Jelle Bulthuis
jelle.bulthuis@outlook.com

Pro-eindige Fibonacci-getallen

Bachelorscriptie

Scriptiebegeleider: Prof. dr. H.W. Lenstra

Datum bachelorexamen: 30 juni 2015

Mathematisch Instituut, Universiteit Leiden

Inhoudsopgave

1 Inleiding

De rij van Fibonacci is een van de bekendste wiskundige rijen. Begin met een 0 en een 1, en maak elk volgende getal de som van zijn twee voorgangers. Dan begint de rij als:

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots$$

In dit onderzoek koppelen we deze rij aan een minder bekend wiskundig fenomeen: $\hat{\mathbb{Z}}$, de verzameling van pro-eindige getallen [1]. Onder een bepaalde metriek vormt deze verzameling een completering van $\mathbb{Z}$. In het eerste hoofdstuk zal deze verzameling preciezer gedefinieerd worden, en zullen enkele topologische eigenschappen bewezen worden. Ook zal de volgende stelling bewezen worden:

Stelling 2.13. Een functie $f : \mathbb{Z} \to \mathbb{Z}$ heeft een continue voortzetting $\hat{f} : \hat{\mathbb{Z}} \to \hat{\mathbb{Z}}$, dan en slechts dan als f periodiek is modulo elk geheel getal m, ongelijk aan 0.

In het tweede hoofdstuk zal dieper worden ingegaan op lineaire recurrenties, rijen waarvoor vanaf een zekere index geldt dat elk element een vaste lineaire combinatie van een eindig aantal voorgangers is. De hoofdvraag is of deze rijen een continue voortzetting tot $\hat{\mathbb{Z}}$ hebben. Dit zal leiden tot de volgende stelling:

Stelling 3.12. Zij $(a_n)_{n=0}^{\infty} \in \mathbb{Z}^{\mathbb{Z}_{\geq 0}}$ een eenzijdige lineaire recurrentie, en $a : \mathbb{Z}^{\mathbb{Z}_{\geq 0}} \to \mathbb{Z}, n \mapsto a_n$ de bijbehorende afbeelding. Dan geldt: a heeft een continue voortzetting tot $\hat{\mathbb{Z}}$, dan en slechts dan als de rij een voortzetting heeft tot een lineaire recurrentie $(a_n)_{n\in\mathbb{Z}} \in \mathbb{Z}^{\mathbb{Z}}$.

Het zal blijken dat het bestaan van voortzettingen naar $\hat{\mathbb{Z}}$ sterk samenhangt met de periodiciteit van afbeeldingen of rijen, modulo gehele getallen ongelijk aan 0. In het laatste hoofdstuk zal het gedrag van de Fibonacci-rij bestudeerd worden, en zal voor $m \in \mathbb{Z}_{\geq 1}$ een bovengrens voor de minimale periode modulo m bepaald worden.

2 Pro-eindige getallen

Om pro-eindige getallen te introduceren is het belangrijk om op te merken dat elk geheel getal a uniek afhangt van zijn restklassen:

$$(a \bmod 1, a \bmod 2, a \bmod 3, \ldots) \in \prod_{m=1}^{\infty} \mathbb{Z}/m\mathbb{Z}.$$

Immers, als twee getallen corresponderen met dezelfde representatie, dan correspondeert hun verschil met $(0, 0, 0, \ldots)$, en het enige getal dat restklasse 0 heeft modulo elk positief getal is 0 zelf. Ook geldt dat voor elke $n, n' \in \{1, 2, \ldots\}$ met $n'|n$, de restklassen 'kloppen', in de zin dat geldt:

$$((a \bmod n) \bmod n') = (a \bmod n').$$

Het is niet moeilijk om een representatie op te schrijven die wel voldoet aan al deze modulo-eisen, maar niet correspondeert met een element uit $\mathbb{Z}$. Laat

deze representatie bijvoorbeeld restklasse 0 hebben modulo elk oneven getal, maar restklasse 1 modulo machten van 2. Dan begint de representatie als volgt: $(0, 1, 0, 1, 0, 3, 0, 1, 0, 5, \dots)$. Deze representatie voldoet per constructie aan de modulo-eisen, maar correspondeert niet met een geheel getal: Het enige gehele getal dat een veelvoud is van alle oneven priemmachten is 0, maar 0 heeft niet restklasse $(1 \mod 2)$. Dit geeft aanleiding tot de definitie van pro-eindige getallen.

Definitie 2.1. De *verzameling van pro-eindige getallen* is:

$$\hat{\mathbb{Z}} := \left\{ a = (a_1, a_2, \dots) \in \prod_{m=1}^{\infty} \mathbb{Z}/m\mathbb{Z} : \forall n, n' \in \mathbb{Z}_{\geq 1} : n' | n \Rightarrow a_n \equiv a_{n'} \mod n' \right\}.$$

Als product van ringen is $\prod_{m=1}^{\infty} \mathbb{Z}/m\mathbb{Z}$ zelf ook een ring. De bewerkingen zijn coördinaatsgewijze optelling en vermenigvuldiging. Het nul-element is $(0, 0, \dots)$ en het eenheidselement is $(1, 1, \dots)$. Het is eenvoudig te controleren dat $0, 1 \in \hat{\mathbb{Z}}$, en dat voor $x, y \in \hat{\mathbb{Z}}$ geldt dat $x + y, xy, -x \in \hat{\mathbb{Z}}$, en dus is $\hat{\mathbb{Z}}$ een deelring van deze productring. Ook is duidelijk dat we $\mathbb{Z}$ als deelring kunnen inbedden in $\hat{\mathbb{Z}}$ via de afbeelding $\phi : \mathbb{Z} \hookrightarrow \hat{\mathbb{Z}}, a \mapsto (a \mod 1, a \mod 2, \dots)$.

We definiëren de volgende afbeelding op $\mathbb{Z}$:

$$\begin{aligned} d &: \mathbb{Z} \times \mathbb{Z} \to \mathbb{R}_{\geq 0}, \\ &(a, b) \mapsto \begin{cases} 0 & , \text{ als } a = b, \\ 1/\min\{n \in \mathbb{Z}_{\geq 1} : a \not\equiv b \bmod n\} & , \text{ anders.} \end{cases} \end{aligned}$$

Het is eenvoudig te controleren dat dit een metriek is op $\mathbb{Z}$. Deze metriek zegt dat elementen $a, b \in \mathbb{Z}$ dicht bij elkaar liggen als de eerste $n \in \mathbb{Z}_{\geq 1}$ waarvoor ze niet overeenkomen modulo n, groot is. Onder deze metriek is $\hat{\mathbb{Z}}$ de completering van $\mathbb{Z}$. De notatie van elementen van $\hat{\mathbb{Z}}$ in de vorm van rijtjes is handig omdat dit het uitvoeren van de operaties gemakkelijk maakt, maar het is natuurlijker om erover na te denken als getallen die niet op te schrijven zijn, maar wel uniek te herkennen zijn aan hun gedrag modulo de gehele getallen.

2.1 Topologie op $\hat{\mathbb{Z}}$

We definiëren een topologie op $\hat{\mathbb{Z}}$ als volgt: Geef elke $\mathbb{Z}/m\mathbb{Z}$ de discrete topologie. Op $\prod_{m=1}^{\infty} \mathbb{Z}/m\mathbb{Z}$ leggen we de bijbehorende producttopologie. Vervolgens krijgt $\hat{\mathbb{Z}}$ als deelverzameling van $\prod_{m=1}^{\infty} \mathbb{Z}/m\mathbb{Z}$ de geïnduceerde topologie.

Voor een product van topologische ruimten $\{X_i\}_{i \in I}$ geldt dat een basis voor de producttopologie wordt gegeven door deelverzamelingen van de vorm:

$$V = \prod_{i \in I} V_i,$$

waarbij $V_i \subset X_i$ open is, en $V_i \neq X_i$ voor slechts eindig veel i. Hiermee kunnen we de open verzamelingen van $\hat{\mathbb{Z}}$ als volgt karakteriseren:

Feit 2.2. Een verzameling $U \subset \hat{\mathbb{Z}}$ is open, dan en slechts dan als er voor elke $x \in U$ een $N \in \mathbb{Z}_{\geq 1}$ bestaat zodat $\{y \in \hat{\mathbb{Z}} : y_N = x_N\} \subset U$.

Bewijs. Voor de implicatie van links naar rechts, laat U in $\hat{\mathbb{Z}}$ open. Dan geldt dat $U = U' \cap \hat{\mathbb{Z}}$ voor een zekere open $U' \subset \prod_{m=1}^{\infty} \mathbb{Z}/m\mathbb{Z}$. Deze U' is per definitie een vereniging van verzamelingen van de vorm $V = \prod_{m=1}^{\infty} U_m$ met $U_m \subset \mathbb{Z}/m\mathbb{Z}$ en $U_m \neq \mathbb{Z}/m\mathbb{Z}$ voor slechts eindig veel m. Laat nu $x \in U$. Dan geldt $x \in V$ voor een zekere V van bovenstaande vorm, en dan $\{x_m\} \subset U_m$ voor alle m. Laat nu J de indexverzameling zijn van alle m waarvoor $U_m \neq \mathbb{Z}/m\mathbb{Z}$. Laat $N := \text{kgv}\{m : m \in J\}$, en $W := \{y \in \hat{\mathbb{Z}} : y_N = x_N\}$. Als nu geldt dat $z \in W$, dan $z \equiv x_m \mod m$ voor alle $m \in J$, dus geldt dat $z \in U'$, zodat $z \in U$.

Voor de andere implicatie, stel dat er voor elke $x \in U$ een $N_x \in \mathbb{Z}_{\geq 1}$ bestaat zodanig dat $V_x := \{y \in \hat{\mathbb{Z}} : y_{N_x} = x_{N_x}\} \subset U$. Dan, omdat $x \in V_x$ voor elke $x \in U$, geldt:

$$U = \bigcup_{x \in U} V_x = \bigcup_{x \in U} \left(\{y \in \prod_{m=1}^{\infty} \mathbb{Z}/m\mathbb{Z} : y_{N_x} = x_{N_x}\} \cap \hat{\mathbb{Z}} \right)$$

Per definitie is $\{y \in \prod_{m=1}^{\infty} \mathbb{Z}/m\mathbb{Z} : y_{N_x} = x_{N_x}\}$ open in $\prod_{m=1}^{\infty} \mathbb{Z}/m\mathbb{Z}$, dus is elke V_x open in $\hat{\mathbb{Z}}$. Dan is U de vereniging van open verzamelingen, dus zelf ook open. □

Feit 2.3. De topologische ruimte $\hat{\mathbb{Z}}$ is compact en Hausdorff.

Bewijs. De verzamelingen $\mathbb{Z}/m\mathbb{Z}$ zijn discreet, dus Hausdorff. Het product van Hausdorff-ruimtes is ook Hausdorff, dus $\prod_{m=1}^{\infty} \mathbb{Z}/m\mathbb{Z}$ is dit ook. Een deelruimte van een Hausdorff-ruimte is ook Hausdorff, dus $\hat{\mathbb{Z}}$ ook.

De verzamelingen $\mathbb{Z}/m\mathbb{Z}$ zijn eindig, dus compact. De stelling van Tychonoff zegt dat het product van compacte ruimtes ook compact is, dus is $\prod_{m=1}^{\infty} \mathbb{Z}/m\mathbb{Z}$ compact. We moeten nu laten zien dat $\hat{\mathbb{Z}} \subset \prod_{m=1}^{\infty} \mathbb{Z}/m\mathbb{Z}$ gesloten is, zodat $\hat{\mathbb{Z}}$ als gesloten deelverzameling van een compacte ruimte zelf ook compact is.
Om te laten zien dat $\hat{\mathbb{Z}}$ gesloten is, laten we zien dat het complement, $\hat{\mathbb{Z}}^C$, open is. Laat $x \in \hat{\mathbb{Z}}^C$. Dan zijn er per definitie $n, n' \in \mathbb{Z}_{\geq 1}$ zodanig dat $a_n \neq a_{n'} \mod n'$, dus geldt dat $x \in V := \{y \in \prod_{m=1}^{\infty} \mathbb{Z}/m\mathbb{Z} : y_n = x_n \wedge y_{n'} = x_{n'}\}$. Deze verzameling is open in $\prod_{m=1}^{\infty} \mathbb{Z}/m\mathbb{Z}$. Voor elke $y \in V$ geldt dat $y_n \not\equiv y_{n'} \mod n'$, dus geldt dat $y \notin \hat{\mathbb{Z}}$, zodat $V \subset \hat{\mathbb{Z}}^C$. Hieruit volgt dat $\hat{\mathbb{Z}}^C$ open is, dus is $\hat{\mathbb{Z}}$ gesloten. We concluderen dat $\hat{\mathbb{Z}}$ compact is. □

Feit 2.4. Voor elke $d \in \mathbb{Z}$ ligt $\mathbb{Z}_{\geq d}$ dicht in $\hat{\mathbb{Z}}$.

Bewijs. Laat $d \in \mathbb{Z}$ gegeven, en laat $x \in \hat{\mathbb{Z}}$ en U een open omgeving van x. Omdat U open is, is er een $N \in \mathbb{Z}_{\geq 1}$ zodanig dat $\{y \in \hat{\mathbb{Z}} : y_N = x_N\} \subset U$. Er is een $y \in \{0, \ldots, N\} \subset \mathbb{Z}$ met $y \equiv x \mod N$, dus $U \cap \mathbb{Z} \neq \emptyset$. Geldt nu dat $y < d$, dan kunnen we een veelvoud van N bij y optellen, om een element uit $U \cap \mathbb{Z}_{\geq d}$ te verkrijgen. Hieruit volgt dat $\mathbb{Z}_{\geq d}$ dicht ligt in $\hat{\mathbb{Z}}$ voor elke $d \in \mathbb{Z}$. □

2.2 Een verband met de p-adische getallen

Er is een natuurlijke manier om $\hat{\mathbb{Z}}$ in verband te brengen met de p-adische getallen. Hiervoor hebben we eerst een aantal begrippen nodig.

Definitie 2.5. Een *topologische ring* R is een ring met een topologie zodanig dat de volgende afbeeldingen continu zijn:

- $R \times R \to R, (x, y) \mapsto x + y$
- $R \times R \to R, (x, y) \mapsto xy$
- $R \to R, x \mapsto -x$

Een *isomorfisme van topologische ringen* is een afbeelding tussen topologische ringen die zowel een ringisomorfisme als een homeomorfisme is.

Het is eenvoudig te controleren dat $\hat{\mathbb{Z}}$ met de gegeven topologie een topologische ring vormt.

Laat nu $\mathcal{P}$ de verzameling van priemgetallen in $\mathbb{Z}_{\geq 1}$ zijn.

Definitie 2.6. Voor $p \in \mathcal{P}$ is *de ring der p-adische getallen*:

$$\mathbb{Z}_p := \left\{ (a_1, a_p, a_{p^2}, \dots) \in \prod_{m=0}^{\infty} \mathbb{Z}/p^m\mathbb{Z} : \forall n \in \mathbb{Z}_{\geq 1} : a_{p^{n+1}} \equiv a_{p^n} \mod p^n \right\}.$$

Als we, analoog aan $\hat{\mathbb{Z}}$, ringoperaties en een topologie op $\mathbb{Z}_p$ definiëren, blijkt dat $\mathbb{Z}_p$ ook een topologische ring vormt. Met hetzelfde argument als bij $\hat{\mathbb{Z}}$ volgt dat $\mathbb{Z}_p$ ook Hausdorff is.

Stelling 2.7. De volgende afbeelding is een isomorfisme van topologische ringen:

$$\begin{aligned} \phi : \hat{\mathbb{Z}} &\to \prod_{p \in \mathcal{P}} \mathbb{Z}_p, \\ (a_1, a_2, \dots) &\mapsto \left((a_{p^m})_{m=0}^{\infty} \right)_{p \in \mathcal{P}}. \end{aligned}$$

Bewijs. Het is duidelijk dat $\phi(0) = 0$, en dat $\phi(1) = 1$. Omdat voor elke priemmacht p^m, en alle $a, b \in \hat{\mathbb{Z}}$ geldt dat $(a + b)_{p^m} = a_{p^m} + b_{p^m}$ en dat $(ab)_{p^m} = a_{p^m} b_{p^m}$, volgt direct dat ϕ een ringhomomorfisme is.
Laat nu $x \in \ker \phi$. Dan geldt dat $x \equiv 0 \mod p^m$ voor elke priemmacht p^m, dus x is een veelvoud van elke priemmacht. Wegens de Chinese Reststelling geldt dan dat $x \equiv 0 \mod n$ voor elke $n \in \mathbb{Z}$, dus volgt dat $x = (0, 0, \dots) = 0$. Hieruit volgt dat ϕ injectief is.
Laat nu $\left((y_{p^m})_{m=0}^{\infty} \right)_{p \in \mathcal{P}} \in \prod_{p \in \mathcal{P}} \mathbb{Z}_p$. Voor surjectiviteit moeten we een $x \in \hat{\mathbb{Z}}$ construeren met $\phi(x) = y$. Laat $x_{p^m} = y_{p^m}$ voor elke priemmacht p^m. Laat nu $n \in \mathbb{Z}_{\geq 1}$ gegeven. Dit getal heeft een unieke priemfactorisatie $n = \prod_{p \in \mathcal{P}} p^{k_p}$ met $k_p = 0$ voor bijna alle $p \in \mathcal{P}$. De Chinese Reststelling zegt nu dat:

$$\mathbb{Z}/n\mathbb{Z} \cong \prod_{p \in \mathcal{P}} \mathbb{Z}/p^{k_p}\mathbb{Z}.$$

Omdat de restklassen van x modulo priemmachten bekend zijn, ligt hiermee ook de restklasse modulo n vast voor alle $n \in \mathbb{Z}_{\geq 1}$. We moeten nog laten zien dat de verkregen x een element van $\hat{\mathbb{Z}}$ is. Stel dat dit niet het geval is. Dan zijn er $n, n' \in \mathbb{Z}_{\geq 1}$ met $n' | n$ zodanig dat $a_n \not\equiv a_{n'} \mod n'$. Dan moet er

een priemmacht p^m zijn met $p^m | n'$, zodanig dat $a_n \not\equiv a_{n'} \mod p^m$. Maar per constructie geldt dat $a_n \equiv a_{p^m} \mod p^m$ en $a_{n'} \equiv a_{p^m} \mod p^m$. Dit geeft een tegenspraak, en dus volgt dat $x \in \hat{\mathbb{Z}}$. Dus is ϕ surjectief. We moeten nog laten zien dat ϕ een homeomorfisme is.

Voor topologische ruimten $Y, (X_i)_{i \in I}$ zegt de universele eigenschap dat een afbeelding $f : Y \to \prod_{i \in I} X_i$ continu is, dan en slechts dan als de samenstelling van f met elk van de projecties $\pi_j : \left(\prod_{i \in I} X_i\right) \to X_j$ continu is. Ook geldt voor topologische ruimten A, B, C met $B \subset C$: Als B de deelruimtetopologie van C krijgt, dan is een afbeelding $g : A \to B$ continu, dan en slechts dan als de samenstelling van g met de inbedding $i : B \to C$ continu is.

Laat nu $l \in \mathcal{P}$, en $m \in \mathbb{Z}_{\geq 0}$. We noteren ϕ_l voor $\rho_l \circ \phi$ en $\phi_{l,m}$ voor $\pi_m \circ i \circ \rho_l \circ \phi$. Hier zijn ρ_l en π_m de projectie-afbeeldingen. We beschouwen het volgende diagram:

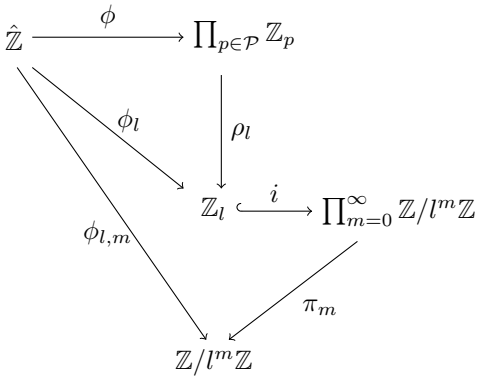


Diagram 1: Een commutatief diagram

We weten nu dat ϕ continu is, dan en slechts dan als ϕ_l continu is voor elke $l \in \mathcal{P}$, en dat ϕ_l continu is, dan en slechts dan als $i \circ \phi_l$ continu is. De afbeelding $i \circ \phi_l$ is een afbeelding naar een product van topologische ruimten, dus deze is continu, dan en slechts dan als $\rho_m \circ i \circ \phi_l = \phi_{l,m}$ continu is voor elke $m \in \mathbb{Z}_{\geq 0}$. De afbeelding $\phi_{l,m}$ is de projectie $\hat{\mathbb{Z}} \to \mathbb{Z}/l^m\mathbb{Z}, (a_1, a_2, \dots) \mapsto a_{l^m}$, en de topologie op $\hat{\mathbb{Z}}$ is zodanig gedefinieerd dat deze projectie continu is voor elke $l \in \mathcal{P}, m \in \mathbb{Z}_{\geq 0}$. Er volgt dat ϕ continu is. De afbeelding ϕ is nu een continue bijectie van een compacte ruimte naar een Hausdorff-ruimte, en is dus een homeomorfisme. □

Stelling 2.7 zegt dat een element $x \in \hat{\mathbb{Z}}$ uniek bepaald wordt door zijn gedrag modulo priemmachten, en deze stelling is hiermee het analogon van de Chinese Reststelling.

Opmerking 2.8. We kunnen nu de kardinaliteit van $\hat{\mathbb{Z}}$ bepalen. We noteren $2^{\aleph_0}$ voor de kardinaliteit van de $\mathbb{R}$. We weten: $\#\hat{\mathbb{Z}} \leq \#\prod_{m=1}^{\infty} \mathbb{Z}/m\mathbb{Z} = 2^{\aleph_0}$. Wegens Stelling 2.7 geldt nu dat $\#\hat{\mathbb{Z}} = \#\prod_{p \in \mathcal{P}} \mathbb{Z}_p \geq \#\{0,1\}^{\mathcal{P}} = 2^{\aleph_0}$. We

concluderen dat de kardinaliteit van $\hat{\mathbb{Z}}$ gelijk is aan die van $\mathbb{R}$. Hiermee hebben we opnieuw bewezen dat $\mathbb{Z} \subsetneq \hat{\mathbb{Z}}$, dus dat $\mathbb{Z}$ een strikte deelverzameling van $\hat{\mathbb{Z}}$ is.

Opmerking 2.9. Er geldt dat $\mathbb{Z}\backslash\{0\}$ geen nuldelers bevat in $\hat{\mathbb{Z}}$: Stel dat er $a \in \mathbb{Z}\backslash\{0\}$ en $b \in \hat{\mathbb{Z}}$ bestaan met $ab = 0$. Wegens Stelling 2.7 geldt dan dat $0 = \phi(0) = \phi(ab) = \phi(a)\phi(b)$, en dus zijn $\phi(a), \phi(b)$ nuldelers in $\prod_{p\in\mathcal{P}} \mathbb{Z}_p$. Dan moet gelden dat $ab \equiv 0 \mod p^k$ voor elke $p \in \mathcal{P}$ en elke $k \in \mathbb{Z}_{\geq 0}$. Omdat $a \in \mathbb{Z}\backslash\{0\}$ geldt voor elke $p \in \mathcal{P}$ dat a slechts eindig veel factoren p bevat. Dit betekent dat moet gelden dat $\phi(b) \equiv 0 \mod p^k$ voor elke $p \in \mathcal{P}, k \in \mathbb{Z}_{\geq 0}$. Maar dan geldt dat $\phi(b) = 0$, en dus dat $b = 0$.

2.3 Convergentie en continuïteit in $\hat{\mathbb{Z}}$

Nu we weten hoe de topologie op $\hat{\mathbb{Z}}$ eruit ziet, kunnen we criteria geven voor de convergentie van rijtjes in $\hat{\mathbb{Z}}$. Ook wordt duidelijk welke functies $f : \mathbb{Z} \to \mathbb{Z}$ een continue voortzetting $\hat{f} : \hat{\mathbb{Z}} \to \hat{\mathbb{Z}}$ hebben.

Stelling 2.10. Een rij $\left(a^{(k)}\right)_{k=0}^{\infty} \subset \hat{\mathbb{Z}}$ convergeert in $\hat{\mathbb{Z}}$, dan en slechts dan als voor elke $n \in \mathbb{Z}_{\geq 1}$ de rij $\left(a_n^{(k)}\right)_{k=0}^{\infty} \subset \mathbb{Z}/n\mathbb{Z}$ uiteindelijk constant is.

Bewijs. Een rij $a^{(k)}$ convergeert naar a in $\hat{\mathbb{Z}}$, dan en slechts dan als voor elke open omgeving U van a geldt dat $a^{(k)} \in U$ voor bijna alle k. We weten dat er voor elke open omgeving U van a een $N \in \mathbb{Z}_{\geq 1}$ is zodat $V_N := \{y \in \hat{\mathbb{Z}} : y_N = a_N\}$ bevat is in U. Ook weten we dat de verzamelingen V_N open zijn. De convergentie van $a^{(k)}$ is dus equivalent met: Voor alle $N \geq 1$ bevat V_N bijna alle $a^{(k)}$, en dit betekent precies dat $\left(a_n^{(k)}\right)_{k=0}^{\infty}$ uiteindelijk constant wordt voor elke $n \geq 1$. □

Voorbeeld 2.11. De rij $(k!)_{k=0}^{\infty} \subset \mathbb{Z}$ convergeert in $\hat{\mathbb{Z}}$ naar 0.

Voorbeeld 2.12. Kies $b \in \mathbb{Z}_{\geq 0}$. Laat $a^{(0)} = b$ en $a^{(k+1)} = 2^{a^{(k)}}$ voor $k \geq 1$. Dan convergeert $\left(a^{(k)}\right)_{k=0}^{\infty}$ in $\hat{\mathbb{Z}}$.

Bewijs. Wegens Stelling 2.10 is het voldoende om te laten zien dat $\left(a^{(k)}\right)_{k=0}^{\infty}$ uiteindelijk constant is modulo n voor alle $n \in \mathbb{Z}_{\geq 1}$.
Voor $n = 1$ is dit triviaal, en voor $n = 2$ is het ook duidelijk waar, omdat $a^{(k)}$ even is voor alle $k \geq 2$.
We gebruiken inductie naar n. Zij $n \in \mathbb{Z}_{\geq 3}$ willekeurig gegeven. We onderscheiden de volgende gevallen:

- $n = 2^m$ voor zekere $m \geq 2$. Omdat $\left(a^{(k)}\right)_{k=0}^{\infty}$ een strikt stijgende rij in $\mathbb{Z}$ is, bestaat er een $k_0 \in \mathbb{Z}_{\geq 0}$ zodanig dat $a^{(k)} > m$ voor alle $k \geq k_0$. Dan geldt dat $n | a^{(k+1)}$ voor alle $k \geq k_0$, en dus is de rij $\left(a_n^{(k)}\right)_{k=0}^{\infty}$ uiteindelijk constant.
- Stel nu dat n oneven is. Dan geldt duidelijk dat n en 2 copriem zijn, dus uit de Kleine Stelling van Fermat volgt: $2^{\phi(n)} \equiv 1 \mod n$. Omdat $\phi(n) < n$ is er een $k_0 \in \mathbb{Z}_{\geq 1}$ zodat $a^{(k)} \equiv a^{(k+1)} \mod \phi(n)$ voor alle $k \geq k_0$. Dan volgt dat $a^{(k+1)} \equiv a^{(k+2)} \mod n$ voor $k \geq k_0$, dus is $\left(a^{(k)}\right)_{k=0}^{\infty}$ uiteindelijk constant modulo n.

- n is een product van 2^m voor zekere $m \in \mathbb{Z}_{\geq 1}$ en een oneven getal n'. Dan volgt uit de inductieveronderstelling dat $\left(a^{(k)}\right)$ uiteindelijk constant is modulo 2^m en modulo n'. Wegens de Chinese Reststelling is de rij dan ook uiteindelijk constant modulo n.

Hieruit volgt voor elke $n \geq 1$ dat de rij uiteindelijk constant is modulo n, en dus convergeert de rij in $\hat{\mathbb{Z}}$. □

Stel nu dat een afbeelding $f : \mathbb{Z} \to \mathbb{Z}$ gegeven is, en dat we een continue voortzetting $\hat{f} : \hat{\mathbb{Z}} \to \hat{\mathbb{Z}}$ willen construeren. Dan is duidelijk wat we moeten doen. Omdat $\mathbb{Z}$ dicht ligt in $\hat{\mathbb{Z}}$, moeten we voor elke $a \in \hat{\mathbb{Z}}$ een rij $\left(a^{(k)}\right)_{k=0}^{\infty} \subset \mathbb{Z}$ maken met $\lim_{k\to\infty} a^{(k)} = a$, en dan definiëren we $\hat{f}(a) := \lim_{k\to\infty} f\left(a^{(k)}\right)$. Het enige probleem is dat $\lim_{k\to\infty} f\left(a^{(k)}\right)$ in het algemeen niet hoeft te bestaan. De volgende stelling zegt ons welke functies continu kunnen worden voortgezet naar $\hat{\mathbb{Z}}$.

Stelling 2.13. Als $f : \mathbb{Z} \to \mathbb{Z}$ een afbeelding is, dan zijn equivalent:

1. Er bestaat een continue afbeelding $\hat{f} : \hat{\mathbb{Z}} \to \hat{\mathbb{Z}}$ met $\hat{f}|_{\mathbb{Z}} = f$.
2. Voor alle $m \in \mathbb{Z}_{\geq 1}$ bestaat er een $l_m \in \mathbb{Z}_{\geq 1}$, zodanig dat voor alle $n, n' \in \mathbb{Z}$ geldt: Als $n \equiv n' \mod l_m$, dan $f(n) \equiv f(n') \mod m$.

Bewijs. Stel dat er een continue uitbreiding $\hat{f} : \hat{\mathbb{Z}} \to \hat{\mathbb{Z}}$ bestaat. Laat dan $m \geq 0$ gegeven, en laat $x \in \hat{\mathbb{Z}}$. Definieer de open verzameling:

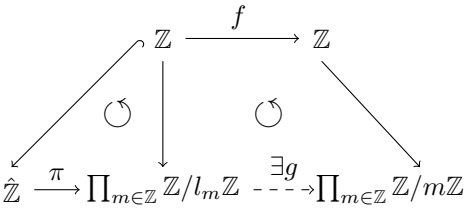
$$U_x := \{y \in \hat{\mathbb{Z}} : y \equiv \hat{f}(x) \mod m\}.$$

Wegens de continuïteit geldt dat $\hat{f}^{-1}(U_x)$ ook open is, dus is er een $N(x) \in \mathbb{Z}$ zodanig dat $V_x := \{z \in \hat{\mathbb{Z}} : z \equiv x \mod N(x)\} \subset \hat{f}^{-1}(U_x)$. Omdat elke $x \in \hat{\mathbb{Z}}$ bevat zit in V_x, vormen de V_x een open overdekking van $\hat{\mathbb{Z}}$. Uit de compactheid van $\hat{\mathbb{Z}}$ volgt een eindige deeloverdekking $\{V_x\}_{x\in I}$. Laat $l_m := \text{kgv}\{N(x) : x \in I\}$. Dan is $\hat{f}$ periodiek modulo m, met periode l_m.

Voor de andere implicatie kiezen we voor elke $m \geq 1$ zo'n $l_m \in \mathbb{Z}_{\geq 1}$. Dan hebben we het volgende commutatieve diagram:

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\quad f \quad} & \mathbb{Z} \\ \downarrow & \circlearrowleft & \downarrow \\ \mathbb{Z}/l_m\mathbb{Z} & \overset{\exists f_m}{\dashrightarrow} & \mathbb{Z}/m\mathbb{Z} \end{array}$$

Hier zijn de pijlen naar beneden de canonieke projecties. Als we al deze diagrammen samenvoegen, krijgen we:



Hier is $\pi : \hat{\mathbb{Z}} \to \prod_{m\in\mathbb{Z}} \mathbb{Z}/l_m\mathbb{Z}, a \mapsto (a_{l_m})_{m=1}^{\infty}$ het product van projecties, en dus continu. Definieer nu $\hat{f} = g \circ \pi : \hat{\mathbb{Z}} \to \prod_{m\in\mathbb{Z}} \mathbb{Z}/m\mathbb{Z}$. Wegens Stelling 2.10 is deze afbeelding continu. Omdat het diagram commuteert, geldt dat $\hat{f}|_{\mathbb{Z}} = f$, dus geldt dat $\hat{f}^{-1}(\hat{\mathbb{Z}}) \supset \mathbb{Z}$, dus ook $\overline{\hat{f}^{-1}(\hat{\mathbb{Z}})} \supset \overline{\mathbb{Z}}$. Bij Feit 2.3 hebben we laten zien dat $\hat{\mathbb{Z}}$ gesloten is in $\prod_{m\in\mathbb{Z}} \mathbb{Z}/m\mathbb{Z}$, dus wegens de continuïteit is $\hat{f}^{-1}(\hat{\mathbb{Z}})$ ook gesloten. Volgens Feit 2.4 ligt $\mathbb{Z}$ dicht in $\hat{\mathbb{Z}}$, dus vinden we nu dat $\hat{\mathbb{Z}} \subset \hat{f}^{-1}(\hat{\mathbb{Z}})$, oftewel $\hat{f}(\hat{\mathbb{Z}}) \subset \hat{\mathbb{Z}}$. We concluderen dat $\hat{f} : \hat{\mathbb{Z}} \to \hat{\mathbb{Z}}$ de gevraagde afbeelding is. □

3 Lineaire recurrenties

Een recurrentie is een vergelijking die recursief een rij definieert. Als deze vergelijking een homogene vergelijking van graad 1 is, spreken we van een lineaire recurrentie. Het bekendste voorbeeld is de Fibonacci-reeks, gegeven door de vergelijking $F_n = F_{n-1} + F_{n-2}$, en startwaarden $F_0 = 0, F_1 = 1$. De rij wordt dan:

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots$$

We kunnen bij deze lineaire recurrentie de afbeelding

$$\begin{aligned} F : \mathbb{Z}_{\geq 0} &\to \mathbb{Z}, \\ n &\mapsto F_n \end{aligned}$$

definiëren. In dit hoofdstuk zal onderzocht worden voor welke lineaire recurrenties de bijbehorende afbeelding kan worden voortgezet tot een continue functie van $\hat{\mathbb{Z}}$ naar $\hat{\mathbb{Z}}$.

3.1 Definities en eigenschappen

Definitie 3.1. Een *eenzijdige lineaire recurrentie* over een domein R is een rij $(a_n)_{n=0}^{\infty} \in R^{\mathbb{Z}_{\geq 0}}$ zodanig dat er een $k \in \mathbb{Z}_{\geq 0}$ en constanten $c_0, \ldots, c_{k-1} \in R$ bestaan, zodat voor alle $n \geq 0$ geldt:

$$a_{n+k} = c_0 a_n + c_1 a_{n+1} + \cdots + c_{k-1} a_{n+k-1}.$$

Een *tweezijdige lineaire recurrentie* over een domein R is een rij $(a_n)_{n\in\mathbb{Z}} \in R^{\mathbb{Z}}$ zodanig dat er een $k \in \mathbb{Z}_{\geq 0}$ en constanten $c_0, \ldots, c_{k-1} \in R$ bestaan, zodat voor alle $n \in \mathbb{Z}$ geldt:

$$a_{n+k} = c_0 a_n + c_1 a_{n+1} + \cdots + c_{k-1} a_{n+k-1}.$$

Opmerking 3.2. Voor een lineaire recurrentie zijn deze constanten niet uniek. Bekijk bijvoorbeeld de constante reeks $(a_n)_{n\in\mathbb{Z}} = (\dots, 1, 1, 1, \dots) \in \mathbb{Z}^{\mathbb{Z}}$. Deze reeks voldoet voor alle $n \in \mathbb{Z}$ aan de vergelijking $a_n = a_{n-1}$, maar ook aan de vergelijking $a_n = 3a_{n-1} - 2a_{n-2}$.

Opmerking 3.3. Als twee rijen $(a_n)_n$ en $(b_n)_n$ aan dezelfde recurrentie voldoen, voldoen ook lineaire combinaties van deze rijen aan deze recurrentie.

Vanaf nu nemen we $R = \mathbb{Q}$. We definiëren de afbeelding

$$\begin{aligned} T : \mathbb{Q}^{\mathbb{Z}_{\geq 0}} &\to \mathbb{Q}^{\mathbb{Z}_{\geq 0}}, \\ (b_0, b_1, \dots) &\mapsto (b_1, b_2, \dots). \end{aligned}$$

Laat $a = (a_n)_{n=0}^{\infty}$ een eenzijdige lineaire recurrentie over $\mathbb{Q}$ zijn.

Feit 3.4. Er is een unieke $d \in \mathbb{Z}_{\geq 0}$ zodanig dat de elementen uit de verzameling $\{a, T(a), \dots, T^{d-1}(a)\}$ lineair onafhankelijk over $\mathbb{Q}$ zijn, en de elementen uit $\{a, T(a), \dots, T^{d-1}(a), T^d(a)\}$ lineair afhankelijk over $\mathbb{Q}$ zijn.

Bewijs. Voor de nulrij zijn de elementen uit $\{a, \dots, T^0(a)\} = \{a\}$ lineair afhankelijk. Laten we nu $T^0(a)$ weg uit deze verzameling, dan hebben we de lege verzameling, en de elementen uit deze verzameling zijn lineair onafhankelijk. Voor elke $d > 0$ zijn de elementen uit $\{a, \dots, T^{d-1}(a)\}$ lineair afhankelijk, dus we concluderen dat $d = 0$ het unieke getal is dat aan de eigenschap voldoet.

Stel nu dat a niet de nulrij is. We weten dat a een eenzijdige lineaire recurrentie is, dus zijn er constanten $c_0, \dots, c_{k-1} \in \mathbb{Q}$ zodat voor elke $n \geq 0$ geldt:

$$a_{n+k} = c_0 a_n + \dots + c_{k-1} a_{n+k-1}.$$

Dit betekent dat de elementen uit de verzameling $\{a, T(a), \dots, T^k(a)\}$ lineair afhankelijk zijn. Immers:

$$\begin{aligned} T^k(a) - \sum_{i=0}^{k-1} c_i T^i(a) &= (a_k, a_{k+1}, \dots) - \sum_{i=0}^{k-1} c_i (a_i, a_{i+1}, \dots) \\ &= \left((a_k - \sum_{i=0}^{k-1} c_i a_i), (a_{k+1} - \sum_{i=0}^{k-1} c_i a_{i+1}), \dots \right) \\ &= (0, 0, \dots). \end{aligned}$$

We kunnen nu $T^k(a)$ uit deze verzameling verwijderen, en kijken of de elementen uit $\{a, T(a), \dots, T^{k-1}(a)\}$ ook lineair afhankelijk zijn. Als dit niet het geval is nemen we $d = k$, en anders verwijderen we ook $T^{k-1}(a)$, en gaan we inductief door, tot de verzameling geen lineaire afhankelijkheid meer vertoont. Het komt niet voor dat $d = 0$, want dan zou gelden dat $c \cdot a = (0, 0, 0, \dots)$ voor zekere $c \in \mathbb{Q}\backslash\{0\}$. Dat zou betekenen dat a de nulrij is, maar we hadden aangenomen dat dit niet het geval is. □

Definitie 3.5. Voor een eenzijdige lineaire recurrentie $a = (a_n)_{n=0}^{\infty}$ over $\mathbb{Q}$ noemen we deze d de *graad van de recurrentie*.

Als een eenzijdige lineaire recurrentie van graad d is, betekent dit dat er constanten $c'_0, c'_1, \ldots, c'_{d-1}, c'_d \in \mathbb{Q}$ zijn zodanig dat $\sum_{i=0}^{d} c'_i T^i(a) = 0$. Verder geldt dat $c'_d \neq 0$, want anders zou de recurrentie niet van graad d zijn. Dan kunnen we alle coëfficiënten delen door c'_d om te krijgen: $T^d(a) = \sum_{i=0}^{d-1} c_i T^i(a)$, met $c_0, \ldots, c_{d-1} \in \mathbb{Q}$. Dit betekent dat $a_{n+d} = \sum_{i=0}^{d-1} c_i a_{n+i}$ voor alle $n \geq 0$, en dit is de 'kortste' recurrentie waaraan de rij voldoet.

Lemma 3.6. Laat a een eenzijdige lineaire recurrentie over $\mathbb{Q}$ van graad d. Dan is er een uniek monisch polynoom $f \in \mathbb{Q}[X]$ van graad d met $f(T)(a) = 0$. We noemen deze f het *minimumpolynoom* van de recurrentie.

Bewijs. Stel allereerst dat a de nulrij is. Er is precies 1 monisch polynoom van graad 0, namelijk $f = 1$. Voor deze f geldt inderdaad $f(T)(a) = a = 0$.
Stel nu dat a niet de nulrij is. Laat $f = X^d - \sum_{i=0}^{d-1} c_i X^i$, waarbij de c_i zijn gedefinieerd zoals hierboven. Dan geldt $f(T)(a) = 0$. Stel nu dat er een monisch polynoom $g \in \mathbb{Q}[X], f \neq g$ met $g(T)(a) = 0$ bestaat. Dan geldt dat $f - g \neq 0$ een polynoom is van graad $m < d$. Als we delen door de kopcoëfficiënt van $f - g$ vinden we een monisch polynoom $h \in \mathbb{Q}[X]$ met $h(T)(a) = (f - g)(T)(a) = f(T)(a) - g(T)(a) = 0 - 0 = 0$. Dan vinden we dus voor alle $n \geq 0$ dat $a_{n+m} = \sum_{i=0}^{m-1} d_i a_{n+i}$ voor $d_0, \ldots, d_{m-1} \in \mathbb{Q}$. Dit is een tegenspraak met de graad van de recurrentie. Er volgt dat f het unieke polynoom is dat aan deze voorwaarden voldoet. □

Gevolg 3.7. Voor elke $g \in \mathbb{Q}[X]$ met $g(T)(a) = 0$ geldt dat $f | g$. Stel immers dat f geen deler is van g. Dan kunnen we deling met rest uitvoeren om een polynoom $h \in \mathbb{Q}[X]$ van graad kleiner dan d vinden, zodanig dat $h(T)(a) = 0$. Dit is een tegenspraak met de minimaliteit van f.

Voorbeeld 3.8. Het minimumpolynoom van de Fibonacci-reeks is het polynoom $f = X^2 - X - 1$, en we zien:

$$\begin{aligned} f(T)(F) &= (1, 2, 3, 5, 8, 13, \ldots) - (1, 1, 2, 3, 5, 8, \ldots) - (0, 1, 1, 2, 3, 5, \ldots) \\ &= (1 - 1 - 0, 2 - 1 - 1, 3 - 2 - 1, 5 - 3 - 2, 8 - 5 - 3, \ldots) \\ &= (0, 0, 0, \ldots). \end{aligned}$$

Definieer nu voor tweezijdige lineaire recurrenties de afbeelding:

$$\widetilde{T} : \mathbb{Z}^{\mathbb{Z}} \xrightarrow{\sim} \mathbb{Z}^{\mathbb{Z}},$$
$$(\ldots, b_{-1}, \boxed{b_0}, b_1, \ldots) \mapsto (\ldots, b_0, \boxed{b_1}, b_2, \ldots).$$

Hier geeft het vierkantje aan wat de nul-index is van het element. De afbeelding $\widetilde{T}$ verschuift de hele rij dus naar links. Deze afbeelding is duidelijk een ring-isomorfisme: het is een ringhomomorfisme omdat de coördinaatsgewijze optelling en vermenigvuldiging commuteren met het opschuiven van de rij. Ook is het niet moeilijk de inverse te geven: We kunnen de rij gewoon terugschuiven.
Analoog aan het geval van eenzijdige lineaire recurrenties kunnen we spreken over de graad, en het minimumpolynoom van een tweezijdige lineaire recurrentie.

Opmerking 3.9. Laat $\widetilde{a}$ een tweezijdige lineaire recurrentie over $\mathbb{Q}$ zijn met minimumpolynoom $g \in \mathbb{Q}[X]$. Dan geldt dat $\widetilde{T} \nmid g(\widetilde{T})$.

Bewijs. Stel dat $\widetilde{T} | g(\widetilde{T})$. Dan geldt dat $g = \widetilde{T} \cdot h(\widetilde{T})$ voor een zeker monisch polynoom $h \in \mathbb{Q}[X]$ van kleinere graad dan g. Dan geldt dat:

$$0 = g(\widetilde{T})(\widetilde{a}) = \widetilde{T}(h(\widetilde{T})(\widetilde{a})).$$

Omdat $\widetilde{T}$ een isomorfisme is, betekent dit dat $h(\widetilde{T})(\widetilde{a}) = 0$. Dit is een tegenspraak met de minimaliteit van g, en dus geldt dat $\widetilde{T} \nmid g(\widetilde{T})$. □

Lemma 3.10. Laat $\widetilde{a}$ een tweezijdige lineaire recurrentie over $\mathbb{Q}$ zijn met minimumpolynoom g. Laat $(a_n)_{n=0}^{\infty}$, gedefinieerd door $a_n := \widetilde{a}_n$ de rechterhelft van $\widetilde{a}$ zijn. Dan is (a_n) een eenzijdige lineaire recurrentie. Laat f het minimumpolynoom van a zijn, van graad d. Dan geldt dat $f = g$.

Bewijs. Wegens de uniciteit van f is het voldoende om te laten zien dat de graad van g gelijk is aan d. Omdat geldt dat $g(\widetilde{T})(\widetilde{a}) = 0 \in \mathbb{Q}^{\mathbb{Z}}$, geldt ook dat $g(T)(a) = 0 \in \mathbb{Q}^{\mathbb{Z}_{\geq 0}}$. Dan geldt wegens Gevolg 2.7 dat $f | g$, en dus vinden we dat $\deg(g) \geq d$. Omdat de graad van f gelijk is aan d, bestaat er een lineaire combinatie $(B_n)_{n \in \mathbb{Z}}$ horend bij f, van elementen uit $\{\widetilde{a}, \widetilde{T}(\widetilde{a}), \widetilde{T}^2(\widetilde{a}), \ldots, \widetilde{T}^d(\widetilde{a})\}$, zodanig dat $B_i = 0$ voor alle $i \geq 0$. Omdat B een lineaire combinatie is van rijen die voldoen aan de recurrentie gegeven door g, voldoet B ook aan de lineaire recurrentie gegeven door g. Dit betekent dat $B_{n+k} = \sum_{i=0}^{k-1} c_i' B_i$ voor zekere $k \in \mathbb{Z}_{\geq d}$ en constanten $c_0', \ldots, c_{k-1}' \in \mathbb{Q}$. Hier is $c_0' \neq 0$, vanwege Opmerking 3.9. Dan geldt dat we B_{-1} kunnen schrijven als lineaire combinatie van $B_0, \ldots, B_{k-1}$, en dus vinden we $B_{-1} = 0$. Inductief vinden we dat B de nulrij is, en dus vinden we dat $\deg(g) \leq d$. We concluderen dat $\deg(g) = d$, en dus dat $g = f$. □

Lemma 3.11. Laat a een eenzijdige lineaire recurrentie over $\mathbb{Q}$ met minimumpolynoom $f = X^d - \sum_{i=0}^{\infty} c_i X^i \in \mathbb{Q}[X]$ van graad d zijn. Als $a \in \mathbb{Z}^{\mathbb{Z}_{\geq 0}}$, dan $f \in \mathbb{Z}[X]$.

Bewijs. Bekijk de volgende matrix:

$$\begin{bmatrix} a \\ T(a) \\ T^2(a) \\ \vdots \\ T^{d-1}(a) \end{bmatrix} = \left|\begin{array}{cccc|cc} a_0 & a_1 & \ldots & a_{d-1} & a_d & \ldots \\ a_1 & a_2 & \ldots & a_d & a_{d+1} & \ldots \\ a_2 & a_3 & \ldots & a_{d+1} & a_{d+2} & \ldots \\ \vdots & \vdots & & \vdots & \vdots & \\ a_{d-1} & a_{d-2} & \ldots & a_{2d-2} & a_{2d-3} & \ldots \end{array}\right|$$

We noteren voor elke $i \geq 0$, voor de i-de kolom:

$$b_i := \begin{bmatrix} a_i \\ \vdots \\ a_{i+d-1} \end{bmatrix}.$$

We weten dat de rijen van deze matrix lineair onafhankelijk zijn. Dit geldt ook voor de eerste d kolommen: Stel dat er een lineaire combinatie $\sum_{i=0}^{d-1} k_i b_i$ bestaat die gelijk is aan 0. Binnen het eerste $(d \times d)$-blok zijn de rijen en kolommen hetzelfde. Als we nu de rijen invullen in de gevonden combinatie, vinden we dus een lineaire recurrentie $(u_n)_{n=0}^{\infty}$ die begint met d opeenvolgende nullen, horend bij een polynoom van graad d. Wegens de recurrentie volgt dan

dat $u_d = \sum_{i=0}^{d-1} c_i u_i = 0$, en inductief volgt dat $(u_n)_{n=0}^{\infty}$ de nulrij is. Dit is een tegenspraak, want we hadden aangenomen dat de rijen lineair onafhankelijk waren. We concluderen dat $b_0, \ldots, b_{d-1}$ lineair onafhankelijk zijn, en dus vormen ze een basis voor $\mathbb{Q}^d$ als vectorruimte over $\mathbb{Q}$. Als we nu $\mathbb{Z}^d$ als additieve ondergroep van $\mathbb{Q}^d$ bekijken, dan vinden we de volgende keten van ondergroepen:

$$\mathbb{Z}^d \cong \sum_{i=0}^{d-1} \mathbb{Z}b_i \subset \sum_{i \geq 0} \mathbb{Z}b_i \subset \mathbb{Z}^d.$$

Omdat elke ondergroep van $\mathbb{Z}^d$ isomorf is met $\mathbb{Z}^k$ voor een $k \leq d$, geldt:

$$F := \sum_{i \geq 0} \mathbb{Z}b_i \cong \mathbb{Z}^d.$$

We definiëren nu een $\mathbb{Q}$-lineaire afbeelding op $\mathbb{Q}^d$:

$$\begin{aligned} \varepsilon : \mathbb{Q}^d &\to \mathbb{Q}^d, \\ b_i &\mapsto b_{i+1} \qquad (0 \leq i \leq d-1). \end{aligned}$$

Omdat $b_0, \ldots, b_{d-1}$ een basis vormen voor $\mathbb{Q}^d$, ligt de afbeelding hiermee vast. Er geldt:

$$\varepsilon(b_d) = \varepsilon\left(\sum_{i=0}^{d-1} c_i b_i\right) = \sum_{i=0}^{d-1} c_i \varepsilon(b_i) = \sum_{i=0}^{d-1} c_i b_{i+1} = b_{d+1}.$$

Met inductie vinden we dat voor alle $n \geq 0$ geldt: $\varepsilon(b_n) = b_{n+1}$, dus geldt dat $\varepsilon(F) \subset F$, oftewel $\varepsilon_{|F} \in \mathrm{End}(F)$. Wegens de Stelling van Cayley-Hamilton bestaat er nu een $h \in \mathbb{Z}[X]$, het karakteristieke polynoom van $\varepsilon_{|F}$, dat monisch is, van graad d, met $h(\varepsilon_{|F}) = 0$. Schrijf $h = X^d - \sum_{i=0}^{d-1} c_i' X^i$, met constanten $c_0', \ldots, c_{d-1}' \in \mathbb{Z}$. Dan geldt dat $h(\varepsilon_{|F}) = \varepsilon^d - \sum_{i=0}^{d-1} c_i' \varepsilon^i$ de nulafbeelding is. Dan vinden we, voor elke $j \geq 0$:

$$0 = \varepsilon^d(b_j) - \sum_{i=0}^{d-1} c_i' \varepsilon^i(b_j) = b_{j+d} - \sum_{i=0}^{d-1} c_i' b_{i+j},$$

en dus vinden we dat $a_{n+d} = \sum_{i=0}^{d-1} c_i' a_{n+i}$ voor alle $n \geq 0$. Dit betekent dat h ook een minimumpolynoom van de recurrentie is. Maar wegens de uniciteit van het minimumpolynoom moet gelden dat $h = f$, en dus dat $f \in \mathbb{Z}[X]$. □

3.2 Recurrenties in $\hat{\mathbb{Z}}$

De volgende stelling vertelt ons precies onder welke voorwaarden een eenzijdige lineaire recurrentie over $\mathbb{Z}$ een continue voortzetting tot $\hat{\mathbb{Z}}$ heeft.

Stelling 3.12. Laat $a \in \mathbb{Z}^{\mathbb{Z}_{\geq 0}}$ een eenzijdige lineaire recurrentie, met minimumpolynoom $f = X^d - \sum_{i=0}^{d-1} c_i X^i \in \mathbb{Z}[X]$. Dan zijn de volgende uitspraken equivalent:

1. $f(0) \in \{\pm 1\}$.
2. Er is een continue afbeelding $\hat{a} : \hat{\mathbb{Z}} \to \hat{\mathbb{Z}}$ met $\hat{a}_{|\mathbb{Z}} = a$.
3. a heeft een voortzetting tot een tweezijdige lineaire recurrentie $\widetilde{a} : \mathbb{Z} \to \mathbb{Z}$.

Bewijs. We zullen bewijzen dat (1) $\Leftrightarrow$ (3) en dat (2) $\Leftrightarrow$ (3).

(1) $\Rightarrow$ (3)

We hebben $a_{n+d} = \sum_{i\geq 0}^{d-1} c_i a_{n+i}$ voor alle $n \geq 0$. Definieer nu:

$$a_{-1} := \frac{a_{d-1} - \sum_{i=1}^{d-1} c_i a_{i-1}}{c_0}.$$

Dan geldt duidelijk dat $a_{-1} \in \mathbb{Z}$, omdat $c_0 \in \{\pm 1\}$. Ook geldt dat de uitgebreide rij $(a_n)_{n=-1}^{\infty}$ voldoet aan de recurrentie, want:

$$c_0 a_{-1} + \sum_{i=1}^{d-1} c_i a_{i-1} = a_{d-1} - \sum_{i=1}^{d-1} c_i a_{i-1} + \sum_{i=1}^{d-1} c_i a_{i-1} = a_{d-1}.$$

Inductief kunnen we nu voor alle $n \in \mathbb{Z}_{\geq 0}$ definiëren:

$$a_{-n} = \frac{a_{-n+d} - \sum_{i=1}^{d-1} a_{i-n}}{c_0}.$$

Hiermee verkrijgen we een voortzetting tot een tweezijdige lineaire recurrentie $\widetilde{a} : \mathbb{Z} \to \mathbb{Z}$.

(3) $\Rightarrow$ (1)

We hebben $\widetilde{a} := (\dots, a_{-2}, a_{-1}, a_0, a_1, a_2, \dots) \in \mathbb{Z}^{\mathbb{Z}}$. Er geldt wegens Lemma 3.10 dat $f(\widetilde{T})(\widetilde{a}) = 0$, en uit Opmerking 3.9 volgt dat $c_0 \neq 0$. Bekijk nu de volgende matrix:

$$\begin{bmatrix} \widetilde{a} \\ \widetilde{T}(\widetilde{a}) \\ \widetilde{T}^2(\widetilde{a}) \\ \vdots \\ \widetilde{T}^{d-1}(\widetilde{a}) \end{bmatrix} = \begin{array}{ccc|cccc|ccc} \dots & a_{-1} & & a_0 & a_1 & \dots & a_{d-1} & a_d & \dots \\ \dots & a_0 & & a_1 & a_2 & \dots & a_d & a_{d+1} & \dots \\ \dots & a_1 & & a_2 & a_3 & \dots & a_{d+1} & a_{d+2} & \dots \\ & \vdots & & \vdots & \vdots & & \vdots & \vdots & \\ \dots & a_d & & a_{d-1} & a_{d-2} & \dots & a_{2d-2} & a_{2d-3} & \dots \end{array}$$

Definieer nu $\overleftarrow{a} := (\dots, a_2, a_1, a_0, a_{-1}, a_{-2}, \dots)$, de omgekeerde rij. Het is duidelijk dat deze rij voldoet aan een recurrentie: Omdat voor elke $n \in \mathbb{Z}$ geldt dat $a_{n+d} = \sum_{i=0}^{d-1} c_i a_{n+i}$, geldt ook dat:

$$\overleftarrow{a}_n = a_{-n} = \frac{a_{-n+d} - \sum_{i=1}^{d-1} c_i a_{-n+i}}{c_0} = \frac{\overleftarrow{a}_{n-d} - \sum_{i=1}^{d-1} c_i \overleftarrow{a}_{n-i}}{c_0}.$$

Definieer nu het polynoom

$$\overleftarrow{f} := \frac{-\sum_{i=0}^{d-1} c_i X^{d-i} + 1}{f(0)} \in \mathbb{Q}[X].$$

Dit polynoom is monisch, en er geldt dat $\overleftarrow{f}(\widetilde{T})(\overleftarrow{a}) = 0$. Omdat de omgekeerde recurrentie in matrixvorm dezelfde kolommen oplevert, vinden we dat deze recurrentie ook van graad d is. Dit betekent dat $\overleftarrow{f}$ het minimumpolynoom is van $\overleftarrow{a}$. Omdat $\overleftarrow{a} \in \mathbb{Z}^{\mathbb{Z}}$ geldt wegens Lemma 3.11 dat $\overleftarrow{f} \in \mathbb{Z}[X]$, en dus is in het bijzonder de constante coëfficiënt $\frac{1}{f(0)}$ geheel. Omdat $f(0) \in \mathbb{Z}$ betekent dit dat $f(0) \in \{\pm 1\}$.

(2) $\Rightarrow$ (3)

We hebben nu een continue voortzetting $\hat{a} : \hat{\mathbb{Z}} \to \hat{\mathbb{Z}}$. We moeten laten zien dat $\hat{a}(\mathbb{Z}) \subset \mathbb{Z}$ en dat $\hat{a}$ aan de recurrentie voldoet voor alle $n \in \mathbb{Z}$. Hiervoor definiëren we de afbeelding:

$$\begin{aligned} \varphi : \hat{\mathbb{Z}} &\to \hat{\mathbb{Z}}, \\ s &\mapsto \hat{a}(s) - \sum_{i=0}^{d-1} c_i \hat{a}(s+i-d). \end{aligned}$$

We moeten laten zien dat dit de nulafbeelding is, want dan geldt dat $\hat{a}(s+d) = \sum_{i=0}^{d-1} c_i \hat{a}(s+i)$ voor alle $s \in \hat{\mathbb{Z}}$, dus voldoet $\hat{a}$ aan de recurrentie. De functie φ is een lineaire combinatie van continue functies, en omdat $\hat{\mathbb{Z}}$ een topologische ring is, is de afbeelding hiermee zelf ook continu. We weten dat a aan de recurrentie voldoet. Omdat $\hat{a}$ een voortzetting van a is, geldt dat $\hat{a}(n) = a(n)$ voor alle $n \in \mathbb{Z}_{\geq 0}$, en dus geldt voor alle $s \in \mathbb{Z}_{\geq d}$ dat $\varphi(s) = a(s) - \sum_{i=0}^{d-1} c_i a(s+i-d) = 0$. We hebben dus:

$$\mathbb{Z}_{\geq d} \subset \varphi^{-1}(\{0\}),$$

en dus ook:

$$\overline{\mathbb{Z}_{\geq d}} \subset \overline{\varphi^{-1}(\{0\})}.$$

Zoals opgemerkt in Feit 2.4 ligt de verzameling $\mathbb{Z}_{\geq d}$ dicht in $\hat{\mathbb{Z}}$. Omdat $\hat{\mathbb{Z}}$ Hausdorff is, is $\{0\}$ gesloten, dus is ook $\varphi^{-1}(\{0\})$ gesloten. Dus vinden we:

$$\hat{\mathbb{Z}} = \overline{\mathbb{Z}_{\geq d}} \subset \overline{\varphi^{-1}(\{0\})} = \varphi^{-1}(\{0\}) \subset \hat{\mathbb{Z}}.$$

Hieruit volgt dat φ de nulafbeelding is, en dus voldoet $\hat{a}$ aan de recurrentie op heel $\hat{\mathbb{Z}}$.

Er geldt nu dat $c_0 \hat{a}_{-1} = \hat{a}_{d-1} - \sum_{i=1}^{d-1} c_i \hat{a}(i-1) = a_{d-1} - \sum_{i=1}^{d-1} c_i a_{i-1} \in \mathbb{Z}$. Ook geldt dat $c_0 \hat{a}_{-1} \in c_0 \hat{\mathbb{Z}}$. Dit betekent dat $c_0 \hat{a}_{-1} \in \mathbb{Z} \cap c_0 \hat{\mathbb{Z}}$, en het is niet moeilijk om in te zien dat deze verzameling gelijk is aan $c_0 \mathbb{Z}$: Het is duidelijk dat $c_0 \mathbb{Z} \subset \mathbb{Z}$ en $c_0 \mathbb{Z} \subset c_0 \hat{\mathbb{Z}}$. Als andersom $x \in \mathbb{Z} \cap c_0 \hat{\mathbb{Z}}$, dan is het een geheel getal (want het is een element van $\mathbb{Z}$) dat een veelvoud is van c_0 (want het is een element van $c_0 \hat{\mathbb{Z}}$). Dit betekent dat $x \in c_0 \mathbb{Z}$. Omdat $c_0 \in \mathbb{Z} \backslash \{0\}$, is c_0 wegens Opmerking 2.9 geen nuldeler, en dus vinden we $\hat{a}_{-1} \in \mathbb{Z}$. Inductief vinden we dat $\hat{a}(\mathbb{Z}) \subset \mathbb{Z}$. Dan is $\widetilde{a} := (\hat{a}(n))_{n \in \mathbb{Z}}$ een voortzetting van a tot een tweezijdige lineaire recurrentie $\mathbb{Z} \to \mathbb{Z}$.

(3) $\Rightarrow$ (2)

We hebben $\widetilde{a} = (\dots, a_{-2}, a_{-1}, a_0, a_1, a_2, \dots)$. Om te laten zien dat de afbeelding $\widetilde{a} : \mathbb{Z} \to \mathbb{Z}$ een continue voortzetting $\hat{a} : \hat{\mathbb{Z}} \to \hat{\mathbb{Z}}$ heeft, willen we Stelling 2.13 gebruiken. Dit betekent dat we voor elke $m \in \mathbb{Z}_{\geq 1}$ een periode l_m moeten geven. Laat $m \in \mathbb{Z}_{\geq 1}$ gegeven. Definieer voor elke $n \in \mathbb{Z}$:

$$b_n := (a_n \bmod m, \dots, a_{n+d-1} \bmod m) \in (\mathbb{Z}/m\mathbb{Z})^d.$$

Omdat $(\mathbb{Z}/m\mathbb{Z})^d$ bestaat uit m^d elementen, geldt:

$$\forall n : \exists i, j : 0 \leq i < j \leq m^d : b_{n+i} = b_{n+j}.$$

Dan geldt dus:

$$\forall h \in \{0, \dots, d-1\} : a_{n+i+h} \equiv a_{n+j+h} \mod m.$$

Wegens de recurrentie geldt dan:

$$a_{n+i+d} \equiv \sum_{p=0}^{d-1} c_i a_{n+i+p} \equiv \sum_{p=0}^{d-1} c_i a_{n+j+p} \equiv a_{n+j+d} \mod m.$$

Dus vinden we:

$$\forall h \geq 0 : a_{n+i+h} \equiv a_{n+j+h} \mod m.$$

We kennen deze gelijkheid nu dus vanaf $n + i$, en we weten $i \leq m^d - 1$. Dus hebben we:

$$\forall n \in \mathbb{Z} : \exists k \in \{1, 2, \dots, m^d\} : \forall l \geq m^d - 1 : a_{n+l} \equiv a_{n+l+k} \mod m.$$

Dan ook $a_{n+l+k} \equiv a_{n+l+2k} \mod m$, en zo ook voor alle veelvouden van k. In het bijzonder geldt voor $(m^d)!$ dat:

$$\forall n \in \mathbb{Z} : \forall l \geq m^d - 1 : a_{n+l} \equiv a_{n+l+(m^d)!} \mod m.$$

Laat nu $l = m^d - 1$ en laat voor elke $g \in \mathbb{Z}$ nu $n = l - g$. Dan hebben we:

$$\forall g \in \mathbb{Z} : a_g \equiv a_{g+(m^d)!} \mod m.$$

We kunnen nu dus $l_m = (m^d)!$ als periode nemen. We concluderen dat a een continue voortzetting $\hat{a} : \hat{\mathbb{Z}} \to \hat{\mathbb{Z}}$ heeft.

We hebben nu bewezen dat (1) $\Leftrightarrow$ (3) $\Leftrightarrow$ (2), en hiermee is de stelling bewezen. $\square$

Omdat voor de Fibonacci-rij geldt dat $f(0) = -1$, hebben we nu met Stelling 3.12 het bestaan van *Pro-eindige Fibonacci-getallen* bewezen. Om voor een element $s \in \hat{\mathbb{Z}}$ te bepalen hoe F_s zich gedraagt modulo m, gaan we als volgt te werk: We nemen een rij $(a_n)_{n=0}^{\infty} \subset \mathbb{Z}$ die naar s convergeert. Uit Stelling 2.13 volgt een periode l_m voor de rij modulo m, en omdat $(a_n)_{n=0}^{\infty}$ convergent is, is deze rij constant modulo l_m vanaf zekere $N \in \mathbb{Z}_{\geq 1}$. Dan geldt dat $F_s \equiv F_N \mod m$ voor deze N. Om het rekenwerk binnen de perken te houden is het zaak om een zo klein mogelijke periode l_m te vinden.

4 Fibonacci-getallen

In dit hoofdstuk zullen we ons iets meer verdiepen in de Fibonacci-getallen. In het vorige hoofdstuk werd een bovengrens gegeven voor de periode van de rij modulo m, namelijk $(m^2)!$. Deze periode is verre van optimaal: Modulo 2 is de rij gelijk aan $0, 1, 1, 0, 1, 1, \ldots$, met periode 3, terwijl de bovengrens gelijk is aan $(2^2)! = 24$. We zullen in dit hoofdstuk een betere bovengrens geven. We noteren vanaf nu $\pi(m)$ voor de minimale periode van de Fibonacci-rij modulo m, voor elke $m \in \mathbb{Z}_{\geq 1}$. In dit hoofdstuk zullen we de volgende stelling bewijzen:

Stelling 4.1.

1. Voor $m \in \mathbb{Z}_{>2}$ is $\pi(m)$ even.
2. Laat $m = \prod_{p \text{ priem}} p^{k_p}$ met $k_p = 0$ voor bijna alle p. Dan geldt:
$$\pi(m) = \text{kgv}_{p \text{ priem}} \left(\pi(p^{k_p})\right).$$
3. Voor q priem en $n \in \mathbb{Z}_{\geq 1}$ geldt dat $\pi(q^n) | \pi(q) \cdot q^{n-1}$
4. Laat q een priemgetal zijn. Dan geldt:
   - Als $q = 2$, dan $\pi(q) = 3$.
   - Als $q = 5$, dan $\pi(q) = 20$.
   - Als $q \equiv 1, 9 \mod 10$, dan $\pi(q) | q - 1$.
   - Als $q \equiv 3, 7 \mod 10$, dan $\pi(q) | 2(q + 1)$, en $\pi(q) \nmid q + 1$.
5. Voor elke $m \in \mathbb{Z}_{\geq 1}$ geldt dat $\pi(m) \leq 6m$.

Voorbeeld 4.2. We vinden dat $\pi(3)$ een deler is van 8, die geen deler is van 4. Dit geeft dat $\pi(3) = 8$, en er geldt inderdaad:

$$(F_n \bmod 3)_{n=0}^{\infty} = 0, 1, 1, 2, 0, 2, 1, 0, 1, \ldots$$

Voorbeeld 4.3. We vinden dat $\pi(11)$ een deler is van 10. Er geldt inderdaad dat $F_{10} \equiv 55 \equiv 0 \mod 11$ en dat $F_{11} \equiv 89 \equiv 1 \mod 11$. Voor elke deler d van 10 die ongelijk is aan 10, geldt dat $F_d \not\equiv 0 \mod 11$, dus geldt dat $\pi(11) = 10$.

Voorbeeld 4.4. Er geldt dat $\pi(10) = \text{kgv}(\pi(2), \pi(5)) = \text{kgv}(3, 20) = 60$, en het komt dus voor dat $\pi(m) = 6m$.

Elke ring R bevat een nulelement en een eenheidselement. Omdat op een ring een optelling is gedefinieerd, kunnen we de Fibonacci-rij $(F_n)_{n=0}^{\infty}$ definiëren over elke ring. Door terug te rekenen kunnen we ook bepalen wat F_{-1} moet zijn, want $F_{-1} + F_0 = F_1$, dus $F_{-1} = 1$. Inductief vinden we $F_{-2} = -1, F_{-3} = 2$, en in het algemeen $F_{-n} = (-1)^{n+1} F_n$ voor elke $n \in \mathbb{Z}$. Met deze gelijkheid kunnen we 4.1.1 bewijzen.

Bewijs. (4.1.1)
Per definitie van $\pi(m)$ hebben we:

$$F_{\pi(m)} \equiv F_0 \equiv 0 \mod m,$$

$$F_{-\pi(m)+1} \equiv F_1 \equiv F_{\pi(m)+1} \equiv 1 \mod m.$$

Ook geldt dat:

$$F_{\pi(m)-1} \equiv (-1)^{\pi(m)} F_{-\pi(m)+1} \equiv (-1)^{\pi(m)} \mod m,$$

en dus volgt:

$$1 \equiv F_{\pi(m)+1} - F_{\pi(m)} \equiv F_{\pi(m)-1} \equiv (-1)^{\pi(m)} \mod m.$$

Stel nu dat $\pi(m)$ oneven is. Dan geldt dat $1 \equiv -1 \mod m$, en dus vinden we $m = 1$ of $m = 2$. Als dus geldt dat $m > 2$, dan vinden we dat $\pi(m)$ even is. □

Bewijs. (4.1.2)
Als de Fibonacci-rij periodiek is modulo m met minimale periode $\pi(m)$, dan is $\pi(m)$ ook een periode van de rij modulo elke deler d van m. In het bijzonder is dan $\pi(d)$ een deler van $\pi(m)$, en dus volgt dat $\pi(p^{k_p})|\pi(m)$ voor alle priemgetallen p, en dus $\text{kgv}_{p \text{ priem}}\left(\pi(p^{k_p})\right) | \pi(m)$.

Andersom geldt vanwege de Chinese Reststelling:

$$\mathbb{Z}/m\mathbb{Z} \cong \prod_{p \text{ priem}} \mathbb{Z}/p^{k_p}\mathbb{Z}.$$

Omdat de rij modulo p^{k_p} periodiek is met periode $\pi(p^{k_p})$, geldt dit ook voor elk veelvoud van $\pi(p^{k_p})$. In het bijzonder betekent dit dat de rij in de rechterkant periodiek is met periode $\text{kgv}_{p \text{ priem}}\left(\pi(p^{k_p})\right)$. Dan is de rij dus ook in de linkerkant periodiek met deze periode. Er volgt dat $\pi(m)$ een deler is van $\text{kgv}_{p \text{ priem}}\left(\pi(p^{k_p})\right)$. We concluderen dat $\pi(m) = \text{kgv}_{p \text{ priem}}\left(\pi(p^{k_p})\right)$. □

Propositie 4.5. Laat R een ring zijn, en $(F_n)_{n\in\mathbb{Z}}$ de Fibonacci-rij over R. Als $\alpha \in R$ een nulpunt is van $f(X) = X^2 - X - 1 \in R[X]$, dan geldt voor elke $n \in \mathbb{Z}$:

$$\alpha^n = F_{n-1} + F_n\alpha.$$

Bewijs. Er geldt:

$$\alpha^0 = 1 = F_{-1} + F_0 \cdot \alpha,$$
$$\alpha^1 = \alpha = F_0 + F_1 \cdot \alpha.$$

Stel nu dat de stelling geldt voor twee opeenvolgende getallen $n, n+1$. Dan geldt:

$$\begin{aligned}
\alpha^{n+2} &= \alpha^n\alpha^2 \\
&= \alpha^n(\alpha + 1) \\
&= \alpha^{n+1} + \alpha^n \\
&= F_n + F_{n+1}\alpha + F_{n-1} + F_n\alpha \\
&= F_{n+1} + F_{n+2}\alpha,
\end{aligned}$$

en ook:

$$\begin{aligned}\alpha^{n-1} &= \alpha^{n+1} - \alpha^n \\ &= F_n + F_{n+1}\alpha - F_{n-1} - F_n\alpha \\ &= F_{n-2} + F_{n-1}\alpha.\end{aligned}$$

Inductief volgt dat de gelijkheid geldt voor elke $n \in \mathbb{Z}$. □

Gevolg 4.6. Laat $m \in \mathbb{Z}_{\geq 2}$. Bekijk de groep $G = \big((\mathbb{Z}/m\mathbb{Z})[X]/(X^2 - X - 1)\big)^*$. Dan geldt dat $\pi(m)$ gelijk is aan de orde van het element

$$\theta = X + (X^2 - X - 1) \in G.$$

Bewijs. Merk op dat de ring $R := (\mathbb{Z}/m\mathbb{Z})[X]/(X^2-X-1)$ bestaat uit elementen van de vorm $a\theta + b$, en dat de elementen $1, \theta$ lineair onafhankelijk zijn over $\mathbb{Z}/m\mathbb{Z}$. Dit betekent dat de elementen $1, \theta$ een basis vormen voor R als moduul over $\mathbb{Z}/m\mathbb{Z}$, en dus laat ieder element van R zich uniek schrijven als lineaire combinatie van 1 en θ. Hetzelfde geldt voor de elementen van G. Noteer nu $\mathrm{ord}(\theta)$ voor de orde van θ in G. Wegens Propositie 4.5 geldt dat $\theta^n = F_{n-1}+F_n\cdot\theta$ voor alle $n \in \mathbb{Z}$. Nu geldt voor elke $k \in \mathbb{Z}_{\geq 1}$:

$$\begin{aligned}\mathrm{ord}(\theta)|k &\Leftrightarrow \theta^k = 1 \\ &\Leftrightarrow F_{k-1} = 1 = F_{-1} \wedge F_k = 0 = F_0 \\ &\Leftrightarrow \forall l \in \mathbb{Z} : F_{k+l} = F_l \\ &\Leftrightarrow \pi(m)|k.\end{aligned}$$

Hier volgt de tweede implicatie uit de unieke schrijfwijze van elementen uit R. We concluderen dat $\mathrm{ord}(\theta) = \pi(m)$. □

Bewijs. (4.1.3)
We zullen inductie naar n toepassen. Voor $n = 1$ is de stelling duidelijk waar: $\pi(q)|\pi(q)$. We definiëren voor elke $n \in \mathbb{Z}_{\geq 1}$ de volgende ring:

$$R_n := (\mathbb{Z}/q^n\mathbb{Z})[X]/(X^2 - X - 1),$$

de afbeelding:

$$\begin{aligned}&\psi_n : R_1 \to R_n, \\ &aX + b \mapsto (aX + b) \cdot q^{n-1},\end{aligned}$$

en de quotiëntafbeelding:

$$\varphi_n : R_n \to R_{n-1}.$$

Het is eenvoudig te controleren dat φ_n een ringhomomorfisme, en ψ_n een groepshomomorfisme is.
Laat nu $n \in \mathbb{Z}_{\geq 2}$. We bekijken de volgende rij:

$$0 \to R_1 \xrightarrow{\psi_n} R_n \xrightarrow{\varphi_n} R_{n-1} \to 0$$

Deze rij is exact:

- Als geldt dat $aX + b \ker \psi$, dan geldt dat $(aX + b) \cdot q^{n-1} \equiv 0 \mod q^n$, dus $a, b \equiv 0 \mod q$, oftewel $aX + b = 0$. Dan volgt dat ψ_n injectief is.
- φ_n is een quotiëntafbeelding, en is dus per definitie surjectief.
- Voor elk element $cX + d \in R_n$, geldt:

$$\begin{aligned} cX + d \in \ker(\varphi_n) &\Leftrightarrow c, d \equiv 0 \mod q^{n-1} \\ &\Leftrightarrow \exists a, b \in \mathbb{Z}/q\mathbb{Z} : c = a \cdot q^{n-1}, d = b \cdot q^{n-1} \\ &\Leftrightarrow \psi_n(aX + b) = cX + d \\ &\Leftrightarrow aX + b \in \mathrm{im}(\varphi_n). \end{aligned}$$

Uit de inductieveronderstelling weten we:

$$X^{\pi(q)\cdot q^{n-2}} = 1 \in R_{n-1}.$$

Voor $X \in R_n$ geldt dat $\varphi_n(X) = X$, en dus dat

$$\varphi(X^{\pi(q)\cdot q^{n-2}}) = X^{\pi(q)\cdot q^{n-2}} = 1 \in R_{n-1}.$$

Omdat ook geldt dat $\varphi_n(1) = 1$, geldt dat $X^{\pi(q)\cdot q^{N-2}} - 1 \in \ker \varphi_n = \mathrm{im}\, \psi_n = \{(aX + b) \cdot q^{n-1} : a, b \in \mathbb{Z}/q\mathbb{Z}\}$. We concluderen dat:

$$X^{\pi(q)\cdot q^{n-2}} = 1 + (aX + b)q^{n-1},$$

voor zekere $a, b \in \mathbb{Z}/q\mathbb{Z}$. Dan geldt in R_n dat:

$$\begin{aligned} X^{\pi(q)\cdot q^{n-1}} &= \left(1 + (aX + b)q^{n-1}\right)^q \\ &= 1 + \sum_{i=1}^{q} \binom{q}{i} \left((aX + b)q^{n-1}\right)^i. \end{aligned}$$

Voor $i \geq 2$ geldt dat:

$$q^{i(n-1)} \equiv 0 \mod q^n,$$

en voor $i = 1$ geldt dat:

$$\binom{q}{i} q^{n-1} \equiv q^n \equiv 0 \mod q^n.$$

Dit betekent dat de hele som verdwijnt, en dus houden we over dat

$$X^{\pi(q)\cdot q^{n-1}} = 1 \in R_n.$$

Er volgt dat $\pi(q^n) | \pi(q) \cdot q^{n-1}$. □

Opmerking 4.7. Sinds het artikel van D.D. Wall [2] uit 1960 bestaat het vermoeden dat er priemgetallen q bestaan met $\pi(q^2) = \pi(q)$, maar tot op de dag van vandaag zijn er alleen priemgetallen bekend waarvoor in feite gelijkheid geldt in Stelling 4.1.3. Wel is met behulp van het Primegrid-project [3] het volgende aangetoond: Als er een priemgetal q bestaat met $\pi(q^2) = \pi(q)$, dan geldt dat $q > 2{,}8 \cdot 10^{16}$.

Om (4.1.4) te bewijzen hebben we eerst het volgende lemma nodig:

Lemma 4.8. Laat $q \in \mathbb{Z}_{\geq 1}$ een priemgetal, ongelijk aan 5. Stel dat $f = X^2 - X - 1 = (X - \alpha)(X - \beta)$ voor zekere $\alpha, \beta \in \mathbb{Z}/q\mathbb{Z}$. Dan geldt voor elke $n \in \mathbb{Z}$:

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \text{ in } \mathbb{Z}/q\mathbb{Z}.$$

Bewijs. Merk op dat $\alpha \neq \beta$, want anders zou uit $X^2 - X - 1 = (X - \alpha)^2$ volgen dat $-2\alpha \equiv -1 \bmod q$, en $\alpha^2 \equiv -1 \bmod q$. Vermenigvuldigen van de eerste vergelijking met α, en de tweede met -2, geeft dan dat $\alpha \equiv -2 \bmod q$. Dan zou gelden dat -2 een nulpunt is van f, dus dat $f(-2) \equiv 5 \equiv 0 \bmod q$. Omdat q priem is zou dit betekenen dat $q = 5$, maar we hadden aangenomen dat $q \neq 5$. Voor $n = 0$ geldt dat:

$$\frac{\alpha^n - \beta^n}{\alpha - \beta} = 0 = F_0.$$

Voor $n = 1$ geldt dat:

$$\frac{\alpha^n - \beta^n}{\alpha - \beta} = 1 = F_1.$$

Stel nu dat de stelling geldt voor opeenvolgende $n, n + 1$. Dan geldt:

$$\begin{aligned} F_{n+2} = F_{n+1} + F_n &= \frac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta} + \frac{\alpha^n - \beta^n}{\alpha - \beta} \\ &= \frac{\alpha^{n+1} + \alpha^n - \beta^{n+1} - \beta^n}{\alpha - \beta} \\ &= \frac{\alpha^{n+2} - \beta^{n+2}}{\alpha - \beta}, \end{aligned}$$

en:

$$\begin{aligned} F_{n-1} = F_{n+1} - F_n &= \frac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta} - \frac{\alpha^n - \beta^n}{\alpha - \beta} \\ &= \frac{\alpha^{n-1} - \beta^{n-1}}{\alpha - \beta}. \end{aligned}$$

Inductief volgt dat de stelling geldt voor alle $n \in \mathbb{Z}$. □

Bewijs. (4.1.4) De gevallen $q = 2$ en $q = 5$ berusten op eenvoudig uitschrijven. Voor de andere priemgetallen vragen we ons af of het polynoom

$$f = X^2 - X - 1 \in \mathbb{Z}/q\mathbb{Z}[X]$$

reducibel is. Het is welbekend dat dit het geval is als de discriminant van f een kwadraat is in $\mathbb{Z}/q\mathbb{Z}$. Deze discriminant is gelijk aan $(-1)^2 - 4 \cdot 1 \cdot (-1) = 5$. We noteren voor twee oneven priemgetallen $p, q \in \mathbb{Z}_{\geq 1}$ het Legendre-symbool met $\left(\frac{p}{q}\right)$. Er geldt dat:

$$\left(\frac{5}{q}\right) \cdot \left(\frac{q}{5}\right) = (-1)^{\frac{(5-1)(q-1)}{4}} = 1.$$

We concluderen dat 5 een kwadraat is modulo q, dan en slechts dan als q een kwadraat is modulo 5. Er geldt dat q een kwadraat is modulo 5, dan

en slechts dan als $q \equiv 1, -1 \bmod 5$. Omdat q oneven is, is dit equivalent met $q \equiv 1, 9 \bmod 10$.
Als dit het geval is, dan geldt dat $X^2 - X - 1 = (X - \alpha)(X - \beta)$ voor elementen $\alpha, \beta \in \mathbb{Z}/q\mathbb{Z}[X]$, en omdat $q \neq 5$ geldt dan wegens Lemma 4.8 voor alle $n \in \mathbb{Z}$ dat $F_n \equiv \frac{\alpha^n - \beta^n}{\alpha - \beta} \bmod q$. Nu geldt dat $\alpha, \beta \in (\mathbb{Z}/q\mathbb{Z})^*$, omdat $\alpha(\alpha - 1) = 1, \beta(\beta - 1) = 1$. Dan is hun orde een deler van de groepsorde van $(\mathbb{Z}/q\mathbb{Z})^*$, en deze is gelijk aan $q - 1$. Er volgt voor elke $n \in \mathbb{Z}$ dat:

$$\begin{aligned} F_{n+q-1} &= \frac{\alpha^{n+q-1} - \beta^{n+q-1}}{\alpha - \beta} \\ &= \frac{\alpha^n - \beta^n}{\alpha - \beta} \\ &= F_n, \end{aligned}$$

en dus is $\pi(q)$ een deler van $q - 1$.

Als geldt dat $q \equiv 3, 7 \bmod 10$, dan is f irreducibel. Noteer nu:

$$\theta = X + (X^2 - X - 1) \in (\mathbb{Z}/q\mathbb{Z})[X]/(X^2 - X - 1).$$

Dan is

$$(\mathbb{Z}/q\mathbb{Z})[X]/(X^2 - X - 1) \cong (\mathbb{Z}/q\mathbb{Z})[\theta]$$

een lichaamsuitbreiding van graad 2 over $\mathbb{Z}/q\mathbb{Z}$. Merk op dat $(1 - \theta) = -\theta^{-1}$ het andere nulpunt is van $X^2 - X - 1$. Immers:

$$(1 - \theta)^2 - (1 - \theta) - 1 = 1 - 2\theta + \theta^2 - 1 + \theta - 1 = \theta^2 - \theta - 1 = 0.$$

Uit de theorie van eindige lichamen volgt dat $\mathbb{Z}/q\mathbb{Z}[\theta]$ een Galois-uitbreiding is van $\mathbb{Z}/q\mathbb{Z}$, met Galois-groep G, voortgebracht door het Frobenius-automorfisme:

$$\begin{aligned} \mathbb{Z}/q\mathbb{Z}[\theta] &\to \mathbb{Z}/q\mathbb{Z}[\theta], \\ x &\mapsto x^q. \end{aligned}$$

Deze afbeelding is de identiteit op $\mathbb{Z}/q\mathbb{Z}$, en beeldt de nulpunten van $X^2 - X - 1$ op elkaar af. Dan geldt dat $\theta^q = (1 - \theta) = -\theta^{-1}$. Dit betekent dan dat $\theta^{q+1} = \theta \cdot (-\theta^{-1}) = -1 \in \mathbb{Z}/q\mathbb{Z}$, en dus geldt dat $\theta^{2(q+1)} = 1$. Omdat $q \neq 2$, geldt dat $-1 \neq 1$, en dus vinden we dat $\pi(q)$ een deler is van $2(q + 1)$ die geen deler is van $q + 1$. □

Bewijs. (4.1.5)
Schrijf opnieuw $m = \prod_{p \text{ priem}} p^{k_p}$. Laat I de verzameling priemgetallen waarvoor $k_p > 0$, zodat $m = \prod_{p \in I} p^{k_p}$. Dan geldt wegens Stelling 4.1.2 en Stelling 4.1.3 dat:

$$\pi(m) = \operatorname{kgv}_{p \in I}\left(\pi(p^{k_p})\right) \Big| \operatorname{kgv}_{p \in I}\left(\pi(p) \cdot p^{k_p - 1}\right),$$

en dus vinden we:

$$\pi(m) \left| \left(\operatorname{kgv}_{p \in I}(\pi(p)) \cdot \prod_{p \in I} p^{k_p - 1} \right) \right.$$

Merk op dat er voor elk oneven priemgetal q een $r \in \mathbb{Z}_{>0}$ bestaat zodanig dat $r \leq q$, en $\pi(q)|4r$. Immers: voor $q = 5$ kunnen we $r = 5$ nemen, voor $q \equiv 1, 9 \mod 10$ kunnen we $r = q - 1$ nemen, en voor $q \equiv 3, 7 \mod 10$ kunnen we $r = \frac{q+1}{2}$ nemen. Laat voor elke $p \in I$ de bijbehorende r_p zoals hierboven.
Stel nu dat m oneven is. Dan geldt dat:

$$\text{kgv}_{p\in I}(\pi(p))|\text{kgv}_{p\in I}(4r_p) = 4 \cdot \text{kgv}_{p\in I}(r_p),$$

en dus geldt $\text{kgv}_{p\in I}(\pi(p)) \leq 4\prod_{p\in I} r_p \leq 4\prod_{p\in I} p$. Er volgt dat:

$$\pi(m) \leq 4\prod_{p\in I} p \cdot \prod_{p\in I} p^{k_p-1} = 4\prod_{p\in I} p^{k_p} = 4m.$$

Stel nu dat m even is. Dan omdat $\pi(2) = 3$, geldt:

$$\text{kgv}_{p\in I}(\pi(p)) = \text{kgv}(3, \text{kgv}_{p\in I, p\neq 2}(\pi(p)))|3\cdot\text{kgv}_{p\in I,p\neq 2}(4r_p) = 12\cdot\text{kgv}_{p\in I,p\neq 2}(r_p),$$

en dus geldt:

$$\text{kgv}_{p\in I}(\pi(p)) \leq 12 \cdot \prod_{p\in I, p\neq 2} p = 6 \cdot \prod_{p\in I} p.$$

We concluderen dat:

$$\pi(m) \leq \text{kgv}_{p\in I}(\pi(p)) \cdot \prod_{p\in I} p^{k_p-1} = 6 \cdot \prod_{p\in I} p^{k_p} = 6m.$$

□

Referenties

[1] Lenstra, H.W. (2005), Profinite Fibonacci Numbers, Nieuw Arch. Wisk. (5) 6, 297-300.

[2] Wall, D. D. (1960), Fibonacci Series Modulo m, American Mathematical Monthly 67 (6): 525-532

[3] Primegrid, (2012), Wall-Sun-Sun Prime Search, geraadpleegd: 24-06-2015

`http://www.primegrid.com/forum_thread.php?id=3008&nowrap=true#45946`