen om jou op het verkeerde been te zetten: de priemgetallen zijn altijd een \mathcal{A}_k -verzameling (het maakt niet uit wat k is), maar mijn antwoord op jouw vraag is altijd ‘Nee’.

Deze stelling is (misschien onverwacht, omdat hij er nu zo simpel uit ziet) moeilijk te bewijzen. En dat terwijl hierboven nog bleek dat het heel makkelijk is om 3 of 4 priemgetallen die even ver van elkaar af liggen op te schrijven.

Het lastige onderdeel van de stelling ligt besloten in het zinsdeel voor *iedere k* : we willen niet alleen 3,4 of 5 priemgetallen vinden die even ver van elkaar af liggen, we willen *ieder denkbaar aantal* priemgetallen dat even ver van elkaar af ligt.

In mijn scriptie bespreek ik de technieken die voor het bewijs van de stelling van Roth nodig zijn en die samen met andere technieken ook gebruikt kunnen worden voor de moeilijkere bewijzen van de stelling van Szemerédi en de stelling van Green-Tao. Deze technieken heten ‘Eindige Fourier-analyse’, vandaar het eerste deel van de titel.

De ‘Additieve Combinatoriek’ uit de titel van deze scriptie is niets anders dan het vakgebied dat vragen over verzamelingen stelt, zoals in de vorm van bovenstaand spel: wat voor informatie over verzamelingen is genoeg om iets te kunnen concluderen over hun structuur en eventuele regelmaat? Zoals bijvoorbeeld: wat voor informatie is voldoende om te kunnen concluderen dat een verzameling een \mathcal{A}_k -verzameling is?

Hoe Eindige Fourier-analyse werkt, staat beschreven in Hoofdstuk 1 van deze scriptie. De stelling van Szemerédi wordt in een aantal verschillende versies besproken in Hoofdstuk 2: de eerste versie lijkt erg op de spel-vorm die hierboven besproken is, de tweede versie is wiskundiger van aard, maar heeft als groot voordeel dat hierop de technieken van de Eindige Fourier-analyse makkelijker toe te passen zijn.

In de daaropvolgende hoofdstukken bespreek ik twee verschillende bewijzen van de stelling van Roth, in Hoofdstuk 3 het ‘moderne’ bewijs zoals Terence Tao dat geeft in zijn boek ‘Additive Combinatorics’ [8], in Hoofdstuk 4 het oorspronkelijke bewijs van Roth, zoals beschreven in zijn artikel uit 1953 [4], maar wel enigszins vertaald naar de moderne terminologie en technieken van de Eindige Fourier-analyse.

Al de hoofdstukken vereisen een zekere wiskundige voorkennis, de eerste twee jaar van een universitaire studie wiskunde moeten volstaan. In het bovenstaande hoop ik desalniettemin aan een breder publiek een indruk te hebben kunnen geven van de ‘smaak’ van het rijke vakgebied van de Additieve Combinatoriek.

Bibliografie

- [1] Euclides, *Elements*, ed. J. L. Heiberg, R. Fitzpatrick (<http://farside.ph.utexas.edu/euclid.html>)
- [2] B. Green, *Arithmetic progressions in sumsets*, *Geom. Funct. Anal.* **12** (2002), 584-597
- [3] B. Green, T. Tao, *The primes contain arbitrarily long arithmetic progressions* (2004), arXiv:math/0404188v5.
- [4] K. F. Roth, *On certain sets of integers*, *J. London Math. Soc.* **28** (1953), 245-252.
- [5] Victor Pessers, Sam van Gool, *Het optellen van deelverzamelingen van Abelse Groepen* (2006), tweedejaarsproject UvA.
- [6] D. J. S. Robinson, *A Course in the Theory of Groups*, Springer-Verlag New York Inc (1982).
- [7] E. M. Stein, R. Shakarchi, *Fourier Analysis: An Introduction*, Princeton University Press (2003).
- [8] T. Tao, V. Vu, *Additive Combinatorics*, Cambridge University Press (2006).