J.M. Kamphuis

Fibonacci-dekpunten en contracties

Bachelorscriptie

17 juni 2019

Scriptiebegeleider: Prof. dr. H. W. Lenstra

Universiteit Leiden
Mathematisch Instituut

Inhoudsopgave

1 Inleiding

De Fibonacci-rij is een van de bekendste wiskundige rijen. Hij wordt geconstrueerd door als nulde element een 0, als eerste element een 1 en voor elk volgend element in de rij de som van zijn twee voorgangers te nemen. Dan begint de rij als volgt:

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, ...$$

Deze rij kunnen we koppelen aan een functie, de zogenaamde Fibonacci-functie. Deze functie stuurt ieder element $n \in \mathbb{Z}_{\geq 0}$ naar het n-de element van de Fibonacci-rij. Deze Fibonacci-functie heeft drie dekpunten, namelijk $n = 0, n = 1$ en $n = 5$. We kunnen deze functie uitbreiden naar de negatieve gehele getallen door iedere $n \in \mathbb{Z}_{<0}$ iteratief te sturen naar $F_{n+2} - F_{n+1}$. Ook na deze uitbreiding heeft de Fibonacci-functie precies drie dekpunten.

In dit onderzoek koppelen we de Fibonacci-functie aan de verzameling van de pro-eindige getallen, $\hat{\mathbb{Z}}$. Deze verzameling vormt onder de volgende metriek een completering van $\mathbb{Z}$:

$$d : \mathbb{Z} \times \mathbb{Z} \to \mathbb{R}_{\geq 0}$$

$$(x, y) \mapsto \begin{cases} \frac{1}{\min\{n \in \mathbb{Z}_{>0} :\ x \not\equiv y \pmod{n}\}} & \text{als } x \neq y \\ 0 & \text{als } x = y \end{cases}$$

Deze metriek geeft ook een topologie op $\hat{\mathbb{Z}}$, waarmee $\hat{\mathbb{Z}}$ een topologische ruimte is, die compact en Hausdorff is.

Het blijkt dat we de Fibonacci-functie F continu kunnen uitbreiden naar de pro-eindige getallen. Deze uitbreiding blijkt niet 3, maar 11 dekpunten te hebben. Deze worden gegeven door de volgende stelling, die bewezen zal worden in hoofdstuk 6.

Stelling 6.1: Zij $F : \hat{\mathbb{Z}} \to \hat{\mathbb{Z}}$ de Fibonacci-functie. Dan geldt:

1. $\{z \in \hat{\mathbb{Z}} : F(z) = z,\ z \text{ even}\} = \{0\}$.
2. Voor iedere $a \in \{1, 5\}, b \in \{-5, -1, 0, 1, 5\}$ is er een unieke $z_{a,b} \in \hat{\mathbb{Z}}$ zodanig dat deze $z_{a,b}$ voldoet aan de volgende eisen:
   - $F(z_{a,b}) = z_{a,b}$;
   - Voor alle $k \in \mathbb{Z}_{\geq 0}$ geldt $z_{a,b} \equiv a \pmod{6^k}$ en $z_{a,b} \equiv b \pmod{5^k}$.
3. $\left\{z \in \hat{\mathbb{Z}} : F(z) = z,\ z \text{ oneven}\right\} = \left\{z_{a,b} \in \hat{\mathbb{Z}} : a \in \{1, 5\},\ b \in \{-5, -1, 0, 1, 5\}\right\}$.

Ook blijken de dekpunten mooie eigenschappen te hebben. Zo wordt in hoofdstuk 6.1 de volgende stelling over $z_{5,-5}$ bewezen.

Stelling: Er geldt $z_{5,-5}^2 \equiv 25 \pmod{201!}$, maar $z_{5,-5}^2 \not\equiv 25 \pmod{202!}$.

Dit onderwerp is eerder bestudeerd door H. Lenstra, J. Bulthuis en D. Hokken. De theorie over de Fibonacci-functie op $\hat{\mathbb{Z}}$ wordt geïntroduceerd door H. Lenstra (Lenstra, 2005) [1]. Daarnaast wordt in dit artikel een aantal bijzondere eigenschappen van de dekpunten genoemd, die zeer de moeite waard zijn om verder onderzocht te worden. In de bachelorscriptie van J. Bulthuis wordt onder andere bewezen dat de Fibonacci-functie F een unieke continue voortzetting $\hat{F} : \hat{\mathbb{Z}} \to \hat{\mathbb{Z}}$ heeft (Bulthuis, 2014) [2]. In de bachelorscriptie van D. Hokken zijn met iteratieve methoden de

eerste 14 decimalen van de dekpunten van deze functie gevonden. Ook wordt hierin stelling 6.1 genoemd als vermoeden, maar het bewijs blijft achterwege (Hokken, 2018) [7].

Voor het bewijs van stelling 6.1 wordt onder andere gebruik gemaakt van p-adische machtreeksen. Daarnaast wordt gebruik gemaakt van een eigen contractiestelling, die enigszins lijkt op de contractiestelling van Banach. Echter heeft deze stelling andere voorwaarden dan de contractiestelling van Banach. Voor de stelling is de volgende definitie nodig.

Definitie: Een *ultrametrische ruimte* is een metrische ruimte (X, d) zodanig dat de metriek d voldoet aan de *ultrametrische eigenschap*: voor iedere $x, y, z \in X$ geldt $d(x, z) \leq \max\{d(x, y), d(y, z)\}$.

De aangepaste versie van de contractiestelling zal in hoofdstuk 5 bewezen worden en luidt als volgt:

Stelling: (Contractiestelling) Zij (X, d) een niet-lege, complete, ultrametrische ruimte zodanig dat 0 het enige verdichtingspunt van $d(X \times X)$ is. Dan heeft iedere contractie $f : X \to X$ een uniek dekpunt.

2 Pro-eindige getallen

Om de pro-eindige getallen te introduceren, merken we eerst op dat ieder element $a \in \mathbb{Z}$ uniek te representeren is aan de hand van al zijn restklassen. Iedere $a \in \mathbb{Z}$ is immers uniek te schrijven als $a = (a \pmod 1), a \pmod 2), a \pmod 3), ...) \in \prod_{n=1}^{\infty} \mathbb{Z}/n\mathbb{Z}$. Daarnaast geldt voor iedere $n, n' \in \mathbb{Z}_{>0}$ met $n'|n$ dat $(a \pmod n) \pmod{n'} = a \pmod{n'}$. Met behulp van deze representatie kunnen we ook een representatie opschrijven die wel voldoet aan deze modulo eis, maar die niet correspondeert met een element uit $\mathbb{Z}$. Bekijk bijvoorbeeld de representatie die 1 is modulo alle 2-machten en 0 is modulo alle oneven priemmachten. Dan ziet het begin van deze representatie er als volgt uit: $(0, 1, 0, 1, 0, 3, 0, 1, 0, 5, 0, 9, ...)$. Deze voldoet per constructie aan de eisen van de representatie, maar correspondeert niet met een geheel getal. Immers, als dit wel zo zou zijn zou dit getal een veelvoud moeten zijn van alle oneven priemmachten. Het enige getal dat een veelvoud is van alle oneven priemmachten is 0, maar 0 is niet $1 \pmod 2$. Dit leidt tot de definitie van de pro-eindige getallen.

Definitie: De *verzameling pro-eindige getallen* is de verzameling:

$$\hat{\mathbb{Z}} := \left\{ (a_n)_{n=1}^{\infty} \in \prod_{m=1}^{\infty} \mathbb{Z}/m\mathbb{Z} : \forall n, n' \in \mathbb{Z}_{\geq 1} : n' \mid n \Rightarrow a_n \equiv a_{n'} \pmod{n'} \right\}.$$

Merk op dat iedere $\mathbb{Z}/m\mathbb{Z}$ een ring is, het product daarmee ook een ring is en $\hat{\mathbb{Z}}$ daarmee een deelverzameling van een ring is. De bewerkingen zijn de coördinaatsgewijze optelling en vermenigvuldiging. Het is gemakkelijk te verifiëren dat $0, 1 \in \hat{\mathbb{Z}}$ en dat voor iedere $x, y \in \hat{\mathbb{Z}}$ geldt $x + y, xy, -x \in \hat{\mathbb{Z}}$. Hiermee is $\hat{\mathbb{Z}}$ een deelring van $\prod_{m=1}^{\infty} \mathbb{Z}/m\mathbb{Z}$. Daarnaast kunnen we $\mathbb{Z}$ als deelring inbedden in $\hat{\mathbb{Z}}$ via de afbeelding $\phi : \mathbb{Z} \to \hat{\mathbb{Z}}$, $a \mapsto (a \pmod 1), a \pmod 2), ...)$. Merk op dat we ook in de pro-eindige getallen kunnen praten over even en oneven. Net als in de gehele getallen is een getal $x \in \hat{\mathbb{Z}}$ even als geldt $x \equiv 0 \pmod 2$ en oneven als geldt $x \equiv 1 \pmod 2$.

We definiëren een topologie op $\hat{\mathbb{Z}}$ door iedere $\mathbb{Z}/m\mathbb{Z}$ de discrete topologie te geven. Het product krijgt vervolgens de producttopologie en $\hat{\mathbb{Z}}$ krijgt de geïnduceerde topologie. Voor deze topologie geldt dan:

Lemma 2.1: $U \subset \hat{\mathbb{Z}}$ is open dan en slechts dan als er voor alle $x \in U$ een $N \in \mathbb{Z}_{\geq 1}$ is zodanig dat $\left\{ y \in \hat{\mathbb{Z}} : y_N = x_N \right\} \subset U$.

Met deze topologie heeft $\hat{\mathbb{Z}}$ een aantal mooie eigenschappen. Omdat $\hat{\mathbb{Z}}$ een deelruimte van een product van Hausdorffruimtes is, is $\hat{\mathbb{Z}}$ zelf ook Hausdorff. De ringen $\mathbb{Z}/m\mathbb{Z}$ zijn compact, dus uit de stelling van Tychonov volgt dat het product $\prod_{m=1}^{\infty} \mathbb{Z}/m\mathbb{Z}$ ook compact is. Aangezien $\hat{\mathbb{Z}}$ een gesloten deelverzameling van deze compacte verzameling is, is $\hat{\mathbb{Z}}$ zelf ook compact. Bovendien ligt $\mathbb{Z}$ dicht in $\hat{\mathbb{Z}}$. De precieze bewijzen van deze eigenschappen en lemma 2.1 zijn te vinden in Bulthuis (2014) [2].

Ook kunnen we $\hat{\mathbb{Z}}$ opvatten als de completering van $\mathbb{Z}$ onder een bepaalde metriek. Definieer hiervoor de volgende afbeelding d op $\mathbb{Z}$:

$$d : \mathbb{Z} \times \mathbb{Z} \to \mathbb{R}_{\geq 0}$$

$$(x, y) \mapsto \begin{cases} \frac{1}{\min\{n \in \mathbb{Z}_{>0} :\ x \not\equiv y \pmod{n}\}} & \text{als } x \neq y \\ 0 & \text{als } x = y \end{cases}.$$

Het is eenvoudig na te gaan dat deze afbeelding een metriek is op $\mathbb{Z}$ en dat deze uitgebreid kan worden naar $\hat{\mathbb{Z}} \times \hat{\mathbb{Z}}$ zodanig dat d ook op $\hat{\mathbb{Z}}$ een metriek is. Dus $\hat{\mathbb{Z}}$ is een complete, metrische ruimte, die $\mathbb{Z}$ als dichte deelverzameling heeft, dus $\hat{\mathbb{Z}}$ is de completering van $\mathbb{Z}$ onder deze metriek. De metriek op $\hat{\mathbb{Z}}$ wordt nu gegeven door de volgende afbeelding:

$$d : \hat{\mathbb{Z}} \times \hat{\mathbb{Z}} \to \mathbb{R}_{\geq 0}$$

$$(x, y) \mapsto \begin{cases} \frac{1}{\min\{n \in \mathbb{Z}_{>0} :\ x_n \neq y_n\}} & \text{als } x \neq y \\ 0 & \text{als } x = y \end{cases}.$$

Definitie: Een *ultrametrische ruimte* is een metrische ruimte (X, d) zodanig dat de metriek d voldoet aan de *ultrametrische eigenschap*: voor iedere $x, y, z \in X$ geldt $d(x, z) \leq \max\{d(x, y), d(y, z)\}$.

Claim: De metriek d op $\hat{\mathbb{Z}}$ voldoet aan de ultrametrische eigenschap.

Bewijs. Zij $x, y, z \in \hat{\mathbb{Z}}$ willekeurig gegeven. Als geldt $x = z$ volgt $d(x, z) \leq \max\{d(x, y), d(y, z)\}$. Neem aan dat $x \neq z$, dan geldt $d(x, z) = \frac{1}{n}$ voor de minimale $n \in \mathbb{Z}_{>0}$ met $x_n \neq z_n$. Dan moet gelden $x_n \neq y_n$ of $y_n \neq z_n$. Stel er geldt $x_n \neq y_n$, dan moet $\min\{m \in \mathbb{Z}_{>0} : x_m \neq y_m\} \leq n$ dus $\max\{d(x, y), d(y, z)\} \geq d(x, y) \geq \frac{1}{n} = d(x, z)$. Uit het andere geval volgt op dezelfde manier $\max\{d(x, y), d(y, z)\} \geq d(y, z) \geq \frac{1}{n} = d(x, z)$. Dus er geldt $d(x, z) \leq \max\{d(x, y), d(y, z)\}$, dus de metriek d voldoet aan de ultrametrische eigenschap. □

Opmerking: De topologie zoals gedefinieerd in lemma 2.1 is dezelfde topologie als de topologie die geïnduceerd wordt door de metriek d. De geïnduceerde topologie wordt immers voortgebracht door de open bollen $B(a, r)$ om punt $a \in \hat{\mathbb{Z}}$ met straal $r \in \mathbb{R}_{>0}$. Dit geeft de open bollen van de vorm $B(a, r) = \{x \in \hat{\mathbb{Z}} : d(a, x) < r\}$. Zij $m \in \mathbb{Z}_{>1}$ zodanig dat $\frac{1}{m} < r$ en $\frac{1}{m-1} \geq r$ en neem $m = 1$ als $r > 1$. Dan geldt:

$$B(a, r) = \bigcup_{N=m}^{\infty} \{x \in \hat{\mathbb{Z}} : x = a \text{ of } N = \min\{n \in \mathbb{Z}_{>0} : x_n \neq a_n\}\} = \bigcap_{N=1}^{m-1} \{x \in \hat{\mathbb{Z}} : x_N = a_N\}.$$

Deze laatste zijn de verzamelingen zoals in lemma 2.1 over de topologie.

Het bewijs van de volgende stelling is te vinden in hoofdstuk 9 van "Topologie" door P. Bruin [3].

Stelling 2.2: Zij (X, d) een compacte, metrische ruimte. Dan is X compleet.

Lemma: De topologische ruimte $\hat{\mathbb{Z}}$ is compleet.

Bewijs. (Lemma) We weten dat $\hat{\mathbb{Z}}$ compact is en dat d een metriek is op $\hat{\mathbb{Z}}$. Dus is $(\hat{\mathbb{Z}}, d)$ een compacte, metrische ruimte dus volgt uit stelling 2.2 dat $(\hat{\mathbb{Z}}, d)$ compleet is. □

2.1 Verband met de p-adische getallen

Er is een natuurlijke manier om de pro-eindige getallen in verband te brengen met de p-adische getallen. Om dit te doen hebben we eerst een paar definities nodig.

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

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

Definitie: Een *isomorfisme van topologische ringen* is een afbeelding f tussen topologische ringen zodanig dat f zowel een ringisomorfisme als een homeomorfisme is.

Opmerking: Door nagaan van de definitie blijkt dat $\hat{\mathbb{Z}}$ een topologische ring is.

Definitie: Zij R een domein. Een *valuatie* $|.|$ is een afbeelding $|.| : R \to \mathbb{R}_{\geq 0}$ die voor iedere $x, y \in R$ voldoet aan de volgende eigenschappen:

- $|x| = 0$ dan en slechts dan als $x = 0$;
- $|xy| = |x| \cdot |y|$;
- $|x + y| \leq |x| + |y|$.

Een valuatie en een metriek zijn op natuurlijke manier met elkaar in verband te brengen door een metriek te definiëren als de afbeelding:

$$d : R \times R \to \mathbb{R}_{\geq 0}$$

$$(x, y) \mapsto |x - y|.$$

Definitie: Een valuatie $|.| : R \to \mathbb{R}_{\geq 0}$ is *ultrametrisch* als voor alle $x, y \in R$ geldt $|x + y| \leq \max\{|x|, |y|\}$.

Laat K een lichaam met een ultrametrische valuatie $|.|$. Dan is $R = \{x \in K : |x| \leq 1\}$ een deelring van K en $m = \{x \in K : |x| < 1\}$ is een maximaal ideaal van R. Als K een lichaam is geldt bovendien $R \setminus m = R^*$.

Zij $\mathcal{P}$ de verzameling van priemgetallen in $\mathbb{Z}$.

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

$$\mathbb{Z}_p := \left\{ (a_{p^k})_{k=0}^{\infty} \in \prod_{m=0}^{\infty} \mathbb{Z}/p^m\mathbb{Z} : \forall n \in \mathbb{Z}_{\geq 0} : a_{p^{n+1}} \equiv a_{p^n} \pmod{p^n} \right\}.$$

Door op analoge manier als bij $\hat{\mathbb{Z}}$ ringoperaties en een topologie op $\mathbb{Z}_p$ te definiëren, vormt $\mathbb{Z}_p$ ook een topologische ring en is $\mathbb{Z}_p$ ook Hausdorff en compact. Daarnaast is $\mathbb{Z}_p$ een hoofdideaaldomein, waarvan $p\mathbb{Z}_p$ het enige maximale ideaal is. Dit impliceert dat er in $\mathbb{Z}_p$ unieke factorisatie bestaat. Zo kunnen we ieder element $z \in \mathbb{Z}_p$ met $z \neq 0$ schrijven als $z = \alpha p^k$ voor een zekere $\alpha \in \mathbb{Z}_p^*$ en $k \in \mathbb{Z}_{\geq 0}$. Het lichaam $\mathbb{Q}_p$ van de p-adische getallen is gedefinieerd als het quotiëntenlichaam van $\mathbb{Z}_p$.

Een equivalente definitie van de ring der p-adische getallen $\mathbb{Z}_p$ wordt gegeven door de projectieve limiet. Er geldt immers:

$$\mathbb{Z}_p = \varprojlim_n (\mathbb{Z}/p^n\mathbb{Z}) .$$

Op dezelfde manier is $\hat{\mathbb{Z}}$ te schrijven als een projectieve limiet. Hiervoor geldt:

$$\hat{\mathbb{Z}} = \varprojlim_m (\mathbb{Z}/m\mathbb{Z}) .$$

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

$$\phi : \hat{\mathbb{Z}} \to \prod_{p \in \mathcal{P}} \mathbb{Z}_p$$

$$(a_n)_{n=1}^{\infty} \mapsto ((a_{p^m})_{m=0}^{\infty})_{p \in \mathcal{P}}.$$

Het bewijs van deze stelling wordt hier niet gegeven, maar is makkelijk terug te vinden, zoals in hoofdstuk 2.2 van "Pro-eindige Fibonacci-getallen" van J. Bulthuis (2014) [2].

Opmerking: Wegens het isomorfisme van bovenstaande stelling, kunnen we ook als definitie van $\hat{\mathbb{Z}}$ het product van alle p-adische ringen nemen. Deze definitie is equivalent met de eerder gegeven definities van $\hat{\mathbb{Z}}$. Het gebruik van deze definitie maakt het mogelijk om elementen van $\hat{\mathbb{Z}}$ op te vatten als rijtjes $z = (z_p)_{p \in \mathcal{P}}$, waarbij z_p de coördinaat van z in $\mathbb{Z}_p$ is.

Definitie: Laat $z \in \mathbb{Z}_p$. Als $z \neq 0$, laat $z = \alpha p^k$ de unieke factorisatie van z met $\alpha \in \mathbb{Z}_p^*$ en $k \in \mathbb{Z}_{\geq 0}$. De *$p$-adische valuatie* is de afbeelding

$$|.|_p : \mathbb{Z}_p \to \mathbb{R}_{>0}$$

$$z \mapsto \begin{cases} p^{-k} & \text{als } z \neq 0 \\ 0 & \text{als } z = 0 \end{cases} .$$

Merk op dat de p-adische valuatie ultrametrisch is. We kunnen deze p-adische valuatie in verband brengen met onze metriek d. Voor de metriek d en de p-adische valuatie geldt namelijk:

$$d(x, y) = \max_{p \in \mathcal{P}} \left\{ \frac{|x - y|_p}{p} \right\} .$$

Opmerking: De p-adische valuatie $|.|_p$ zal in het vervolg vaak genoteerd worden als $|.|$. Het is aan de lezer om uit de context op te maken dat het hier om een p-adische valuatie gaat en welke p-waarde hierbij hoort.

3 Fibonacci-getallen

De Fibonacci-rij is een rij met waarden in $\mathbb{Z}_{\geq 0}$ waarbij het nulde element gelijk is aan 0 en het eerste element gelijk is aan 1. Ieder volgend element in de rij is de som van zijn twee voorgangers. Dit geeft de volgende rij:

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, ...$$

Aan deze rij kennen we een functie $F : \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0}$ toe die iedere $n \in \mathbb{Z}_{\geq 0}$ naar het n-de Fibonacci-getal stuurt. Deze functie is uit te breiden naar heel $\mathbb{Z}$, door voor $n \leq 0$ het $n - 1^{\text{ste}}$ Fibonacci-getal te definiëren als $F_{n-1} = F_{n+1} - F_n$. Deze functie heeft precies drie dekpunten, namelijk $n = 0, n = 1$ en $n = 5$.

Zoals bewezen in (Bulthuis, 2014) [2] is deze functie continu uit te breiden naar de pro-eindige getallen. Voor iedere $m \in \mathbb{Z}_{\geq 1}$ kunnen we de Fibonacci-rij modulo m bekijken. Voor $m = 2$ geeft dit bijvoorbeeld de volgende rij:

$$(F_n \pmod 2)_{n=0}^{\infty} = (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, ...).$$

Deze rij heeft periode 3. Aangezien de Fibonacci-rij periodiek is modulo iedere $m \in \mathbb{Z}$ kunnen we spreken over de periode van de rij modulo m. Dat de Fibonacci-functie continu uit te breiden is naar $\hat{\mathbb{Z}}$ wordt bewezen door te bewijzen dat F periodiek is modulo elk geheel getal $m \in \mathbb{Z}_{>0}$.

We noteren $\pi(m)$ voor de minimale periode van de Fibonacci-rij modulo m voor iedere $m \in \mathbb{Z}_{\geq 1}$. In de scriptie van J. Bulthuis (2014) is de volgende stelling over deze periode bewezen [2].

Stelling 3.1:

1. Voor $m \in \mathbb{Z}_{>2}$ is $\pi(m)$ even.
2. Voor p priem en $n \in \mathbb{Z}_{\geq 1}$ geldt $\pi(p^n)|\pi(p)p^{n-1}$.
3. Laat $m = \prod_{p \text{ priem}} p^{k_p}$ met $k_p = 0$ voor bijna iedere p. Dan geldt:
$$\pi(m) = \text{kgv}_p(\pi(p^{k_p})).$$
4. Voor p priem geldt:
   - Als $p = 2$, dan $\pi(p) = 3$;
   - Als $p = 5$, dan $\pi(p) = 20$;
   - Als $p \equiv 1, 9 \pmod{10}$, dan $\pi(p)|p - 1$;
   - Als $p \equiv 3, 7 \pmod{10}$, dan $\pi(p)|2(p + 1)$ maar $\pi(p) \nmid p + 1$.
5. Voor elke $m \in \mathbb{Z}_{\geq 1}$ geldt $\pi(m) \leq 6m$.

Met behulp van de periode krijgen we het onderstaande, commutatieve diagram. Hierin zijn de horizontale pijlen de Fibonacci-functie en de pijlen naar beneden de kanonieke projecties.

$$\begin{array}{ccc} \hat{\mathbb{Z}} & \xrightarrow{F} & \hat{\mathbb{Z}} \\ \downarrow & & \downarrow \\ \mathbb{Z}/\pi(m)\mathbb{Z} & \xrightarrow{F} & \mathbb{Z}/m\mathbb{Z} \end{array}$$

3.1 De pro-eindige Fibonacci-functie

Om de pro-eindige Fibonacci-functie te kunnen definiëren is eerst een aantal definities nodig.

Zij R een commutatieve ring. Definieer $R[\vartheta] = R[X]/(X^2 - X - 1)$, en laat $\vartheta = (X \pmod{X^2 - X - 1})$. Definieer de volgende afbeelding op $R[\vartheta]$:

$$\bar{\cdot} : R[\vartheta] \to R[\vartheta]$$

$$a + b\vartheta \mapsto (a + b) - b\vartheta.$$

Het is eenvoudig na te gaan dat $\bar{\cdot}$ een ringautomorfisme is, en dat geldt $\bar{\cdot} \circ \bar{\cdot} = \mathrm{id}$. Voor ϑ gelden nu de volgende identiteiten:

- $\overline{\vartheta} = 1 - \vartheta$;
- $\vartheta^2 = \vartheta + 1$;
- $\vartheta\overline{\vartheta} = -1$;
- $(\vartheta - \overline{\vartheta})^2 = 5$.

Aangezien ϑ een eenheid is in $R[\vartheta]$ is ϑ^n voor $n \in \mathbb{Z}$ goed gedefinieerd.

Lemma: Voor $n \in \mathbb{Z}$ geldt $\overline{\vartheta^n} = \overline{\vartheta}^n$.

Bewijs. Aangezien $\bar{\cdot}$ een automorfisme is volgt voor $n \geq 0$ het lemma direct. Voor $n \in \mathbb{Z}_{<0}$ volgt het lemma omdat ϑ een eenheid is. □

Lemma 3.1.1: $\vartheta - \overline{\vartheta}$ is geen nuldeler in $\hat{\mathbb{Z}}[\vartheta]$.

Bewijs. Laat $\gamma \in \hat{\mathbb{Z}}[\vartheta]$ en stel $\gamma(\vartheta - \overline{\vartheta}) = 0$. Dan geldt ook $0 = \gamma(\vartheta - \overline{\vartheta})^2 = 5\gamma$. Aangezien we $\gamma \in \hat{\mathbb{Z}}[\vartheta]$ uniek kunnen schrijven als $\gamma = a + b\vartheta$ met $a, b \in \hat{\mathbb{Z}}$ geeft dit $5\gamma = 5a + 5b\vartheta = 0$. Aangezien 5 geen nuldeler is in $\hat{\mathbb{Z}}$ moet gelden $a = b = 0$, dus $\gamma = 0$. Dus $\vartheta - \overline{\vartheta}$ is geen nuldeler in $\hat{\mathbb{Z}}[\vartheta]$. □

Lemma 3.1.2: Zij R een commutatieve ring. Voor $n \in \mathbb{Z}$ geldt $\vartheta^n - \overline{\vartheta}^n \in R[\vartheta] \cdot (\vartheta - \overline{\vartheta})$.

Bewijs. Noem $I := R[\vartheta] \cdot (\vartheta - \overline{\vartheta})$. Zij $n \in \mathbb{Z}$. Er geldt

$$\vartheta \equiv \overline{\vartheta} \pmod{I},$$

$$\text{dus } \vartheta^n \equiv \overline{\vartheta}^n \pmod{I},$$

$$\text{dus } \vartheta^n - \overline{\vartheta}^n \in I.$$

Dus er geldt $\vartheta^n - \overline{\vartheta}^n \in R[\vartheta] \cdot (\vartheta - \overline{\vartheta})$. □

Lemma: Voor $n \in \mathbb{Z}$ geldt $\vartheta^n = F_{n-1} + F_n\vartheta$ en $\overline{\vartheta}^n = F_{n-1} + F_n\overline{\vartheta}$.

Bewijs. Laat eerst $n \in \mathbb{Z}_{\geq 0}$. Voor $n = 0$ geldt $F_{-1} + F_0\vartheta = 1 = \vartheta^0$. Voor $n = 1$ geldt $F_0 + F_1\vartheta = 0 + \vartheta = \vartheta^1$. Stel voor $N \in \mathbb{Z}_{\geq 0}$ geldt $\vartheta^N = F_{N-1} + F_N\vartheta$ en $\vartheta^{N-1} = F_{N-2} + F_{N-1}\vartheta$. Voor $N + 1$ volgt uit de inductiehypothese dat geldt $\vartheta^{N+1} = \vartheta^N + \vartheta^{N-1} = F_{N-1} + F_N\vartheta + F_{N-2} + F_{N-1}\vartheta = F_N + F_{N+1}\vartheta$. Uit volledige inductie volgt dat voor iedere $n \in \mathbb{Z}_{\geq 0}$ geldt $\vartheta^n = F_{n-1} + F_n\vartheta$.

Stel voor $N \in \mathbb{Z}_{\leq 0}$ geldt $\vartheta^N = F_{N-1} + F_N\vartheta$ en $\vartheta^{N+1} = F_N + F_{N+1}\vartheta$. Voor $N - 1$ volgt uit de inductiehypothese dat geldt $\vartheta^{N-1} = \vartheta^{N+1} - \vartheta^N = F_N + F_{N+1}\vartheta - F_{N-1} - F_N\vartheta = F_{N-2} + F_{N-1}\vartheta$. Uit volledige inductie volgt dat voor iedere $n \in \mathbb{Z}_{\leq 0}$ geldt $\vartheta^n = F_{n-1} + F_n\vartheta$.

Dus voor iedere $n \in \mathbb{Z}$ geldt $\vartheta^n = F_{n-1} + F_n\vartheta$. Aangezien $\overline{\vartheta}$ het andere nulpunt is van $X^2 - X - 1 = 0$ geldt ook $\overline{\vartheta}^2 = \overline{\vartheta} + 1$, dus volgt analoog aan het bewijs voor ϑ dat voor iedere $n \in \mathbb{Z}$ geldt $\overline{\vartheta}^n = F_{n-1} + F_n\overline{\vartheta}$. □

Stelling: Zij $\vartheta \in \mathbb{Z}[\vartheta]$ een nulpunt van $X^2 - X - 1 = 0$. De Fibonacci-functie $F : \mathbb{Z} \to \mathbb{Z}$ is de functie gegeven door

$$n \mapsto \frac{\vartheta^n - \overline{\vartheta}^n}{\vartheta - \overline{\vartheta}}.$$

Bewijs. Er geldt

$$\vartheta^n - \overline{\vartheta}^n = F_{n-1} + F_n\vartheta - F_{n-1} - F_n\overline{\vartheta} = F_n(\vartheta - \overline{\vartheta}).$$

Aangezien $(\vartheta - \overline{\vartheta})$ geen nuldeler is en $\vartheta^n - \overline{\vartheta}^n \in \hat{\mathbb{Z}}[\vartheta](\vartheta - \overline{\vartheta})$ geeft dit

$$F_n = \frac{\vartheta^n - \overline{\vartheta}^n}{\vartheta - \overline{\vartheta}} \in \hat{\mathbb{Z}}[\vartheta].$$

Merk op dat wegens lemma's 3.1.1 en 3.1.2 deze deling bestaat en eenduidig is. Aangezien geldt $F_n \in \mathbb{Z}$ volgt nu dat geldt $F : \mathbb{Z} \to \mathbb{Z}$. □

Definitie: Laat $n = (n_m)_{m=1}^{\infty} \in \lim_{\leftarrow m} \mathbb{Z}/m\mathbb{Z} = \hat{\mathbb{Z}}$ en $\mu \in \lim_{\leftarrow m}((\mathbb{Z}/m\mathbb{Z})[\vartheta])^* = \hat{\mathbb{Z}}[\vartheta]^*$. Laat $k(m) = \mathrm{ord}(\mu_m)$. We definiëren *machtsverheffing* in $\hat{\mathbb{Z}}[\vartheta]$ als volgt:

$$\mu^n = (\mu^{n_{k(m)}})_{m=1}^{\infty} \in \varprojlim_m((\mathbb{Z}/m\mathbb{Z})[\vartheta])^* = \hat{\mathbb{Z}}[\vartheta]^*.$$

Laat $\mu, \nu \in \hat{\mathbb{Z}}[\vartheta]^*$ en $n, n' \in \hat{\mathbb{Z}}$, dan gelden voor deze machtsverheffing de volgende eigenschappen:

- $\mu^1 = \mu$
- $\mu^n \cdot \mu^{n'} = \mu^{n+n'}$
- $(\mu \cdot \nu)^n = \mu^n\nu^n$
- $(\mu^n)^{n'} = \mu^{n \cdot n'}$
- $\overline{\mu}^n = \overline{\mu^n}$
- De afbeelding $\hat{\mathbb{Z}} \times \hat{\mathbb{Z}}[\vartheta]^* \to \hat{\mathbb{Z}}[\vartheta]^*$, gegeven door $(n, \mu) \mapsto \mu^n$ is continu.

Wegens de eerste vier eigenschappen is $\hat{\mathbb{Z}}[\vartheta]^*$ een moduul over $\hat{\mathbb{Z}}$.

Lemma: Voor $\vartheta \in ((\mathbb{Z}/m\mathbb{Z})[\vartheta])^*$ geldt $\mathrm{ord}(\vartheta) = \pi(m)$.

Bewijs. Voor alle $n \in \mathbb{Z}$ gelden de volgende equivalenties:

$$\begin{aligned}
&\mathrm{ord}(\vartheta)|n \\
\iff &1 = \vartheta^n = F_{n-1} + F_n\vartheta \\
\iff &F_{n-1} = 1 \text{ en } F_n = 0 \\
\iff &F_{n-1} = F_{-1} \text{ en } F_n = F_0 \\
\iff &\text{voor alle } i \in \mathbb{Z} : F_{n+i} = F_i \\
\iff &\pi(m)|n.
\end{aligned}$$

Dus er moet gelden $\text{ord}(\vartheta) = \pi(m)$. □

Merk op dat $\vartheta\overline{\vartheta} = -1$, dus $(\vartheta - 1)\vartheta = 1$, dus voor alle $m \in \mathbb{Z}_{>0}$ geldt $\vartheta \in ((\mathbb{Z}/m\mathbb{Z})[\vartheta])^*$ en $\text{ord}(\vartheta) = \pi(m)$. Dit betekent dat voor $n \in \hat{\mathbb{Z}}$ geldt $\vartheta^n := (\vartheta^{n_{\pi(m)}})_{m=1}^{\infty} \in \lim_{\leftarrow m} \mathbb{Z}/m\mathbb{Z}$.

Lemma: Voor $n \in \hat{\mathbb{Z}}$ geldt $\vartheta^n - \overline{\vartheta}^n \in \hat{\mathbb{Z}}[\vartheta] \cdot (\vartheta - \overline{\vartheta})$.

Bewijs. Zij $m \in \mathbb{Z}_{>0}$ en laat $I_m := (\mathbb{Z}/m\mathbb{Z})[\vartheta] \cdot (\vartheta - \overline{\vartheta})$. Dan geldt:

$$\vartheta \equiv \overline{\vartheta} \pmod{I_m},$$

$$\text{dus } \vartheta^{n_{\pi(m)}} \equiv \overline{\vartheta}^{n_{\pi(m)}} \pmod{I_m},$$

$$\text{dus } \vartheta^{n_{\pi(m)}} - \overline{\vartheta}^{n_{\pi(m)}} \in I_m.$$

Dus voor iedere $m \in \mathbb{Z}_{>0}$ geldt $\vartheta^{n_{\pi(m)}} - \overline{\vartheta}^{n_{\pi(m)}} \in (\mathbb{Z}/m\mathbb{Z})[\vartheta] \cdot (\vartheta - \overline{\vartheta})$, dus er geldt $\vartheta^n - \overline{\vartheta}^n \in \hat{\mathbb{Z}}[\vartheta] \cdot (\vartheta - \overline{\vartheta})$. □

Lemma: Voor $n \in \hat{\mathbb{Z}}$ geldt $\vartheta^n = F_{n-1} + F_n\vartheta$ en $\overline{\vartheta}^n = F_{n-1} + F_n\overline{\vartheta}$.

Bewijs. Beschouw de volgende functies:

$$g : \hat{\mathbb{Z}} \to \hat{\mathbb{Z}}[\vartheta]$$

$$n \mapsto \vartheta^n,$$

$$h : \hat{\mathbb{Z}}[\vartheta] \to \hat{\mathbb{Z}} \times \hat{\mathbb{Z}}$$

$$a + b\vartheta \mapsto (a, b).$$

Dan is h een homeomorfisme en $f_1 = h \circ g$ is continu op $\hat{\mathbb{Z}}$.

Beschouw ook de volgende functie:

$$f_2 : \hat{\mathbb{Z}} \to \hat{\mathbb{Z}} \times \hat{\mathbb{Z}}$$

$$n \mapsto (F_{n-1}, F_n).$$

Merk op dat f_2 ook continu is op $\hat{\mathbb{Z}}$. De functies f_1 en f_2 zijn beide continu op $\hat{\mathbb{Z}}$, ze vallen samen op $\mathbb{Z}$ en $\mathbb{Z}$ ligt dicht in $\hat{\mathbb{Z}}$. Dus er volgt dat ze gelijk zijn op $\hat{\mathbb{Z}}$. Dus voor alle $n \in \hat{\mathbb{Z}}$ geldt $\vartheta^n = F_{n-1} + F_n\vartheta$. □

Stelling 3.1.3: Zij $\vartheta \in \mathbb{Z}[\vartheta]$ een nulpunt van $X^2 - X - 1 = 0$. De pro-eindige Fibonacci-functie $F : \hat{\mathbb{Z}} \to \hat{\mathbb{Z}}$ is de functie gegeven door

$$n \mapsto \frac{\vartheta^n - \overline{\vartheta}^n}{\vartheta - \overline{\vartheta}}.$$

Bewijs. Er geldt

$$\vartheta^n - \overline{\vartheta}^n = F_{n-1} + F_n\vartheta - F_{n-1} - F_n\overline{\vartheta} = F_n(\vartheta - \overline{\vartheta}).$$

Aangezien $(\vartheta - \overline{\vartheta})$ geen nuldeler is en $\vartheta^n - \overline{\vartheta}^n \in \hat{\mathbb{Z}}[\vartheta](\vartheta - \overline{\vartheta})$ geeft dit

$$F_n = \frac{\vartheta^n - \overline{\vartheta}^n}{\vartheta - \overline{\vartheta}} \in \hat{\mathbb{Z}}[\vartheta].$$

Aangezien geldt $F_n \in \hat{\mathbb{Z}}$ volgt nu dat geldt $F : \hat{\mathbb{Z}} \to \hat{\mathbb{Z}}$. □

4 Machtreeksen

Net als voor reële getallen kunnen we ook p-adische machtreeksen maken. Laat R een domein en definieer een ultrametrische valuatie op R waaronder R compleet is. Beschouw de machtreeks $f(X) = \sum_{n=0}^{\infty} f_n X^n$, met $f_n \in R$ voor alle $n \in \mathbb{Z}_{\geq 0}$. Deze machtreeks kunnen we opvatten als een functie op het moment dat f convergeert. Door te eisen dat $f_n \to 0$ als $n \to \infty$ wordt voor een $z \in R$ met $|z| \leq 1$ de waarde $f(z) = \sum_{n=0}^{\infty} f_n z^n$ bepaald door de beginstukken van de oneindige som. Deze beginstukken vormen een Cauchy-rij, die wegens de compleetheid van R convergeert. Een functie die gegeven wordt door een dergelijke machtreeks is continu.

De volgende stelling geeft informatie over het aantal nulpunten van een machtreeks. Het bewijs van deze stelling is terug te vinden in het artikel "Über den Wertevorrat von Potenzreihen im Gebiet der p-adischen Zahlen" van R. Strassmann (1928) [4] of in hoofdstuk 4.4 van Cassels (1986) [5].

Stelling (Strassmann, 1928): Zij R een compleet domein met de ultrametrische valuatie $|.|$ en zij $f(X)$ de machtreeks gegeven door $f(X) = \sum_{n=0}^{\infty} f_n X^n$, met $f_n \in R$. Stel dat $f_n \to 0$ als $n \to \infty$, maar dat niet alle f_n gelijk zijn aan 0. Dan is er slechts een eindig aantal $b \in R$ met $|b| \leq 1$ zodanig dat $f(b) = 0$. Sterker nog, er zijn hoogstens $N \in \mathbb{Z}_{\geq 0}$ dergelijke b, waarbij N voldoet aan $|f_N| = \max_n |f_n|$ en $|f_n| < |f_N|$ voor alle $n > N$.

In het komende hoofdstuk maken we gebruik van een uitbreiding van $\mathbb{Z}_5$. Definieer $\mathbb{Z}_5[\sqrt{5}] := \mathbb{Z}_5[X]/(X^2 - 5)$. Merk op dat $\mathbb{Z}_5$ een deelring is van het lichaam $\mathbb{Q}_5$ en dat $X^2 - 5$ irreducibel is in $\mathbb{Z}_5$, dit maakt $\mathbb{Z}_5[\sqrt{5}]$ een domein.

Definieer nu de volgende afbeelding op $\mathbb{Z}_5[\sqrt{5}]$:

$$\bar{.} : \mathbb{Z}_5[\sqrt{5}] \to \mathbb{Z}_5[\sqrt{5}]$$

$$a + b\sqrt{5} \mapsto a - b\sqrt{5}.$$

Het is eenvoudig na te gaan dat $\bar{.}$ een ringautomorfisme is, en dat geldt $\bar{.} \circ \bar{.} = \mathrm{id}$.

4.1 De p-adische logaritme en exponentiële functie

Net als voor de reële getallen bestaan er ook een een p-adische logaritme en exponentiële functie. In de volgende definities en lemma's is K een complete uitbreiding van $\mathbb{Z}_p$ met valuatie $|.|$.

Om het aantal factoren p in $n!$, met p priem en $n \in \mathbb{Z}_{\geq 0}$, te bepalen komt de volgende stelling van pas. Het bewijs is de vinden in het eerste hoofdstuk van Gupta (1980) [6].

Stelling 4.1: Zij p priem, $n \in \mathbb{Z}_{\geq 0}$ en schrijf n als zijn unieke representatie $n = \sum_{j=0}^{k} \alpha_j p^j$, $\alpha_j \in \mathbb{Z}_{\geq 0}$, $\alpha_j \leq p - 1$ en $\alpha_k \neq 0$ als $n > 0$ voor een zekere $k \in \mathbb{Z}_{\geq 0}$. Noteer $s_p(n) = \sum_{j=0}^{k} \alpha_j$. Het aantal factoren p in $n!$ wordt gegeven door:

$$\mathrm{ord}_p(n!) = \frac{n - s_p(n)}{p - 1}.$$

Definitie: De *p-adische logaritme* is gedefinieerd als:

$$\log_p : \{z \in K : |z - 1| < 1\} \to K$$

$$z \mapsto \sum_{i=1}^{\infty} (-1)^{i+1} \frac{(z-1)^i}{i}.$$

Definitie: De *p-adische exponentiële functie* is gedefinieerd als:

$$\exp_p : \left\{ w \in K : |w| < |p|^{\frac{1}{p-1}} \right\} \to \left\{ z \in K : |z-1| < |p|^{\frac{1}{p-1}} \right\}$$

$$w \mapsto \sum_{i=0}^{\infty} \frac{w^i}{i!}.$$

Merk op dat de logaritme en de exponentiële functie op een goed gekozen domein elkaars inverse zijn. Laat $m = \{w \in K : |w| < |p|^{\frac{1}{p-1}}\}$. Dan is m een additieve groep, en het is een ideaal van K. Verder is $1 + m$ een multiplicatieve groep. Beide groepen kunnen we met elkaar in verband brengen door middel van de p-adische logaritme en de p-adische exponentiële functie. Zo komt machtsverheffen in $1 + m$ overeen met vermenigvuldigen in m. Dit geeft de volgende definitie voor machtsverheffing in $1 + m$.

Definitie: Laat $x \in 1 + m$ voor $m = \{w \in K : |w| < |p|^{\frac{1}{p-1}}\}$ en laat $s \in \{w \in K : |w| \leq 1\}$. Dan definiëren we *machtsverheffing* als volgt:

$$x^s = \exp_p(s \cdot \log_p(x)).$$

Voor deze logaritme en exponentiële functie gelden de volgende eigenschappen:

- Voor iedere $z_1, z_2 \in \{z \in K : |z-1| < 1\}$ geldt $\log_p(z_1 z_2) = \log_p(z_1) + \log_p(z_2)$.
- Voor iedere $w_1, w_2 \in \{w \in K : |w| < |p|^{\frac{1}{p-1}}\}$ geldt $\exp_p(w_1 + w_2) = \exp_p(w_1) \cdot \exp_p(w_2)$.
- Voor iedere $w_1 \in \{w \in K : |w| < |p|^{\frac{1}{p-1}}\}$ en $z_1 \in \{z \in K : |z-1| < |p|^{\frac{1}{p-1}}\}$ geldt $\log_p(\exp_p(w_1)) = w_1$ en $\exp_p(\log_p(z_1)) = z_1$.
- Voor iedere $z_1 \in \{z \in K : |z-1| < |p|^{\frac{1}{p-1}}\}$ en $s \in \{x \in K : |x| \leq 1\}$ geldt $\log_p(z_1^s) = s \log_p(z_1)$.

Lemma 4.1.1: Zij $x \in K$ zodanig dat $|x| < |p|^{\frac{1}{p-1}}$, dan geldt $|\log_p(1-x)| = |x|$. Daarnaast geldt $|\log_p(1-x) + x| < |x|$.

Lemma 4.1.2: Zij $x \in K$ zodanig dat $|x| < |p|^{\frac{1}{p-1}}$, dan geldt $|\exp_p(x) - 1| = |x|$. Daarnaast geldt $|\exp_p(x) - (x+1)| < |x|$.

Bewijs. (Lemma 4.1.1) Merk eerst op dat voor de gegeven x de p-adische logaritme goed gedefinieerd is. Er geldt $\log_p(1-x) = -\sum_{i=1}^{\infty} \frac{x^i}{i}$, dus $\log_p(1-x) + x = -\sum_{i=2}^{\infty} \frac{x^i}{i}$.

Claim: Voor iedere $i \geq 2$ geldt $\left|\frac{x^i}{i}\right| < |x|$.

Bewijs. (Claim) Bekijk voor iedere $i \geq 2$ de valuatie $\left|\frac{x^i}{i}\right|$. Zij $i \in \mathbb{Z}_{\geq 2}$ met $p \nmid i$. Dan geldt $|i| = 1$, dus $\left|\frac{x^i}{i}\right| = \frac{|x|^i}{|i|} = |x|^i$. Aangezien $|x| < 1$ geldt $|x|^i < |x|$. Dus $\left|\frac{x^i}{i}\right| < |x|$ voor alle $i \in \mathbb{Z}_{\geq 2}$ zodanig dat $p \nmid i$.

Zij nu $i \in \mathbb{Z}_{\geq 2}$ zodanig dat $p|i$. Dan kunnen we i schrijven als $i = ap^k$ met $a, k \in \mathbb{Z}_{\geq 1}$ en $p \nmid a$. Dan geldt $|i| = |p|^k = p^{-k}$, dus $\frac{|x|^i}{|i|} = \frac{|x|^{ap^k}}{|p|^k} = p^k |x|^{ap^k}$. Aangezien $|x| < 1$ volgt $|x|^{ap^k} \leq |x|^{p^k}$.

Ook geldt $|p| < 1$ en $\frac{k}{p^k-1} \leq \frac{1}{p-1} \leq 1$, dus er volgt $|p|^{\frac{k}{p^k-1}} \geq |p|^{\frac{1}{p-1}}$. Aangezien $|x| < |p|^{\frac{1}{p-1}}$ volgt dat er geldt $|x| < |p|^{\frac{1}{p-1}} \leq |p|^{\frac{k}{p^k-1}}$. Hieruit volgt $|x|^{p^k-1} < |p|^k$, dus $p^k|x|^{p^k} < |x|$. Dit betekent dat het volgende geldt:

$$\left|\frac{x^i}{i}\right| = \frac{|x|^i}{|i|} = \frac{|x|^{ap^k}}{|p|^k} = p^k|x|^{ap^k} \leq p^k|x|^{p^k} < |x|.$$

Dus als $|x| < |p|^{\frac{1}{p-1}}$ geldt voor alle $i \in \mathbb{Z}_{\geq 2}$:

$$\left|\frac{x^i}{i}\right| < |x|.$$

□

Wegens de ultrametrische ongelijkheid geldt nu $\left|-\sum_{i=2}^{\infty} \frac{x^i}{i}\right| < |x|$. Dus $\left|\sum_{i=2}^{\infty} \frac{x^i}{i} + x\right| = |x|$. Aangezien $\log_p(1-x) = -x - \sum_{i=2}^{\infty} \frac{x^i}{i}$ geldt nu:

$$\left|\log_p(1-x)\right| = \left|-x - \sum_{i=2}^{\infty} \frac{x^i}{i}\right| = |x|.$$

Daarnaast geldt

$$\left|\log_p(1-x) + x\right| = \left|\sum_{i=2}^{\infty} \frac{x^i}{i}\right| < |x|.$$

Dus voor $x \in \mathbb{Z}_p$ zodanig dat $|x| < |p|^{\frac{1}{p-1}}$ geldt $|\log_p(1-x)| = |x|$ en $|\log_p(1-x) - x| < |x|$. □

Bewijs. (Lemma 4.1.2) Merk eerst op dat voor de gegeven x de p-adische exponentiële functie goed gedefinieerd is.

Claim: Voor iedere $i \in \mathbb{Z}_{\geq 2}$ geldt $|\frac{x^i}{i!}| < |x|$.

Bewijs. (Claim) Zij $i \in \mathbb{Z}_{\geq 1}$ willekeurig. Met behulp van de formule $\mathrm{ord}_p(i!) = \frac{i-s_p(i)}{p-1}$ krijgen we $|i!| = |p|^{\frac{i-s_p(i)}{p-1}}$. Aangezien $|x| \cdot |p|^{\frac{1}{p-1}} < 1$ geeft dit:

$$\left|\frac{x^i}{i!}\right| = |x|^{s_p(i)} \cdot \left(|x| \cdot |p|^{\frac{1}{p-1}}\right)^{i-s_p(i)} \leq |x|,$$

met gelijkheid dan en slechts dan als $i - s_p(i) = 0$ en $s_p(i) = 1$. Dus de gelijkheid geldt dan en slechts dan als $i = s_p(i) = 1$, dus als $i = 1$.

Dus voor iedere $i \in \mathbb{Z}_{\geq 2}$ geldt $|\frac{x^i}{i!}| < |x|$. □

Voor $i = 1$ geldt $\left|\frac{x^1}{1!}\right| = |x|$. Uit de ultrametrische eigenschap volgt nu:

$$\left|\sum_{i=1}^{\infty} \frac{x^i}{i!}\right| = |x|.$$

Dit geeft

$$|\exp_p(x) - 1| = \left|\sum_{i=1}^{\infty} \frac{x^i}{i!}\right| = |x|.$$

Daarnaast geldt

$$|\exp_p(x) - (x+1)| = \left|\sum_{i=2}^{\infty} \frac{x^i}{i!}\right| < |x|.$$

Dus voor $x \in \mathbb{Z}_p$ zodanig dat $|x| < |p|^{\frac{1}{p-1}}$ geldt $|\exp_p(x)-1| = |x|$ en $|\exp_p(x)-(x+1)| < |x|$. □

Lemma 4.1.3: Laat $z \in \mathbb{Z}_5[\sqrt{5}]$ zodanig dat $|z-1| < 1$. Dan geldt $\overline{\log_5(z)} = \log_5(\overline{z})$.

Bewijs. Merk op dat voor de gegeven z de 5-adische logaritme goed is gedefinieerd. Aangezien de afbeelding $\bar{\cdot}$ een automorfisme is, geldt voor iedere $n \in \mathbb{Z}$ dat $\overline{z^n} = \overline{z}^n$. Nu geldt:

$$\overline{\log_5(z)} = \overline{\sum_{i=1}^{\infty}(-1)^{i+1}\frac{(z-1)^i}{i}} = \sum_{i=1}^{\infty}(-1)^{i+1}\frac{\overline{(z-1)^i}}{i}$$

$$= \sum_{i=1}^{\infty}(-1)^{i+1}\frac{(\overline{z-1})^i}{i} = \sum_{i=1}^{\infty}(-1)^{i+1}\frac{(\overline{z}-1)^i}{i} = \log_5(\overline{z}).$$

□

4.2 Een andere uitdrukking voor ϑ

In deze paragraaf wordt gebruik gemaakt van de theorie van Teichmüller, zie ook paragraaf 8.2 uit Cassels (1986) [5].

Lemma 4.2.1: Er bestaat een $\mathtt{i} \in \mathbb{Z}_5$ zodanig dat $\mathtt{i} \equiv 3 \pmod 5$ en $\mathtt{i}^2 = -1$ en er bestaat een $\eta \in 1 + \sqrt{5}\mathbb{Z}_5[\sqrt{5}]$ zodanig dat geldt $\vartheta = \mathtt{i} \cdot \eta$.

Bewijs. Zij φ het ringhomomorfisme:

$$\varphi : \mathbb{Z}_5[\sqrt{5}] \to \mathbb{F}_5$$

$$a + b\sqrt{5} \mapsto a \pmod 5.$$

Definieer analoog de afbeelding φ^* op de eenheden:

$$\varphi^* : \mathbb{Z}_5[\sqrt{5}]^* \to \mathbb{F}_5^*$$

$$a + b\sqrt{5} \mapsto a \pmod 5.$$

Er geldt $\vartheta, \overline{\vartheta} \in \mathbb{Z}_5[\sqrt{5}]^*$, want $\vartheta, \overline{\vartheta} \in \mathbb{Z}_5[\sqrt{5}]$ en $\vartheta\overline{\vartheta} = -1$. Verder geldt $\vartheta = \frac{1+\sqrt{5}}{2} \equiv 3 + 3\sqrt{5} \pmod 5$. Dus geldt $\varphi^* : \vartheta \mapsto 3 \pmod 5$ en $\varphi^* : \overline{\vartheta} \mapsto 3 \pmod 5$. Wegens de theorie van Teichmüller heeft φ^* een rechtsinverse, ω, die ook een groepshomomorfisme is. Laat $\mathtt{i} = \omega(3) \in \mathbb{Z}_5$ de zogenaamde Teichmüller representant van $3 \in \mathbb{F}_5$. Dan geldt $\mathtt{i} \equiv 3 \pmod 5$ en $\mathtt{i}^2 = -1$. Het is eenvoudig in te zien dat φ^* een groepsisomorfisme tussen $\langle \mathtt{i} \rangle$ en $\mathbb{F}_5^*$ geeft, er geldt immers $\langle \mathtt{i} \rangle = \{1, -1, \mathtt{i}, -\mathtt{i}\}$.

De kern van φ^* wordt gegeven door $\ker(\varphi^*) = 1+\sqrt{5}\mathbb{Z}_5[\sqrt{5}]$. Dit geeft het volgende korte exacte rijtje:

$$0 \to 1 + \sqrt{5}\mathbb{Z}_5[\sqrt{5}] \to \mathbb{Z}_5^* \to \mathbb{F}_5^* \to 0.$$

Door de Teichmüller afbeelding splitst dit rijtje en krijgen we de volgende decompositie:

$$\mathbb{Z}_5[\sqrt{5}]^* \cong \mathbb{F}_5^* \times \left(1 + \sqrt{5}\mathbb{Z}_5[\sqrt{5}]\right) \cong \langle \mathtt{i} \rangle \times \left(1 + \sqrt{5}\mathbb{Z}_5[\sqrt{5}]\right).$$

Dus ieder element $\mu \in \mathbb{Z}_5[\sqrt{5}]^*$ is te schrijven als product van een element van $\langle \mathtt{i} \rangle$ met een element uit $(1 + \sqrt{5}\mathbb{Z}_5[\sqrt{5}])$. Dus we kunnen schrijven $\vartheta = \mathtt{i}\eta$ voor een zekere $\eta \in 1 + \sqrt{5}\mathbb{Z}_5[\sqrt{5}]$. □

Lemma 4.2.2: Voor $\eta \in 1 + \sqrt{5}\mathbb{Z}_5[\sqrt{5}]$ zoals in lemma 4.2.1 geldt $\overline{\eta} = \eta^{-1}$, $|1-\eta| = |\sqrt{5}|$, dus $|1-\eta| < |p|^{\frac{1}{p-1}}$ voor $p = 5$, en $|\eta| = 1$.

Bewijs. Merk eerst op dat $\overline{\mathtt{i}} = \mathtt{i}$, dus $\overline{\eta} = \overline{\mathtt{i}\vartheta} = \mathtt{i}\overline{\vartheta}$. Verder geldt $\eta^{-1} = (\mathtt{i}\vartheta)^{-1} = -\mathtt{i}\vartheta^{-1} = -\mathtt{i} \cdot -\overline{\vartheta} = \mathtt{i}\overline{\vartheta} = \overline{\eta}$. Dus er geldt $\overline{\eta} = \eta^{-1}$. Ook geldt:

$$\frac{\eta - 1}{\sqrt{5}} = \frac{\vartheta - \mathtt{i}}{\mathtt{i}\sqrt{5}} = \frac{1 + \sqrt{5} - 2\mathtt{i}}{2\mathtt{i}\sqrt{5}} = \frac{(1-2\mathtt{i})(1+2\mathtt{i}) + (1+2\mathtt{i})\sqrt{5}}{(1+2\mathtt{i})2\mathtt{i}\sqrt{5}} = \frac{\sqrt{5}}{(1+2\mathtt{i})2\mathtt{i}} + \frac{1}{2\mathtt{i}}.$$

Laat φ het ringhomomorfisme zoals gedefinieerd in het bewijs van lemma 4.2.1. Aangezien $(1+2\mathtt{i})2\mathtt{i}$ en $\frac{1}{2\mathtt{i}}$ eenheden zijn in $\mathbb{Z}_5[\sqrt{5}]$ en $\varphi(\frac{1}{2i}) = \frac{1}{6} = 1$, volgt dat $\varphi(\frac{\eta-1}{\sqrt{5}}) = 1$. Dit betekent dat $|\frac{\eta-1}{\sqrt{5}}| = 1$, dus $|\eta - 1| = |\sqrt{5}| < |5|^{\frac{1}{4}}$. Daarnaast geldt $|\eta| = |\eta\overline{\eta}|_5^{\frac{1}{2}} = |1|_5^{\frac{1}{2}} = 1$. □

Merk op dat geldt $\eta \in 1 + \sqrt{5}\mathbb{Z}_5[\sqrt{5}]$ en $|\eta - 1| = |\sqrt{5}| < 1$. Dit betekent dat $\log_5(\eta)$ goed gedefinieerd is volgens de definitie uit paragraaf 4.1.

Lemma 4.2.3: Laat $\ell \in \mathbb{Z}_5[\sqrt{5}]$ met $\ell = \frac{\log_5(\eta)}{\sqrt{5}}$. Dan geldt $\ell = \overline{\ell}$, $\ell \in \mathbb{Z}_5$ en $\ell \equiv 1 \pmod 5$.

Bewijs. Zoals bewezen in lemma 4.1.3 commuteren de afbeelding $\bar{\cdot}$ en de logaritme. Aangezien $\overline{\eta} = \eta^{-1}$ geldt $\overline{\ell} = \overline{\left(\frac{\log_5(\eta)}{\sqrt{5}}\right)} = \frac{\overline{\log_5(\eta)}}{-\sqrt{5}} = \frac{\log_5(\overline{\eta})}{-\sqrt{5}} = \frac{\log_5(\eta^{-1})}{-\sqrt{5}} = \frac{-\log_5(\eta)}{-\sqrt{5}} = \ell$. Aangezien $\ell \in \mathbb{Z}_5[\sqrt{5}]$ en $\ell = \overline{\ell}$ volgt direct dat geldt $\ell \in \mathbb{Z}_5$.

Aangezien $|1-\eta| = |5|^{\frac{1}{2}}$ volgt uit lemma 4.1.1 dat $|\log_5(\eta) - (\eta - 1)| < |5|^{\frac{1}{2}}$, dus $|\ell - \frac{\eta-1}{\sqrt{5}}| < 1$. Laat φ het ringhomomorfisme zoals gedefinieerd in het bewijs van lemma 4.2.1. Dan zijn de elementen van de kern van φ precies de elementen $z \in \mathbb{Z}_5[\sqrt{5}]$ met $|z| < 1$. Dus $\ell - \frac{\eta-1}{\sqrt{5}}$ zit in de kern van φ, dus $\varphi(\ell) = \varphi(\frac{\eta-1}{\sqrt{5}})$. Zoals bewezen in het bewijs van lemma 4.2.2 geldt $\varphi(\frac{\eta-1}{\sqrt{5}}) = 1$, dus er geldt ook $\varphi(\ell) = 1$, dus $\ell \equiv 1 \pmod 5$. □

4.3 Een machtreeksontwikkeling

Beschouw de functie $F : \hat{\mathbb{Z}} \to \mathbb{Z}_5$. Dit kunnen we doen door voor iedere $k \in \mathbb{Z}_{\geq 0}$ de functie $F : \hat{\mathbb{Z}} \to \mathbb{Z}/5^k\mathbb{Z}$ te beschouwen. Wegens stelling 3.1 en het bijbehorende diagram kunnen we voor iedere $k \in \mathbb{Z}_{\geq 0}$ deze functie beschouwen als

$$F : \mathbb{Z}/(4 \cdot 5^k)\mathbb{Z} \to \mathbb{Z}/5^k\mathbb{Z}.$$

Wegens de Chinese reststelling geldt $\mathbb{Z}/(4 \cdot 5^k)\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5^k\mathbb{Z}$. Dit geeft dat we voor iedere $k \geq 0$ de afbeelding F kunnen beschouwen als

$$F : \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5^k\mathbb{Z} \to \mathbb{Z}/5^k\mathbb{Z}.$$

Aangezien $\mathbb{Z}_5 = \lim_{\leftarrow k} \mathbb{Z}/5^k\mathbb{Z}$, weten we hoe F zich gedraagt op $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}_5$ door voor iedere $k \in \mathbb{Z}_{\geq 0}$ te kijken naar $F : \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5^k\mathbb{Z} \to \mathbb{Z}/5^k\mathbb{Z}$. Door vervolgens de projectieve limiet te nemen over al deze k, kunnen we de functie $F : \hat{\mathbb{Z}} \to \mathbb{Z}_5$ beschouwen door te kijken naar $F : \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}_5 \to \mathbb{Z}_5$.

Stelling 4.3.1: Laat $\ell, \mathtt{i} \in \mathbb{Z}_5$ zoals gedefinieerd in voorgaande paragraaf. Beschouw $F : \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}_5 \to \mathbb{Z}_5$. Dan wordt voor $i \in \mathbb{Z}/4\mathbb{Z}$ en $s \in \mathbb{Z}_5$ een machtreeksontwikkeling van F gegeven door:

$$F : \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}_5 \to \mathbb{Z}_5$$

$$(i, s) \mapsto \mathtt{i}^i \sum_{\substack{j=0 \\ j \text{ oneven}}}^{\infty} \frac{2\ell^j 5^{\frac{j-1}{2}} s^j}{j!}.$$

Bewijs. Merk ten eerste op dat geldt $\vartheta^n = (\mathtt{i}\eta)^n = \mathtt{i}^n\eta^n$. Aangezien $\mathtt{i}$ een eenheid is in $\langle \mathtt{i} \rangle$, mogen we deze verheffen met elementen uit $\mathbb{Z}/4\mathbb{Z}$. Aangezien geldt $\eta \equiv 1 \pmod{\sqrt{5}}$ mogen we deze verheffen met machten uit $\mathbb{Z}_5$. Er geldt $\mathbb{Z}_5[\vartheta]^* = \lim_{\leftarrow k}((\mathbb{Z}/5^k\mathbb{Z})[\vartheta])^*$. De orde van $((\mathbb{Z}/5^k\mathbb{Z})[\vartheta])^*$ is $4 \cdot 5^{2k-1}$, dus alle elementen van $((\mathbb{Z}/5^k\mathbb{Z})[\vartheta])^*$ hebben een orde die $4 \cdot 5^{2k-1}$ deelt. Ook geldt $n \in \lim_{\leftarrow k} \mathbb{Z}/4 \cdot 5^{k-1}\mathbb{Z} = \lim_{\leftarrow k}(\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5^{k-1}\mathbb{Z})$. Aangezien $\mathtt{i} \in \langle \mathtt{i} \rangle$, geldt wegens de definitie van machtsverheffing uit paragraaf 3.1 dat $\mathtt{i}^n = (\mathtt{i}_{5^k}^{n \pmod 4})_{k=0}^{\infty}$. Voor $\eta \in 1 + \sqrt{5}\mathbb{Z}_5[\sqrt{5}]$ geldt $\eta^n = (\eta_{5^k}^{n \pmod{5^{k-1}}})_{k=0}^{\infty}$. Dit geeft:

$$\vartheta^n = \mathtt{i}^n\eta^n = \left(\mathtt{i}_{5^k}^{n \pmod 4}\right) \cdot \left(\eta_{5^k}^{n \pmod{5^{k-1}}}\right) = \mathtt{i}^i \cdot \eta^s,$$

voor $i \in \mathbb{Z}/4\mathbb{Z}$ en $s \in \mathbb{Z}_5$. Dus er geldt $(\mathtt{i} \cdot \eta)^{(i,s)} = \mathtt{i}^i \cdot \eta^s$. Nu geldt wegens stelling 3.1.3 voor $F : \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}_5 \to \mathbb{Z}_5$:

$$F(i, s) = \frac{(\mathtt{i}\eta)^{(i,s)} - (\mathtt{i}\overline{\eta})^{(i,s)}}{\sqrt{5}} = \frac{\mathtt{i}^i\eta^s - \mathtt{i}^i\overline{\eta}^s}{\sqrt{5}} = \frac{\mathtt{i}^i}{\sqrt{5}}(\eta^s - \eta^{-s}).$$

We kunnen een machtreeksontwikkeling van F maken door gebruik te maken van de p-adische logaritme en exponentiële functie. Er geldt $|\eta - 1| < |5|^{\frac{1}{4}}$ en voor alle $s \in \mathbb{Z}_5$ geldt $|s| \leq 1$, dus $\log_5(\eta^s)$ is goed-gedefinieerd en $|\eta^s| < |5|^{\frac{1}{4}}$. Dit geeft:

$$\eta^s = \exp_5(\log_5(\eta^s)) = \exp_5(s \cdot \log_5(\eta)) = \exp_5(s\sqrt{5}\ell) = \sum_{j=0}^{\infty} \frac{\ell^j \sqrt{5}^j s^j}{j!}.$$

Aangezien geldt $\overline{\ell} = \ell$, geldt:

$$\eta^{-s} = \sum_{j=0}^{\infty} \frac{\ell^j(-\sqrt{5})^j s^j}{j!}.$$

Dit geeft:

$$\eta^s - \eta^{-s} = \sum_{\substack{j=0 \\ j \text{ oneven}}}^{\infty} \frac{2\ell^j \sqrt{5}^j s^j}{j!} = \sqrt{5} \sum_{\substack{j=0 \\ j \text{ oneven}}}^{\infty} \frac{2\ell^j 5^{\frac{j-1}{2}} s^j}{j!}.$$

Dit geeft voor F de volgende machtreeksontwikkeling:

$$F(i,s) = \frac{\mathtt{i}^i}{\sqrt{5}}(\eta^s - \eta^{-s}) = \mathtt{i}^i \sum_{\substack{j=0 \\ j \text{ oneven}}}^{\infty} \frac{2\ell^j 5^{\frac{j-1}{2}} s^j}{j!}.$$

□

Definitie: Voor $i \in \mathbb{Z}/4\mathbb{Z}$, laat $F_i : \mathbb{Z}_5 \to \mathbb{Z}_5$ en $F_i(s) := F(i,s)$.

Lemma: Voor $f_j = \frac{\mathtt{i}^i 2\ell^j 5^{\frac{j-1}{2}}}{j!} \in \mathbb{Z}_5$ met j oneven geldt $f_j \to 0 \in \mathbb{Z}_5$ als $j \to \infty$.

Bewijs. Zij $f_j = \frac{\mathtt{i}^i 2\ell^j 5^{\frac{j-1}{2}}}{j!}$ met $j > 1$ oneven. Aangezien $\mathtt{i}$ en ℓ eenheden zijn bevatten deze geen factoren 5. Het aantal factoren 5 in de teller is gelijk aan $\frac{j-1}{2}$. Voor het aantal factoren 5 in de noemer maken we gebruik van stelling 4.1. Dit geeft $\mathrm{ord}_5(j!) = \frac{j-s_5(n)}{5-1}$. Dit betekent dat $\mathrm{ord}_5(f_j) = \frac{j-1}{2} - \frac{j-s_5(j)}{4} = \frac{j-2+s_5(j)}{4}$.

Dus voor $j \to \infty$ gaat het aantal factoren 5 in f_j naar oneindig en daarmee gaat $f_j \to 0$ als $j \to \infty$. □

Lemma: Voor iedere $j > 5$ met j oneven geldt $5^2 | f_j$.

Bewijs. Er is reeds laten zien dat voor $j > 1$ geldt $\mathrm{ord}_5(f_j) = \frac{j-2+s_5(j)}{4}$. Aangezien $s_5(j) \geq 1$, geldt $\mathrm{ord}_5(f_j) \geq \frac{j-1}{4}$. Er geldt $\mathrm{ord}_5(f_j) \geq 2$ als $\frac{j-1}{4} \geq 2$, wat waar is voor $j \geq 9$. Dus voor $j \geq 9$ geldt $5^2 | f_j$. Voor $j = 7$ geldt $s_5(j) = 3$, dus $\mathrm{ord}_5(f_7) = \frac{7-2+3}{4} = 2$, dus er geldt $5^2 | f_7$. Dus voor alle $j > 5$ en j oneven geldt $5^2 | f_j$. □

Stelling 4.3.2: De machtreeks F uit stelling 4.3.1 voldoet aan de volgende eigenschappen:

- Voor $i = 0$ heeft $F_0 : \mathbb{Z}_5 \to \mathbb{Z}_5$ precies 1 dekpunt, deze wordt gegeven door $s = 0$.
- Voor $i = 1$ heeft $F_1 : \mathbb{Z}_5 \to \mathbb{Z}_5$ precies 5 dekpunten, deze worden gegeven door $s \in \{-5, -1, 0, 1, 5\}$.

Bewijs. Merk op dat $\mathbb{Z}_5$ een domein is en met de in hoofdstuk 2.1 gedefinieerde 5-adische valuatie ook ultrametrisch en compleet is. We beschouwen de machtreeks $F_i(s) = \mathtt{i}^i \sum_{\substack{j>0 \\ j \text{ oneven}}}^{\infty} \frac{2\ell^j 5^{\frac{j-1}{2}} s^j}{j!}$ in $\mathbb{Z}_5$. Wegens bovenstaand lemma geldt $f_j \to 0$ als $j \to \infty$. Dit betekent dat we de stelling van Strassmann toe kunnen passen. Aangezien we geïnteresseerd zijn in de dekpunten van F en niet in de nulpunten, bekijken we $F_i(s) - s$.

Voor $i = 0$ worden de eerste termen van deze machtreeks gegeven door:

$$f_1 - 1 = 2\ell - 1 \equiv 1 \pmod 5, \text{ dus } |f_1 - 1| = 1;$$

$$f_3 = \frac{1}{3}\ell^3 5 \equiv 0 \pmod 5, \text{ dus } |f_3| \leq 5^{-1};$$

$$f_5 = \frac{1}{12}\ell^5 5 \equiv 0 \pmod 5, \text{ dus } |f_5| \leq 5^{-1}.$$

Aangezien voor $j > 5$ het aantal factoren 5 in f_j minstens gelijk is aan 2, volgt voor $j > 5$ dat $|f_j| \leq 5^{-2}$ en weten we dat de f_j met het laagst aantal factoren 5 de term f_1 moet zijn. Uit Strassmann volgt nu dat F_0 maximaal $N = 1$ dekpunt heeft. Aangezien 0 een dekpunt is van F_0 volgt dat $s = 0$ het het enige dekpunt is voor F_0.

Voor $i = 1$ worden de eerste termen van de machtreeks gegeven door:

$$f_1 - 1 = 2\ell\mathtt{i} - 1 \equiv 0 \pmod 5, \text{ dus } |f_1 - 1| \leq 5^{-1};$$

$$f_3 = \frac{1}{3}\ell^3 5\mathtt{i} \equiv 0 \pmod 5, \text{ dus } |f_3| \leq 5^{-1};$$

$$f_5 = \frac{1}{12}\ell^5 5\mathtt{i} \equiv 0 \pmod 5, \ f_j \equiv 20 \pmod{5^2}, \text{ dus } |f_5| = 5^{-1};$$

$$f_7 = \frac{1}{504}\ell^7 5^2\mathtt{i} \equiv 0 \pmod{5^2}, \text{ dus } |f_7| \leq 5^{-2}.$$

Aangezien voor $j > 5$ het aantal factoren 5 in f_j minstens gelijk is aan 2, geldt voor $j > 5$ dat $|f_j| \leq 5^{-2}$ dus hebben f_3 en f_5 het minst aantal factoren 5. Uit de stelling van Strassmann volgt nu dat $F_1(s)$ maximaal $N = 5$ dekpunten heeft.

Het is eenvoudig in te zien dat $s = 0$ een vast punt is van $F_1(s)$. Aangezien F een uitbreiding is van de Fibonacci-functie op $\mathbb{Z}$ en voor $s \in \mathbb{Z}_5$ moet gelden $s \equiv 1 \pmod 4$ weten we dat $s = 1, s = 5$ dekpunten van $F_1(s)$ zijn.

Voor $F_i(-s)$ geldt:

$$F_i(-s) = \mathtt{i}^i \sum_{\substack{j=0 \\ j \text{ oneven}}}^{\infty} \frac{2\ell^j 5^{\frac{j-1}{2}}(-s)^j}{j!} = -\mathtt{i}^i \sum_{\substack{j=0 \\ j \text{ oneven}}}^{\infty} \frac{2\ell^j 5^{\frac{j-1}{2}} s^j}{j!} = -F_i(s).$$

Stel $s \in \mathbb{Z}_5$ is een nulpunt van $F_i(s) - s$. Dan geldt voor $-s$: $F_i(-s) - (-s) = -F_i(s) + s = -1 \cdot 0 = 0$. Oftewel, als $s \in \mathbb{Z}_5$ een nulpunt is van $F_i(s) - s$, dan moet $-s$ hier ook een nulpunt van zijn. Dit geeft de resterende nulpunten van $F_i(s) - s$, namelijk $s = -1$ en $s = -5$. Dus de dekpunten van $F_1(s)$ zijn $s = -5, s = -1, s = 0, s = 1$ en $s = 5$. □

Opmerking: Ter compleetheid van stelling 4.3.2 merken we op dat voor $i = 2$ en $i = 3$ geldt dat $F_i : \mathbb{Z}_5 \to \mathbb{Z}_5$ precies 1 dekpunt heeft en dat deze gegeven wordt door $s = 0$. De bewijzen hiervan gaan analoog aan het bewijs van stelling 4.3.2.

5 Contracties

Contracties zijn afbeeldingen die onder bepaalde voorwaarden een uniek dekpunt hebben. Contracties kunnen dus goed van pas komen bij het vinden van dekpunten van een functie. Hoewel de pro-eindige Fibonacci-functie zelf geen contractie is, blijken hier contracties wel een handige rol te spelen.

Definitie: Een *contractie* op een metrische ruimte (X, d) is een afbeelding $f : X \to X$ zodanig dat voor alle $x, y \in X$ met $x \neq y$ geldt $d(f(x), f(y)) < d(x, y)$.

De volgende stelling lijkt enigszins op de contractiestelling van Banach. Hij heeft echter andere voorwaarden, waardoor deze beter toepasbaar is voor de pro-eindige Fibonacci-functie dan de stelling van Banach.

Stelling: (Contractiestelling) Zij (X, d) een niet-lege, complete, ultrametrische ruimte zodanig dat 0 het enige verdichtingspunt van $d(X \times X)$ is. Dan heeft iedere contractie $f : X \to X$ een uniek dekpunt.

Voor we deze stelling gaan bewijzen, bewijzen we eerst de volgende claim.

Claim: Neem dezelfde voorwaarden als in de stelling en laat $x \in X$ gegeven. Dan is de rij $(f^n(x))_{n=0}^{\infty}$ een Cauchy-rij.

Bewijs. (Claim) Laat $x \in X$ gegeven en bekijk de rij $(f^n(x))_{n=0}^{\infty}$. Laat $\varepsilon \in \mathbb{R}_{>0}$. Stel er is een $n \in \mathbb{Z}_{\geq 0}$ zodanig dat $f^n(x) = f^{n+1}(x)$, kies dan $N = n$. Dan geldt voor alle $m, n \geq N$ dat $f^n(x) = f^m(x)$, dus $d(f^n(x), f^m(x)) = 0 < \varepsilon$.

Stel voor alle $n \in \mathbb{Z}_{\geq 0}$ geldt $f^n(x) \neq f^{n+1}(x)$. Dan geldt

$$d\left(x, f(x)\right) > d\left(f(x), f^2(x)\right) > d\left(f^2(x), f^3(x)\right) > ....$$

Dit is een dalende reeks positieve getallen. Aangezien 0 het enige verdichtingspunt van $d(X \times X)$ is geldt $\lim_{n\to\infty} d(f^n(x), f^{n+1}(x)) = 0$. Dus er is een $N \in \mathbb{Z}_{\geq 0}$ zodanig dat voor alle $n \geq N$ geldt $d(f^n(x), f^{n+1}(x)) < \varepsilon$. Zij $m, n \geq N$ en neem zonder verlies van algemeenheid aan dat $m > n$. Wegens de ultrametrische eigenschap geldt $d(f^n(x), f^m(x)) \leq \max_{n\leq k<m} d(f^k(x), f^{k+1}(x)) = d(f^n(x), f^{n+1}(x)) < \varepsilon$. Dus voor iedere $\varepsilon \in \mathbb{R}_{>0}$ is er een $N \in \mathbb{Z}_{\geq 0}$ zodanig dat voor alle $m, n \geq N$ geldt $d(f^n(x), f^m(x)) < \varepsilon$, dus $(f^n(x))_{n=0}^{\infty}$ is een Cauchy-rij. □

Bewijs. (Contractiestelling) Zij (X, d) een niet-lege, complete, ultrametrische ruimte zodanig dat 0 het enige verdichtingspunt van $d(X \times X)$ is. Kies $x \in X$ en zij $f : X \to X$ een contractie op X. Wegens de claim is $(f^n(x))_{n=0}^{\infty}$ een Cauchy-rij in een complete metrische ruimte, dus $(f^n(x))_{n=0}^{\infty}$ convergeert in X. Dus er is een $y \in X$ zodanig dat $\lim_{n\to\infty} d(f^n(x), y) = 0$. Dan geldt ook $d(f^{n+1}(x), f(y)) < d(f^n(x), f(y))$, dus er geldt $\lim_{n\to\infty} d(f^{n+1}(x), f(y)) = 0$. Hieruit volgt $f(y) = y$, dus y is een dekpunt van f.

Stel dat er $x, y \in X$ zijn zodanig dat $f(x) = x$, $f(y) = y$ en $x \neq y$. Aangezien f een contractie is moet gelden $d(f(x), f(y)) < d(x, y)$, maar dit is in tegenspraak met $f(x) = x$ en $f(y) = y$. Dus f heeft een uniek dekpunt in X. □

5.1 De Fibonacci-functie als contractie

Door het domein van de Fibonacci-functie te beperken wordt de Fibonacci-functie op een goed gekozen beperkt domein ook een contractie. In deze paragraaf worden hier een aantal voorbeelden met toepassing van de contractiestelling van gegeven.

Voorbeeld 1

Neem voor dit voorbeeld $a \in \{0, 1, 5\}$ en definieer $X_a := \{s \in \mathbb{Z}_2 \times \mathbb{Z}_3 : s \equiv a \pmod{24}\}$. Dan gelden de volgende stellingen:

Stelling 5.1: De afbeelding $F : X_a \to X_a$ is een contractie op X_a.

Bewijs. Merk eerst op dat F goed gedefinieerd is. Merk hiervoor op dat voor iedere $x \in X_a$ en voor iedere $k \in \mathbb{Z}_{\geq 1}$ geldt dat we de waarde van de k-de coördinaat van x in $\mathbb{Z}_2$ en $\mathbb{Z}_3$ wegens stelling 3.1 als volgt kunnen bepalen:

$$F(x) \pmod{2^k} = F(x \bmod(3 \cdot 2^{k-1}))$$

$$F(x) \pmod{3^k} = F(x \bmod(8 \cdot 3^{k-1}))$$

Dit betekent dat voor iedere $x \in X_a$ geldt $F(x) \in \mathbb{Z}_2 \times \mathbb{Z}_3$. Daarnaast geldt voor iedere $s \equiv a \pmod{24}$ dat $F(s) \pmod{24} = F(s \bmod(24)) \equiv F(a \bmod(24)) = a \pmod{24}$, dus er geldt $F : X_a \to X_a$.

Zij $x, y \in X$ zodanig dat $x \neq y$. Zij $p, q \in \{2, 3\}$ en $l, m \in \mathbb{Z}_{\geq 1}$ zodanig dat $d(x, y) = q^{-m}$ en $p^l \leq q^m$. Dan geldt:

- $x \equiv y \pmod 3$;
- $x \equiv y \pmod{2^3}$;
- Als voor $p = 2$ en een zekere $n \in \mathbb{Z}_{\geq 3}$ geldt $p^l = 2^n$, geldt $2^{n-1} < 2^n \leq q^m$, dus $x \equiv y \pmod{2^{n-1}}$;
- Als voor $p = 3$ en een zekere $n \in \mathbb{Z}_{\geq 1}$ geldt $p^l = 3^n$, geldt $3^{n-1} < 3^n \leq q^m$, dus $x \equiv y \pmod{3^{n-1}}$.

Aangezien $\pi(2^n) = 3 \cdot 2^{n-1}$ en $\pi(3^n) = 2^3 \cdot 3^{n-1}$ volgt uit de Chinese reststelling dat geldt $x \equiv y \pmod{\pi(p^l)}$, dus $F(x) \equiv F(y) \pmod{p^l}$. Aangezien $p^l \leq q^m$ moet gelden $\min\{p^l : p \text{ priem}, l \in \mathbb{Z}_{\geq 1},\ x \not\equiv y \pmod{p^l}\} > q^m$, dus $d(F(x), F(y)) < q^{-m} = d(x, y)$. Dus voor iedere $x, y \in X$ geldt $d(F(x), F(y)) < d(x, y)$, dus F is een contractie op X_a. □

Stelling 5.2: De afbeelding $F : X_a \to X_a$ heeft een uniek dekpunt $s = a$ in X_a.

Bewijs. Merk op dat X_a een gesloten deelverzameling is van een product van compacte verzamelingen, dus X_a is ook compact. Laat $d = d|_{X_a}$ met d de metriek gedefinieerd in hoofdstuk 2, dan is d een ultrametrische metriek op X_a. Dus X_a is een compacte, metrische ruimte dus volgt uit stelling 2.2 dat X_a compleet is.

Bovendien geldt $d(X_a \times X_a) = \{0\} \cup \{p^{-l} : p \in \{2, 3\}, l \in \mathbb{Z}_{\geq 1}\}$, deze verzameling heeft enkel het punt 0 als verdichtingspunt. Wegens stelling 5.1 is $F : X_a \to X_a$ een contractie. Nu volgt uit de contractiestelling uit hoofdstuk 5 dat F een uniek dekpunt heeft in X_a. Aangezien $0, 1$ en 5 reeds bekende dekpunten zijn van respectievelijk $F|_{X_0}$, $F|_{X_1}$ en $F|_{X_5}$ volgt dat dit de enige dekpunten moeten zijn. Het dekpunt van $F : X_a \to X_a$ is dus $s = a$. □

Voorbeeld 2

Zij voor dit voorbeeld $X := \{0\} \times \{0\} \times \{0\} \times \prod_{p>5} \mathbb{Z}_p \subset \hat{\mathbb{Z}}$. Dan gelden de volgende stellingen:

Stelling 5.3: De afbeelding $F : X \to X$ is een contractie op X.

Bewijs. Merk eerst op dat F goed gedefinieerd is. Immers, beschouw de afbeelding $F : X \to \hat{\mathbb{Z}}$. Wegens stelling 5.1 en 5.2 geldt voor alle $x \in X$ dat $F(x) \in \{0\} \times \{0\} \times \prod_{p>3} \mathbb{Z}_p$. Wegens stelling 4.3.2 geldt bovendien $F(x) \in \{0\} \times \{0\} \times \{0\} \times \prod_{p>5} \mathbb{Z}_p$. Dus de afbeelding $F : X \to X$ is goed gedefinieerd.

Zij $x, y \in X$ zodanig dat $x \neq y$. Laat p, q priem en $l, m \in \mathbb{Z}_{>0}$ zodanig dat $p^l \leq q^m$ en $d(x, y) = q^{-m}$. Dan geldt:

- $p^{l-1} < p^l \leq q^m$;
- $p - 1 < p \leq p^l \leq q^m$;
- Voor $p > 2$ geldt $\frac{p+1}{2} < p \leq p^l \leq q^m$;
- Voor $p = 2$ en iedere $k \in \mathbb{Z}_{>0}$ geldt $x \equiv y \pmod{2^k}$;
- $\pi(p^l) | p^{l-1}\pi(p)$, dus voor $p > 5$ geldt $\pi(p^l) | (p - 1)p^{l-1}$ of $\pi(p^l) | 2^2 \frac{p+1}{2} \pi(p)$.

Wegens de Chinese reststelling geldt nu $x \equiv y \pmod{\pi(p^l)}$ voor iedere $p^l \leq q^m$. Dit betekent $F(x) \equiv F(y) \pmod{p^l}$, dus $\min\{p^l, p \text{ priem}, l \in \mathbb{Z}_{\geq 0}\} > q^m$, dus $d(F(x), F(y)) < q^{-m}$, dus $d(F(x), F(y)) < d(x, y)$ dus $F : X \to X$ is een contractie. □

Stelling 5.4: De afbeelding $F : X \to X$ heeft een uniek dekpunt $s = 0$ in X.

Bewijs. Merk op dat X een gesloten deelverzameling is van een compacte verzameling, dus X is ook compact. Laat $d = d|_X$ met d de metriek uit hoofdstuk 2, dan is (X, d) een ultrametrische ruimte. Uit stelling 2.2 volgt nu dat X ook compleet is. Daarnaast geldt $d(X \times X) = \{0\} \cup \{p^{-l} : p > 5 \text{ priem}, l \in \mathbb{Z}_{\geq 1}\}$, deze verzameling heeft enkel het punt 0 als verdichtingspunt. Aangezien $F : X \to X$ een contractie is op X volgt uit de contractiestelling dat F een uniek dekpunt heeft op X. Aangezien we weten dat $s = 0$ een dekpunt is van F, volgt dat $s = 0$ het enige dekpunt is van F. □

Voorbeeld 3

Laat in het volgende voorbeeld $a \in \{1, 5\}$ en $b \in \{-5, -1, 0, 1, 5\}$.

Definieer $X_{a,b} := \{a\} \times \{a\} \times \{b\} \times \prod_{p>5} \mathbb{Z}_p \subset \hat{\mathbb{Z}}$.

Stelling 5.5: De afbeelding $F : X_{a,b} \to X_{a,b}$ is een contractie op $X_{a,b}$.

Bewijs. Merk eerst op dat $F : X_{a,b} \to X_{a,b}$ goed gedefinieerd is. Immers, laat $F : X_{a,b} \to \hat{\mathbb{Z}}$. Wegens voorbeeld 1 geldt $F(a) = a \in \mathbb{Z}_2$ en $F(a) = a \in \mathbb{Z}_3$. Aangezien geldt $a \equiv 1 \pmod 4$ bekijken we $F_1 : \mathbb{Z}_5 \to \mathbb{Z}_5$ en volgt uit stelling 4.3.2 dat $F(b) = b \in \mathbb{Z}_5$. Dus er geldt:

$$F : \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \to \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$$

$$(a, a, b) \mapsto (a, a, b).$$

Dus voor alle $x \in X_{a,b}$ geldt $F(x) \in X_{a,b}$, dus $F : X_{a,b} \to X_{a,b}$.

Zij $x, y \in X_{a,b}$ zodanig dat $x \neq y$. Laat p, q priem en $l, m \in \mathbb{Z}_{\geq 1}$ zodanig dat $d(x, y) = q^{-m}$ en $p^l \leq q^m$. Dan geldt:

- $p^{l-1} < p^l \leq q^m$;
- $p - 1 < p \leq p^l \leq q^m$;
- Voor iedere $k \in \mathbb{Z}_{\geq 0} : x \equiv y \pmod{2^k}$;
- Voor $p > 2$ geldt $\frac{p+1}{2} < p \leq p^l \leq q^m$;
- Voor $p > 5$ geldt $\pi(p^l) | p^{l-1}(p-1)$ of $\pi(p^l) | p^{l-1} 2^2 \frac{p+1}{2}$.

Dan geldt $x \equiv y \pmod{p^l}$ voor alle $p^l < q^m$. Uit de bovenstaande ongelijkheden en de Chinese reststelling volt nu $x \equiv y \pmod{\pi(p^l)}$, dus er geldt $F(x) \equiv F(y) \pmod{p^l}$. Aangezien $p^l \leq q^m$ moet $\min\{p^l : p \text{ priem}, l \in \mathbb{Z}_{\geq 1},\ x \not\equiv y \pmod{p^l}\} > q^m$, dus $d(F(x), F(y)) < q^{-m} = d(x, y)$. Dus voor iedere $x, y \in X_{a,b}$ geldt $d(F(x), F(y)) < d(x, y)$, dus F is een contractie op $X_{a,b}$. □

Stelling 5.6: De afbeelding $F : X_{a,b} \to X_{a,b}$ heeft een uniek dekpunt in $X_{a,b}$.

Bewijs. Merk op dat $X_{a,b}$ een gesloten deelverzameling van de compacte verzameling $\prod_{p \in \mathcal{P}} \mathbb{Z}_p$ is, dus $X_{a,b}$ is compact. Laat $d = d|_{X_{a,b}}$, met d de metriek uit hoofdstuk 2. Dit maakt $(X_{a,b}, d)$ een ultrametrische ruimte, die wegens stelling 2.2 ook compleet is. Bovendien geldt $d(X_{a,b} \times X_{a,b}) = \{0\} \cup \{p^{-l} : p > 5 \text{ priem}, l \in \mathbb{Z}_{\geq 1}\}$, deze verzameling heeft enkel het punt 0 als verdichtingspunt.

Aangezien $F : X_{a,b} \to X_{a,b}$ een contractie is volgt uit de contractiestelling dat F een uniek dekpunt heeft op $X_{a,b}$. □

6 Dekpunten

In $\mathbb{Z}$ heeft de Fibonacci-functie precies drie dekpunten, namelijk $z = 0, z = 1$ en $z = 5$. Door het uitbreiden van F naar $\hat{\mathbb{Z}}$ blijken hier nog 8 dekpunten bij te komen, die gegeven worden door de volgende stelling.

Stelling 6.1: Zij $F : \hat{\mathbb{Z}} \to \hat{\mathbb{Z}}$ de Fibonacci-functie. Dan geldt:

1. $\{z \in \hat{\mathbb{Z}} : F(z) = z,\ z \text{ even}\} = \{0\}$.
2. Voor iedere $a \in \{1, 5\}, b \in \{-5, -1, 0, 1, 5\}$ is er een unieke $z_{a,b} \in \hat{\mathbb{Z}}$ zodanig dat deze $z_{a,b}$ voldoet aan de volgende eisen:
   - $F(z_{a,b}) = z_{a,b}$;
   - Voor alle $k \in \mathbb{Z}_{\geq 0}$ geldt $z_{a,b} \equiv a \pmod{6^k}$ en $z_{a,b} \equiv b \pmod{5^k}$.
3. $\big\{z \in \hat{\mathbb{Z}} : F(z) = z,\ z \text{ oneven}\} = \{z_{a,b} \in \hat{\mathbb{Z}} : a \in \{1, 5\},\ b \in \{-5, -1, 0, 1, 5\}\big\}$.

Bewijs. Laat $z \in \hat{\mathbb{Z}}$ zodanig dat $F(z) = z$. Beschouw het commutatieve diagram van stelling 3.1. Merk op dat we enkel over dekpunten van F kunnen praten als F een verzameling naar zichzelf afbeeldt. Er moet dus gelden $\pi(m)|m$. Kies $m = 24$, dan geldt $\pi(m) = m$. Simpelweg uitschrijven van de Fibonnaci-getallen modulo 24 geeft:

$$\{s \in \mathbb{Z}/24\mathbb{Z} : F(s) \equiv s \pmod{24}\} = \{0, 1, 5\}.$$

Dus voor iedere $z \in \hat{\mathbb{Z}}$ met $F(z) = z$ geldt $z \equiv s \pmod{24}$ voor $s \in \{0, 1, 5\}$. Neem nu $a \in \{0, 1, 5\}$ en definieer $X_a := \{s \in \mathbb{Z}_2 \times \mathbb{Z}_3 : s \equiv a \pmod{24}\}$. Dan heeft wegens stelling 5.3 de functie $F : X_a \to X_a$ een uniek dekpunt $s = a$. Dus voor $z \in \hat{\mathbb{Z}}$ met $F(z) = z$ en $z \equiv a \pmod{24}$ moet gelden $z_2 = a \in \mathbb{Z}_2$ en $z_3 = a \in \mathbb{Z}_3$.

Beschouw eerst de even dekpunten van F. Hiervoor moet gelden $z = 0 \pmod{24}$, dus er geldt $z_2 = 0$ en $z_3 = 0$. Uit stelling 4.3.2 volgt dan dat $F(z) = 0 \in \mathbb{Z}_5$ en uit stelling 5.4 volgt dat F een uniek dekpunt $z = 0$ in $\hat{\mathbb{Z}}$ heeft. Dus $z = 0$ is het enige even dekpunt, dus er geldt $\{z \in \hat{\mathbb{Z}} : F(z) = z,\ z \text{ even}\} = \{0\}$.

Beschouw vervolgens de oneven dekpunten van F. Dan geldt $z \equiv a \pmod{24}$ voor een $a \in \{1, 5\}$, dus $z_2 = a$ en $z_3 = a$ en $z \equiv 1 \pmod{4}$. Dan kunnen we kijken naar $F_1(s)$, uit stelling 4.3.2 volgt dat er in $\mathbb{Z}_5$ precies 5 mogelijkheden zijn voor de dekpunten, namelijk $z_5 = b$ voor $b \in \{-5, -1, 0, 1, 5\}$. Dan geldt $z \in X_{a,b}$. Uit stelling 5.6 volgt vervolgens dat $F : X_{a,b} \to X_{a,b}$ een uniek dekpunt heeft in $X_{a,b}$, dus $F : \hat{\mathbb{Z}} \to \hat{\mathbb{Z}}$ heeft precies 10 oneven dekpunten $z_{a,b}$ met $a \in \{1, 5\}$ en $b \in \{-5, -1, 0, 1, 5\}$. Voor deze dekpunten geldt bovendien dat voor alle $k \in \mathbb{Z}_{\geq 0}$ geldt $z_{a,b} \equiv a \pmod{6^k}$ en $z_{a,b} \equiv b \pmod{5^k}$.

Dus voor iedere $a \in \{1, 5\}, b \in \{-5, -1, 0, 1, 5\}$ is er een unieke $z_{a,b} \in \hat{\mathbb{Z}}$ zodanig dat deze $z_{a,b}$ voldoet aan de volgende eisen:

- $F(z_{a,b}) = z_{a,b}$;
- Voor alle $k \in \mathbb{Z}_{\geq 0}$ geldt $z_{a,b} \equiv a \pmod{6^k}$ en $z_{a,b} \equiv b \pmod{5^k}$.

Dus er geldt:

$$\big\{\{z \in \hat{\mathbb{Z}} : F(z) = z, z \text{ oneven}\} = \{z_{a,b} \in \hat{\mathbb{Z}} : a \in \{1, 5\}, b \in \{-5, -1, 0, 1, 5\}\big\}.$$

□

6.1 Bijzondere eigenschappen

De dekpunten van de pro-eindige Fibonacci-functie zijn niet alleen bijzonder omdat ze dekpunten zijn, maar ze blijken mooie eigenschappen te hebben. Merk ten eerste op dat $z_{1,1} = 1$ en $z_{5,5} = 5$. Voor de overige 8 oneven dekpunten blijkt dat deze, onnauwkeurig gezegd, de 'neiging hebben de eigenschappen van a en b over te nemen', zoals vermeld in Lenstra (2005) [1]. De, volgens dit artikel, meest mysterieuze is $z_{5,-5}$, dus hier zullen we in deze paragraaf dieper op ingaan.

Noem $z := z_{5,-5}$. Het lijkt dat z^2 'heel dicht' bij 25 komt, het blijkt namelijk dat voor kleine priemen p geldt $z_p^2 = 25$. Aangezien $\mathbb{Z}_p$ een domein is heeft 25 twee wortels, namelijk 5 en -5, dus dit betekent dat in deze $\mathbb{Z}_p$ geldt $z_p = \pm 5$.

Laat $Q := \{p \text{ priem} : z_p = 5\}$. Dan geldt $2, 3 \in Q$, maar $5 \notin Q$.

Lemma 6.1.1: Stel p priem, $p > 5$ en neem aan dat:

- Iedere priemdeler l van $\pi(p)$ met $l \neq 5$ voldoet aan $l \in Q$;
- $5^2 \nmid \pi(p)$.

Dan geldt $p \in Q$.

Bewijs. Wegens priemfactorisatie kunnen we zeggen $\pi(p) = 5^n \prod_{l \in Q,\ l<p} l^{k_l}$, waarbij $k(l) \in \mathbb{Z}$ eindig is en $n \in \{0, 1\}$. Voor iedere $l \in Q$ geldt $z \equiv 5 \pmod{l^{k_l}}$ en er geldt $5 \equiv -5 \pmod 5$. Wegens de Chinese reststelling geldt nu $z \equiv 5 \pmod{\pi(p)}$. Dan geldt $F(z) \equiv F(5) \pmod p$, maar aangezien z en 5 dekpunten zijn betekent dit $z \equiv 5 \pmod p$. Stel nu dat voor zekere $N \in \mathbb{Z}_{\geq 0}$ geldt $z \equiv 5 \pmod{p^N}$. Voor $N+1$ geldt dan $\pi(p^{N+1}) | \pi(p) p^N$, dus uit de Chinese reststelling volgt dat $z \equiv 5 \pmod{\pi(p^{N+1})}$. Dus $F(z) \equiv F(5) \pmod{p^{N+1}}$, dus $z \equiv 5 \pmod{p^{N+1}}$. Dus met inductie volgt dat voor alle $n \in \mathbb{Z}_{\geq 0}$ geldt $z \equiv 5 \pmod{p^n}$, dus er geldt $z = 5 \in \mathbb{Z}_p$, dus $p \in Q$. □

Lemma: Voor p priem, $p < 200$ en $p \notin \{5, 101, 151\}$ geldt $p \in Q$.

Bewijs. Stel dat het lemma niet waar is. Neem dan de kleinste priem p zodanig dat $p < 200$, $p \notin \{5, 101, 151\}$ en $p \notin Q$. Dan moet gelden $p > 5$. Zij l een priemdeler van $\pi(p)$. Aangezien $\pi(p)$ even is, geldt $l \neq 101$ en $l \neq 151$. Immers, stel $l = 101$, dan moet l een deler zijn van $\frac{p-1}{2}$ of van $\frac{p+1}{2}$. Als dit zo zou zijn dan geldt $p \geq 201$, terwijl $p < 200$ dus $l \neq 101$. Op dezelfde manier volgt dat $l \neq 151$. Dus voor iedere $l | \pi(p)$ geldt $l < p$, $l \notin \{101, 151\}$ dus als $l \neq 5$ geldt $l \in Q$.

Stel $5^2 | \pi(p)$. Dan moet gelden $5^2 | p - 1$ of $5^2 | p + 1$. Als $5^2 | p - 1$ dan moet $p = 101$ of $p = 151$, maar aangezien was aangenomen dat $p \notin \{101, 151\}$ volgt $5^2 \nmid p - 1$. Als $5^2 | p + 1$ geldt $p \equiv -1 \pmod 5$ en zelfs $p \equiv -1 \pmod{10}$. Dit betekent wegens stelling 3.1.4 dat $\pi(p) | p - 1$, maar dan geldt $5^2 \nmid \pi(p)$. Dus er geldt $5^2 \nmid \pi(p)$.

Er wordt nu aan de voorwaarden van lemma 6.1.1 voldaan, dus met behulp van dit lemma volgt $p \in Q$. Dit is in tegenspraak met hetgeen dat eerder is aangenomen, dus voor alle priemen $p < 200$ met $p \notin \{5, 101, 151\}$ geldt $p \in Q$. □

Lemma: Er geldt $\pi(101) = \pi(151) = 2 \cdot 5^2$.

Bewijs. Merk op dat $101 \equiv 1 \pmod 5$ en $151 \equiv 1 \pmod 5$, dus 5 heeft een kwadraat-wortel in $\mathbb{F}_{101}$ en in $\mathbb{F}_{151}$. Aangezien 101 en 151 priemgetallen zijn, geldt voor $m \in \{101, 151\}$ dat $(\mathbb{Z}/m\mathbb{Z})[\vartheta] = (\mathbb{Z}/m\mathbb{Z})[X]/(X^2 - X - 1) = \mathbb{F}_m[X]/(X^2 - X - 1)$. Uit het bewijs van stelling 4.1.4 uit Bulthuis (2014) [2] volgt dat als geldt $X^2 - X - 1 = (X - \alpha)(X - \beta)$ voor zekere $\alpha, \beta \in \mathbb{F}_m$ de orde van ϑ gegeven door door $\mathrm{ord}(\vartheta) = \mathrm{kgv}(\mathrm{ord}(\alpha), \mathrm{ord}(\beta))$.

Modulo 101 geldt $11^2 = 121 \equiv 20 \pmod{101} = 2^2 \cdot 5 \pmod{101}$, dus $\sqrt{5} = \pm\frac{11}{2} \pmod{101} = \mp 45 \pmod{101}$. Voor ϑ geldt dan:

$$\vartheta = \frac{1+\sqrt{5}}{2} \equiv \frac{1 \mp 45}{2} \pmod{101} = \begin{cases} -22 \pmod{101} \\ 23 \pmod{101} \end{cases}.$$

Verder geldt $23 \equiv 225 \pmod{101} = 15^2 \pmod{101}$. Dus wegens de kleine stelling van Fermat geldt $23^{\frac{p-1}{2}} \equiv 15^{p-1} \pmod{101} \equiv 1 \pmod{101}$. Dus $23^{50} = 1$, dus $\text{ord}(23)|50$. Verder geldt $(-22)^{50} = 22^{50} = 23^{-50} = 1$, dus $\text{ord}(-22)|50$. Dus $\text{ord}(\vartheta)|50$, dus $\pi(101)|50$.

Stel dat $\pi(101) \neq 50$, dan moet omdat $\pi(p)$ even is gelden $\pi(p)|10$. Simpelweg uitschrijven van de eerste termen van de Fibonacci-rij modulo 101 geeft:

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, ...$$

Aangezien modulo 101 geldt $F(0) = 0 \neq F(10) = 55$, geldt $\pi(101) \nmid 10$. Dus er moet gelden $\pi(101) = 50$.

Modulo 151 geldt $14^2 = 196 \equiv 45 \pmod{151} = 3^2 \cdot 5 \pmod{151}$, dus $\sqrt{5} = \pm\frac{14}{3} \pmod{151} = \pm 55 \pmod{151}$. Voor ϑ geldt dan:

$$\vartheta = \frac{1+\sqrt{5}}{2} \equiv \frac{1 \pm 55}{2} \pmod{151} = \begin{cases} 28 \pmod{151} \\ -27 \pmod{151} \end{cases}.$$

Er geldt $-27 = (-3)^3$, dus wegens de kleine stelling van Fermat geldt $(-27)^{50} = (-3)^{150} \equiv 1 \pmod{151}$, dus $\text{ord}(-27)|50$. Verder geldt $28^{50} = (-27)^{-50} = 1$, dus voor de orde van ϑ geldt $\text{ord}(\vartheta) = \text{kgv}(\text{ord}(\alpha), \text{ord}(\beta))|50$. Dus $\pi(151)|50$. Stel $\pi(151) \neq 50$, dan moet gelden $\pi(151)|10$, want $\pi(151)$ is even. Echter geldt modulo 151 dat $F(0) = 0 \neq F(10) = 55$, dus $\pi(151) \nmid 10$, dus $\pi(151) = 50$. □

Gevolg: Er geldt $z \equiv 5 \pmod{101}$ en $z \equiv 5 \pmod{151}$. Immers, aangezien $z = -5 \in \mathbb{Z}_5$, geldt ook $z \equiv -5 \pmod{5^2}$. Daarnaast geldt $z \equiv -5 \pmod 2$, dus uit de Chinese reststelling volgt $z \equiv -5 \pmod{2 \cdot 5^2}$. Dus voor $p \in \{101, 151\}$ geldt $F(z) \equiv F(-5) \pmod p$. Dus $z \equiv 5 \pmod{101}$ en $z \equiv 5 \pmod{151}$.

Stelling: Er geldt $z_{5,-5}^2 \equiv 25 \pmod{201!}$. maar $z_{5,-5}^2 \not\equiv 25 \pmod{202!}$.

Bewijs. Voor de priemfactorisatie $201! = \prod_{p \text{ priem},\ p<200} p^{k(p)}$ geldt $k(101) = 1$ en $k(151) = 1$. Voor $p \in \{101, 151\}$ geldt $z \equiv 5 \pmod p$, dus $z^2 \equiv 25 \pmod p$. Verder geldt voor alle priemen $p < 200$, $p \notin \{101, 151\}$ dat $z^2 \equiv 25 \mod p^k$ met $k \in \mathbb{Z}_{\geq 0}$. Uit de Chinese reststelling volgt nu $z^2 \equiv 25 \pmod{201!}$.

Er geldt $202! = 201! \cdot 2 \cdot 101$. We weten dat $z_{5,-5}^2 \equiv 25 \pmod{201!}$ en voor alle $k \in \mathbb{Z}_{\geq 0}$ geldt $z_{5,-5}^2 \equiv 25 \pmod{2^k}$. Nu geldt echter $101^2|202!$. Voor 101^2 geldt $\pi(101^2)|50 \cdot 101$. Er geldt $z \equiv 5 \pmod{101}$ en $z \equiv -5 \pmod{50}$. Met de Chinese reststelling volgt nu $z \equiv 4045 \pmod{\pi(101^2)}$, dus $F(z) \equiv F(4045) \pmod{101^2}$. Met behulp van een computerberekening geeft dit $z \equiv 8388 \pmod{101^2}$ en $8388^2 \equiv 2247 \pmod{101^2} \neq 25 \pmod{101}^2$.

Dus er volgt $z_{5,-5}^2 \not\equiv 25 \pmod{202!}$. □

Referenties

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

[2] Bulthuis, J. (2014). *Pro-eindige Fibonacci-getallen* (bachelor scriptie Universiteit Leiden). Geraadpleegd op 08 april 2019 op `https://www.math.leidenuniv.nl/scripties/BachBulthuis.pdf`

[3] Bruin, P. (2017). *Topologie.* Universiteit Leiden.

[4] Strassmann, R. (1928). Über den Wertevorrat von Potenzreihen im Gebiet der p-adischen Zahlen. *Journal für die reine und angewandte Mathematik, 159*, 13-28. https://doi.org/10.1515/crll.1928.159.13

[5] Cassels, J.W.S. (1986). *Local Fields.* Cambridge, United Kingdom: Cambridge University Press.

[6] Gupta, H. (1980). *Selected topics in number theory.* Tunbridge Wells: Abacus Press.

[7] Hokken, D. (2018). *Profinite Number Theory* (bachelor scriptie Universiteit Utrecht). Geraadpleegd op 08 april 2019 via: `http://studenttheses.library.uu.nl/search.php?language=en`