Hilal Moussa

Lineaire recurrente rijen

Bachelorscriptie, 17 juni 2010

Scriptiebegeleider: J.-H. Evertse

Mathematisch Instituut, Universiteit Leiden

Inhoudsopgave

Inleiding

Een lineaire recurrente rij (lrr) $U = \{u_n\}_{n=0}^{\infty}$ in $\mathbb{C}$ wordt gegeven door een lineaire recurrentie:

$$u_n = c_1 u_{n-1} + c_2 u_{n-2} + \cdots + c_k u_{n-k} (n \geq k)$$

met coëfficiënten $c_1, \ldots, c_k \in \mathbb{C}$ en beginwaarden $u_0, \ldots, u_{k-1} \in \mathbb{C}$.

In deze scriptie behandelen we de volgende Stelling van Skolem-Mahler-Lech:

Zij U een lrr. Dan is de verzameling $N(U) = \{n \in \mathbb{Z}_{\geq 0}; u_n = 0\}$ de vereniging van een eindige verzameling met een eindig aantal rekenkundige rijen.

Deze stelling kan worden bewezen met behulp van de methode van p-adische getallen en p-adische machtreeksen.
Skolem bedacht de methode gebaseerd op p-adische getallen en p-adische machtreeksen en bewees de stelling (1934)[4] [5] in het geval $U = \{u_n\}_{n=0}^{\infty}$ al zijn termen in $\mathbb{Q}$ heeft.
Mahler (1935)[3] bewees de stelling in het geval alle termen van U algebraïsche getallen zijn. Lech (1953)[2] bewees de stelling in het algemene geval. Het idee van Lech was een nieuwe inbeddingsstelling waarmee hij een willekeurige lrr de rij kon afbeelden in het lichaam van de p-adische getallen .

Voorbeeld: 1) Rij aan Fibonacci: $u_n = u_{n-1} + u_{n-2}$ $(n \geq 2)$,
$u_0 = 0, u_1 = 1$. Dan $N(U) = \{0\}$.

2) Zij $u_n = \frac{n-3}{12}(3^n - (-3)^n)$
Er geldt $u_0 = 0, u_1 = -1, u_2 = 0, u_3 = 0$.
Verder is $u_n = 18u_{n-2} - 81u_{n-4}$ voor $n \geq 4$. Er geldt dat $u_n = 0$ voor alle even waarden van n, en $u_n \neq 0$ voor alle oneven waarden van n met $n \geq 5$. Dus $N(U) = \{3\} \cup \{0, 2, 4, 6, \ldots\}$.

Ten eerste definiëren we lineaire recurrente rijen en geven enkele eigenschappen daarvan.
Ten tweede definiëren we lichaam het $\mathbb{Q}_p$ van de p-adische getallen We gaan daarna de nodige eigenschappen van p-adische getallen en p-adische machtreeksen bestuderen.

Verder gebruiken we de Inbeddingsstelling van Lech (zonder bewijs), die een relatie geeft tussen de stelling van Skolem-Mahler-Lech en p-adische getallen.

Tenslotte passen wij de stelling van Strassman over nulpunten van p-adische machtreeksen samen met lemma's en stellingen toe die eerder in deze scriptie worden behandeld en geven hiermee een bewijs van de stelling van Skolem-Mahler-Lech.

1 Lineaire recurrente rijen

Definitie: Een lineaire recurente rij (lrr) $U = \{u_n\}_{n=0}^{\infty}$ in $\mathbb{C}$
wordt gegeven door een lineaire recurrentie:

$$u_n = c_1 u_{n-1} + c_2 u_{n-2} + \cdots + c_k u_{n-k} \quad (n \geq k) \tag{1}$$

met coëfficiënten $c_1, \ldots, c_k \in \mathbb{C}$ en beginwaarden $u_0, \ldots, u_{k-1} \in \mathbb{C}$.

Onder alle lineaire recurrenties waaraan een gegeven lrr voldoet is er een unieke recurrentie, waarvoor de lengte k minimaal is. Deze minimale waarde van k heet de orde van U.

Zij $U = \{u_n\}_{n=0}^{\infty}$ een lrr van orde k met recurrentie zoals gegeven bij (1). Het *karakteristiek polynoom van* U is gegeven door $F_U(X) := X^k - c_1 X^{k-1} - \cdots - c_k$. We kunnen dit ook opschrijven als

$$F_U(X) = (X - \alpha_1)^{e_1} \ldots (X - \alpha_r)^{e_r} \tag{2}$$

waarbij $\alpha_1, \ldots, \alpha_r \in \mathbb{C}$ verschillend zijn, en $e_i > 0$ voor $i = 1, \ldots, r$.

Stelling 1. *Er zijn uniek bepaalde polynomen $f_i \in \mathbb{C}[X]$ van graad $e_i - 1$ voor $i = 1, \ldots, r$ zodat:*

$$u_n = \sum_{i=1}^{r} f_i(n) \alpha_i^n \tag{3}$$

waarbij α_i en e_i $(i = 1, \ldots, r)$ worden gegeven door (2).

Bewijs. Er zijn een polynoom A van graad $< k$ en constanten c_{ij} met

$$\sum_{n=0}^{\infty} u_n X^n = \frac{A(X)}{1 - c_1 X - c_2 X^2 - \cdots - c_k X^k} = \sum_{i=1}^{r} \sum_{j=1}^{e_i} \frac{c_{ij}}{(1 - \alpha_i X)^j}$$

$$= \sum_{i=1}^{r} \sum_{j=1}^{e_i} c_{ij} \sum_{n=0}^{\infty} \binom{n+j-1}{j-1} \alpha_i^n X^n = \sum_{n=0}^{\infty} \left(\sum_{i=1}^{r} \sum_{j=1}^{e_i} c_{ij} \binom{n+j-1}{j-1} \alpha_i^n \right) X^n$$

$$= \sum_{i=1}^{r} f_i(n) \alpha_i^n$$

Waarbij

$$f_i(n) := \sum_{j=1}^{e_i} c_{ij} \binom{n+j-1}{j-1} \text{ voor } i = 1, \ldots r.$$

□

In deze scriptie geven we het bewijs van de volgende stelling:

Stelling 2 (Skolem,Mahler,Lech) *De verzameling* $N(U) = \{n \in \mathbb{Z}_{\geq 0}; u_n = 0\}$ *is de vereniging van een eindige verzameling en een aantal rekenkundige rijen.*

Het bewijs is gebaseerd op de theorie van *p-adische getallen en p-adische machtreeksen.*

2 p-adische absolute waarde

Definitie: Zij p een priemgetal , dan definiëren we de orde van $a \in \mathbb{Q}$ door

$$\begin{aligned} \mathrm{ord}_p(a) &= m \text{ als } a = p^m b/c \text{ met } m, b, c \in \mathbb{Z} \text{ en } p \text{ geen deler van } b \text{ en } c, \\ \mathrm{ord}_p(0) &= \infty \end{aligned}$$

Dan definiëren we de p-adische absolute waarde van $a \in \mathbb{Q}$ door:

$$|a|_p := p^{-\mathrm{ord}_p(a)}.$$

Voorbeeld: Zij $a = 3^{-5}7^2 11^6$,dan $|a|_3 = 3^5, |a|_{11} = 11^{-6}$ en $|a|_p = 1$ voor alle priemgetallen $p \neq 3, 7, 11$.

Eigenschappen :

- $|ab|_p = |a|_p |b|_p$ voor alle a en $b \in \mathbb{Q}$;
- $|a + b|_p \leq \max(|a|_p, |b|_p)$ voor alle a en $b \in \mathbb{Q}$;
- $|a + b|_p = \max(|a|_p, |b|_p)$ voor alle a en $b \in \mathbb{Q}$ met $|a|_p \neq |b|_p$.

3 Lichaam van p-adische getallen

Voor meer informatie over p-adische getallen zie [1].

$|.|_p$ definieert een norm op $\mathbb{Q}$. De rij $\{x_n\}_{n=0}^{\infty} \in \mathbb{Q}$ heet een Cauchy-rij m.b.t $|.|_p$ als $\lim_{m,n\to\infty} |x_m - x_n|_p = 0$
De rij $\{x_n\}_{n=0}^{\infty}$ in $\mathbb{Q}$ heet een nulrij m.b.t $|.|_p$ als $\lim_{n\to\infty} |x_n|_p = 0$.
De Cauchy-rijen m.b.t $|.|_p$ met termsgewijze optelling en vermenigvuldiging vormen een ring R. De nulrijen vormen een maximaal ideaal M in R.

Het quotient R/M is een lichaam, dat we aangeven met $\mathbb{Q}_p$, *het lichaam van de p-adische getallen.* We identificeren $a \in \mathbb{Q}$ met de restklasse modulo M van de constante Cauchy-rij $\{a\}$. Dan kunnen we $\mathbb{Q}$ opvatten als deellichaam van $\mathbb{Q}_p$. We kunnen $|.|_p$ eenduidig voortzetten tot $\mathbb{Q}_p$, door te definiëren:
$|\alpha|_p := \lim_{n\to\infty} |a_n|_p$ als α de restklasse $\mod M$ is van de Cauchy-rij $\{a_n\}_{n=0}^{\infty}$.

Lemma 1

1. *De absolute waarde $|.|_p$ is niet–archimedisch.*

2. *De waardenverzameling van $|.|_p$ op $\mathbb{Q}_p$ is $\{0\} \cup \{p^m : m \in \mathbb{Z}\}$.*

Bewijs. (1) Zijn $x, y \in \mathbb{Q}_p$ neem rijen $\{x_n\}$,$\{y_n\}$ uit $\mathbb{Q}$ die convergeren naar respectievelijk x en y,
dan $|x+y|_p = \lim_{t\to\infty} |x_t + y_t|_p \leq \lim_{t\to\infty} \max(|x_t|_p, |y_t|_p) = \max(|x|_p, |y|_p)$.

(2) Zij $x \in \mathbb{Q}_p$. Dan er is een rij $\{x_n\}$ in $\mathbb{Q}$ die convergeert naar x,dus $|x|_p = \lim_{k\to\infty} |x_k|_p$. Voor alle k geldt $|x_k|_p = p^{m_k}$ voor zekere $m_k \in \mathbb{Z}$. De rij van $\{p^{m_k}\}$ convergeert, dus er zijn m en k_0 zodat $m_k = m$ voor alle $k \geq k_0$. Dus $|x|_p = p^m$. □

De verzameling $\mathbb{Z}_p$=$\{x \in \mathbb{Q}_p : |x|_p \leq 1\}$ *is een deelring van $\mathbb{Q}_p$, de ring van p-adische gehelen.*
Er geldt $\mathbb{Z} \subset \mathbb{Z}_p \subset \mathbb{Q}_p$.

Lemma 2. *Voor alle $\alpha \in \mathbb{Z}_p$ en alle $m \in \mathbb{Z}_{\geq 0}$, is er een unieke $a_m \in \mathbb{Z}$, zodat $|\alpha - a_m|_p \leq p^{-m}$ en $0 \leq a_m < p^m$.*

Bewijs. Als $a, b \in \mathbb{Q}$, dan schrijven we $a \equiv b \pmod{p^m}$ als $(a-b)/p^m \in \mathbb{Z}_p$. Omdat $\mathbb{Q}$ dicht ligt in $\mathbb{Q}_p$ is er een rationaal getal (a/b) met a en $b \in \mathbb{Z}$ met
$\text{ggd}(a,b) = 1$ zodat $|\alpha - (a/b)|_p \leq p^{-m}$.
b is niet deelbaar door p want $|a/b|_p \leq 1$, dus er is een geheel getal a_m met
$(ba_m) \equiv a \pmod{p^m}$ en $0 \leq a_m < p^m$.
Dus $|\alpha - a_m|_p \leq \max(|\alpha - (a/b)|_p, |(a/b) - a_m|_p) \leq p^{-m}$
Zij z_m een ander geheel getal met de eigenschap van het lemma, dan geldt $|a_m - z_m|_p \leq p^{-m}$ dus $z_m \equiv a_m \pmod{p^m}$. Maar dan is $z_m = a_m$, dus a_m is uniek bepaald. □

Gevolg: $\mathbb{Z}$ ligt dicht in $\mathbb{Z}_p$.

Stelling 3. (i) De eenhedengroep van $\mathbb{Z}_p$ is

$$\mathbb{Z}_p^* = \{x \in \mathbb{Q}_p : |x|_p = 1\}$$

(ii) De idealen ongelijk aan (0) van $\mathbb{Z}_p$ zijn $p^m\mathbb{Z}_p$, $(m = 0, 1, 2, \cdots)$ .Verder is $\mathbb{Z}_p/p^m\mathbb{Z}_p \cong \mathbb{Z}/p^m\mathbb{Z}$.

Bewijs. (i) Wij hebben $x \in \mathbb{Z}_p^* \iff |x|_p \leq 1, |x^{-1}|_p \leq 1 \iff |x|_p \leq 1$ en $|x|_p \geq 1 \Leftrightarrow |x|_p = 1$.
(ii) Zij I een ideaal ongelijk aan (0) van $\mathbb{Z}_p$. Kies $\alpha \in I$ zodat $|\alpha|_p$ maximaal is, en zij $|\alpha|_p = p^{-m}$. Dan is $|p^{-m}\alpha|_p = p^m p^{-m} = 1$, dus $p^{-m}\alpha \in \mathbb{Z}_p^*$, m.a.w. $p^m\alpha^{-1} \in \mathbb{Z}_p^*$. Omdat I een ideaal is volgt dat $p^m = \alpha(p^m\alpha^{-1}) \in I$.
Zij $\beta \in I$ met $|\beta p^{-m}|_p \leq 1$. Dan is $\beta p^{-m} \in \mathbb{Z}_p$, dus $\beta \in p^m\mathbb{Z}_p$. Bijgevolg is $I \subset p^m\mathbb{Z}_p$. Omdat ook $p^m\mathbb{Z}_p \subset I$, volgt dat $p^m\mathbb{Z}_p = I$.
Volgens Lemma 2 is de inclusie $\mathbb{Z}_p/p^m\mathbb{Z}_p \hookrightarrow \mathbb{Z}/p^m\mathbb{Z}$ surjectief. Hieruit volgt (ii). □

Lemma 3. Zij $\{a_n\}_{n=0}^{\infty}$ een rij in $\mathbb{Q}_p$. Dan is $\sum_{k=0}^{\infty} a_k$ convergent in $\mathbb{Q}_p \iff \lim_{k\to\infty} a_k = 0$.

Bewijs. $\Rightarrow$) Stel dat $\alpha = \sum_{k=0}^{n} a_k$ convergeert. Dan $a_n = \sum_{k=0}^{n} a_k - \sum_{k=0}^{n-1} a_k \to \alpha - \alpha = 0$ als $n \to \infty$.
$\Leftarrow$) Stel $a_k \to 0$ als $k \to \infty$. Zij $\alpha_n = \sum_{k=0}^{n} a_k$, dan geldt voor alle m, n met $m > n > 0$ dat $|\alpha_m - \alpha_n|_p = |\sum_{k=n+1}^{m} a_k|_p \leq \max(|a_{n+1}|_p, \cdots, |a_m|_k) \to 0$ als
$m, n \to \infty$, dus α_n is een Cauchy rij in $\mathbb{Q}_p$ dus α_n convergeert want $\mathbb{Q}_p$ is compleet. □

- **Opmerking (belangrijk):** Iedere reeks $\sum_{n=0}^{\infty} a_n$ die in $\mathbb{Q}_p$ convergeert is onvoorwaardelijk convergent, m.a.w. als we de termen van $\{a_n\}$ permuteren dan blijft de reeks convergent, en blijft de waarde van de reeks onveranderd.

Feit 1. Definieer de bal $B(a, r) = \{x \in \mathbb{Q}_p : |x - a|_p \leq r\}$. Als $b \in B(a, r)$, dan is $B(a, r) = B(b, r)$, m.a.w ieder punt in een bal is een middelpunt van die bal.

Bewijs. Zij $x \in B(a, r)$. Dan $|x - b|_p \leq \max(|x - a|_p, |a - b|_p) \leq r$ dus $x \in B(b, r)$. Bijgevolg is $B(a, r) \subset B(b, r)$. Op dezelfde manier volgt dat $B(b, r) \subset B(a, r)$. Dus $B(a, r) = B(b, r)$. □

Definitie. We zeggen dat $U \subset \mathbb{Q}_p$ open is, als $U = \emptyset$ of als er voor alle $a \in U$ een $m > 0$ is met $B(a, p^{-m}) \subset U$. De open verzamelingen in $\mathbb{Q}_p$ vormen de *p-adische topologie.*

Stelling 4. *Zij $a \in \mathbb{Q}_p, m \in \mathbb{Z}$. Dan is $B(a, p^{-m})$ open en compact in de p-adische topologie*

Bewijs. Uit Feit 1 volgt direct dat $B(a, p^{-m})$ open is. Stel $B_0 := B(a, p^{-m})$ is niet compact. Dan is er een oneindige open overdekking $\{U_i\}_{i\in A}$ van B_0, zodat geen eindige deelcollectie van $\{U_i\}_{i\in A}$ de verzameling B_0 overdekt. Zij $x \in B(a, p^{-m})$. Dan is $|\frac{x-a}{p^m}|_p \leq 1$. Dus volgens Lemma 2, is er een $b \in \{0, \ldots, p-1\}$ zodat

$$|\frac{x-a}{p^m} - b|_p \leq p^{-1}. \text{ Met andere woorden, } x \in B(a + bp^m, p^{-m-1}).$$

Dan volgt:

$$B(a, p^{-m}) = \bigcup_{b=0}^{p-1} B(a + bp^m, p^{-m-1}).$$

Dus er is een bal $B_1 \subset B(a, p^{-m}) = B_0$ van straal p^{-m-1}, die niet overdekt wordt door een eindige deelverzameling van $\{U_i\}_{i\in A}$. Door dit argument te herhalen, vinden we een oneindige rij $B_0 \supset B_1 \supset B_2 \supset \ldots$, waarbij B_i een bal van straal p^{-m-i} is die geen eindige deelverzameling van $\{U_i\}_{i\in A}$ heeft.

We laten zien dat de doorsnede van deze ballen niet leeg is:
Kies voor alle $i \geq 0$ een $x_i \in B_i$. Dus $B_i = B(x_i, p^{-m-i})$. Dan is de rij $\{x_i\}$ een Cauchy-rij want

$$|x_i - x_j|_p \leq p^{-m-\min(i,j)} \to 0 \text{ als } i, j \to \infty.$$

Maar $\mathbb{Q}_p$ is compleet dus deze rij heeft een limiet x^* in $\mathbb{Q}_p$. Dan $x^* \in B_i$ voor alle i want

$$|x_i - x^*|_p = \lim_{j\to\infty} |x_i - x_j|_p \leq p^{-m-i}.$$

Dus $B_i = B(x^*, p^{-m-i})$ voor alle $i \geq 0$. Het punt x^* ligt in een open verzameling U uit $\{U_i\}_{i\in A}$, dus er is een $m_1 > 0$ zodat $B(x^*, p^{-m_1}) \subset U$. Wij kiezen i zo groot mogelijk zodat $B_i(x^*, p^{-m-i}) \subset B(x^*, p^{-m_1}) \subset U$. Dus B_i wordt overdekt door een eindige deelcollectie van $\{U_i\}_{i\in A}$. Dus de aanname dat $B_0 := B(a, p^{-m})$ niet compact is, was onjuist. □

.

Gevolg 2. *$\mathbb{Z}_p$ is open en compact.*

Belangrijk. De volgende stelling geeft de relatie tussen de stelling van Skolem-Mahler-Lech en p-adische getallen.

Inbeddingsstelling van Lech. *Zij k het lichaam voortgebracht over $\mathbb{Q}$ door de α_i en de coëfficiënten van f_i $(i = 1, \ldots, r)$, waarbij α_i en de coëfficiënten van f_i en r worden gegeven door (2) en (3) voor $i = 1, \ldots, r$. Dan er zijn een priemgetal p en een injectief homomorfisme $\Phi : k \longrightarrow \mathbb{Q}_p$ met $|\phi(\alpha_i)|_p = 1$ $\forall i = 1, \ldots, r$.*

Bewijs. Zie [2]. □

Gevolg 3:

We kunnen $\phi(x)$ identificeren met $x \in k$, dus wij mogen aannemen dat α_i en de coëfficiënten van f_i $(i = 1, \ldots, r)$ in $\mathbb{Q}_p$ liggen en dat $|\alpha_i|_p = 1$ voor $i = 1, \ldots, r$.

4 Theorie van machtreeksen in $\mathbb{Q}_p$

We proberen een machtreeks $G(X) = \sum_{k=0}^{\infty} a_k x^k$ te definiëren op $\mathbb{Z}_p$ zodat $G(n) = \sum_{n=0}^{r} f_i(n)\alpha_i^n$ voor alle $n \in \mathbb{Z}_{\geq 0}$.

Feit 2. zij $a_n \in \mathbb{Q}_p$ voor alle $n \geq 0$ en $x \in \mathbb{Q}_p$. Dan convergeert $\sum_{n=0}^{\infty} a_n x^n$ in $\mathbb{Q}_p \Longleftrightarrow \lim_{n\to\infty} |a_n x^n|_p = 0$.

Bewijs. Gevolg van Lemma 3. □

Definitie. Wij definiëren $\exp_p(x) = \sum_{n=0}^{\infty} x^n/n!$ en $\log_p(x+1) = \sum_{n=1}^{\infty}(-1)^{n-1}x^n/n$ voor alle $x \in \mathbb{Q}_p$ waarvoor de machtreeksen convergeren.

Wij gaan nu convergentiegebieden van $\exp_p$ en $\log_p$ bepalen.

Lemma 4.

1. $\lim_{n\to\infty} |x^n/n!|_p = 0$ *als* $|x|_p < p^{-1/(p-1)}$.
2. $\lim_{n\to\infty} |(-1)^{n-1}x^n/n|_p = 0$ *als* $|x|_p < 1$.

Bewijs. 1. Zij r_k het aantal getallen in $\{1, \ldots, n\}$ dat deelbaar is door p^k. Dan

$$\begin{aligned} \mathrm{ord}_p(n!) &= \sum_{k=1}^{\infty} k(r_k - r_{k+1}) = \sum_{k=1}^{\infty} kr_k - \sum_{k=2}^{\infty}(k-1)r_k \\ &= \sum_{k=1}^{\infty} r_k = \sum_{k=1}^{\infty}[n/p^k]. \end{aligned}$$

Neem nu aan dat $|x|_p < p^{-1/p-1}$. Dan is $\mathrm{ord}_p(x) = \alpha$ met $\alpha > 1/(p-1)$, dus

$$\begin{aligned} \mathrm{ord}_p(x^n/n!) &= n\alpha - \sum_{k=1}^{\infty}[n/p^k] \\ &\geq n\alpha - \sum_{k=1}^{\infty} n/p^k = n(\alpha - \frac{1}{p-1}) \longrightarrow \infty \text{ als } n \to \infty. \end{aligned}$$

Dus $\lim_{n\to\infty} |x^n/n!|_p = p^{\lim_{n\to\infty}(-\mathrm{ord}_p(x^n/n!))} = 0$

2. Er geldt $|(-1)^{n-1}x^n/n|_p = |x^n/n|_p$

Stel $|x|_p = \alpha$, en $|n|_p = p^{-m}$. Dan volgt $\alpha < 1$ en $m > 0$

$|x^n/n|_p = \alpha^n p^m \leq \alpha^n n$. Zij $z = \alpha^n n$, dan $\log(z) = n(\log(\alpha) + \log(n)/n) \longrightarrow -\infty$ als

$n \to \infty$ want $\log(\alpha) < 0$. Dus $\alpha^n n \to 0$ en vervolgens $\lim_{n\to\infty} |(-1)^{n-1}x^n/n|_p = 0$ als $|x| < 1$.

□

Gevolg 5. $\exp_p(x)$ en $\log_p(x)$ convergeren respectievelijk op $\{x \in \mathbb{Q}_p : |x|_p < p^{-1/(p-1)} \}$ en op $\{x \in \mathbb{Q}_p : |x|_p < 1 \}$.

Definitie. Zij U een open deelverzameling van $\mathbb{Q}_p$ en $f : U \longrightarrow \mathbb{Q}_p$ een functie. We zeggen dat f differentieerbaar is op U als

$$\lim_{x\to a} \frac{f(x) - f(a)}{x - a} \text{ bestaat voor alle } a \in U.$$

We noemen deze limiet $f'(a)$, m.a.w voor alle $a \in U$ is er een getal $f'(a)$ met de volgende eigenschap: voor alle $\epsilon > 0$ is er een $\delta > 0$ zodat

$$|\frac{f(x) - f(a)}{x - a} - f'(a)|_p < \epsilon \text{ voor alle } x \in \mathbb{Q}_p \text{ met } |x - a|_p < \delta.$$

Eigenschappen:
Zijn f, g differentieerbare functies op een open deelverzameling U van $\mathbb{Q}_p$. Dan geldt:

- $(f + g)' = f' + g'$,
- $(cf)' = cf'$ voor $c \in \mathbb{Q}_p$,
- $(fg)' = f'g + g'f$,
- $(f/g)' = \frac{gf' - g'f}{g^2}$ als $g(x) \neq 0$ voor alle $x \in \mathbb{Q}_p$.
- Zij V een open deelverzameling van $\mathbb{Q}_p$ en $h : V \to \mathbb{Q}_p$ differentieerbaar functie zodat $h(V) \subset U$. Dan is $f \circ h$ een differentieerbare functie van V naar $\mathbb{Q}_p$ en $f(h(x))' = f'(h(x))h'(x)$ voor $x \in V$.

Het bewijs gaat op dezelfde manier als in de reële analyse.

Stelling . Zij $f(x) = \sum_{n=0}^{\infty} a_n x^n$ met $a_n \in \mathbb{Q}_p$ een machtreeks die convergeert op $B(0, r)$, $r > 0$, dan is f een differentieerbare op $B(0, r)$ en $f'(x) = \sum_{n=1}^{\infty} n a_n x^{n-1}$ voor $x \in B(0, r)$.

Bewijs. zij $\epsilon > 0$ en $a \in B(0, r)$. Dan

$$|\frac{f(x) - f(a)}{x - a} - \sum_{n=1}^{\infty} n a_n x^{n-1}|_p = |\sum_{n=1}^{\infty} \frac{a_n(x^n - a^n)}{x - a} - n a_n x^{n-1}|_p \tag{4}$$

Maar

$$|\frac{a_n(x^n-a^n)}{x-a} - na_nx^{n-1}|_p$$

$$\begin{aligned}
&= |a_n(x^{n-1}+ax^{n-2}+a^2x^{n-3}+\cdots+a^{n-1}-nx^{n-1})|_p \\
&= |a-x|_p|a_n(x^{n-2}+x^{n-3}\cdot\frac{x^2-a^2}{x-a}+\cdots+\frac{x^{n-1}-a^{n-1}}{x-a})|_p \\
&= |x-a|_p|a_n(x^{n-2}+x^{n-3}(x+a)+\cdots+x^{n-2}+ax^{n-3}+\cdots+a^{n-2}|_p \\
&= |x-a|_p|a_n(x^{n-2}+(x^{n-2}+ax^{n-3})+\cdots|_p \quad .
\end{aligned}$$

In de tweede factor zijn alle termen van de vorm $a_nx^{(n-2-i)}a^i$ met $i \geq 0$. We kiezen δ zodat $\delta < |a|_p$. Dan geldt voor alle x met $|x-a|_p < \delta$ dat $|x|_p = |a|_p$. Dan volgt $|a_nx^{n-2-i}a^i|_p = |a_na^{n-2}|_p$.
Zij $M := \max_{n\geq 0}|a_na^n|_p$. Dan M is eindig omdat $\sum_{n=0}^{\infty} a_na^n$ convergent is. Kies nu δ zodat $\frac{M}{|a|_p^2}\delta < \epsilon$. Dan volgt

$$|\frac{f(x)-f(a)}{x-a} - \sum_{n=1}^{\infty} na_nx^{n-1}|_p < \frac{M}{|a|_p^2}|x-a|_p < \frac{M}{|a|_p^2}\delta < \epsilon$$

voor alle x met $|x-a|_p < \delta$, $x \neq a$. Dus f is differentieerbaar en $f'(x) = \sum_{n=1}^{\infty} na_nx^{n-1}$. □

Lemma 5.

1. $|\log_p(x+1)|_p = |x|_p$ als $|x|_p < p^{-1/(p-1)}$.
2. $\exp_p(x_1+x_2) = \exp_p(x_1)\exp(x_2)$ als $|x_1|_p < p^{-1/(p-1)}$ en $|x_2|_p < p^{-1/(p-1)}$.
3. $\exp_p(\log_p(1+x)) = 1+x$ als $|x|_p < p^{-1/(p-1)}$.
4. $\log_p(\exp_p(x)) = x$ als $|x|_p < p^{-1/(p-1)}$.
5. $\exp_p(x\log_p(1+\beta))$ is goed gedefinieerd als $x \in \mathbb{Z}_p$ en $|\beta|_p < p^{-1/(p-1)}$.
6. $\exp_p(m\log_p(1+\beta)) = (1+\beta)^m$ voor $m \in \mathbb{Z}_{\geq 0}$ en $|\beta|_p < p^{-1/(p-1)}$.

Bewijs. 1. Wij hebben

$$\begin{aligned}
\log_p(1+x) &= x - x^2/2 + x^3/3 - x^4/4 + \cdots \\
\text{dus } |\log_p(1+x)|_p &\leq \max(|x|_p, |x|_p^2/|2|_p, |x|_p^3/|3|_p, \ldots.)
\end{aligned}$$

Er geldt $|\log_p(x+1)|_p = |x|_p$ als $\frac{|x|_p^i}{|i|_p} < |x|_p$ voor alle $i \geq 2$ (zie eigenschappen van $|.|_p$). Dus het is voldoende om te bewijzen dat

$$|x|_p^{i-1} < |i|_p \text{ voor alle } i \geq 2, x \in \mathbb{Q}_p, |x|_p < p^{-1/(p-1)}. \tag{5}$$

Wij hebben twee mogelijkheden:
1. p is geen deler van i, dan volgt dat $|i|_p = 1$ en dus is (5) zeker juist.
2. p is een deler van i, dus er is een geheel getal i' met $|i'|_p = 1$ en $i = p^m \cdot i'$ met $m > 0$, dus geldt (5) d.e.s.d. als

$$|x|_p^{p^m \cdot i' - 1} < p^{-m} \text{ voor alle } m \geq 0 \text{ en alle } i' \geq 1. \tag{6}$$

Er geldt

$$|x|_p^{p^m \cdot i' - 1} \leq |x|_p^{p^m - 1}$$

want $|x|_p < 1$ en $p^m \cdot i' - 1 \geq p^m - 1$, dus (6) geldt d.e.s.d. als

$$|x|_p^{p^m - 1} < p^{-m} \tag{7}$$

voor alle $m \geq 1$, dus er geldt ook (5) $\Longleftrightarrow$ (7)
Nu is $|x|_p < p^{\frac{-1}{(p-1)}}$, d.e.s.d. als

$$|x|_p^{p-1} < p^{-1}.$$

Dan geldt

$$|x|_p^{p^m - 1} = |x|_p^{(p-1)(1+p+p^2+\cdots+p^{m-1})} \leq (p^{-1})^{1+p+p^2+\cdots+p^{m-1}} \leq p^{-m}.$$

Dus (7) geldt . Hieruit volgt (5).

2. Als $|x_1|_p < p^{-1/(p-1)}$ en $|x_2|_p < p^{-1/(p-1)}$ dan geldt ook
$|x_1 + x_2|_p < \max(|x_1|_p, |x_2|_p) < p^{-1/(p-1)}$ (eigenschappen van $|.|_p$). Dus enerzijds

$\exp_p(x_1+x_2) = \sum_{k=0}^{\infty} \frac{(x_1+x_2)^n}{k!}$, en anderszijds wegens onvoorwaardelijke convergentie,

$$\begin{aligned}
\exp_p(x_1)\exp_p(x_2) &= \sum_{n=0}^{\infty} x_1^n/n! \sum_{m=0}^{\infty} x_2^m/m! \\
&= \sum_{n=0}^{\infty}\sum_{m=0}^{\infty} \frac{x_1^n x_2^m}{n!m!} \\
&= \sum_{k=0}^{\infty}\left(\sum_{m+n=k} \frac{x_1^n x_2^m}{n!m!}\right) \\
&= \sum_{k=0}^{\infty}\sum_{m=0}^{k} \frac{x_1^{k-m} x_2^m}{(k-m)!m!} \\
&= \sum_{k=0}^{\infty}\sum_{m=0}^{k} \frac{1}{k!}\frac{k!}{(k-m)!m!} x_1^{k-m} x_2^m \\
&= \sum_{k=0}^{\infty}\frac{1}{k!}\sum_{m=0}^{k}\binom{k}{m} x_1^{k-m} x_2^m \\
&= \sum_{k=0}^{\infty}\frac{1}{k!}(x_1+x_2)^k \\
&= \exp_p(x_1+x_2).
\end{aligned}$$

3.

$$\text{Definieer } f(x) := \exp_p(\log_p(1+x), \quad g(x) = 1+x.$$

Dan is $f(x) = \sum_{n=0}^{\infty} a_n x^n$ met zekere $a_n \in \mathbb{Q}$
Volgens 2. is $|\log_p(x+1)|_p = |x|_p$ als $|x|_p < p^{-1/(p-1)}$ dus $f(x)$ convergeert voor alle $x \in \mathbb{Q}_p$ met $|x|_p < p^{-1/(p-1)}$. Nu geldt voor alle $x \in \mathbb{Q}_p$ met $|x|_p < p^{-1/(p-1)}$ dat enerzijds $f'(x) = \sum_{n=1}^{\infty} n a_n x^{n-1}$ en anderzijds

$$\begin{aligned}
f'(x) &= \exp_p'(\log_p(1+x)).\log_p'(1+x) \\
&= \exp_p(\log_p(1+x))\frac{1}{1+x} = \frac{f(x)}{1+x}
\end{aligned}$$

$$\text{Dus } (1+x)\sum_{n=1}^{\infty} n a_n x^{n-1} = \sum_{n=0}^{\infty} a_n x^n \text{ voor alle } x \in \mathbb{Q}_p \text{ met } |x|_p < p^{-1/(p-1)}.$$

Uitwerking geeft:

$$\sum_{n=0}^{\infty}[(n+1)a_{n+1} + n a_n]x^n = \sum_{n=0}^{\infty} a_n x^n \text{ voor alle } x \in \mathbb{Q}_p \text{ met } |x|_p < p^{-1/(p-1)}$$

$$\text{dus } (n+1)a_{n+1} + n a_n = a_n \text{ voor alle } n \geq 0.$$

Omdat $f(0) = 1$ volgt dat $a_0 = 1$. En dan volgt $a_1 = 1$ en met inductie $a_n = 0$ voor alle $n \geq 2$. Dus $f(x) = \sum_{n=0}^{\infty} a_n x^n = 1 + x$ voor alle $x \in \mathbb{Q}_p$ met $|x|_p < p^{-1/(p-1)}$

4. Wij laten eerst zien dat $\log_p(\exp_p(x))$ is goed gedefinieerd als $|x|_p < p^{-1/(p-1)}$. Dan moeten we bewijzen $|\exp_p(x) - 1|_p < 1$:

$$|\exp_p(x) - 1|_p = |x + x^2/2! + x^3/3! + \cdots|_p \leq \max(|x|_p, |x^2/2!|_p, |x^3/3!|_p, \ldots).$$

Dus het is voldoende te bewijzen dat $|x^i/i!|_p < 1,$ voor alle $i \geq 1$ met $|x|_p < p^{-1/(p-1)}$

Er geldt $\mathrm{ord}_p(x^i/i!) \geq i(\mathrm{ord}_p(x) - \frac{1}{(p-1)})$, voor alle $i \geq 1$ en $x \in \mathbb{Q}_p$ met $|x|_p < p^{-1/(p-1)}$. (zie het bewijs van lemma 4.1).

$$\text{Dus } |x^i/i!|_p \leq p^{-i(\mathrm{ord}_p(x) - \frac{1}{(p-1)})} < 1 \text{ want } \mathrm{ord}_p(x) > 1/(p-1) \text{ en } i \geq 1.$$

Dan volgt $|\exp_p(x) - 1|_p < 1$.

$$\begin{aligned} \text{Definieer } f(x): &= \log_p(\exp_p(x)) \text{ voor alle } x \in \mathbb{Q}_p \text{ met } |x|_p < p^{-1/(p-1)}. \\ \text{Dan is } f'(x) &= \frac{1}{\exp_p(x)} \exp_p(x) = 1, \end{aligned}$$

dus $f(x) = x + c$. Maar $f(0) = 0$ dus $c = 0$ en $f(x) = x$.

5 . Er geldt:

$$|x \log(1+\beta)|_p = |x|_p |\beta|_p < p^{-1/(p-1)} \text{ als } x \in \mathbb{Z}_p \text{ en } |\beta|_p < p^{-1/(p-1)} (\text{ volgens 1.})$$

Dus $\exp_p(x \log_p(1+\beta))$ is goed gedefiniëerd als $x \in \mathbb{Z}_p$ en $|\beta|_p < p^{-1/(p-1)}$.

6. Met inductie naar m. Als $m = 1$ dan geldt volgens (3) dat $\exp_p(\log_p(1+x)) = 1+x$ als $|x|_p < p^{-1/(p-1)}$. Stel de bewering waar is voor $m-1$. Dan geldt

$$\exp_p\big((m-1)\log_p(1+x)\big) = (1+x)^{m-1}$$

$$\begin{aligned} \text{en Volgens 2. geldt } \exp_p(m \log_p(1+x)) &= \exp_p\big((m-1)\log_p(1+x)\big) \exp\log(1+x) \\ &= (1+x)^m \end{aligned}$$

□

Lemma 6. Zij $\beta \in \mathbb{Z}_p$ met $|\beta|_p = 1$ en $d = p(p-1)$. Dan

$$|\beta^d - 1|_p < p^{-1/(p-1)}.$$

Bewijs. Volgens Stelling 3 is : $(\mathbb{Z}_p/p^2\mathbb{Z}_p)^* \cong (\mathbb{Z}/p^2\mathbb{Z})^*$.

Dus het aantal elementen van $(\mathbb{Z}_p/p^2\mathbb{Z}_p)^*$ is gelijk aan het Euler-getal: $\phi(p^2) = p(p-1)$.

Maar dan is $\beta_i^{p(p-1)} \equiv 1(\mod p^2)$.

Dus $|\beta_i^d - 1|_p \leq p^{-2} < p^{-1/(p-1)}$ waarbij $d = p(p-1)$.

□

Gevolg 6. Wegens Gevolg 3 mogen we aannemen dat $|\alpha_i|_p = 1$ voor $i = 1 \ldots, r$. Dan volgt :

$$\text{er is } d > 0 \text{ met } |\alpha_i^d - 1|_p < p^{-1/(p-1)} \text{ voor alle } i = 1, \ldots, r \tag{8}$$

In de volgende Stelling bekijken we de nulpunten van een machtreeks die convergeert op een bal en bestuderen we wanneer deze eindig of oneindig veel nulpunten heeft.

Stelling 5 (Strassman) Zij $f(x) = \sum_{n=0}^{\infty} b_n x^n$ een machtreeks met $b_n \in \mathbb{Q}_p$ voor alle $n > 0$ die convergeert voor alle $x \in \mathbb{Z}_p$. Dan geldt het volgende :

- Stel $f(x)$ is niet identiek nul op $\mathbb{Z}_p$, dan heeft $f(x)$ maar eindig veel nulpunten in $\mathbb{Z}_p$

Bewijs. Definieer $S := \{x \in \mathbb{Z}_p\colon\ f(x) = 0\}$. Stel dat S oneindig is, $\mathbb{Z}_p$ is compact. Dus S heeft een ophopingspunt $y_0 \in \mathbb{Z}_p$. Dan is er een een rij $\{y_n\}_{n=0}^{\infty}$ in S met $\lim_{n\to\infty} y_n = y_0$ en met $y_n \neq y_0$ voor alle n.
Wij kunnen $f(x)$ omschrijven als :

$$\begin{aligned} f(x) &= \sum_{n=0}^{\infty} b_n \left((x - y_0) + (y_0)\right)^n \\ &= \sum_{n=0}^{\infty} b_n \left(\sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} y_0^{n-k} (x - y_0)^k \right) \\ &= \sum_{k=0}^{\infty} \left(\sum_{n=k}^{\infty} b_n \binom{n}{k} (-1)^{n-k} y_0^{n-k} \right) (x - y_0)^k, \end{aligned}$$

vanwege de onverwaardelijke convergentie van reeksen in $\mathbb{Q}_p$.

$$\text{Dus } f(x) = \sum_{k=0}^{\infty} c_k (x - y_0)^k = c_0 + c_1(x - y_0) + c_2(x - y_0)^2 + \cdots,$$

waarbij $c_k = \sum_{n=k}^{\infty} b_n \binom{n}{k} (-1)^{n-k} y_0^{n-k}$.

Omdat $f(y_0) = 0$ dan geldt $c_0 = 0$.

Zij k_0 de eerste k met $c_{k_0} \neq 0$. Dan is

$$\begin{aligned} f(x) &= c_{k_0}(x-y_0)^{k_0} + c_{k_0+1}(x-y_0)^{k_0+1} + c_{k_0+2}(x-y_0)^{k_0+2} + \cdots \\ &= (x-y_0)^{k_0}(c_{k_0} + c_{k_0+1}(x-y_0) + c_{k_0+2}(x-y_0)^2 \cdots) \\ &= (x-y_0)^{k_0} H(x) \text{ waarbij } H(x) = c_{k_0} + c_{k_0+1}(x-y_0) + \cdots \end{aligned}$$

$H(x)$ is continu in y_0 en $H(y_0) = c_0 \neq 0$. Dus er is een $\epsilon > 0$ zodat $H(x) \neq 0$ voor alle x met $|x-y_0|_p < \epsilon$. Dan volgt dat $f(x) \neq 0$ voor alle $x \in \mathbb{Z}_p$ met $|x-y_0|_p < \epsilon$ en $x \neq y_0$. Maar er is een $y_n \in S$ met $|y_n - y_0|_p < \epsilon$ en daarvoor zou dan gelden $f(y_n) \neq 0$, tegenspraak.

Dus f heeft maar eindig veel nulpunten in $\mathbb{Z}_p$. □

5 Bewijs van de Stelling van Skolem-Mahler-Lech

Nu gaan wij terug naar de Stelling 2 van Skolem-Mahler-Lech. Om die te bewijzen gebruiken de lemma's en stellingen die eerder in deze scriptie zijn behandeld.

Bewijs. Volgens Stelling 1 is $u_n = \sum_{i=1}^{r} f_i(n)\alpha_i^n$ voor alle $n \geq 0$. Wegens gevolg 3 van de Inbeddingsstelling van Lech mogen we aannemen dat α_i en de coëfficiënten van f_i $(i = 1, \ldots, r)$ tot $\mathbb{Q}_p$ behoren en dat $|\alpha_i|_p = 1$ voor $i = 1, \ldots, r$.

We schrijven $n = md + e$ waarbij d is gegeven door (8) en waarbij $e \in \{0, \ldots, d-1\}$. Dan is:

$$u_{md+e} = \sum_{i=1}^{r} g_i(m)(1+\beta_i)^m \text{ ; waarbij } g_i(m) := \sum_{i=1}^{r} f_i(md+e)\alpha_i^e, \text{ en } \alpha_i^d := 1+\beta,$$

met $|\beta_i|_p = |\alpha_i^d - 1|_p < p^{-\frac{1}{(p-1)}}$ (Gevolg 6).

Uit Lemma 6.5 en 6.6 volgt dat $\exp_p(m \log(1+\beta_i))$ goed gedefinieerd is en

$(1+\beta_i)^m = \exp_p(m \log(1+\beta_i))$ voor alle $m \in \mathbb{Z}$. Dus

$$\begin{aligned} u_{md+e} &= \sum_{i=1}^{r} g_i(m) \exp_p(m \log(1+\beta_i)) \text{ voor } m \in \mathbb{Z} \\ &= G_e(m) \text{ waarbij } G_e(x) := \sum_{i=1}^{r} g_i(x) \exp_p(x \log_p(1+\beta_i)) \text{ voor } x \in \mathbb{Z}_p \end{aligned}$$

Wij gaan nu de stelling van Strassman op de machtreeks $G_e(x)$ toepassen:

$G_e(X)$ convergeert op $\mathbb{Z}_p$. Dus er zijn twee mogelijkheden:

1. $G_e(x)$ is niet identiek nul. Dan heeft G_e hoogstens eindig veel nulpunten in $\mathbb{Z}_p$.

2. $G_e(X)$ is identiek nul. Dan is $G_e(x) = 0$ voor alle $x \in \mathbb{Z}_p$.

Definieer $N_e(U) = \{md + e : m \in \mathbb{Z}_{\geq 0}, u_{md+e} = 0\}$.

Gevolg van mogelijkheid 1:

$u_{md+e} = G_e(m) = 0$ voor hoogstens eindig veel $m \in \mathbb{Z}_{\geq 0}$. Dus $N_e(U)$ is eindig.

Gevolg van mogelijkheid 2:

$u_{md+e} = G_e(m) = 0$ voor alle $m \in \mathbb{Z}_{\geq 0}$. M.a.w.$N_e(U)$ is een rekenkundige rij.

We concluderen dat

$$N(U) = \bigcup_{e=0}^{d-1} N_e(U) \tag{9}$$

de vereniging is van een eindige verzameling met een eindig aantal rekenkundige rijen.

Dit bewijst de stelling van Skolem-Mahler-Lech.

□

LITERATUUR

[1] N.KOBLITZ, p-adic numbers,p-adic Analysis.
[2] C.LECH A note on recurring series. Arkiv för matematik Band 2 nr 22,1953,417-421.
[3] K.MAHLER, Eine arithmetische Eigenschaft der Taylor-Koeffizienten rationaler Funktionen, Akad. wetensch. Amesterdam, Proc. 38,50-60 (1935).
[4]Th. SKOLEM, Einige Sätze über gewisse Reihenentwicklungen und exponentiale Beziehungen mit Anwendung auf diophantische Gleichungen. Oslo Vid. akad. Skrifter I 1933 Nr 6.
[5]Th.Skolem, Ein verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen, C.r. 8 congr. scand. à Stockholm 1934, 163-188