over p-adische benade-ringen

OVER

P-ADISCHE

BENADERINGEN

doctoraalscriptie van
Benne de Weger
Leiden, maart 1983
o.l.v. prof. dr. R. Tijdeman.

INHOUDSOPGAVE

VOORWOORD

Met deze scriptie sluit ik mijn studietijd af. Van augustus 1976 tot en met februari 1983 heb ik mij te Leiden beziggehouden met veelerlei aktiviteiten die ik onder de term 'studeren' wil vangen. Wiskunde is er slechts één van.
Ik wil de vele mensen die bijgedragen hebben tot het succes dat mijn studie is geworden, bedanken.
Mijn vader kan ik niet meer persoonlijk bedanken. Ruim twee jaar geleden ging hij naar zijn Vader, zijn erfdeel, dat hem bekoort. Zijn steun voor mij was meer dan financieel.
Dat geldt evenzo voor mijn moeder, die ik gelukkig nog wel kan bedanken. Aan haar draag ik deze scriptie op. Dat houdt overigens niet in dat ik op me neem om uit te leggen wat er in staat.
Mijn wiskundeleraar van het gymnasium, dhr. C. Rijke, heeft me zowel de beginselen als een groot brok interesse voor zijn vak bijgebracht. Dat werk is voortgezet door de docenten van de Subfaculteit Wiskunde van de Rijksuniversiteit te Leiden, die niet schroomden om voldoendes te geven als dat nodig was.
Met name spreek ik mijn dank uit aan prof. dr. R. Tijdeman, niet alleen omdat hij me allemaal voldoendes gaf (zelfs eens een 10 terwijl ik toch slechts 27 van de 30 te behalen punten had), maar ook omdat hij me enthousiast heeft gemaakt voor de getallentheorie, niet in de laatste plaats bij het begeleiden van deze scriptie. Ook aan hem heb ik mijn

huidige werk te danken. Ik hoop de komende jaren nog veel van zijn bemoeiingen te kunnen genieten.
Van geheel andere aard is de steun die Gonarus, en vele Gonarianen, me hebben gegeven. Ik heb me er zes en een half jaar lang thuis gevoeld, al was ik doorgaans de enige wiskundige. Met name de leden van H.E.E.D.H.D. Avogadro bedank ik voor het bewonderenswaardige geduld waarmee ze mijn geklets telkens weer aanhoorden.
Tenslotte noem ik dhr. en mevr. Burger, die me zes jaar lang een kamer in hun huis hebben afgestaan, en me meer gezelligheid hebben gegeven dan uit de maandelijkse giro-overschrijvingen kan worden opgemaakt.
Dank, allemaal.

Leiden, maart 1903
Benne de Weger.

SOLI DEO GLORIA !

HOOFDSTUK 1: INLEIDING.

In de wiskunde zijn er vele nog onontgonnen gebieden. Dat is een merkwaardig verschijnsel. Het wiskunde-onderwijs op middelbare scholen, op kandidaatsniveau, en ook nogal eens op doctoraal niveau, geeft vaak de indruk dat het allemaal wel zo'n beetje is uitgezocht. De stof wordt immers veelal gebracht als een gesloten systeem van stellingen en definities, een compleet ogende theorie, terwijl de marges en de vrijheidsgraden grotendeels beperkt lijken te zijn tot de kennis van voorbeelden, toepassingen en huiswerkopgaven. Zo komt een wiskunde-student er pas na enige jaren studie achter dat er nog veel origineel werk gedaan kan worden. En we zwijgen maar over het beeld dat vele niet-wiskundigen van de activiteiten van de mathematici hebben.

Een tweede merkwaardig aspekt aan het bestaan van veel nog onuitgezochte problemen is, dat er een aantal onder zijn waarvan het niet voor de hand ligt dat er nog nauwelijks werk aan is verricht. Een voorbeeld daarvan is wellicht het probleemgebied dat in deze scriptie aan de orde wordt gesteld: de vraag naar beste benaderingen van p-adische getallen. Voor reële getallen is de beste-benaderingen-theorie een klassiek stukje getallentheorie geworden, nl. de kettingbreukentheorie, of ruimer: de

diophantische approximatie theorie. Zowel deze, als ook de p-adische theorie hebben een hoge vlucht genomen. Hun doorsnede echter, voorzover het kettingbreuken, en in het algemeen algorithmische aspecten van p-adische benaderingen betreft, is tot nu toe geen hoogvlieger gebleken. Is dat niet het merken waard, gezien de unieke positie die, naar Ostowski, de p-adische getallen innemen naast de reële?

Omdat in het reële geval beste benaderingen nauw samenhangen met kettingbreuken, is het een voor de hand liggende gedachte om p-adische kettingbreuken te gaan maken, als rationale benaderingen van p-adische getallen gewenst zijn. Zo is gedaan door K. Mahler in 1934, en Th. Schneider in 1970. Naar analogie van reële kettingbreuken zetten zij een theorietje van kettingbreuken van p-adische getallen op. De benaderingen die met deze kettingbreuken berekend kunnen worden, zijn doorgaans verre van beste benaderingen. Mahler stelde daarom in 1934 al een andere aanpak voor: probeer direkt benaderingen te vinden van een p-adisch getal; je kunt er dan naderhand wel een kettingbreuk van maken als je dat nodig vindt. Deze suggestie schijnt echter alleen verder uitgewerkt te zijn in een hoofdstuk van Mahlers boekje Lectures on Diophantine Approximations uit 1961. Op deze lijn zal in deze scriptie verder gewerkt worden.

De reden om de draad nu op te pakken waar hij ligt, is, en weer noem ik het merkwaardig, niet gelegen in een interesse voor die theorie als zodanig. De theorie zou vermoedelijk nog lang in de doofpot gebleven zijn, ware het niet dat de reële theorie van de diophantische approximatie gebaat schijnt te zijn bij p-adische argumenten. Men zie Agrawal et.al.(1980) voor een voorbeeld hiervan. Het ene probleem roept motivatie op om een aantal andere te gaan bestuderen, die dan in zichzelf ook interessant blijken te zijn. Wiskundigen kiezen voor hun onderzoek vaak geen probleem uit dat zijzelf leuk vinden, maar dat anderen leuk vinden. Dat geldt zeker voor jonge wiskundigen. Hiermee bedoel ik overigens geen tegenstelling te suggereren tussen wat ik leuk vind, en wat anderen leuk vinden : ik heb met veel plezier gewerkt aan de p-adische benaderingen.

Zo getuigt ook deze sciptie ervan dat wiskunde een vak in ontwikkeling is, waarin niet iedere beoefenaar zijn eigen gang gaat. Wellicht kan er zelfs van modes gesproken worden : de algorithmische aspecten van de getallentheorie staan de laatste tijd volop in de belangstelling. Deze sciptie is tijdgebonden. Vandaag, in maart 1983, bevat zij nieuwe resultaten. Morgen zijn ze óf bekend geworden en opgenomen in een groter geheel, óf vergeten omdat het probleem niet meer interessant geworden wordt.

Dit werkstuk bevat, naast deze inleiding, nog zeven andere hoofdstukken. In hoofdstuk 2 en 3 wordt een kort resumé gegeven van de klassieke theorieën van de reële kettingbreuken en p-adische getallen. Zonder bezwaar kan de lezer die dat allemaal weet, meteen met hoofdstuk 4 beginnen. Dat bevat een aantal fundamentele definities en observaties voor wat volgt. Hoofdstuk 5 geeft een overzicht van wat bekend is over kettingbreuken van p-adische getallen; het is historisch van aard, bevat vrijwel geen nieuwe resultaten, en kan overgeslagen worden door de lezer met haast. Hoofdstuk 6 behandelt Mahlers algorithme uit 1961, geeft er een verbetering van, en toont aan dat het een best algorithme is in deze zin dat er beste benaderingen mee gevonden worden. Hoofdstuk 7 is een intermezzo, waarin een criterium gegeven wordt voor beste benaderingen. Hoofdstuk 8 tenslotte behandelt een nieuw algorithme om beste benaderingen te vinden van p-adische getallen, m.b.v. reductie van bases van roosters in $\mathbb{Z} \times \mathbb{Z}$. Dit algorithme blijkt voor- en nadelen te hebben t.o.v. Mahlers algorithme.

HOOFDSTUK 2 : P-ADISCHE GETALLEN.

Dit hoofdstuk biedt een korte inleiding tot de theorie van de p-adische getallen. Dat is de omgeving waarin we met kettingbreuken en beste benaderingen zullen gaan werken. In dit hoofdstuk zal veel beweerd en weinig bewezen worden. Het naadje van de kous is te vinden in hoofdstuk 1 van Koblitz (1977), in hoofdstuk 1 en 2 van Mahler (1961), en in Mahler (1973).

Het lichaam van de reële getallen, $\mathbb{R}$, kan opgevat worden als de completering van $\mathbb{Q}$ ten aanzien van de Euclidische norm. Er bestaan andere normen op $\mathbb{Q}$. Die zullen tot andere completeringen leiden.

<u>definitie</u> Een <u>norm</u> $\|\cdot\|$ op een ring R is een afbeelding

$$\|\cdot\| : R \longrightarrow \mathbb{R}_{\geq 0}$$

die voldoet aan: i) $\|x\| = 0 \iff x = 0$

ii) $\|x \cdot y\| = \|x\| \cdot \|y\| \quad \forall x, y \in R$

iii) $\|x+y\| \leq \|x\| + \|y\| \quad \forall x, y \in R$.

Op $\mathbb{Q}$ zijn er in essentie drie verschillende typen normen: de triviale, de Euclidische en de p-adische normen.

De triviale norm wordt als volgt gedefinieerd:

$$\begin{cases} \|x\| = 0 & \text{als } x = 0 \\ \|x\| = 1 & \text{als } x \neq 0, x \in \mathbb{Q}. \end{cases}$$

De Euclidische norm is de bekende absolute waarde:

$$\begin{cases} \|x\| = |x| = x & \text{als } x \in \mathbb{Q}_{\geq 0} \\ \|x\| = |x| = -x & \text{als } x \in \mathbb{Q}_{< 0}. \end{cases}$$

De p-adische norm berust op de volgende definitie:

<u>definitie</u> Zij p een priemgetal, en $a, b \in \mathbb{Z} - \{0\}$.
Dan definiëren we $\text{ord}_p(a)$ als de grootste $m \in \mathbb{Z}$ zodat $p^m \mid a$, we definiëren $\text{ord}_p(\frac{a}{b})$ door $\text{ord}_p(\frac{a}{b}) = \text{ord}_p(a) - \text{ord}_p(b)$, en $\text{ord}_p(0) = \infty$. [1]

Nu is $\text{ord}_p(x)$ een geheel getal voor iedere $x \in \mathbb{Q} - \{0\}$.

<u>definitie</u> De <u>p-adische norm</u> op $\mathbb{Q}$, met p een priemgetal, wordt genoteerd als $|\cdot|_p$, en gedefinieerd door

---

[1] Om verwarring te voorkomen dient vermeld te worden dat er een andere definitie van $\text{ord}_p(a)$ in omloop is, nl. de kleinste $m \in \mathbb{Z}_{>0}$ zo dat $a^m \equiv 1 \bmod p$. Die betekenis van $\text{ord}_p(a)$ zal in deze scriptie niet gebruikt worden.

$$\begin{cases} |x|_p = \frac{1}{p^{\mathrm{ord}_p(x)}} & \text{als } x \neq 0 \\ |0|_p = 0 \end{cases}$$

Stelling 2.1 De p-adische norm is een norm op $\mathbb{Q}$. Het is zelfs een niet-Archimedische norm, d.w.z. de eis $|x+y|_p \leq |x|_p + |y|_p$ kan verscherpt worden tot $|x+y|_p \leq \max(|x|_p, |y|_p)$.

lemma 2.2. i) Als $x \neq 0$ dan $|x|_p \in \{\dots, \frac{1}{p^2}, \frac{1}{p}, 1, p, p^2, \dots\}$.
ii) Als $0 \neq x \in \mathbb{Z}$ dan $1 \leq |x| \cdot |x|_p \leq |x|$.

Het construeren van een completering van $\mathbb{Q}$ t.a.v. een zekere norm gebeurt m.b.v. Cauchy-rijen.

definitie Een rij $\{a_n\}_{n=1}^{\infty}$ in een ring R met een norm $\|\cdot\|$ heet Cauchyrij (of fundamentaalrij) t.a.v. de norm $\|\cdot\|$ als voor iedere $\varepsilon > 0$ er een $N \in \mathbb{N}$ is zodat $\|a_m - a_n\| < \varepsilon$ als $m, n > N$.

definitie Twee normen $\|\cdot\|_1$ en $\|\cdot\|_2$ op R heten equivalent als iedere Cauchyrij t.a.v. $\|\cdot\|_1$ ook een Cauchyrij is t.a.v. $\|\cdot\|_2$, en omgekeerd.

lemma 2.3 Voor niet-triviale normen $\|\cdot\|_1$, $\|\cdot\|_2$ op R geldt:

$$\begin{aligned} &\|\cdot\|_1 \text{ en } \|\cdot\|_2 \text{ zijn equivalent} \iff \\ \iff &\|x\|_1 < 1 \text{ d.e.s.d.a.v. } \|x\|_2 < 1 \iff \\ \iff &\text{er is een } \alpha \in \mathbb{R}_{>0} \text{ zodat } \|\cdot\|_1 = \|\cdot\|_2^{\alpha}. \end{aligned}$$

Het belang van p-adische normen wordt aangegeven door de volgende stelling.

Stelling 2.4. (Ostrowski) Iedere norm op $\mathbb{Q}$ is equivalent met de triviale, de Euclidische, of één van de p-adische normen.

Zij K de verzameling van alle Cauchyrijen t.a.v. een zekere norm $\|\cdot\|$ op $\mathbb{Q}$. We noemen twee rijen $\{a_n\}$ en $\{b_n\}$ equivalent als $\lim_{n\to\infty} \|a_n - b_n\| = 0$. We kunnen nu spreken over equivalentieklassen van Cauchyrijen.

Zij K^* de verzameling van equivalentieklassen van Cauchyrijen. Op K^* kan dan een norm gedefinieerd worden:

$$\|\overline{\{a_n\}}\|^* = \lim_{n\to\infty} \|a_n\|.$$

Iedere Cauchyrij van elementen uit K^* heeft zijn limiet nu in K^* zelf. Dit bedoelen we als we zeggen dat K^* compleet is t.a.v. de erop gedefinieerde norm, in dit geval $\|\cdot\|^*$.

Er kan bewezen worden dat K^* een lichaam is.

Het is niet moeilijk in te zien dat equivalente normen tot dezelfde completering leiden. De stelling van Ostrowski toont dan aan dat $\mathbb{Q}$ slechts drie typen completeringen kent:

Ten aanzien van de triviale norm is $\mathbb{Q}$ z'n eigen completering.
Ten aanzien van de Euclidische norm is $\mathbb{R}$ de completering van $\mathbb{Q}$.
Voor ieder priemgetal p is er dan nog de completering t.a.v. de p-adische norm:

<u>definitie</u> Het <u>lichaam van de p-adische getallen $\mathbb{Q}_p$</u> is de completering van $\mathbb{Q}$ t.a.v. de p-adische norm.

In de rest van dit hoofdstuk zullen we $\mathbb{Q}_p$ bestuderen, met p een vast, maar willekeurig priemgetal.

Er geldt $\mathbb{Q} \subset \mathbb{Q}_p$ in de volgende zin: we identificeren $x \in \mathbb{Q}$ met de klasse van de Cauchyrij waarvan alle termen gelijk zijn aan x.
De p-adische norm, die we alleen op $\mathbb{Q}$ gedefinieerd hebben, kan uitgebreid worden tot $\mathbb{Q}_p$:

<u>definitie</u> Zij $a \in \mathbb{Q}_p$, en $\{a_n\}$ een representant van a, dan: $|a|_p = \lim_{n\to\infty} |a_n|_p$.

Deze limiet bestaat, want $|a_n - a_m|_p \geq \big||a_n|_p - |a_m|_p\big|$, dus $\{|a_n|_p\}$ is een Cauchyrij in $\mathbb{R}$, en heeft daar dus een limiet.

$\mathbb{Q}_p$ is een lichaam, <u>met de 'gewone' optelling en vermenigvuldiging</u>: $\overline{\{a_n\}} + \overline{\{b_n\}} = \overline{\{a_n + b_n\}}$ en $\overline{\{a_n\}} \cdot \overline{\{b_n\}} = \overline{\{a_n b_n\}}$.

De volgende stelling maakt de p-adische getallen grijpbaar:

Stelling 2.5. Iedere $0 \neq a \in \mathbb{Q}_p$ is eéndudig te schrijven

$$\text{als} \quad a = \sum_{i=k}^{\infty} a_i p^i$$

met $a_i \in \{0, 1, \ldots, p-1\}$, en $k \in \mathbb{Z}$, en $a_k \neq 0$

Deze schrijfwijze noemen we de p-adische ontwikkeling van a.

definitie We noemen $\text{ord}_p(a)$ de kleinste $m \in \mathbb{Z}$ zodat $a_m \neq 0$; of wel $\text{ord}_p(a) = k$, met a_m en k als in stelling 2.5.

Deze definitie van $\text{ord}_p(a)$ met $a \in \mathbb{Q}_p$ komt overeen met de eerder gegeven definitie van $\text{ord}_p(a)$ met $a \in \mathbb{Q}$.
Ook voor $a \in \mathbb{Q}_p$, $a \neq 0$, geldt $|a|_p = \frac{1}{p^{\text{ord}_p(a)}}$.

definitie We noemen $a \in \mathbb{Q}_p$ p-adisch geheel als $|a|_p \leq 1$.

Van positieve gehele getallen is de p-adische ontwikkeling makkelijk te vinden: het is analoog aan het vinden van de decimale ontwikkeling, maar dan niet met grondtal 10, maar met grondtal p. Bijvoorbeeld: de 5-adische ontwikkeling van 328 is $3 + 0 \cdot 5 + 3 \cdot 5^2 + 2 \cdot 5^3$. De ontwikkeling is eindig, d.w.z. er is een $N \in \mathbb{N}$ zodat $a_n = 0$ voor alle $n \geq N$.

We zouden 328 nu kunnen noteren als 2303 (5-adisch). Het is echter gebruikelijk om de notatie $3+0\cdot 5+3\cdot 5^2+2\cdot 5^3$ te handhaven, in de eerste plaats omdat zo de precieze betekenis beter aan het licht komt, in de tweede plaats omdat op deze manier meer naar rechts staande termen p-adisch 'kleiner' zijn dan meer naar links staande, analoog aan de decimale schrijfwijze van reële getallen.

Er is een simpel algorithme om van een gegeven $a \in \mathbb{Q}$ de p-adische ontwikkeling te berekenen.

Algorithme 2.6.

i) bereken $k = \mathrm{ord}_p(a)$
bereken $x_k, q \in \mathbb{Z}$ zodat $a = \frac{x_k}{q} \cdot p^k$, $p \nmid q$ en $\mathrm{ggd}(x_k, q) = 1$.
bereken $q^{-1} \in \{1, 2, \dots, p-1\}$ zodat $q \cdot q^{-1} \equiv 1 \bmod p$
zet $i = k$

ii) bereken $a_i \equiv x_i \cdot q^{-1} \bmod p$ met $0 \leq a_i \leq p-1$
bereken $x_{i+1} = \frac{x_i - a_i q}{p}$

iii) zet $i = i+1$
als $x_i \neq 0$, ga dan naar ii)
anders stop.

Voorbeelden: 1) $a = 328 \in \mathbb{Q}_5$: $k = 0$, $x_0 = 328$, $q = 1$, $q^{-1} = 1$,

i	x_i	a_i
0	328	3
1	65	0
2	13	3
3	2	2
4	0	-

$328 = 3 + 0\cdot 5 + 3\cdot 5^2 + 2\cdot 5^3$.

2) $a = \frac{2}{3} \in \mathbb{Q}_5$: $k=0$, $x_0 = 2$, $q = 3$, $q^{-1} = 2$,

i	x_i	a_i
0	2	4
1	-2	1
2	-1	3
3	-2	1
4	-1	3
⋮	⋮	⋮

$\frac{2}{3} = 4 + 1\cdot 5 + 3\cdot 5^2 + 1\cdot 5^3 + \cdots$

3) $a = -1 \in \mathbb{Q}_5$: $k=0$, $x_0 = -1$, $q = 1$, $q^{-1} = 1$,

i	x_i	a_i
0	-1	4
1	-1	4
2	-1	4
⋮	⋮	⋮

$-1 = 4 + 4\cdot 5 + 4\cdot 5^2 + 4\cdot 5^3 + \cdots$

Merk op dat de uitdrukking $-1 = 4 + 4\cdot 5 + 4\cdot 5^2 + 4\cdot 5^3 + \cdots$ wonderwel overeenkomt met de bekende formule voor meetkundige reeksen $\frac{a}{1-r} = a + ar + ar^2 + ar^3 + \cdots$.
Bij nader inzien is het niet zo wonderlijk: met p-adische getallen kan net zo worden gerekend als we gewend zijn met decimale getallen: $\sum_{i=k}^{\infty} a_i p^i + \sum_{j=k}^{\infty} b_j p^j = \sum_{i=k}^{\infty} (a_i + b_i) p^i$,

en $\left(\sum_{i=k}^{\infty} a_i p^i\right) \cdot \left(\sum_{j=\ell}^{\infty} b_j p^j\right) = a_k b_\ell p^{k+\ell} + (a_k b_{\ell+1} + a_{k+1} b_\ell) p^{k+\ell+1} + \cdots$.

Natuurlijk kunnen de coëfficiënten groter dan $p-1$ worden, de zo ontstane 'overflow' kan simpel weggewerkt worden:
bv. in $\mathbb{Q}_5$ hebben we $(3 + 0\cdot 5 + 2\cdot 5^2 + 3\cdot 5^3) + (3 + 2\cdot 5) =$

$= 6 + 2\cdot 5 + 2\cdot 5^2 + 3\cdot 5^3 =$

$= \underbrace{1 + 1\cdot 5}_{6} + \underbrace{2\cdot 5}_{2\cdot 5} + 2\cdot 5^2 + 3\cdot 5^3 =$

$= 1 + 3\cdot 5 + 2\cdot 5^2 + 3\cdot 5^3$.

Er geldt voor $a \in \mathbb{Q}_p$:

<u>Stelling 2.7.</u> $a \in \mathbb{Q} \Leftrightarrow$ a heeft een periodieke (of eindige) p-adische ontwikkeling.

Soms kan in $\mathbb{Q}_p$ wortel getrokken worden, zoals blijkt uit de volgende voorbeelden:

1) $\sqrt{2}$ in $\mathbb{Q}_7$: stel $\sqrt{2} = a_0 + a_1 \cdot 7 + a_2 \cdot 7^2 + \cdots$, dan:
$a_0^2 \equiv 2 \bmod 7$, $\Rightarrow a_0 = 3$ of $a_0 = 4$ voldoen. Kies $a_0 = 3$.
Verder: $(3 + a_1 \cdot 7)^2 = 9 + 42 a_1 + 49 a_1^2 \equiv 2 \bmod 49 \Rightarrow a_1 = 1$
en: $(3 + 1 \cdot 7 + a_2 \cdot 7^2)^2 = 100 + 200 \cdot 7 \cdot a_2 + 7^4 a_2^2 \equiv 2 \bmod 7^3 \Rightarrow a_2 = 2$
etc.

2) $\sqrt{-1}$ in $\mathbb{Q}_5$: stel $\sqrt{-1} = a_0 + a_1 \cdot 5 + a_2 \cdot 5^2 + \cdots$, dan:
$a_0^2 \equiv -1 \bmod 5$, kies $a_0 = 2$
$(2 + a_1 \cdot 5)^2 \equiv -1 \bmod 5^2 \Rightarrow a_1 = 1$
$(2 + 1 \cdot 5 + a_2 \cdot 5^2)^2 \equiv -1 \bmod 5^3 \Rightarrow a_2 = 2$
enz.

3) $\sqrt{2}$ in $\mathbb{Q}_5$: stel $\sqrt{2} = a_0 + a_1 \cdot 5 + a_2 \cdot 5^2 + \cdots$ dan:
$a_0^2 \equiv 2 \bmod 5$ is onoplosbaar. Blijkbaar bestaat $\sqrt{2}$ niet in $\mathbb{Q}_5$.

We zullen ons in het vervolg p-adische getallen alleen voorstellen door hun p-adische ontwikkeling.

HOOFDSTUK 3 : REËLE KETTINGBREUKEN.

De klassieke methode waarmee men reële getallen benadert met rationale getallen maakt gebruik van kettingbreuken. In dit hoofdstuk wordt een korte samenvatting gegeven van de voor ons belangrijke delen van de kettingbreukentheorie. We verkrijgen zo vergelijkingsmateriaal voor de later te behandelen p-adische kettingbreuken.

De bewijzen die hier achterwege gelaten zijn, zijn te vinden in hoofdstuk 10 van Hardy en Wright (1938), en in hoofdstuk 1 en 2 van Perron (1913).

Een kettingbreuk is een uitdrukking van de vorm

$$b_0 + \cfrac{a_1}{b_1 + \cfrac{a_2}{b_2 + \cfrac{a_3}{b_3 + \cdots}}}$$

al of niet oneindig lang, en doorgaans met $a_i, b_i \in \mathbb{R}$. Een handige notatie voor deze kettingbreuk is

$$b_0 + \frac{a_1|}{|b_1} + \frac{a_2|}{|b_2} + \frac{a_3|}{|b_3} + \cdots$$

Van groot belang zijn kettingbreuken met $a_i = 1$ voor $i = 1, 2, 3, \cdots$; $b_i \in \mathbb{Z}$ voor $i = 0, 1, 2, 3, \cdots$ en $b_i > 0$ voor $i = 1, 2, 3, \cdots$.
Zulke kettingbreuken noemen we simpel, en we noteren ze als $[b_0, b_1, b_2, b_3, \cdots]$.

Een reëel getal x kan ontwikkeld worden in een simpele kettingbreuk, met behulp van het volgende algorithme.

Algorithme 3.1.
i) zet $x_0 = x$ en $i = 0$
ii) bereken $a_i = [x_i]$
als $a_i \neq x_i$, bereken dan $x_{i+1} = \frac{1}{x_i - a_i}$
als $a_i = x_i$ dan stop.
iii) zet $i = i + 1$ en ga naar ii).

Stelling 3.2. Zij $x \in \mathbb{R}$, en $a_i, x_i (i = 0, 1, 2, \cdots)$ verkregen uit algorithme 3.1. Dan geldt:
$x = [a_0, a_1, a_2, \cdots, a_{n-1}, x_n]$ voor ieder $n = 1, 2, 3, \cdots$
en $x = [a_0, a_1, a_2, \cdots]$ is een simpele kettingbreuk.

Stelling 3.3. $x \in \mathbb{Q} \Leftrightarrow x$ heeft een eindige kettingbreuk-ontwikkeling.

Stelling 3.4. i) Er is een één-één-duidig verband tussen rationale getallen en simpele eindige kettingbreuken $[a_0, a_1, \cdots, a_n]$ met $a_n \neq 1$.
ii) Er is een één-een-duidig verband tussen reële, niet-rationale getallen en simpele oneindige kettingbreuken.

definitie De getallen $a_0, a_1, a_2, \cdots$ heten **wijergetallen** van x. (Ze zijn alle geheel, en alle (behalve evt. a_0) positief).
De getallen $[a_0], [a_0, a_1], \cdots, [a_0, a_1, \cdots, a_n], \cdots$ heten **convergenten** van x. (Allen zijn ze rationaal).

We definieren, zolang dat zinvol is, voor $k = 0, 1, 2, \cdots$

$$\begin{cases} P_{-2} = 0 \\ q_{-2} = 1 \end{cases}, \quad \begin{cases} P_{-1} = 1 \\ q_{-1} = 0 \end{cases}, \quad \begin{cases} P_k = a_k P_{k-1} + P_{k-2} \\ q_k = a_k q_{k-1} + q_{k-2} \end{cases}.$$

Stelling 3.5. Voor $0 \neq y \in \mathbb{R}$ geldt

$$[a_0, a_1, \cdots, a_{n-1}, y] = \frac{y P_{n-1} + P_{n-2}}{y q_{n-1} + q_{n-2}}$$

Van deze stelling geven we bij uitzondering het bewijs:

bewijs: m.b.v. inductie naar n.

$n = 1$: $[a_0, y] = a_0 + \frac{1}{y}$, en $\frac{y \cdot P_0 + P_{-1}}{y \cdot q_0 + q_{-1}} = \frac{y a_0 + 1}{y \cdot 1 + 0}$, klopt.

$n > 1$: veronderstel $[a_0, a_1, \cdots, a_{n-2}, y'] = \frac{y' P_{n-2} + P_{n-3}}{y' q_{n-2} + q_{n-3}}$ voor alle $0 \neq y' \in \mathbb{R}$.

Welnu, $[a_0, a_1, \cdots, a_{n-1}, y] = [a_0, a_1, \cdots, a_{n-2}, a_{n-1} + \frac{1}{y}] =$

$$= \frac{a_{n-1} P_{n-2} + \frac{1}{y} P_{n-2} + P_{n-3}}{a_{n-1} q_{n-2} + \frac{1}{y} q_{n-2} + q_{n-3}} = \frac{y P_{n-1} + P_{n-2}}{y q_{n-1} + q_{n-2}} \quad \text{qed.}$$

Gevolg 3.6. (i) $\alpha - \frac{P_n}{q_n} = \frac{(-1)^n}{q_n (\alpha_{n+1} q_n + q_{n-1})}$

(ii) $\frac{p_n}{q_n} = [a_0, a_1, \cdots, a_n]$, m.a.w. $\frac{p_n}{q_n}$ is de n-e convergent van x.

lemma 3.7. (i) $p_n q_{n-1} - p_{n-1} q_n = (-1)^{n+1}$ $(n = -1, 0, 1, 2, \cdots)$

(ii) $p_n q_{n-2} - p_{n-2} q_n = (-1)^n a_n$ $(n = 0, 1, 2, \cdots)$

(iii) $ggd(p_n, q_n) = 1$ $(n = 0, 1, 2, \cdots)$

(iv) $\frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \cdots \leq x \leq \cdots < \frac{p_5}{q_5} < \frac{p_3}{q_3} < \frac{p_1}{q_1}$.

(v) $1 = q_0 < q_1 < q_2 < q_3 < \cdots$

(vi) $|q_0\alpha - p_0| > |q_1\alpha - p_1| > |q_2\alpha - p_2| > \cdots$

Stelling 3.8 $\lim_{n\to\infty} \frac{p_n}{q_n}$ bestaat, en is gelijk aan x,

en $|x - \frac{p_n}{q_n}| \leq \frac{1}{q_n q_{n+1}} < \frac{1}{q_n^2}$

Het belang van het kettingbreukalgorithme 3.1. is erin gelegen dat de convergenten van x, die ermee berekend kunnen worden, altijd beste benaderingsbreuken zijn.

definitie Zij $x \in \mathbb{R}$. We noemen $\frac{p}{q} \neq x$ een beste benaderingsbreuk (beste benadering, bbb) van x als voor alle breuken $\frac{r}{s} \neq \frac{p}{q}$ met $0 < s \leq q$ geldt: $|qx - p| < |sx - r|$.

Met andere woorden: $\frac{p}{q}$ is een beste benadering van x, als alle breuken, die x beter benaderen, een grotere noemer hebben dan $\frac{p}{q}$ heeft.

Stelling 3.9. Zij $x \in \mathbb{R}, x \notin \mathbb{Q}$. Dan geldt:
$\frac{p}{q}$ is bbb van $x \Leftrightarrow \frac{p}{q}$ is convergent van x.

Stelling 3.10. Zij $x \in \mathbb{R}$, en $\frac{p}{q} \in \mathbb{Q}$. Dan geldt:
als $|x - \frac{p}{q}| < \frac{1}{2q^2}$ dan is $\frac{p}{q}$ convergent van x.

Stelling 3.11. De kettingbreukontwikkeling van x is periodiek
$\Leftrightarrow$ x is kwadratisch irrationaal.

HOOFDSTUK 4: P-ADISCHE BENADERINGEN.

Reele getallen kunnen we benaderen door rationale getallen omdat $\mathbb{R}$ een completering is van $\mathbb{Q}$. Begrippen als 'benaderen', 'dicht bij' vooronderstellen een bepaalde norm; in het geval dat we $\mathbb{R}$ bekijken, is dat de euclidische norm.

Een begrip als 'dichtbij' kunnen we ook opvatten in p-adische zin. Twee p-adische getallen liggen dicht bij elkaar als de p-adische norm van hun verschil klein is. Bijvoorbeeld, $\frac{1}{3}$ en 4167 liggen 5-adisch dicht bij elkaar, immers

$\frac{1}{3} = 2 + 3\cdot 5 + 1\cdot 5^2 + 3\cdot 5^3 + 1\cdot 5^4 + 3\cdot 5^5 + 1\cdot 5^6 + \cdots$

$4167 = 2 + 3\cdot 5 + 1\cdot 5^2 + 3\cdot 5^3 + 1\cdot 5^4 + 1\cdot 5^5$

dus $\frac{1}{3} - 4167 = 2\cdot 5^5 + 1\cdot 5^6 + \cdots$ en $\left|\frac{1}{3} - 4167\right|_5 = \frac{1}{3125}$.

We kunnen p-adische getallen, zowel rationale als niet-rationale, benaderen met rationale getallen. Precies geformuleerd:

<u>definitie</u> We noemen het paar $(P, Q) \in \mathbb{Z}\times\mathbb{Z}$ een <u>m-e orde (p-adische) benadering</u> van het p-adische getal α, als $|Q\alpha - P|_p = p^{-m}$

Bijvoorbeeld, $(1, 3)$ is een 5-e orde benadering van het 5-adische getal 4167; $(-38, 41)$ is een 5-e orde benadering van $\sqrt{-1} = 2 + 1\cdot 5 + 2\cdot 5^2 + 1\cdot 5^3 + 3\cdot 5^4 + 4\cdot 5^5 + \cdots \in \mathbb{Q}_5$.

We hadden, net als in het reële geval, ook benaderingsbreuken P/Q kunnen definiëren, daarbij $\frac{P}{Q}$ en $\frac{P/d}{Q/d}$ identificerend, met $d = \text{ggd}(P,Q)$.
We doen dat niet, omdat we bijvoorbeeld de 5-adische getallenparen $(5,10)$ en $(1,2)$ niet willen identificeren, terwijl de bijbehorende breuken $\frac{5}{10}$ en $\frac{1}{2}$ wel gelijk zijn. Immers, $|10\alpha - 5|_5$ en $|2\alpha - 1|_5$ zijn niet gelijk.
Als de grootste gemene deler d van P en Q geen factor van p bevat, kunnen we eventueel (P,Q) en $(P/d, Q/d)$ wel identificeren.

We gaan in deze scriptie op zoek naar methoden om goede benaderingen te vinden voor in principe ieder willekeurig p-adisch getal.

De p-adische ontwikkeling, zoals we die met algoritme 2.6. kunnen berekenen, geeft direkt aanleiding tot zo'n methode. Als $\alpha \in \mathbb{Q}_p$ de p-adische ontwikkeling
$\alpha = a_k p^k + a_{k+1} p^{k+1} + a_{k+2} p^{k+2} + \cdots$, $0 \le a_i \le p-1$
heeft, dan kunnen we de "m-e afkapping" definiëren door $\alpha_m = a_k p^k + a_{k+1} p^{k+1} + \cdots + a_{m-1} p^{m-1}$, voor iedere $m \in \mathbb{Z}$ (als $m < k$, dan $\alpha_m = 0$).
Bijvoorbeeld, $\alpha = \sqrt{-1} \in \mathbb{Q}_5$ leidt tot:

m	0	1	2	3	4	5
a_m	2	1	2	1	3	4
α_m	2	7	57	182	2057	14557

We kunnen nu $(P, Q) = (\alpha_m, 1)$ opvatten als benadering van α. Er geldt: $Q\alpha - P = \alpha - \alpha_m = a_m p^m + a_{m+1} p^{m+1} + \cdots$, dus $|Q\alpha - P|_p \leq p^{-m}$.

Van de twee 5-e orde benaderingen $(-30, 41)$ en $(14557, 1)$ van $\sqrt{-1}$ geven we de voorkeur echter aan de eerste. Hij lijkt immers veel kleiner. Deze voorkeur wordt precies gemaakt in de verderop te geven definitie van beste benaderingen.

Uit het reële geval herinneren we ons dat we een benadering van een getal α niet alleen meten aan hoe dicht hij α benadert; ook de noemer van de benaderingsbreuk is van belang.
Zo zullen we in de definitie van p-adische beste benaderingen ook de benadering zelf willen meten, m.b.v. een zekere norm.

<u>definitie</u> Op $\mathbb{R} \times \mathbb{R}$ definiëren we een <u>convexe norm</u> als een functie $\Phi(X, Y) : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}_{\geq 0}$ die voldoet aan:

1. $\Phi(0, 0) = 0$; $\Phi(X, Y) > 0$ als $(X, Y) \neq (0, 0)$
2. $\Phi(tX, tY) = |t| \, \Phi(X, Y)$ voor alle $t \in \mathbb{R}$
3. $\Phi(X_1 + X_2, Y_1 + Y_2) \leq \Phi(X_1, Y_1) + \Phi(X_2, Y_2)$
4. Het gebied $\{(X, Y) \in \mathbb{R} \times \mathbb{R} : \Phi(X, Y) \leq 1\}$ is convex.

Opmerking: 4. volgt uit 1., 2., 3.

Voorbeelden: $\Phi(X, Y) = \max(|X|, |Y|)$ ('vierkante norm')
$\Phi(X, Y) = \sqrt{X^2 + Y^2}$ ('Euclidische norm')

We zullen convexe normen op $\mathbb{Z} \times \mathbb{Z}$ beschouwen.

Nu kunnen we beste benaderingen definiëren voor p-adische getallen, t.a.v. een convexe norm $\Phi : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}_{\geq 0}$.

<u>definitie</u> We noemen $(P, Q) \in \mathbb{Z} \times \mathbb{Z}$ een <u>beste benadering</u> van $\alpha \in \mathbb{Q}_p$ t.a.v. de convexe norm Φ, als geldt:

(1. de g.g.d. van P en Q is een macht van p.)

2. voor alle $(P', Q') \in \mathbb{Z} \times \mathbb{Z}$ met $(P', Q') \neq (0,0)$ en $\Phi(P', Q') < \Phi(P, Q)$ geldt : $|Q'\alpha - P'|_p > |Q\alpha - P|_p$.

3. voor alle $(P', Q') \in \mathbb{Z} \times \mathbb{Z}$ met $(P', Q') \neq (0,0)$ en $\Phi(P', Q') = \Phi(P, Q)$ geldt : $|Q'\alpha - P'|_p \geq |Q\alpha - P|_p$.

Opmerking : eis 1. kan weggelaten worden.
De analogie met reële beste benaderingen is duidelijk.

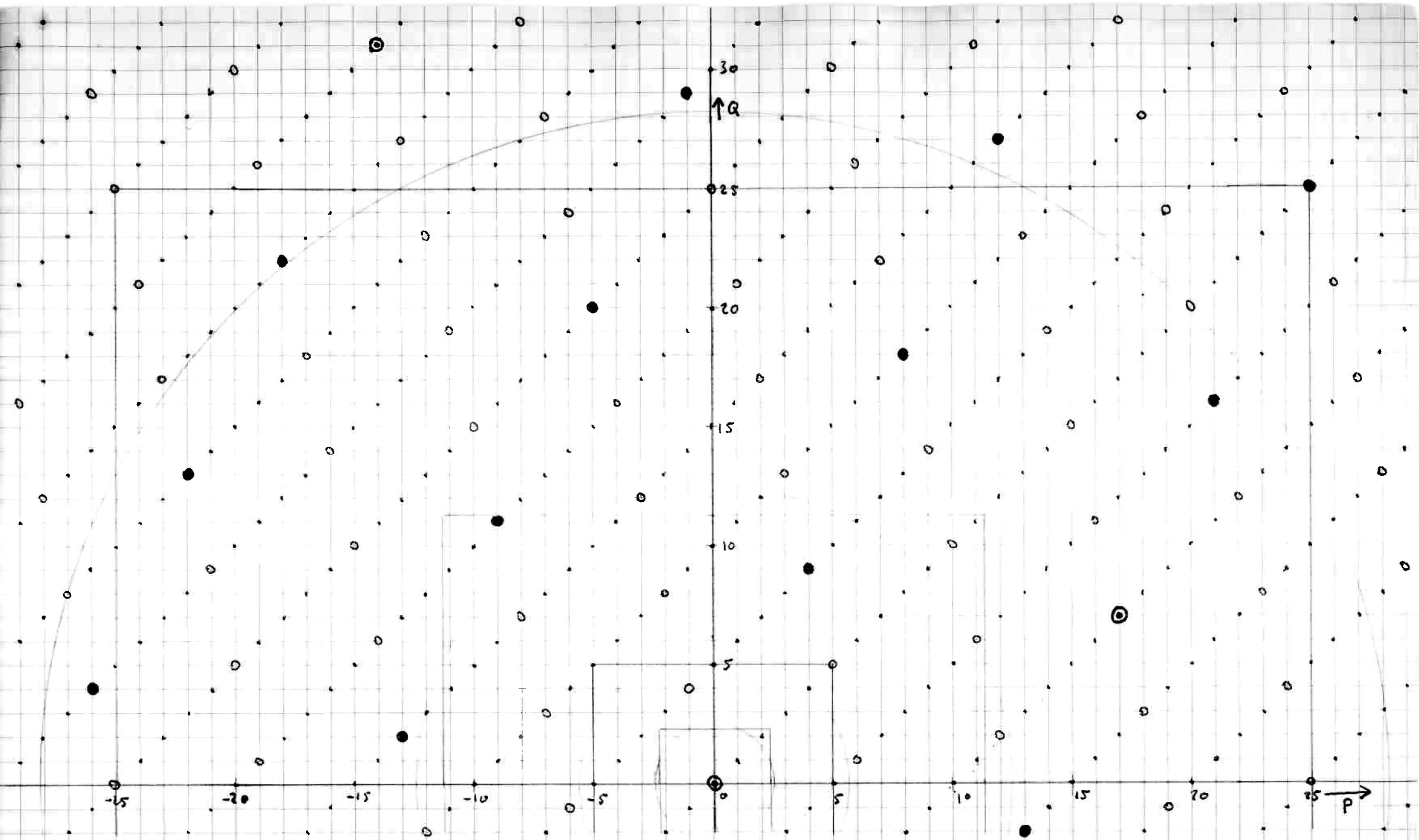
Ons doel is om van een gegeven p-adisch getal een beste benadering van orde n te vinden. Naar analogie van het reële geval ligt het voor de hand kettingbreuken van p-adische getallen te gaan bestuderen. In de schaarse literatuur over dit onderwerp zijn drie algoritmen te vinden, twee van K. Mahler uit 1934, en één van Th. Schneider uit 1970, die een p-adisch getal in een kettingbreuk ontwikkelen. In 1961 stelde Mahler een algoritme voor dat m.b.v. reele kettingbreuken van afkappingen p-adische getallen benadert. Deze 4 algoritmen zijn onderwerp van studie in de komende hoofdstukken.
Vervolgens presenteer ik een nieuw algoritme, gebaseerd op roosters in $\mathbb{Z} \times \mathbb{Z}$. De idee achter dit algoritme werd mij aan de hand gedaan door prof. Tijdeman.

Omdat de roosterstruktuur, die we aan p-adische benaderingen kunnen toekennen, verhelderend is, zullen we er nu kort op ingaan, zonder aan algorithmes te denken.
Kies een priemgetal p, een $\alpha \in \mathbb{Q}_p$, en een $m \in \mathbb{Z}$. We bestuderen alleen gehele α, dus $|\alpha|_p \leq 1$, en $\alpha \neq 0$. Voorts $m \geq 0$.
Zij $\Gamma_m = \{(P,Q) \in \mathbb{Z} \times \mathbb{Z} : |Q\alpha - P|_p \leq p^{-m}\}$ de verzameling van alle m-e en hogere-orde benaderingen van α.

<u>lemma 4.1.</u> Γ_m is een rooster in $\mathbb{Z} \times \mathbb{Z}$.

bewijs: We moeten aantonen dat Γ_m een additieve ondergroep van $\mathbb{Z} \times \mathbb{Z}$ is, van rang 2.
Als (P_1, Q_1) en (P_2, Q_2) in Γ_m liggen, dan zijn er R_1 en R_2 in $\mathbb{Z}$ zodat $Q_i\alpha - P_i = R_i p^m \ (i = 1,2)$.
Er geldt $(P_1, Q_1) + (P_2, Q_2) = (P_1 + P_2, Q_1 + Q_2)$, en $(Q_1 + Q_2)\alpha - (P_1 + P_2) = Q_1\alpha - P_1 + Q_2\alpha - P_2 = (R_1 + R_2)p^m$, en er volgt $|(Q_1+Q_2)\alpha - (P_1+P_2)|_p \leq p^{-m}$. Het is verder triviaal te verifiëren dat Γ_m een additieve groep is.
De rang van Γ_m is 2, omdat er twee onafhankelijke elementen te vinden zijn in Γ_m, bijvoorbeeld $(p^m, 0)$ en $(\alpha_m, 1)$, met α_m de 'm-e afkapping' van α. qed.

Merk op:
1. Als α geheel, dan is $\Gamma_0 = \mathbb{Z} \times \mathbb{Z}$.
2. $|Q\alpha - P|_p \leq p^{-m} \Leftrightarrow |Q\alpha_k - P|_p \leq p^{-m} \quad \forall\, k \geq m$
   m.a.w. het 'staartstuk' van α is niet interessant.
3. Γ_m hangt niet alleen af van m, ook van α en p.
4. Voor alle $m \in \mathbb{Z}$ geldt $\Gamma_{m+1} \subset \Gamma_m$.



Figuur 4.1.: Γ_m voor $\alpha = 181 \in Q_5$ en $m = 1$: ·
$m = 2$: o
$m = 3$: ●
$m = 4$: ⊙

Voorbeeld: De roosters Γ_m voor $m = 1, 2, 3, 4$ van $\alpha = 18/1 \in Q_5$ zijn weergegeven in figuur 4.1.

Met behulp van de roosterstelling van Minkowski kunnen we een bovengrens vinden (t.a.v. een norm Φ) voor de beste benaderingen van α. We moeten dan het volume van een fundamentaalgebied van Γ_m weten, en dat leidt ons tot de bestudering van bases van Γ_m.

Stelling 4.2. Een stelsel punten $\{(P, Q); (P', Q')\} \subset \Gamma_m$ is een basis van $\Gamma_m \Leftrightarrow \begin{vmatrix} P & Q \\ P' & Q' \end{vmatrix} = \pm p^m$.

bewijs: We beschouwen bij ieder tweetal punten (X, Y) en (Z, U) in Γ_m de determinant $\begin{vmatrix} X & Y \\ Z & U \end{vmatrix}$.

1. Alle bases van Γ_m hebben dezelfde determinant, op het teken na. Immers, voor twee bases $\{(X,Y); (Z,U)\}$ en $\{(X',Y'); (Z',U')\}$ geldt dat er $a, b, c, d \in \mathbb{Z}$ zijn

$$\text{met } \begin{pmatrix} X & Y \\ Z & U \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} X' & Y' \\ Z' & U' \end{pmatrix}, \text{ en } \begin{vmatrix} a & b \\ c & d \end{vmatrix} = \pm 1.$$

We noemen Δ de absolute waarde van de determinant van een basis van Γ_m.

2. Ieder tweetal punten in Γ_m met determinant $\pm\Delta$ is een basis van Γ_m. Immers, zij $\{(X',Y'); (Z',U')\}$ een basis van Γ_m, en $(X,Y), (Z,U)$ twee punten met $\begin{vmatrix} X & Y \\ Z & U \end{vmatrix} = \pm\Delta$. Er zijn $a, b, c, d \in \mathbb{Z}$ zodat

$$\begin{pmatrix} X & Y \\ Z & U \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} X' & Y' \\ Z' & U' \end{pmatrix}.$$ Neem determinanten,

er volgt dan $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = \pm 1$. Uit de identiteit $\begin{pmatrix} X' & Y' \\ Z' & U' \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}\begin{pmatrix} X & Y \\ Z & U \end{pmatrix}$ volgt dat iedere lineaire combinatie van (X', Y') en (Z', U') ook te schrijven is als lineaire combinatie van (X, Y) en (Z, U).

3. Voor ieder tweetal punten (X, Y) en (Z, U) in Γ_m geldt: $\Delta \mid \begin{vmatrix} X & Y \\ Z & U \end{vmatrix}$.

Namelijk, zij $\{(X', Y'); (Z', U')\}$ basis van Γ_m, dan zijn er $a, b, c, d \in \mathbb{Z}$ zodat $\begin{pmatrix} X & Y \\ Z & U \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} X' & Y' \\ Z' & U' \end{pmatrix}$.

Neem nu determinanten.

4. Voor ieder tweetal punten (X, Y) en (Z, U) in Γ_m geldt: $p^m \mid \begin{vmatrix} X & Y \\ Z & U \end{vmatrix}$.

Namelijk, zij $V, W \in \mathbb{Z}$ zo dat $\begin{cases} Y\alpha_m - X = V p^m \\ U\alpha_m - Z = W p^m \end{cases}$,

dan: $\begin{vmatrix} X & Y \\ Z & U \end{vmatrix} = XU - YZ = U(Y\alpha_m - Vp^m) - Y(U\alpha_m - Wp^m)$
$= p^m(WY - VU)$.

5. Er is in Γ_m een tweetal punten met determinant p^m, nl. $(-\alpha_m, 1)$ en $(p^m, 0)$.

6. Uit 4. volgt: $p^m \mid \Delta$; uit 3. en 5. volgt: $\Delta \mid p^m$, dus $\Delta = \pm p^m$. Uit 1. en 2. volgt nu de stelling. qed.

Gevolg: Het volume van een fundamentaalgebied van Γ_m is p^m.

Verschillende normen zullen vaak tot dezelfde beste benadering van gegeven $\alpha \in Q_p$ leiden, maar niet altijd, zo toont het volgende voorbeeld aan.

Voorbeeld : $\alpha = 22 \in Q_7$, $m = 3$. Zie fig. 4.2.

(P, Q)	$\max(\lvert P\rvert, \lvert Q\rvert)$	$\sqrt{P^2 + Q^2}$	$\lvert P\rvert + \lvert Q\rvert$
$(-13, 15)$	15 *	19,85	28
$(9, 16)$	16	18,36 *	25
$(22, 1)$	22	22,02	22 *

* betekent : t.a.v. deze norm is (P, Q) een beste benadering.

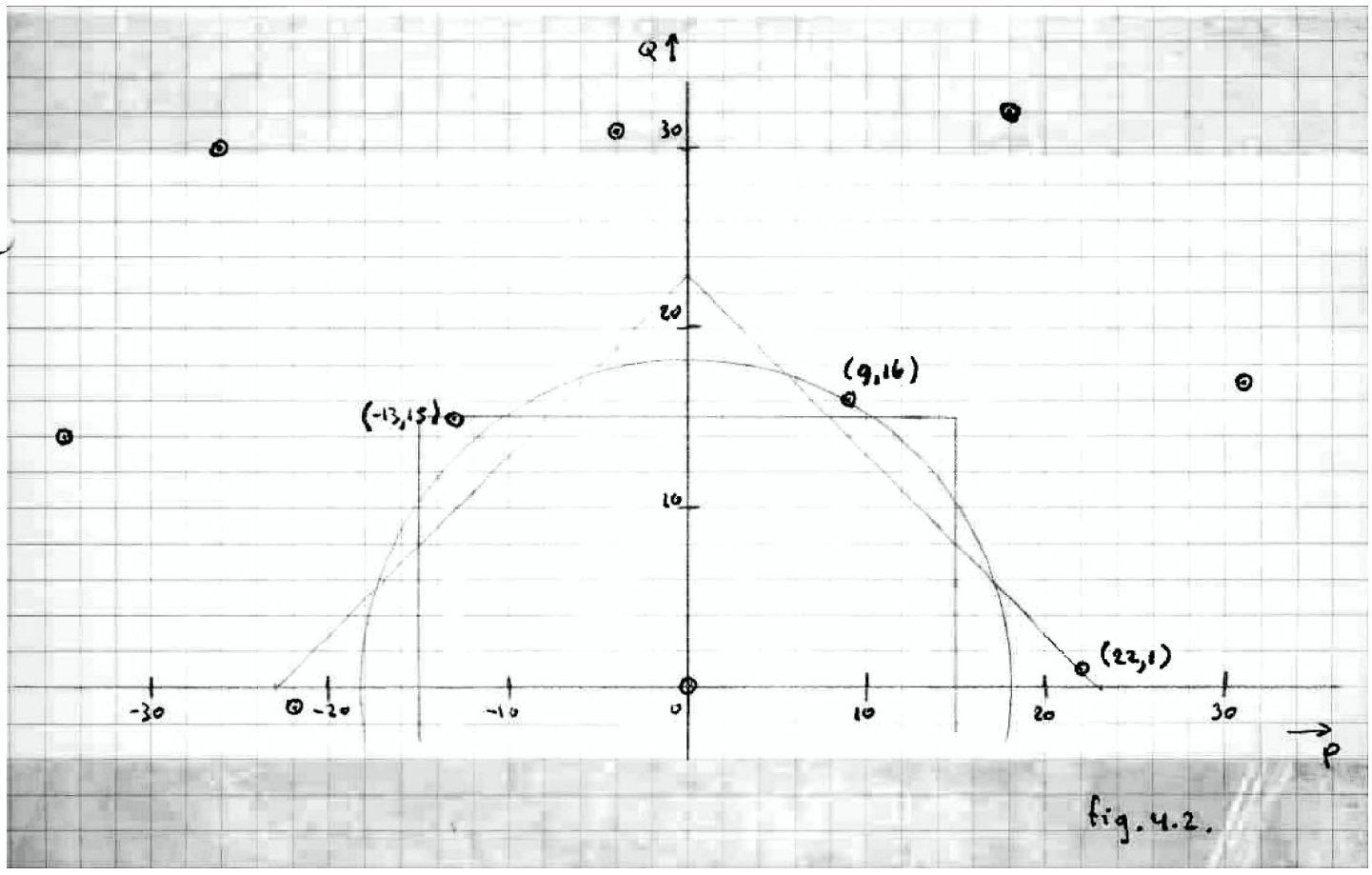


fig. 4.2.

Zij $v_m \in \mathbb{R}$ zo, dat het volume van het gebied $G = \{ (X,Y) \in \mathbb{R} \times \mathbb{R} : \Phi(X,Y) \leq v_m \}$ precies $4 \cdot p^m$ is. Met behulp van een roosterstelling van Minkowski volgt nu direkt:

<u>Stelling 4.3</u> Zij $\alpha \in \mathbb{Q}_p$ geheel. Dan is er een benadering $(P,Q) \neq (0,0)$ van α, die voldoet aan $|Q\alpha - P|_p \leq p^{-m}$, en $\Phi(P,Q) \leq v_m$.

<u>Gevolg</u> Voor een m-e orde beste benadering van α geldt $\Phi(P,Q) \leq v_m$.

Met de 'vierkante norm' $\Phi(X,Y) = \max(|X|, |Y|)$ is $v_m = p^{\frac{1}{2}m}$. Stelling 4.3 met deze Φ is te vinden bij Mahler (1934) en Schneider (1970). Met behulp van het ladenprincipe geven zij een simpel bewijs.
Het gebied G is in dit geval een vierkant. In fig. 4.1. is zo'n vierkant ingetekend, voor $m = 1,2,3,4$. De naam 'vierkante norm' vindt hier zijn motivering.

Voor $\Phi(X,Y) = \sqrt{X^2 + Y^2}$ wordt G een cirkelschijf, met straal $v_m = \frac{2}{\sqrt{\pi}} \cdot p^{\frac{1}{2}m}$. In figuur 4.1. is ook de cirkel met straal v_m ingetekend voor $m = 1,2,3,4$.

Het zal duidelijk zijn dat (P,Q) een beste benadering van α is als het van alle roosterpunten in Γ_m het dichtst bij $(0,0)$ ligt t.a.v. de gehanteerde norm.

Tenslotte geven we een direkt gevolg van stelling 4.3.:

Stelling 4.4. Zij $\alpha \in \mathbb{Q}_p$, $|\alpha|_p \leq 1$, $\alpha \notin \mathbb{Q}$.
Er zijn oneindig veel $(P, Q) \in \mathbb{Z} \times \mathbb{Z}$,
met $Q > 0$, en $|Q\alpha - P|_p \leq \frac{1}{\max(|P|,|Q|)^2}$.

bewijs Uit stelling 4.3. volgt, met $\Phi(X, Y) = \max(|X|, |Y|)$,
dat er bij iedere $m > 0$ P, Q zijn zodat
$|Q\alpha - P|_p \leq p^{-m}$ en $\max(|P|, |Q|) \leq p^{\frac{1}{2}m}$.
Q kan positief gekozen worden door eventueel P van teken te laten wisselen; en $Q \neq 0$ omdat $Q = 0$ zou inhouden dat $|P|_p \leq p^{-m}$ en dus $|P| \geq p^m$, in tegenspraak met $\max(|P|, |Q|) \leq p^{\frac{1}{2}m}$.
Uit $\max(|P|,|Q|) \leq p^{\frac{1}{2}m}$ volgt nu: $|Q\alpha - P|_p \leq \frac{1}{p^m} \leq \frac{1}{\max(|P|,|Q|)^2}$.
Tenslotte: omdat $\alpha \notin \mathbb{Q}$ is $|Q\alpha - P|_p \neq 0$, en is
er een $m' > m$ te vinden met $\frac{1}{p^{m'}} < |Q\alpha - P|_p$.
Voor deze m' kan het bovenstaande herhaald worden.

q.e.d.

We zullen een iets zwakker begrip dan beste benaderingen ook nodig hebben: we doopen het 'bijna-beste benadering':

definitie. $(P, Q) \in \mathbb{Z} \times \mathbb{Z}$, $(P, Q) \neq (0, 0)$ heet m-e orde
bijna-beste benadering van α als $|Q\alpha - P|_p \leq p^{-m}$,
en voor iedere $(P', Q') \in \mathbb{Z} \times \mathbb{Z}$, $(P', Q') \neq (0, 0)$ met
$|Q'\alpha - P'|_p \leq p^{-m}$ geldt:
$\max(|P'|, |Q'|) \geq \max(|P|, |Q|)$.

Natuurlijk kunnen we in deze definitie $\max(|X|, |Y|)$ vervangen door een andere norm $\Phi(X, Y)$.

Voorbeeld :

$\alpha = 413 \in \mathbb{Q}_7$, $m = 2$: $(7,5)$, $(-7,2)$ en $(0,7)$ zijn alle drie 2-e orde bijna-beste benaderingen. Er geldt:
$|2 \cdot 413 + 7|_7 = 7^{-2}$; $|7 \cdot 413 - 0|_7 = 7^{-2}$; en
$|5 \cdot 413 - 7|_7 = 7^{-5}$. Dus alleen $(7,5)$ is ook een beste benadering.

Direkt is in te zien dat iedere beste benadering (P, Q) met $|Q\alpha - P|_p = p^{-m}$ een m-e orde bijna-beste benadering is.

Stelling 4.3. is direkt uit te breiden tot bijna-beste benaderingen: voor iedere p en m is er tenminste één m-e orde bijna-beste benadering (P, Q) met $|Q\alpha - P|_p \leq p^{-m}$ en $\max(|P|, |Q|) \leq p^{\frac{1}{2}m}$.

We hebben in het voorbeeldje hierboven gezien dat er meer bijna-beste benaderingen kunnen bestaan. We zullen nagaan hoeveel.

We hebben het volgende lemma nodig:

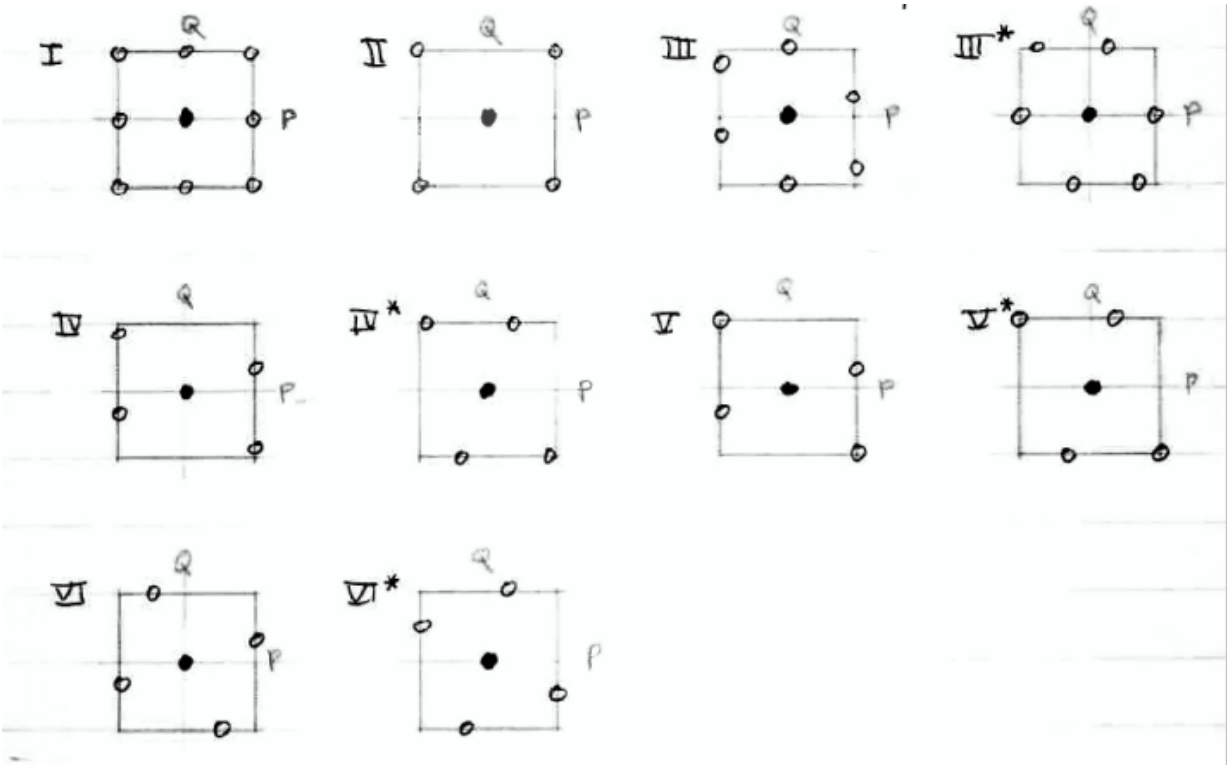
<u>lemma 4.5</u> Zij $\alpha \in \mathbb{Q}_p$ geheel, en $m \in \mathbb{Z}$, $m \geq 1$, maar $m \geq 3$ als $p = 2$. Laat (P_1, Q_1), (P_2, Q_2) beide voldoen aan $(P_i, Q_i) \neq (0,0)$; $Q_i \geq 0$; $|Q_i\alpha - P_i|_p \leq p^{-m}$ en $\max(|P_i|, |Q_i|) \leq p^{\frac{1}{2}m}$. Dan geldt:

als $Q_1 = Q_2$ dan $P_1 = P_2$.

bewijs: Er geldt: $P_1 \equiv Q_1\alpha = Q_2\alpha \equiv P_2 \bmod p^m$.
Stel $P_1 \neq P_2$, dan: $p^m \leq |P_1 - P_2| \leq |P_1| + |P_2| \leq 2 \cdot p^{\frac{1}{2}m}$
en dus $p^m \leq 4$. De enige uit te sluiten mogelijkheid is $p = 3$, $m = 1$. Maar dan geldt:
$|P_i| \leq \sqrt{3} \Rightarrow |P_i| \leq 1$, en dus volgt:
$3 \leq |P_1 - P_2| \leq |P_1| + |P_2| \leq 2$, tegenspraak. qed.

- Voorbeelden: $p^m = 2$, $\alpha = 1$, $Q_1 = Q_2 = 1$, $P_1 = 1$, $P_2 = -1$
$p^m = 4$, $\alpha = 1$, $Q_1 = Q_2 = 2$, $P_1 = 2$, $P_2 = -2$.

Alle mogelijkheden voor minstens twee verschillende m-e orde bijna-beste benaderingen (P, Q) van α $(Q \geq 0)$ zijn makkelijk na te gaan. Er zijn 10 typen:



Alle m-e orde bijna-beste benaderingen liggen op de rand van een vierkant met zijde $2 \cdot M$.

Dus : $M = \max(|P|, |Q|)$ voor alle (P, Q) bijna-best.

I en II zijn alle mogelijkheden met $|P|, |Q| \in \{0, M\}$ voor alle (P, Q).

Als we III, IV, V en VI spiegelen in de lijn $P = Q$, krijgen we III*, IV*, V* en VI*.

We hebben de volgende karakterisaties:

III. we hebben $(P_1, Q_1) = (M, X)$ met $0 < X < M$,
$(P_2, Q_2) = (0, M)$ en $(P_1 - P_2, Q_1 - Q_2) = (M, X - M)$.

IV. we hebben $(P_1, Q_1) = (M, X)$ met $0 < X < M$,
en $(P_2, Q_2) = (M, Y)$ met $-M < Y < X - M$

V. we hebben $(P_1, Q_1) = (M, X)$ met $0 < X < M$,
en $(P_2, Q_2) = (M, -M)$.

VI. we hebben $(P_1, Q_1) = (M, X)$ met $0 < X < M$,
en $(P_2, Q_2) = (Y, -M)$ met $0 < Y < M$.

Als we $p^m = 2$ en $p^m = 4$ uitsluiten, dan zijn op grond van lemma 4.5. I, II, III*, IV* en V* niet mogelijk.

<u>Stelling 4.6.</u> Zij $\alpha \in \mathbb{Q}_p$ gebeel, en $m \geq 1$ met $m \geq 3$ als $p = 2$. Als er twee verschillende (P, Q) zijn met $Q > 0$ en alle bei m-e orde bijna-beste benaderingen van α, dan kunnen we slechts kiezen uit typen III, VI en VI*.

bewijs: We hoeven alleen nog IV en V uit te sluiten.
Stel we hebben type IV of V. Dan:
$(P_1, Q_1) = (M, X)$ met $0 < X < M$, en
$(P_2, Q_2) = (M, Y)$ met $-M \leq Y < X - M$.
Er volgt: $M < X - Y < 2M$.
We zullen aantonen: $M \mid X - Y$, en dat levert een tegenspraak hiermee op.
Er geldt: $0 < M \leq p^{\frac{1}{2}m}$.

Zij $k = \mathrm{ord}_p(M)$ en $\ell = \mathrm{ord}_p(X - Y)$. Dan:
$p^k \mid M \Rightarrow p^k \leq M \leq p^{\frac{1}{2}m} \Rightarrow k \leq \frac{1}{2}m$.
Uit $p^m \mid (X\alpha - M)$ en $p^m \mid (Y\alpha - M)$ volgt:
$p^m \mid M(X - Y)$ en dus: $m \leq \ell + k$, en $\ell \geq \frac{1}{2}m$.
Nu hebben we: $p^\ell \leq X - Y < 2M \leq 2p^{\frac{1}{2}m}$.
Als $p > 5$, krijgen we: $p^\ell < p^{\frac{1}{2}(m+1)} \Rightarrow \ell < \frac{1}{2}(m+1)$
$\Rightarrow \ell \leq \frac{1}{2}m$ Dus: $\ell = \frac{1}{2}m$.
Als $p = 2$ of $p = 3$, krijgen we: $p^\ell < p^{\frac{1}{2}m+1} \Rightarrow \ell < \frac{1}{2}m + 1$
$\Rightarrow \ell \leq \frac{1}{2}(m+1)$. Dus: $\ell = \frac{1}{2}m$ of $\ell = \frac{1}{2}(m+1)$.

$\ell = \frac{1}{2}m$: we hebben $\frac{1}{2}m \geq k \geq m - \ell = \frac{1}{2}m \Rightarrow k = \frac{1}{2}m$.
Maar dan: $p^{\frac{1}{2}m} \mid M \leq p^{\frac{1}{2}m} \Rightarrow M = p^{\frac{1}{2}m}$,
en dus $M = p^\ell \mid (X - Y)$.

$\ell = \frac{1}{2}(m+1)$: $\frac{1}{2}m \geq k \geq m - \ell = \frac{1}{2}(m-1)$. Blijkbaar is m oneven, en moet $k = \frac{1}{2}(m-1)$.
Schrijf $M = p^{\frac{1}{2}(m-1)} \cdot M_0$, $M_0 \in \mathbb{N}$. Uit $M \leq p^{\frac{1}{2}m}$ volgt $M_0 \leq p^{\frac{1}{2}}$. Maar $p = 2$ of $p = 3$, dus $M_0 = 1$, $M = p^{\frac{1}{2}(m-1)}$
en $M = p^{\frac{1}{2}(m-1)} \mid p^{\frac{1}{2}(m-1)} = p^\ell \mid (X - Y)$. qed.

Voorbeelden:

$\alpha = 413 \in \mathbb{Q}_7$ heeft drie 2-e orde bijna-beste benaderingen:
$(7,5)$, $(-7,2)$ en $(0,7)$. Dus: type III.

$\alpha = 60 \in \mathbb{Q}_7$ heeft twee 3-e orde bijna-beste benaderingen:
$(17,6)$ en $(-9,17)$. Dus: type VI.

$\alpha = 341 \in \mathbb{Q}_5$ heeft twee 3-e orde bijna-beste benaderingen:
$(1,11)$ en $(-11,4)$. Dus: type VI*.

Het volgende blijkt te gelden voor type III:

Stelling 4.7. Zij $\alpha \in \mathbb{Q}_p$ geheel, en $m \geq 1$ zodat $m \geq 3$ als $p = 2$. Dan geldt: er zijn drie verschillende m-e orde bijna-beste benaderingen (P,Q) met $Q \geq 0$ $\Leftrightarrow$
$\Leftrightarrow$ we hebben type III $\Leftrightarrow$ m is even en $|\alpha|_p = p^{-\frac{1}{2}m}$.
In die situatie is $M = \max(|P|,|Q|) = p^{\frac{1}{2}m}$.

bewijs: de eerste equivalentie is, gezien stelling 4.6., triviaal.

"$\Rightarrow$": Zij (M,X), $(0,M)$ en $(M,X-M)$ met $M = \max(|P|,|Q|)$ en $0 < X < M < p^{\frac{1}{2}m}$ de drie bijna-beste benaderingen.
Zij $M = p^k M^*$ met $p \nmid M^*$, en $\alpha = p^l \alpha^*$, met $p \nmid \alpha^*$.
Uit $M \leq p^{\frac{1}{2}m}$ volgt nu: $k \leq \frac{1}{2}m$
Omdat $p^m \mid M\alpha$, is $m \leq k+l$, en dus $l \geq m-k \geq \frac{1}{2}m$.
Ook: $p^m \mid (X\alpha - M) = p^k (p^{l-k}\alpha_0 X - M_0)$.
Omdat $m > k$ en $p \nmid M_0$ moet $l-k = 0$, en $l = k = \frac{1}{2}m$.

"$\Leftarrow$": Zij $M = p^{\frac{1}{2}m}$, en $\alpha = p^{\frac{1}{2}m} \cdot \alpha^*$. Omdat $p \nmid \alpha^*$, is er een $X \in \mathbb{Z}$ met $0 < X < p^{\frac{1}{2}m}$ en $X - \alpha^* \equiv 1 \bmod p^{\frac{1}{2}m}$. Dan voldoen (M,X), $(0,M)$ en $(-M,-X+M)$. qed.

HOOFDSTUK 5 : KETTINGBREUKEN VAN P-ADISCHE GETALLEN.

In dit hoofdstuk komen drie algorithmen aan de orde, die een p-adisch getal ontwikkelen in een kettingbreuk. De eerste twee, één van K. Mahler uit 1954, en één van Th. Schneider uit 1970, lijken sterk op elkaar, en zijn opgezet naar analogie van het reële kettingbreukalgorithme. De ermee te berekenen convergenten zijn echter in het algemeen geen beste benaderingen.
Het derde algorithme werd door Mahler voorgesteld in 1954. Dit algorithme levert wel beste benaderingen, maar is nogal onpraktisch: er kan een aanzienlijke hoeveelheid rekenwerk nodig zijn.

Dit hoofdstuk is voornamelijk historisch van aard. Voor zover bewijzen achterwege zijn gelaten, zijn ze te vinden in Mahler (1934) en Schneider (1970).

Het eerste kettingbreukalgorithme voor p-adische getallen van Mahler wordt in zijn Mahler (1934) slechts kort beschreven. Zoals het reële kettingbreukalgorithme berust op het bestaan van de entier-functie op $\mathbb{R}$, zo berust dit algorithme op een soortgelijke p-adische functie.

<u>definitie</u> Voor $\alpha \in \mathbb{Q}_p$ met $\mathrm{ord}_p(\alpha) = f$ en $\alpha = a_f p^f + a_{f+1} p^{f+1} + \cdots$ wordt de <u>p-adische entier</u> $[\alpha]_p$ gedefinieerd door

$$[\alpha]_p = 0 \quad \text{als} \quad |\alpha|_p < 1 ;$$
$$[\alpha]_p = a_f p^f + a_{f+1} p^{f+1} + \cdots + a_{-1} p^{-1} + a_0 \quad \text{als} \quad |\alpha|_p \geq 1.$$

De volgende triviale eigenschappen gelden :

<u>lemma 5.1.</u> (i) $|\alpha - [\alpha]_p|_p < 1$

(ii) $|[\alpha]_p|_p = |\alpha|_p$ als $|\alpha|_p \geq 1$.

Voorbeelden met $p = 3$:

$\alpha = 36 = 1 \cdot 3^2 + 1 \cdot 3^3$; $|36|_3 = \frac{1}{3^2}$; $[36]_3 = 0$

$\alpha = \frac{4}{9} = 1 \cdot 3^{-2} + 1 \cdot 3^{-1}$; $|\frac{4}{9}|_3 = 3^2$; $[\frac{4}{9}]_3 = 1 \cdot 3^{-2} + 1 \cdot 3^{-1} = \frac{4}{9}$

$\alpha = \frac{1}{36} = 1 \cdot 3^{-2} + 2 \cdot 3^{-1} + 0 \cdot 3^0 + 2 \cdot 3^1 + \cdots$; $|\frac{1}{36}|_3 = 3^2$; $[\frac{1}{36}]_3 = 1 \cdot 3^{-2} + 2 \cdot 3^{-1} = \frac{7}{9}$.

De p-adische entier $[\alpha]_p$ kent belangrijke verschillen met de reële entier $[x]$. Zo is $[x]$ geheel, terwijl $[\alpha]_p$ niet p-adisch geheel hoeft te zijn. De p-adische entier $[\alpha]_p$ is juist het niet-gehele deel van α, terwijl $[x]$ wel het gehele deel van x is.
De overeenkomst tussen beide entier-functies is dat zowel $|x - [x]| < 1$ als $|\alpha - [\alpha]_p|_p < 1$ gelden voor alle $x \in \mathbb{R}$, $\alpha \in \mathbb{Q}_p$.
En juist deze eigenschap ligt ten grondslag aan het kettingbreukalgorithme.

Mahlers p-adische kettingbreukalgorithme verloopt nu geheel analoog aan algorithme 3.1., het reële kettingbreukalgorithme.

Zij $\alpha \in \mathbb{Q}_p$.

Algorithme 5.2. i) zet $\alpha_0 = \alpha$ en $i = 0$

ii) bereken $a_i = [\alpha_i]_p$.
als $a_i \neq \alpha_i$, bereken dan $\alpha_{i+1} = \dfrac{1}{\alpha_i - a_i}$
als $a_i = \alpha_i$, dan stop.

iii) zet $i = i+1$ en ga naar ii).

Direkt volgt: $\alpha = [a_0, a_1, a_2, \cdots, a_{n-1}, \alpha_n] =$
$= [a_0, a_1, a_2, a_3, \ldots\ldots]$, eindig of oneindig lang.
De wijzergetallen a_i zullen in het algemeen niet geheel zijn.
Het zijn rationale getallen, met noemers machten van p.

De convergenten vinden we als gebruikelijk als volgt:

Zij $\begin{cases} P_{-2} = 0 \\ Q_{-2} = 1 \end{cases}$, $\begin{cases} P_{-1} = 1 \\ Q_{-1} = 0 \end{cases}$, $\begin{cases} P_k = a_k P_{k-1} + P_{k-2} \\ Q_k = a_k Q_{k-1} + Q_{k-2} \end{cases}$

voor $k = 0, 1, 2, \ldots$ zolang het zinvol is

Analoog aan stelling 3.5. en gevolg 3.6. kan bewezen worden:

Stelling 5.3 $\dfrac{P_n}{Q_n} = [a_0, a_1, a_2, \cdots, a_n]$ voor $n = 0, 1, 2, \ldots$

De $\frac{P_n}{Q_n}$ convergeren inderdaad p-adisch naar α, zo volgt uit:

Stelling 5.4. $\left|\alpha - \dfrac{P_n}{Q_n}\right|_p \leq \dfrac{1}{p^{2n+1}}$.

bewijs: Analoog aan st. 3.5. met $\gamma = \alpha_n$ geldt

$$\alpha = [a_0, a_1, \cdots, a_{n-1}, \alpha_n] = \frac{\alpha_n P_{n-1} + P_{n-2}}{\alpha_n Q_{n-1} + Q_{n-2}} \quad \Rightarrow$$

$$\Rightarrow \alpha = \frac{a_n P_{n-1} + P_{n-2} + (\alpha_n - a_n) P_{n-1}}{a_n Q_{n-1} + Q_{n-2} + (\alpha_n - a_n) Q_{n-1}} \Rightarrow$$

$$\Rightarrow Q_n \alpha - P_n = -(\alpha_n - a_n)(Q_{n-1}\alpha - P_{n-1}).$$

Met inductie volgt nu uit $|\alpha_n - a_n|_p \leq \frac{1}{p}$:

$|Q_n \alpha - P_n| \leq \frac{1}{p^{n+1}}$

We bewijzen met inductie: $|Q_n|_p \geq p^n$ voor $n = 0, 1, 2, \ldots$:

$n=0$: $Q_0 = 1$ klopt.

$n>0$: veronderstel $|Q_k|_p \geq p^k$ voor $k = n-2, n-1$.

Schrijf $Q_k = q_k / p^k$, dan $|q_k|_p \geq 1$.

Voor $k \geq 1$ geldt $|a_k|_p \geq p$; schrijf $a_k = \frac{a_k'}{p}$, dan $|a_k' q_k|_p \geq 1$.

Uit de identiteit $Q_n = \frac{a_n' q_{n-1} + p^2 q_{n-2}}{p^n}$ volgt nu $|Q_n|_p \geq p^n$. qed.

Voorbeeld: $\alpha = \frac{1}{7} \in \mathbb{Q}_5$, $\frac{1}{7} = 3 + 3\cdot 5 + 0\cdot 5^2 + 2\cdot 5^3 + 1\cdot 5^4 + 4\cdot 5^5 + 2\cdot 5^6 + \cdots$

$a_0 = [\alpha]_5 = 3$, $\quad \alpha_1 = -\frac{7}{20} = 2\cdot 5^{-1} + 3 + 3\cdot 5 + \cdots$

$a_1 = [\alpha_1]_5 = \frac{17}{5}$, $\quad \alpha_2 = -\frac{4}{15} = 2\cdot 5^{-1} + 1 + 3\cdot 5 + \cdots$

$a_2 = [\alpha_2]_5 = \frac{7}{5}$, $\quad \alpha_3 = -\frac{3}{5} = 2\cdot 5^{-1} + 4 + 4\cdot 5 + \cdots$

$a_3 = [\alpha_3]_5 = \frac{22}{5}$, $\quad \alpha_4 = -\frac{1}{5} = 4\cdot 5^{-1} + 4 + 4\cdot 5 + \cdots$

$a_4 = [\alpha_4]_5 = \frac{24}{5}$ $\quad \alpha_5 = -\frac{1}{5}$

de kettingbreuk is verder periodiek.

Dus: $\frac{1}{7} = [3, \frac{17}{5}, \frac{7}{5}, \frac{22}{5}, \frac{24}{5}, \frac{24}{5}, \ldots]$

Convergenten:

$\frac{P_0}{Q_0} = \frac{3}{1}$; $\left|\frac{1}{7} - \frac{3}{1}\right|_5 = \frac{1}{5}$

$\frac{P_1}{Q_1} = \frac{56/5}{17/5}$; $\left|\frac{1}{7} - \frac{56}{17}\right|_5 = \frac{1}{5^3}$

$\frac{P_2}{Q_2} = \frac{467/25}{144/25}$; $\left|\frac{1}{7} - \frac{467}{144}\right|_5 = \frac{1}{5^5}$

Als we stelling 4.3. toepassen met $\Phi(X,Y) = \max(|X|,|Y|)$, dan weten we dat er een 1-e orde benadering is met $\max(|P|,|Q|) \leq 2$; een 3-e orde benadering met $\max(|P|,|Q|) \leq 11$, en een 5-e orde benadering met $\max(|P|,|Q|) \leq 55$. Er blijkt dat $\frac{P_0}{Q_0}, \frac{P_1}{Q_1}, \frac{P_2}{Q_2}$ bepaald niet de beste benaderingen zijn.

Voorbeeld : $\alpha = \sqrt{-1} \in \mathbb{Q}_5$, $\sqrt{-1} = 2 + 1.5 + 2.5^2 + 1.5^3 + 3.5^4 + 4.5^5 + \cdots$

$\sqrt{-1} = [2, \frac{16}{5}, \frac{3}{5}, \frac{69}{25}, \ldots]$

$\frac{P_0}{Q_0} = \frac{2}{1}$; $\left|\sqrt{-1} - \frac{2}{1}\right|_5 = \frac{1}{5}$

$\frac{P_1}{Q_1} = \frac{37/5}{16/5}$; $\left|\sqrt{-1} - \frac{37}{16}\right|_5 = \frac{1}{5^3}$

$\frac{P_2}{Q_2} = \frac{161/25}{73/25}$; $\left|\sqrt{-1} - \frac{161}{73}\right|_5 = \frac{1}{5^6}$

en $\frac{P_1}{Q_1}$ en $\frac{P_2}{Q_2}$ zijn geen beste benaderingen met $\Phi(X,Y) = \max(|X|,|Y|)$.

Schneiders algorithme voor de kettingbreukontwikkeling van p-adische getallen lijkt veel op het bovengenoemde algorithme 5.2. Een verschil tussen de twee is dat Schneiders algorithme meer benaderingen vindt. Bij voorbeeld bij $\alpha = \frac{1}{7} \in \mathbb{Q}_5$ vindt Mahlers algorithme 5.2. geen 2-e en 4-e orde benaderingen ; we zullen zien dat Schneiders algorithme deze wel vindt.
Echter, beste benaderingen hoeven we ook bij Schneiders algorithme niet veel te verwachten.

Zij $\alpha \in \mathbb{Q}_p$ zo dat $|\alpha|_p = 1$. Dit is geen wezenlijke beperking.

Algorithme 5.5. i) zet $\alpha_0 = \alpha$, en $i = 0$

ii) bereken $b_i = [\alpha_i]_p$

als $b_i = \alpha_i$, dan stop.

als $b_i \neq \alpha_i$, bereken dan $e_{i+1} = \mathrm{ord}_p(\alpha_i - b_i)$

en bereken $\alpha_{i+1} = p^{e_{i+1}} \cdot \frac{1}{\alpha_i - b_i}$

iii) zet $i = i+1$ en ga naar ii).

De kettingbreuk ziet er als volgt uit:

$$\alpha = b_0 + \cfrac{p^{e_1}}{b_1} + \cfrac{p^{e_2}}{b_2} + \cdots \quad \text{al of niet eindig.}$$

Merk op dat in stap ii) α_{i+1} zo gedefinieerd wordt dat $|\alpha_{i+1}|_p = 1$. Bij het binnengaan van stap ii) is dus altijd $|\alpha_i|_p = 1$. De entier van α_i is dan de nulde coëfficiënt van de p-adische ontwikkeling van α_i.
Merk voorts op dat altijd geldt: $e_{i+1} \geq 1$.

Het verschil tussen Mahlers algorithme 5.c. en Schneiders algorithme 5.5. is dat Schneider telkens de α_i normeert. Dat dat inderdaad een andere kettingbreuk geeft, kan geïllustreerd worden aan een voorbeeld:

Voorbeeld: $\alpha = \frac{1}{7} \in \mathbb{Q}_5$, $\frac{1}{7} = 3 + 3 \cdot 5 + 0 \cdot 5^2 + 2 \cdot 5^3 + 1 \cdot 5^4 + \cdots$

geeft:

i	0	1	2	3	4	5	6
e_i	–	1	1	1	1	1	1
α_i	$\frac{1}{7}$	$-\frac{7}{4}$	$-\frac{4}{3}$	$-\frac{3}{2}$	-2	-1	-1
b_i	3	2	2	1	3	4	4

en verder is de kettingbreuk periodiek, met periode 1.

Schneiders kettingbreuk is nu:

$$\frac{1}{7} = 3 + \cfrac{5}{2} + \cfrac{5}{2} + \cfrac{5}{1} + \cfrac{5}{3} + \cfrac{5}{4} + \cfrac{5}{4} + \cdots$$

of $\frac{1}{7} = 3 + \cfrac{1}{2/5} + \cfrac{1}{2} + \cfrac{1}{1/5} + \cfrac{1}{3} + \cfrac{1}{4/5} + \cfrac{1}{4} + \cdots$,

een wezenlijk andere dan Mahlers kettingbreuk voor $\frac{1}{7}$.

Voorbeeld: $\alpha = 200182 \in \mathbb{Q}_5$; $200182 = 2 + 1\cdot 5 + 2\cdot 5^2 + 1\cdot 5^3 + 3\cdot 5^4 + 4\cdot 5^5 + 2\cdot 5^6 + 3\cdot 5^7$

(deze α is zo gekozen dat $|\alpha - \sqrt{-1}|_5 \leq 5^{-8}$)

geeft:

i	0	1	2	3	4	5	6
e_i	–	1	1	2	1	1	1
α_i	200182	$\frac{1}{56036}$	$\frac{-56036}{11207}$	$\frac{-11207}{3138}$	$\frac{-3138}{2069}$	$\frac{-2069}{2349}$	$\frac{-2349}{2453}$
b_i	2	1	2	1	3	4	2

$$\alpha = 2 + \cfrac{5}{1} + \cfrac{5}{2} + \cfrac{25}{1} + \cfrac{5}{3} + \cfrac{5}{4} + \cfrac{5}{2} + \cdots$$

We definiëren als gebruikelijk voor $k = 1, 2, 3, \cdots$

$$\begin{cases} P_{-1} = 1 \\ Q_{-1} = 0 \end{cases}, \quad \begin{cases} P_0 = b_0 \\ Q_0 = 1 \end{cases}, \quad \begin{cases} P_k = b_k P_{k-1} + p^{e_k} P_{k-2} \\ Q_k = b_k Q_{k-1} + p^{e_k} Q_{k-2} \end{cases}$$

(en eventueel $P_{-2} = 0$, $Q_{-2} = 1$, $e_0 = 0$).

Niet moeilijk te bewijzen is:

<u>Stelling 5.6.</u> (i) $\dfrac{P_n}{Q_n} = b_0 + \cfrac{p^{e_1}}{b_1 + \cdots + \cfrac{p^{e_n}}{b_n}}$ $\quad n = 0, 1, 2, \cdots$

(ii) De rij convergenten $\dfrac{P_n}{Q_n}$ convergeert p-adisch naar α.

(iii) $$\left| \alpha - \frac{P_n}{Q_n} \right|_p = \frac{1}{\prod_{i=1}^{n+1} p^{e_i}} \leq \frac{1}{p^{n+1}} .$$

Voorbeeld: $\alpha = \frac{1}{7} \in \mathbb{Q}_5$, $\frac{1}{7} = 3 + \cfrac{5}{2 + \cfrac{5}{2 + \cfrac{5}{1 + \cfrac{5}{3 + \cfrac{5}{4 + \cfrac{5}{4 + \cdots}}}}}}$

n	0	1	2	3	4	5
P_n	3	11	37	92	461	2304
Q_n	1	2	9	19	102	503
$\left\lvert \frac{1}{7} - \frac{P_n}{Q_n} \right\rvert_5$	5^{-1}	5^{-2}	5^{-3}	5^{-4}	5^{-5}	5^{-6}

Voorbeeld: $\alpha = 2801.02 \in \mathbb{Q}_5$, $\alpha = 2 + \cfrac{5}{1 + \cfrac{5}{2 + \cfrac{25}{1 + \cfrac{5}{3 + \cfrac{5}{4 + \cfrac{5}{2 + \cdots}}}}}}$

n	0	1	2	3	4	5
P_n	2	7	24	199	717	3063
Q_n	1	1	7	32	131	604
$\left\lvert \alpha - \frac{P_n}{Q_n} \right\rvert_5$	5^{-1}	5^{-2}	5^{-4}	5^{-5}	5^{-6}	5^{-7}

Uit beide voorbeelden blijkt weer dat de convergenten geen beste benaderingen zijn in het algemeen. Bij voorbeeld met $\Phi(X,Y) = \max(|X|,|Y|)$ als norm is er een 5-e orde benadering met $\Phi(X,Y) \leq 55$, volgens stelling 4.3.; de nu gevonden 5-e orde benaderingen zijn beduidend slechter.

We kunnen, zoals Schneider (1970) doet, een benadering $\frac{P}{Q}$ van $\alpha \in \mathbb{Q}_p$ c-goed noemen voor zekere constante c, als er een X bestaat met $|P|, |Q| \leq X$ zodat $|\alpha - \frac{P}{Q}|_p \leq \frac{c}{X^2}$.
Uit stelling 4.3. volgt dan dat er bij iedere $X > 0$ een c-goede benadering bestaat voor zekere c. Immers, als $\gamma \in \mathbb{Z}$ zo is dat $p^\gamma < X \leq p^{\gamma+1}$, dan zijn er P, Q met $\max(|P|,|Q|) \leq p^\gamma < X$ zodat $|\alpha - \frac{P}{Q}|_p \leq p^{-2\gamma} \leq \frac{p^2}{X^2}$.

Nu kan aangetoond worden dat Schneiders algorithme 5.5. niet altijd goede benaderingen oplevert in bovenstaande zin:

Stelling 5.7 Als $\alpha \in \mathbb{Q} \cap \mathbb{Q}_p$ een oneindige kettingbreukontwikkeling heeft volgens algorithme 5.5., dan zijn niet alle convergenten c-goede benaderingen, voor iedere constante c.

bewijs: Stel er is een c zodat alle convergenten c-goede benaderingen zijn. Zij $\alpha = \frac{r}{s}$, $r,s \in \mathbb{Z}$, en $\frac{P_n}{Q_n}$ de convergenten van α.
$\frac{P_n}{Q_n}$ zijn c-goede benaderingen $\Rightarrow |\frac{r}{s} - \frac{P_n}{Q_n}|_p \leq \frac{c}{\max(|P_n|,|Q_n|)^2}$

$$\Rightarrow |rQ_n - sP_n|_p \leq \frac{c}{\max(|P_n|,|Q_n|)^2}.$$

Voor n groot genoeg is $|rQ_n - sP_n| < \frac{\max(|P_n|,|Q_n|)^2}{c}$,
zodat voor die n geldt $|rQ_n - sP_n| \cdot |rQ_n - sP_n|_p < 1$.
Echter, voor alle $x \in \mathbb{Z}$, $x \neq 0$ geldt $|x| \cdot |x|_p \geq 1$.
Omdat $rQ_n - sP_n \in \mathbb{Z}$ moet dus $rQ_n - sP_n = 0$,
en dat kan alleen als de kettingbreuk van α
eindig is. Tegenspraak. qed.

Voorbeeld: $\alpha = \frac{1}{7} \in \mathbb{Q}_5$ heeft een oneindige kettingbreuk.
Ter illustratie berekenen we $\max(|P_n|,|Q_n|)^2 \cdot |\alpha - \frac{P_n}{Q_n}|_p$
voor enkele convergenten:

n	0	1	2	3	4	5
P_n	3	11	37	92	461	2304
Q_n	1	2	9	19	102	503
$\max(\lvert P_n\rvert,\lvert Q_n\rvert)^2 \cdot \lvert\alpha - \frac{P_n}{Q_n}\rvert_p$	1.8	≈ 4.8	≈ 11	≈ 14	≈ 68	≈ 340

De vraag is nu welke rationale p-adische getallen een eindige dan wel oneindige kettingbreuk hebben volgens Schneiders algorithme. Hier gaat P. Bundschuh op in. Hij bewijst:

<u>Stelling 5.8</u> Zij $\alpha \in \mathbb{Q}_p$, $\alpha \neq 0$. Dan geldt: $\alpha \in \mathbb{Q} \iff$
$\iff$ de kettingbreuk van α volgens Schneider is
óf eindig, óf oneindig, maar dan geldt voor
alle n groot genoeg: $e_n = 1$, $b_n = p - 1$.

<u>bewijs</u>: zie Bundschuh (1977).

Het lijkt niet eenvoudig om over de eindigheid van de kettings-

breuk volgens Schneider van $\alpha \in \mathbb{Q} \cap \mathbb{Q}_p$ te beslissen zonder de kettingbreuk expliciet te berekenen. Bij voorbeeld: in $\mathbb{Q}_5$ is

$$\frac{91}{19} = 4 + \cfrac{5}{3} + \cfrac{5}{4} + \cfrac{5}{3} + \cfrac{5}{4} + \cfrac{5}{4} + \cfrac{5}{4} + \cfrac{5}{4} + \cdots \quad \text{oneindig}$$

$$\frac{92}{19} = 3 + \cfrac{5}{2} + \cfrac{5}{2} + \cfrac{5}{1} \quad \text{eindig}$$

$$\frac{93}{19} = 2 + \cfrac{5}{4} + \cfrac{25}{4} + \cfrac{5}{4} + \cfrac{5}{4} + \cfrac{5}{4} + \cdots \quad \text{oneindig}.$$

Schneider en Bundschuh besteden ook aandacht aan een analogon voor stelling 3.11, over het verband tussen periodieke kettingbreuken en kwadratisch irrationale getallen. Er geldt:

<u>Stelling 5.9.</u> Als $\alpha \in \mathbb{Q}_p$ een periodieke kettingbreuk volgens algorithme 5.5. heeft, dan $\alpha \in \mathbb{Q}$, of α is kwadratisch irrationaal.

Voor de omgekeerde bewering is er weinig hoop, aldus Bundschuh (1977).

Voor Mahlers algorithme 5.2. zijn wellicht analoge stellingen voor 5.7., 5.8. en 5.9. af te leiden. Omdat dat voor ons doel, het vinden van beste benaderingen, niet van belang lijkt te zijn, gaan we verder niet in op de algorithmes 5.2. en 5.5.

We komen nu toe aan Mahlers tweede algorithme, dat hij uitgebreid beschrijft in Mahler (1954).

Dit algoritme ziet er heel anders uit dan 5.2. en 5.5.
De convergenten worden niet met behulp van een kettingbreuk berekend, maar het gaat nu precies andersom: eerst worden benaderingen berekend, en daar wordt een kettingbreuk mee berekend. We zouden eventueel kunnen volstaan met het berekenen van de benaderingen.

Zij $\alpha \in \mathbb{Q}_p$ gehéél. Voor $P_n, Q_n \in \mathbb{Z}$ noemen we
$E_n = \max(|P_n|, |Q_n|) \cdot |Q_n \alpha - P_n|_p$.
Als norm voor een benadering (P, Q) kiezen we
$\Phi(P,Q) = \max(|P|, |Q|)$.
Uit stelling 4.3. volgt nu direkt dat er bij iedere $n \in \mathbb{Z}$, $n \geq 0$, P_n en Q_n in $\mathbb{Z}$ zijn, niet beide gelijk 0, zodat
$|Q_n \alpha - P_n|_p \leq p^{-n}$; $\max(|P_n|, |Q_n|) \leq p^{\frac{1}{2}n}$, en dus
$E_n \leq p^{-\frac{1}{2}n}$.

Kies uit alle benaderingen (P, Q) met $|Q\alpha - P|_p \leq p^{-n}$ en $\max(|P|,|Q|) \leq p^{\frac{1}{2}n}$ één van degenen met $E = |Q\alpha - P|_p \cdot \max(|P|, |Q|)$ minimaal, en noem deze (P_n, Q_n).
De g.g.d. van P_n en Q_n is dan een macht van p.

Kies bij gegeven n een n' zo dat $p^{-\frac{1}{2}n'} < E_n \leq p^{-\frac{1}{2}(n'-1)}$, en kies weer $(P_{n'}, Q_{n'})$ uit alle (P, Q) met $|Q\alpha - P|_p \leq p^{-n'}$ en $\max(|P|, |Q|) \leq p^{\frac{1}{2}n'}$ zo dat $E_{n'}$ minimaal is.
We noemen $(P_{n'}, Q_{n'})$ de opvolger van (P_n, Q_n).

<u>lemma 5.10.</u> Er geldt: (i) $n' > n$
(ii) $E_{n'} < E_n$

(iii) $\max(|P_{n'}|,|Q_{n'}|) > \max(|P_n|,|Q_n|)$

(iv) $|Q_{n'}\alpha - P_{n'}|_p < |Q_n\alpha - P_n|_p$

(v) $P_n Q_{n'} - P_{n'} Q_n \neq 0$.

Evenals voor de komende stelling 5.12. verwijs ik naar Mahler (1953) voor een bewijs.

Algorithme 5.11. i) zet $P_{-1}=1$, $Q_{-1}=0$, $P_0=0$, $Q_0=1$,
$\Delta_0 = 1$ en $i=0$

ii) bepaal een opvolger van (P_i, Q_i), en noem deze (P_{i+1}, Q_{i+1}).
bereken $\Delta_{i+1} = P_i Q_{i+1} - P_{i+1} Q_i$
$\delta_i = P_{i-1} Q_{i+1} - P_{i+1} Q_{i-1}$

en $a_i = -\frac{\Delta_{i+1}}{\Delta_i}$, $b_i = \frac{\delta_i}{\Delta_i}$

iii) Als $E_{i+1} = 0$, dan stop,
anders: zet $i = i+1$ en ga naar ii).

Stelling 5.12. (i) $\frac{P_n}{Q_n} = \cfrac{a_0|}{|b_0} + \cfrac{a_1|}{|b_1} + \cdots + \cfrac{a_{n-1}|}{|b_{n-1}}$ $n = 1, 2, 3, \cdots$

(ii) $\alpha = \cfrac{a_0|}{|b_0} + \cfrac{a_1|}{|b_1} + \cfrac{a_2|}{|b_2} + \cdots$, eindig of oneindig lang.

(iii) We kunnen schrijven: $a_n = \frac{e_n p^{\alpha_n}}{d_n}$, $b_n = \frac{c_n}{p \cdot d_n}$
met $c_n, d_n, e_n, \alpha_n \in \mathbb{Z}$, $\alpha_n \geq 0$,
$c_n, d_n, e_n \neq 0$, $p \nmid d_n$, $p \nmid e_n$, en
$|d_n| \leq 2\sqrt{p}$, $|e_n| \leq 2\sqrt{p}$, $|b_n| < 2\sqrt{p}\,|a_n|$.
voor $n = 0, 1, 2, \cdots$

(iv) Voor de convergenten $\frac{P_n}{Q_n}$ geldt:

$$\frac{1/2}{\max(|P_n|,|Q_n|)\cdot\max(|P_{n+1}|,|Q_{n+1}|)} \leq |Q_n\alpha - P_n|_p \leq$$

$$\leq \frac{\sqrt{p}}{\max(|P_n|,|Q_n|)\cdot\max(|P_{n+1}|,|Q_{n+1}|)} .$$

(v) $\Delta_n = (-1)^n \prod_{i=0}^{n-1} a_i \neq 0$, en $1 \leq |\Delta_n|\,|Q_n|_p \leq 2\sqrt{p}$.

(vi) We kunnen α in een kettingbreuk met gehele tellers en noemers ontwikkelen:

$$\alpha = \cfrac{e_0 p^{\alpha_0+1}}{c_0} + \cfrac{d_0 e_1 p^{\alpha_1+2}}{c_1} + \cfrac{d_1 e_2 p^{\alpha_2+2}}{c_2} + \cdots$$

Stelling 5.13. De convergenten van α die verkregen worden m.b.v. algorithme 5.11. zijn beste benaderingen t.a.v. de norm $\Phi(X,Y) = \max(|X|,|Y|)$.

bewijs: Zij (P,Q) co'n convergent, met $|Q\alpha - P|_p = p^{-m}$.
Dan is $\max(|P|,|Q|) \leq p^{\frac{1}{2}m}$, en voor iedere benadering (P',Q') met $|Q'\alpha - P'|_p \leq p^{-m}$ en $\max(|P'|,|Q'|) \leq p^{\frac{1}{2}m}$ geldt: $\max(|P'|,|Q'|)\cdot|Q'\alpha - P'|_p \geq \max(|P|,|Q|)\cdot|Q\alpha - P|_p \Rightarrow$

$$\Rightarrow \max(|P'|,|Q'|) \geq \max(|P|,|Q|)\cdot\frac{|Q\alpha - P|_p}{|Q'\alpha - P'|_p} \geq \max(|P|,|Q|).$$

$\Rightarrow$ (P,Q) is beste benadering. qed.

Deze laatste stelling geeft een groot voordeel aan van algorithme 5.11. boven algorithmes 5.2 en 5.5. De flessehals in dit algorithme is echter het bepalen van een opvolger. Mahler geeft in zijn Mahler (1953) geen methode aan om opvolgers te vinden.

Een zeer omslachtige methode is de volgende:
Laat Q de verzameling $\{1, 2, 3, \cdots, [p^{\frac{1}{2}m}]\}$ doorlopen, en bereken bij iedere Q een P met $P \equiv Q\alpha_m \bmod p^m$ en $|P| \leq p^{\frac{1}{2}m}$ ($\alpha_m = a_0 + a_1 p + \cdots + a_{m-1} p^{m-1}$ als $\alpha = a_0 + a_1 p + a_2 p^2 + \cdots$).
Zoek die P en Q eruit met minimale $\max(|P|, |Q|) \cdot |Q\alpha - P|_p$.
Op grond van stelling 4.3. hoeven we niet meer Q's af te zoeken.
Iets sneller kan het als volgt:
Laat R de verzameling $\{1, 2, 3, \cdots, [\frac{\alpha_m + 1}{p^{\frac{1}{2}m}}]\}$ doorlopen, en neem telkens $Q \in \mathbb{Z}$ zodat $|Q - R\frac{p^m}{\alpha_m}| \leq \frac{1}{2}$, en bereken dan $P = Q\alpha_m - Rp^m$. Dit is een verbetering, omdat alle Q's die tot een P zouden leiden met $|P| > \frac{1}{2}\alpha_m$ direkt worden overgeslagen. De verbetering is m.n. groot als $\alpha_m \ll p^m$

Voorbeeld: $\alpha = \frac{1}{7} \in \mathbb{Q}_5$ $\quad \alpha = 3 + 3\cdot 5 + 0\cdot 5^2 + 2\cdot 5^3 + \cdots$
$P_0 = 0$, $Q_0 = 1$, $E_0 = 1$, als opvolger zoeken we een 1-e orde benadering: we vinden met $R = 1$: $Q_1 = 2$, $P_1 = 1$.
Er volgt $E_1 = \frac{2}{5}$. ($(-2, 1)$ is een even goede benadering als $(1, 2)$).
De volgende opvolger moet orde 2 hebben.
We vinden:

R:	Q:	P:	E:
1	1	-7	$^7/_{25}$
2	3	4	$^4/_{25}$
3	4	-3	$^4/_{25}$
4	6	8	$^8/_{25}$

Kies $(P_2, Q_2) = (4, 3)$, $E_2 = {}^4/_{25}$
De 3-e opvolger wordt $(P_3, Q_3) = (1, 7)$ en het algoritme breekt af.

De bijbehorende kettingbreuk van $\frac{1}{7}$ wordt als volgt:

n	-1	0	1	2	3
P_n	1	0	1	4	1
Q_n	0	1	2	3	7
Δ_n		1	-1	-5	25
δ_n		2	-4	5	
a_n		1	-5	5	
b_n		2	4	-1	

zodat $\frac{1}{7} = \left[\begin{matrix}1\\2\end{matrix}\right] + \left[\begin{matrix}-5\\4\end{matrix}\right] + \left[\begin{matrix}5\\-1\end{matrix}\right]$.

Voorbeeld: $\alpha = 2{,}01012 \in \mathbb{Q}_5$, $\alpha = 2 + 1.5 + 2.5^2 + 1.5^3 + 3.5^4 + 4.5^5 + 2.5^6 + 3.5^7$

Een 4-e orde benadering vinden we als volgt:

$\alpha_4 = 182$,

R:	Q:	P:	
1	3	-79	
2	7	24	beste benadering
3	10	-55	
4	14	48	
5	17	-31	
6	21	72	
7	24	-7	beste benadering.

HOOFDSTUK 6 : EEN BESTE-BENADERINGEN-ALGORITHME VAN MAHLER

In hoofdstuk 4 van Mahler (1961) presenteert K. Mahler een algorithme om rationale benaderingen te vinden van p-adische getallen dat nogal afwijkt van de drie in het vorige hoofdstuk behandelde algorithmes. Twee opvallende eigenschappen van dit snelle en praktische algorithme zijn : ten eerste, dat het gebruik maakt van het kettingbreukalgorithme voor reële getallen ; ten tweede, dat het een m-e orde benadering vindt zonder gebruik te maken van benaderingen met kleinere orde.
Voorts heeft het algorithme de eigenschap bijna altijd beste benaderingen te geven. Het algorithme is zo aan te passen dat altijd beste benaderingen gevonden worden, en zelfs alle beste benaderingen worden gevonden.
We beschouwen in dit hoofdstuk beste benaderingen t.o.v. de norm $\Phi(X,Y) = \max(|X|, |Y|)$.
Men zou kunnen zeggen dat dit algorithme precies doet waarin algorithme 5.11. tekort schiet. Het is, net als in algorithme 5.11., mogelijk uit de gevonden benaderingen een kettingbreuk te construeren.

We leggen het volgende vast : Zij $\alpha \in \mathbb{Q}_p$ niet 0 en p-adisch geheel. Zij $\alpha = a_0 + a_1 p + a_2 p^2 + \cdots$ zijn p-adische ontwikkeling, en zij $\alpha_m = a_0 + a_1 p + \cdots + a_{m-1} p^{m-1}$ de m-e afkapping van α, $m = 1, 2, 3, \ldots$.
Kies een $m \in \mathbb{N}$ willekeurig, maar vast.
We zoeken nu $P, Q \in \mathbb{Z}$, niet beide gelijk 0, zo dat $|Q\alpha - P|_p \leq p^{-m}$. Dat is gelijkwaardig met $|Q\alpha_m - P|_p \leq p^{-m}$,

en dus met $Q\alpha_m - P_m \equiv 0 \bmod p^m$.
Met andere woorden: we zoeken $P, Q, R \in \mathbb{Z}$, P en Q niet beide gelijk 0, zodat $Q\alpha_m - P = R\,p^m$, en $\max(|P|, |Q|)$ zo klein mogelijk. We kunnen altijd $Q \geq 0$ kiezen.

Stelling 4.3. verzekert ons van het bestaan van $P, Q \in \mathbb{Z}$ zodat $|Q\alpha_m - P|_p \leq p^{-m}$ en $0 \leq |P|, Q \leq p^{\frac{1}{2}m}$.
Met $R \in \mathbb{Z}$ gedefinieerd door $Q\alpha_m - P = R\,p^m$ hebben we dan:

$$\left| \frac{\alpha_m}{p^m} - \frac{R}{Q} \right| = \frac{|P|}{p^m Q} \leq \frac{p^{\frac{1}{2}m}}{p^{\frac{1}{2}m} \cdot Q^2} = \frac{1}{Q^2}.$$

We kunnen $\frac{R}{Q}$ opvatten als een benadering van het rationale getal $\frac{\alpha_m}{p^m}$. Het volgende algorithme maakt daarvan gebruik: het bepaalt convergenten van $\frac{\alpha_m}{p^m}$ met het gewone, reële kettingbreukalgorithme 3.1.; met behulp van een geschikte convergent wordt dan een goede p-adische benadering van α_m berekend.

<u>Algorithme 6.1.</u> i) bereken de kettingbreuk van $\frac{\alpha_m}{p^m}$:

$$\frac{\alpha_m}{p^m} = [0, b_1, b_2, \cdots, b_N]$$

en de convergenten $\frac{R_0}{Q_0}, \frac{R_1}{Q_1}, \cdots, \frac{R_N}{Q_N}$ [1]

ii) als $Q_N < p^{\frac{1}{2}m}$, zet dan $P = 0$, $Q = Q_N$.
als $Q_N \geq p^{\frac{1}{2}m}$, zoek dan k_0 zo dat $Q_{k_0} \leq p^{\frac{1}{2}m} \leq Q_{k_0+1}$, en zet $Q = Q_{k_0}$ en $P = \alpha_m Q_{k_0} - p^m R_{k_0}$.

[1] Alle wijergetallen en convergenten hangen uiteraard van m af.

Stelling 6.2. Voor (P, Q) gevonden m.b.v. algorithme 6.1. geldt:
$|Q\alpha - P|_p \leq p^{-m}$, $\max(|P|, |Q|) \leq p^{\frac{1}{2}m}$.

bewijs: Merk eerst op dat het eerste wijzergetal van de kettingbreuk $\frac{\alpha_m}{p^m} = [0, b_1, b_2, \cdots, b_N]$ 0 is omdat $0 < \frac{\alpha_m}{p^m} < 1$.
Voor de convergenten van $\frac{\alpha_m}{p^m}$ geldt, voor $k = 1, 2, \cdots, N$:

$$\begin{cases} R_{-1} = 1 \\ Q_{-1} = 0 \end{cases}, \quad \begin{cases} R_0 = 0 \\ Q_0 = 1 \end{cases}, \quad \begin{cases} R_k = b_k R_{k-1} + R_{k-2} \\ Q_k = b_k Q_{k-1} + Q_{k-2} \end{cases},$$

en $\text{ggd}(R_k, Q_k) = 1$.
Zij $P_k = \alpha_m Q_k - p^m R_k$, dan is $\text{ggd}(P_k, Q_k)$ een macht van p.
Er geldt: $\frac{R_N}{Q_N} = \frac{\alpha_m}{p^m}$, en omdat $\text{ggd}(R_N, Q_N) = 1$ volgt: $Q_N \mid p^m$.
Zij c_k zodat $\frac{\alpha_m}{p^m} = [0, b_1, b_2, \cdots, b_{k-1}, c_k]$, $k = 0, 1, \cdots, N$.
De kettingbreuken theorie leert (gevolg 3.6.(i)):

$$\frac{\alpha_m}{p^m} - \frac{R_k}{Q_k} = \frac{(-1)^k}{Q_k(c_{k+1} Q_k + Q_{k-1})} \Rightarrow$$

$$\Rightarrow \quad P_k = \frac{(-1)^k p^m}{c_{k+1} Q_k + Q_{k-1}}, \quad k = 0, 1, \cdots, N-1.$$

Uit $b_{k+1} \leq c_{k+1} < b_{k+1} + 1$ halen we een bovengrens en een ondergrens voor $|P_k|$ voor $k = 0, 1, \cdots, N-1$:

$$|P_k| \leq \frac{p^m}{b_{k+1} Q_k + Q_{k-1}} = \frac{p^m}{Q_{k+1}}$$

$$|P_k| > \frac{p^m}{b_{k+1} Q_k + Q_{k-1} + Q_k} = \frac{p^m}{Q_{k+1} + Q_k} \geq \frac{p^m}{2 Q_{k+1}}.$$

(we gebruiken $Q_k \leq Q_{k+1}$).

Merk op: $P_{-1} = -p^m$, en $P_N = 0$.
Uit de definitie van P_k volgt:

$$|Q_k \alpha_m - P_k|_p = |p^m R_k|_p \leq p^{-m}, \quad k = -1, 0, 1, \cdots, N.$$

Voorts geldt voor $k = 0, 1, \cdots, N-1$:

$$0 \neq |P_k| \cdot |Q_k| \leq |P_k| \cdot |Q_{k+1}| \leq p^m$$

En: $0 = Q_{-1} \leq 1 = Q_0 \leq Q_1 < Q_2 < \cdots < Q_N \leq p^m$.

Als $Q_N \geq p^{\frac{1}{2}m}$, dan is er een $k_0 \in \{1, 2, \cdots, N-1\}$ zodat $Q_{k_0} \leq p^{\frac{1}{2}m} < Q_{k_0+1}$. Dan volgt:

$$|P_{k_0}| \leq \frac{p^m}{Q_{k_0+1}} < p^{\frac{1}{2}m}.$$

Dus voldoet $(P, Q) = (P_{k_0}, Q_{k_0})$.

Als $Q_N < p^{\frac{1}{2}m}$, dan is zo'n k_0 niet meer te vinden in $\{1, 2, \cdots, N-1\}$. Neem dan $k_0 = N$, en blijkt dat $(P, Q) = (P_N, Q_N) = (0, Q_N)$ voldoet. qed.

Opmerking: Slechts de convergenten $\frac{R_0}{Q_0}, \frac{R_1}{Q_1}, \cdots$ met noemer $Q \leq p^{\frac{1}{2}m}$ hoeven te worden berekend.

Voorbeelden:

$\alpha = \frac{1}{7} \in \mathbb{Q}_5$, $\frac{1}{7} = 3 + 3 \cdot 5 + 0 \cdot 5^2 + 2 \cdot 5^3 + 1 \cdot 5^4 + 4 \cdot 5^5 + 2 \cdot 5^6 + \cdots$

$\frac{\alpha_1}{p} = \frac{3}{5} = [0, 1, 1, 2]$

R_k:	1	0	1	1	3
Q_k:	0	1	1	2	5
P_k:	-5	3	-2	1	0

$(P, Q) = (1, 2)$

$|2 \cdot \frac{1}{7} - 1|_5 = 5^{-1}$

$\frac{\alpha_2}{p^2} = \frac{18}{25} = [0, 1, 2, 1, 1, 3]$

R_k:	1	0	1	2	3	5	18
Q_k:	0	1	1	3	4	7	25
P_k:	-25	18	-7	4	-3	1	0

$(P,Q) = (-3,4)$, $|4\cdot\frac{1}{7}+3|_5 = 5^{-2}$

$\frac{\alpha_6}{p^6} = \frac{13393}{15625} = [0,1,6,2232]$

R_k:	1	0	1	6	13393
Q_k:	0	1	1	7	15625
P_k:	-15625	13393	-2232	1	0

We vinden natuurlijk $(P,Q) = (1,7)$, $|7\cdot\frac{1}{7}-1|_5 = 0$

$\alpha = 1029 \in \mathbb{Q}_7$, $1029 = 3\cdot 7^3$

$\frac{\alpha_5}{p^5} = \frac{1029}{7^5} = \frac{3}{49} = [0,16,3]$

R_k:	1	0	1	3
Q_k:	0	1	16	49
P_k:	-7^5	1029	-343	0

Nu is $Q_N = 49 < 7^{2\frac{1}{2}} = p^{\frac{1}{2}m}$, dus $(P,Q) = (0,49)$
en $|49\cdot 1029 - 0|_7 = 7^{-5}$.

$\alpha = 181 \in \mathbb{Q}_5$, $181 = 1 + 1\cdot 5 + 2\cdot 5^2 + 1\cdot 5^3$

$\frac{\alpha_5}{p^5} = \frac{181}{3125} = [0,17,3,1,3,2,1,3]$

R_k:	1	0	1	3	4 ...
Q_k:	0	1	17	52	69 ...
P_k:	-3125	181	-48	37	-11 ...

Het algorithme 6.1. kiest k_0 zodat $Q_{k_0} \leq p^{\frac{1}{2}m} = 5^{\frac{5}{2}} \approx 55{,}9$
en Q_{k_0} zo groot mogelijk, dus $(P_{k_0}, Q_{k_0}) = (37,52)$
Echter, $(P_{k_0-1}, Q_{k_0-1}) = (-40,17)$ is een betere benadering van $181 \in \mathbb{Q}_5$ t.a.v. de norm $\Phi(X,Y) = \max(|X|,|Y|)$.

Het laatste voorbeeld toont aan dat algorithme 6.1. niet altijd beste benaderingen oplevert.

Het volgende algoritme doet het beter:

Algoritme 6.3. i) als $p^m = 2^l$ en $|\alpha|_2 = 1$, kies dan (P,Q) uit $\{(1,1),(-1,1)\}$ zo dat $|Q\alpha - P|_p$ minimaal, en stop.

anders: bereken de convergenten $\frac{R_0}{Q_0}, \frac{R_1}{Q_1}, \ldots, \frac{R_N}{Q_N}$ van $\frac{\alpha_m}{p^m}$.

ii) als $Q_N < p^{\frac{1}{2}m}$, kies dan $(P,Q) = (0, Q_N)$ en stop.
als $Q_N \geq p^{\frac{1}{2}m}$, zoek dan k^* zo dat $Q_{k^*} \leq p^{\frac{1}{2}m} < Q_{k^*+1}$.

iii) bereken $P_k = \alpha_m Q_k - p^m R_k$ voor $k = k^*-1, k^*$.
als $|\alpha|_p \neq p^{-\frac{1}{2}m}$ en $\max(|P_{k^*-1}|, Q_{k^*-1}) \neq \max(|P_{k^*}|, Q_{k^*})$, kies dan $k_0 \in \{k^*-1, k^*\}$ zo dat $\max(|P_{k_0}|, Q_{k_0})$ minimaal is, en zet $(P,Q) = (P_{k_0}, Q_{k_0})$.
als $|\alpha|_p \neq p^{-\frac{1}{2}m}$ en $\max(|P_{k^*-1}|, Q_{k^*-1}) = \max(|P_{k^*}|, Q_{k^*})$. kies dan $k_0 \in \{k^*-1, k^*\}$ zo dat $|Q_{k_0}\alpha - P_{k_0}|_p$ minimaal is, en zet $(P,Q) = (P_{k_0}, Q_{k_0})$.
als $|\alpha|_p = p^{-\frac{1}{2}m}$, kies dan (P,Q) uit $\{(P_{k^*-1}, Q_{k^*-1}), (P_{k^*}, Q_{k^*}), (P_{k^*}-P_{k^*-1}, Q_{k^*}-Q_{k^*-1})\}$ zo dat $|Q\alpha - P|_p$ minimaal is.

Stelling 6.4. Voor (P,Q) gevonden met algoritme 6.3. geldt: $|Q\alpha - P|_p \leq p^{-m}$ en $\max(|P|, |Q|) \leq p^{\frac{1}{2}m}$.

bewijs: geheel analoog aan het bewijs van stelling 6.2.

We zullen eerst bewijzen dat we voor k_0 slechts de keus hebben uit k^*-1 en k^*, daarna geven we aan of de m.b.v. algoritme 6.3. gevonden (P, Q) een beste benadering van α is t.o.v. $\Phi(X,Y) = \max(|X|,|Y|)$.

Zij (P_k, Q_k) voor $k = 0, 1, \ldots, N$ de rij benaderingen van α met $P_k = \alpha_m Q_k - p^m R_k$ en $\frac{R_k}{Q_k}$ convergenten van $\frac{\alpha_m}{p^m}$.

Uit de reële kettingbreukentheorie (lemma 3.7.(vi)): de rij $|Q_k \frac{\alpha_m}{p^m} - R_k|$ daalt, en dus volgt:

$$p^m = |P_0| > |P_1| > |P_2| > \cdots > |P_{N-1}| > |P_N| = 0$$

en ook: $1 = Q_0 \leq Q_1 < Q_2 < \cdots < Q_{N-1} < Q_N \leq p^m$.

Er is dus een 'omslagpunt' k', zodat $|P_k| \geq Q_k$ voor $k \leq k'$, en $|P_k| < Q_k$ voor $k > k'$. Het ligt voor de hand dat de gezochte k_0 in de buurt van k' ligt.

We zetten k^*, k_0 en k' nog eens op een rijtje:

k^* is maximaal zodat $Q_{k^*} \leq p^{\frac{1}{2}m}$
k' is maximaal zodat $|P_{k^*}| \geq Q_{k^*}$
k_0 is zodat $\max(|P_{k_0}|, Q_{k_0})$ minimaal

Het volgende lemma geeft de mogelijke verbanden tussen deze drie indices aan: er blijken slechts 4 combinaties mogelijk te zijn.

lemma 6.5. i) $k' = k_0$ of $k' = k_0 - 1$

ii) $k^* = k_0$ of $k^* = k_0 + 1$

bewijs i) Als $k < k'$ is $\max(|P_k|, Q_k) = |P_k| > |P_{k'}| =$
$= \max(|P_{k'}|, Q_{k'})$, en k_0 kan per definitie niet gelijk aan k zijn.

Als $k > k'+1$ is evenzo $k_0 \neq k$, omdat

$$\max(|P_k|, Q_k) = Q_k > Q_{k'+1} = \max(|P_{k'+1}|, Q_{k'+1}).$$

ii) Als $k > k^*$, dan is $Q_k > p^{\frac{1}{2}m} \geq \max(|P_{k^*}|, Q_{k^*})$ volgens stelling 6.2., en kan niet $k = k_0$.

Als $k_0 \leq k^* - 3$, dan geldt, volgens de keuze van k_0,

$$|P_{k_0}| \leq \max(|P_{k^*}|, Q_{k^*}) \leq p^{\frac{1}{2}m}.$$

Bij stelling 6.2. hebben we bewezen:

$$|P_{k_0}| > \frac{p^m}{2 Q_{k_0+1}}$$

Samen geeft dit: $Q_{k_0+1} > \frac{1}{2} p^{\frac{1}{2}m}$, en dus

$$\tfrac{1}{2} p^{\frac{1}{2}m} < Q_{k_0+1} \leq Q_{k^*-2} < Q_{k^*-1} \leq Q_{k^*} \leq p^{\frac{1}{2}m}$$

Echter, $Q_{k^*} = b_{k^*} Q_{k^*-1} + Q_{k^*-2}$, waarbij b_{k^*} een wijzergetal is uit de kettingbreuk van $\frac{\alpha_m}{p^m}$. Dan volgt:

$$p^{\frac{1}{2}m} \geq Q_{k^*} > b_{k^*} \cdot \tfrac{1}{2} p^{\frac{1}{2}m} + \tfrac{1}{2} p^{\frac{1}{2}m} \Rightarrow$$

$$\Rightarrow b_{k^*} < 1, \text{ en dat is een tegenspraak.}$$

We moeten nog de mogelijkheid $k_0 = k^* - 2$ uitsluiten. Dat vereist een subtieler argument.

Veronderstel $k_0 = k^* - 2$.

Omdat $k_0 + 1 > k'$ volgt: $Q_{k_0+1} = \max(|P_{k_0+1}|, Q_{k_0+1})$

en, analoog aan bovenstaande,

$$Q_{k_0+1} \geq |P_{k_0}| > \frac{p^m}{2\,Q_{k_0+1}} \quad , \text{ zodat } \quad Q_{k_0+1} > \tfrac{1}{\sqrt{2}}\, p^{\frac{1}{2}m}.$$

Nu hebben we : $Q_{k_0+2} = b_{k_0+2}\, Q_{k_0+1} + Q_{k_0} > \frac{1}{\sqrt{2}}\, p^{\frac{1}{2}m} \cdot b_{k_0+2}$.

Anderzijds : $Q_{k_0+2} = Q_{k^*} \leq p^{\frac{1}{2}m}$, dus volgt : $b_{k_0+2} < \sqrt{2}$.
Omdat echter $b_{k_0+2} \in \mathbb{Z}$ en $b_{k_0+2} \geq 1$, moet $b_{k_0+2} = 1$.

Dan : $p^{\frac{1}{2}m} \geq Q_{k^*} = Q_{k_0+1} + Q_{k_0} > \frac{1}{\sqrt{2}}\, p^{\frac{1}{2}m} + Q_{k_0} \Rightarrow$

$\Rightarrow Q_{k_0} < \left(1 - \frac{1}{\sqrt{2}}\right) p^{\frac{1}{2}m}$. Zij $c \in \mathbb{R}$ zo dat
$Q_{k_0} = c \cdot p^{\frac{1}{2}m}$, dan volgt : $c < 1 - \frac{1}{\sqrt{2}}$.
En omdat $Q_{k_0} \geq 1$, is $c > 0$.

Ook geldt : $|P_{k_0}| > \frac{p^m}{2\,Q_{k_0+1}} \geq \frac{p^m}{2\,p^{\frac{1}{2}m}} = \frac{1}{2}\, p^{\frac{1}{2}m} > c \cdot p^{\frac{1}{2}m}$

en dus $\max(|P_{k_0}|, Q_{k_0}) = |P_{k_0}|$ (olwel $k_0 = k'$).

Met behulp van een ongelijkheid uit het bewijs van stelling 6.2. vinden we :

$$Q_{k_0+1} \geq |P_{k_0}| > \frac{p^m}{Q_{k_0+1} + Q_{k_0}} \geq \frac{p^m}{p^{\frac{1}{2}m}(1+c)} = \frac{1}{1+c} \cdot p^{\frac{1}{2}m},$$

en daaruit halen we :

$$Q_{k_0} = Q_{k_0+2} - Q_{k_0+1} \leq p^{\frac{1}{2}m}\left(1 - \frac{1}{1+c}\right) = \frac{c}{1+c}\, p^{\frac{1}{2}m},$$

ofwel $c \leq \frac{c}{1+c}$, in tegenspraak met $c > 0$ qed.

Dit lemma laat vier mogelijkheden open : $k' = k_0 = k^*$;
$k'+1 = k_0 = k^*$; $k' = k_0 = k^*-1$; $k'+1 = k_0 = k^*-1$.

Van alle vier geven we een voorbeeld:

$\alpha = 181 \in \mathbb{Q}_5$, $\frac{\alpha_3}{p^3} = \frac{56}{125} = [0, 2, 4, 3, 4]$

R_k :	1	0	1	4	13	....
Q_k :	0	1	2	9	29	....
P_k :	-125	56	-13	4	-1	....
			↑ k'	↑↑ $k_0 k^*$		

$k'+1 = k_0 = k^*$

$\alpha = 181 \in \mathbb{Q}_5$, $\frac{\alpha_4}{p^4} = \frac{181}{625} = [0, 3, 2, 4, 1, \cdots]$

R_k :	1	0	1	2	9	....
Q_k :	0	1	3	7	31	....
P_k :	-625	181	-82	17	-14	....
				↑↑↑ $k' k_0 k^*$		

$k' = k_0 = k^*$

$\alpha = 181 \in \mathbb{Q}_5$, $\frac{\alpha_5}{p^5} = \frac{181}{3125} = [0, 17, 3, 1, \cdots]$

R_k :	1	0	1	3	4	....
Q_k :	0	1	17	52	69	....
P_k :	-3125	181	-48	37	-11	....
			↑↑ $k' k_0$	↑ k^*		

$k' = k_0 = k^* - 1$

$\alpha = 382 \in \mathbb{Q}_5$, $\frac{\alpha_7}{p^7} = \frac{382}{78125} = [0, 204, 1, 1, \cdots]$

R_k :	1	0	1	1	2	....
Q_k :	0	1	204	205	409	....
P_k :	-78125	382	-197	185	-12	....
			↑ k'	↑ k_0	↑ k^*	

$k'+1 = k_0 = k^* - 1.$

We gaan nu onderzoeken of algorithme 6.3. beste benaderingen geeft. Dit blijkt inderdaad het geval te zijn.

lemma 6.6. (i) Zij $\alpha \in \mathbb{Q}_p$ geheel, $m \geq 1$ en $m \geq 3$ als $p=2$.
Zij (P, Q) een m-e orde bijna-beste benadering van α, $Q>0$. Dan geldt: $Q_{k'} \leq Q \leq Q_{k'+1}$.

(ii) Als bovendien geldt: $Q_{k'} < Q < Q_{k'+1}$, dan geldt:
$\max(|P_{k'}|, Q_{k'}) = |P_{k'}| = |P| = \max(|P|, Q)$.

bewijs: (i) Omdat (P, Q) m-e orde bijna-beste benadering van α is, geldt: $Q = \max(|P|, Q) \leq \max(|P_{k'+1}|, Q_{k'+1}) = Q_{k'+1}$.
Stel $Q < Q_{k'}$. Omdat $\frac{R_{k'}}{Q_{k'}}$ een veelbeste benaderingsbreuk van $\frac{\alpha_m}{p^m}$ is, geldt, met $R = Q\frac{\alpha_m}{p^m} - \frac{P}{p^m}$,
$|Q\frac{\alpha_m}{p^m} - R| > |Q_{k'}\frac{\alpha_m}{p^m} - R_{k'}| \Rightarrow$
$\Rightarrow |P| > |P_{k'}| = \max(|P_{k'}|, Q_{k'}) \geq \max(|P|, Q)$,
en dat is een tegenspraak.

(ii) Er is geen convergent $\frac{R'}{Q'}$ van $\frac{\alpha_m}{p^m}$ met $Q_{k'} < Q' < Q_{k'+1}$, dus moet $|Q\frac{\alpha_m}{p^m} - R| \geq |Q_{k'}\frac{\alpha_m}{p^m} - R_{k'}| \Rightarrow$
$\Rightarrow |P| \geq |P_{k'}| = \max(|P_{k'}|, Q_{k'}) \geq \max(|P|, |Q|)$,
er moeten dus gelijk tekens gelden. qed.

lemma 6.7. (i) Zij $\alpha \in \mathbb{Q}_p$ met $|\alpha|_p = p^{-\frac{1}{2}m}$, m even, $m \geq 4$ als $p=2$.
Dan geldt: $|P_{k^*-1}| = Q_{k^*} = p^{\frac{1}{2}m}$, en $k^* = N$.

(ii) Zij $\alpha \in \mathbb{Q}_p$ **geheel**, en $m \geq 1$, $m \geq 3$ als $p=2$.
Stel er zijn twee verschillende m-e orde bijna-beste benaderingen (P, Q) met $Q > 0$.
Dan zijn deze twee gelijk aan $(P_{k'}, Q_{k'})$ en $(P_{k'+1}, Q_{k'+1})$.

Dit lemma laat zien wat er gebeurt als er minstens twee verschillende m-e orde bijna-beste benaderingen zijn: (i) gaat over type III, en (ii) behandelt type VI en VI* (vgl st. 4.6.).

bewijs: (i) $\frac{R_N}{Q_N} = \frac{\alpha_m}{p^m}$ omdat $\frac{R_M}{Q_N}$ de laatste convergent is van $\frac{\alpha_m}{p^m}$. Schrijf $\alpha_m = \alpha_m^* p^{im}$, dan $p \nmid \alpha_m^*$, en omdat $ggd(R_N, Q_N) = 1$, volgt $R_N = \alpha_m^*$ en $Q_N = p^{im}$, en ook $k^* = N$.

Omdat het kettingbreukalgorithme in essentie het euclidische ggd-algorithme is, is
$$P_{N-1} = \alpha_m Q_{N-1} - p^m R_{N-1} = \pm ggd(\alpha_m, p^m) = \pm p^{im}.$$

(ii) Laat (M, X) en (Y, M) met $0 < |X| < M$ en $0 < |Y| < M$ de twee m-e orde bijna-beste benaderingen van α zijn. Volgens lemma 6.6. (i) geldt: $Q_{k'} \leq |X| < M \leq Q_{k'+1}$.

Stel $Q_{k'} < |X| < Q_{k'+1}$, dan is volgens lemma 6.6. (ii) $M = |P_{k'}|$. Dat betekent echter dat $(P_{k'}, Q_{k'})$ ook een m-e orde bijna-beste benadering is, en dat is een tegenspraak. Dus $(M, X) = \pm(P_{k'}, Q_{k'})$.

Stel $Q_{k'} < M < Q_{k'+1}$, dan is volgens lemma 6.6. (ii) $|Y| = |P_{k'}|$. We zagen zojuist echter dat $|P_{k'}| = M$, in tegenspraak met $|Y| < M$. Dus:
$(Y, M) = (P_{k'+1}, Q_{k'+1})$. qed.

Nu zijn we klaar voor drie belangrijke stellingen:

Stelling 6.8. Zij $\alpha \in \mathbb{Q}_p$ geheel, en $m \geq 1$, met $m \geq 3$ als $p=2$. Zij (P,Q) een m-e orde bijna-beste benadering van α. Dan geldt:

$$(*)\begin{cases} \text{als } |\alpha|_p \neq p^{-\frac{1}{2}m}, \text{ dan is er een } k \text{ zodat } (P,Q)=(P_k,Q_k). \\ \text{als } |\alpha|_p = p^{-\frac{1}{2}m}, \text{ dan is } (P,Q) \text{ gelijk aan één van} \\ \quad (P_{k^*-1}, Q_{k^*-1}),\ (P_{k^*}, Q_{k^*}),\ (P_{k^*}-P_{k^*-1},\ Q_{k^*}-Q_{k^*-1}). \end{cases}$$

Stelling 6.9. Zij $\alpha \in \mathbb{Q}_p$ geheel, en $m \geq 1$, met $m \geq 3$ als $p=2$. Zij (P,Q) een beste benadering van α met $|Q\alpha - P|_p = p^{-m}$. Dan geldt $(*)$ voor (P,Q).

Stelling 6.10. Zij $\alpha \in \mathbb{Q}_p$ geheel, en $m \in \mathbb{N}$. Zij (P,Q) de benadering van α die m.b.v. algorithme 6.3. gevonden wordt. Dan is (P,Q) een beste benadering van α.

bewijzen: 6.8.: als $|\alpha|_p = p^{-\frac{1}{2}m}$, dan hebben we volgens stelling 4.7. type III, volgens lemma 6.7 (i) geldt $Q_{k^*-1} < Q_{k^*} = p^{\frac{1}{2}m} = |P_{k^*-1}|$ en $P_{k^*} = 0$, en dus $k' = k^*-1$. Volgens lemma 6.6. (i) geldt $Q_{k'} \leq Q \leq Q_{k'+1}$. Als $Q = Q_{k'}$ of $Q = Q_{k'+1}$, dan is $P = P_{k'}$ resp. $P = P_{k'+1}$; als $Q_{k'} < Q < Q_{k'+1}$, dan is volgens lemma 6.6. (ii) $|P| = |P_{k'}| = p^{\frac{1}{2}m}$, en dan moet $Q = Q_{k'+1} - Q_{k'}$.

Als $|\alpha|_p \neq p^{-\frac{1}{2}m}$ dan zijn er volgens stelling 4.7. hoogstt 2 m-e orde bijna-beste benaderingen. Als er 2 zijn, kunnen we lemma 6.7. (ii) toepassen. Stel (P,Q) is de enige, en $Q_{k'} < Q < Q_{k'+1}$.

Volgens lemma 6.6 (ii) is dan $\max(|P|, |Q|) = \max(|P_{k'}|, Q_{k'})$, in tegenspraak met de veronderstelling dat (P,Q) de enige m-e orde bijna-beste benadering van α is. qed.

6.9.: volgt zonder meer uit stelling 6.8.

6.10.: als $p^m = 2^l$, en $|\alpha|_2 < 1$, dan is $\alpha_1 = 0$, en $(P,Q) = (0,1)$. Dat is duidelijk de beste.

als $p^m = 2^l$, en $|\alpha|_2 = 1$, dan is $\alpha_1 = 1$. Direkt is in te zien dat de beste benadering één van $(1,1)$ en $(-1,1)$ is.

als $p^m = 2^l$, en $\alpha_2 = 0, 1$ of 3, is (P,Q) resp. $(0,1)$, $(1,1)$ en $(-1,1)$, inderdaad allen beste benaderingen. Als $\alpha_2 = 2$, moeten we de beste zoeken onder $(2,1)$, $(-2,1)$, $(0,2)$. Omdat $|\alpha|_p = p^{-\frac{l}{m}}$ in dit geval, zoekt het algorithme 6.3. uit (P_{k^*-1}, Q_{k^*-1}), (P_{k^*}, Q_{k^*}) en $(P_{k^*} - P_{k^*-1}, Q_{k^*} - Q_{k^*-1})$, en dat zijn precies $(2,1)$, $(0,2)$ resp. $(-2,1)$.

als $p^m \neq 2$, $p^m \neq 4$ laat stelling 6.9. zien dat algorithme 6.3. altijd een beste benadering tegenkomt. qed.

We constateren dat het aangepaste algorithme van Mahler, 6.3, precies doet wat we willen: het vindt beste benaderingen, volgens st. 6.10, en het vindt alle beste benaderingen, volgens st. 6.9.

Voorbeelden:

$\alpha = 375 \in \mathbb{Q}_5$, $m=4$: $\frac{\alpha_4}{5^4} = \frac{375}{625} = \frac{3}{5} = [0,1,1,2]$

R_k:	1	0	1	1	3
Q_k:	0	1	1	2	5

$Q_N = 5 < p^{\frac{1}{2}m} = 25$

$\Rightarrow (P, Q) = (0, 5)$.

$\alpha = 181 \in \mathbb{Q}_5$, $m=5$:

R_k:	1	0	1	3	4	...
Q_k:	0	1	17	52	69	....

$Q_{k^*} = 52$, $P_{k^*-1} = -48$, $P_{k^*} = 37$,

$k_0 = k^*-1$, en $(P, Q) = (-48, 17)$.

$\alpha = 60 \in \mathbb{Q}_7$, $m=3$: $\frac{\alpha_3}{7^3} = \frac{60}{343} = [0,5,1,2,1,1,0]$

R_k:	1	0	1	1	3	4	...
Q_k:	0	1	5	6	17	23	...

$Q_{k^*} = 23$, $P_{k^*-1} = 17$, $P_{k^*} = -9$, dus we moeten kiezen uit $(17, 6)$ en $(-9, 17)$

Er geldt: $|6 \cdot 60 - 17|_7 = |17 \cdot 60 + 9|_7 = 7^{-3}$, dus het maakt niet uit welke we kiezen.

$\alpha = 341 \in \mathbb{Q}_5$, $m=3$: $\frac{\alpha_3}{5^3} = \frac{91}{125} = [0,1,2,1,2,11]$

R_k:	1	0	1	2	3	8	91
Q_k:	0	1	1	3	4	11	125

$Q_{k^*} = 11$, $(P_{k^*-1}, Q_{k^*-1}) = (-11, 4)$; $(P_{k^*}, Q_{k^*}) = (1, 11)$

Nu maakt het wel uit welke we kiezen:

immers $|4 \cdot 341 + 11|_5 = 5^{-3}$, terwijl $|11 \cdot 341 - 1|_5 = 5^{-4}$.

Dus $(P, Q) = (1, 11)$.

$\alpha = 637 \in \mathbb{Q}_7$, $m=4$: nu is $|\alpha|_p = p^{-\frac{1}{2}m}$.

$\frac{\alpha_4}{7^4} = \frac{637}{2401} = \frac{13}{49} = [0,3,1,3,3]$

R_k:	1	0	1	1	4	13
Q_k:	0	1	3	4	15	49

$(P_{k^*-1}, Q_{k^*-1}) = (-49, 15)$, $(P_{k^*}, Q_{k^*}) = (0, 49)$,
en nu moeten we ook $(P_{k^*} - P_{k^*-1}, Q_{k^*} - Q_{k^*-1}) = (49, 34)$
meenemen: voor alle drie geldt $|Q\alpha - P|_p = 7^{-4}$.

$\alpha = 413 \in \mathbb{Q}_7$, $m=2$: $\frac{\alpha_2}{7^2} = \frac{21}{49} = \frac{3}{7} = [0,2,3]$

R_k:	1	0	1	3
Q_k:	0	1	2	7

$(P_{k^*-1}, Q_{k^*-1}) = (-7, 2)$, $(P_{k^*}, Q_{k^*}) = (0, 7)$ en
$(P_{k^*} - P_{k^*-1}, Q_{k^*} - Q_{k^*-1}) = (7, 5)$
Er geldt: $|2 \cdot 413 + 7|_7 = |7 \cdot 413 - 0|_7 = 7^{-2}$, $|5 \cdot 413 - 7|_7 = 7^{-3}$.
dus $(P, Q) = (7, 5)$.

$\alpha = 339 \in \mathbb{Q}_5$, $m=5$: $\frac{\alpha_5}{5^5} = \frac{339}{3125} = [0,9,4,1,1,2,1,1,2,2]$

R_k:	1	0	1	5	6	11 ⋯
Q_k:	0	1	9	37	46	83 ⋯

$(P_{k^*}, Q_{k^*}) = (-31, 46)$, $|46 \cdot 339 + 31|_5 = 5^{-6}$
$(P_{k^*-1}, Q_{k^*-1}) = (43, 37)$, $|37 \cdot 339 - 43|_5 = 5^{-5}$
dus $(P, Q) = (43, 37)$, hoewel $(-31, 46)$ 5-adisch dichter bij α ligt. Met $m=6$ levert het algorithme $(-31, 46)$ op.

Met behulp van algorithme 6.3. kunnen we een benadering van α, (P_m, Q_m) vinden met $|Q_m \alpha - P_m|_p \leq p^{-m}$ en $\max(|P_m|, |Q_m|) \leq p^{\frac{1}{2}m}$ voor iedere $m \in \mathbb{N}$. We definieren $(P_{-1}, Q_{-1}) = (1, 0)$ en $(P_0, Q_0) = (0, 1)$.

Als $\alpha \in \mathbb{Q}_p \cap \mathbb{Q}$, dan kunnen we m zo groot kiezen, dat $\max(|t|, |n|) \leq p^{\frac{1}{2}m}$ met $\alpha = \frac{t}{n}$, $t, n \in \mathbb{Z}$. Algorithme 6.3. zal voor deze m, en voor alle m die groter zijn, dan $(P_m, Q_m) = (t, n)$ geven.

Voorbeeld: $\alpha = 181 \in \mathbb{Q}_7$

m:	-1	0	1	2	3	4	5	6	7	...
P_m:	1	0	-1	4	-10	37	26	181	181	....
Q_m:	0	1	1	3	17	40	93	1	1	....

Met zo een rij benaderingen kunnen we een kettingbreuk van α maken, op dezelfde manier als in algorithme 5.11. gebeurt. Daarvoor is het nodig dat voor $m = 0, 1, 2, \ldots$ geldt: $\Delta_m = P_{m-1} Q_m - P_m Q_{m-1} \neq 0$. Er geldt: $\Delta_m = 0$ dan en slechts dan als (P_m, Q_m) een veelvoud is van (P_{m-1}, Q_{m-1}). Bij voorbeeld, als $\alpha \in \mathbb{Q}_p \cap \mathbb{Q}$, zal $\Delta_m = 0$ voor m groot genoeg (bij $\alpha = 181 \in \mathbb{Q}_7$ voor $m \geq 7$).

Voorbeeld: $\alpha = 337 \in \mathbb{Q}_5$

m:	-1	0	1	2	3	4	5	6	7	8	9	...
P_m:	1	0	-1	-1	-5	6	-31	91	59	337	337	...
Q_m:	0	1	2	2	10	13	37	93	232	1	1	...
Δ_m:		1	1	0	0	-125	625	-6250	15625	-78125	0	...

We laten nu uit de rij $\{(P_m, Q_m)\}$ die benaderingen weg waarvoor $\Delta_m = 0$, en we hernummeren de rest zodat

de indices aansluiten, en we berekenen de nieuwe Δ_m.
In ons voorbeeld $\alpha = 337 \in \mathbb{Q}_5$ krijgen we zo:

m:	-1	0	1	2	3	4	5	6
P_m:	1	0	-1	6	-31	91	59	337
Q_m:	0	1	2	13	37	93	232	1
Δ_m:	$-$	1	1	-25	625	-6250	15625	-78125

Mocht $\text{ggd}(P_m, Q_m) \neq 1$, dan kunnen we de ggd nog wegdelen.
Als $\alpha \in \mathbb{Q}_p \cap \mathbb{Q}$ is de rij benaderingen $\{(P_m, Q_m)\}$ nu eindig geworden, en als $\alpha \notin \mathbb{Q}$, oneindig lang. Altijd geldt: $\Delta_m \neq 0$.
Met het volgende algorithme kunnen we uit zo'n rij een kettingbreuk maken:

<u>Algorithme 6.11.</u>

i) zet $m = 0$ en $\Delta_0 = 1$

ii) bereken $\Delta_{m+1} = P_m Q_{m+1} - P_{m+1} Q_m$
als het teken van Δ_{m+1} $(-1)^{m+1}$ is,
zet dan $P_m = -P_m$, $Q_m = -Q_m$, $\Delta_m = -\Delta_m$.

iii) bereken $\delta_m = P_{m-1} Q_{m+1} - P_{m+1} Q_{m-1}$,
$a_m = -\dfrac{\Delta_{m+1}}{\Delta_m}$ en $b_m = \dfrac{\delta_m}{\Delta_m}$

iv) zet $m = m+1$; als (P_m, Q_m) bestaat, ga dan naar ii), anders stop.

<u>Stelling 6.12.</u> (i) $a_m > 0$ en $\text{ord}_p(a_m) \geq 1$ voor $m \geq 1$.

(ii) $\alpha = \dfrac{a_0|}{|b_0} + \dfrac{a_1|}{|b_1} + \dfrac{a_2|}{|b_2} + \cdots$

bewijs : (i) Omdat het teken van Δ_m teken is $(-1)^m$ is, is het teken van a_m : $-\frac{(-1)^{m+1}}{(-1)^m} = +1$, dus $a_m > 0$.

Zij $m_1, m_2 \in \mathbb{Z}$ zo dat $|Q_{m-2}\alpha - P_{m-2}|_p = p^{-m_2}$ en $|Q_{m-1}\alpha - P_{m-1}|_p = p^{-m_1}$. Dan : $m_2 < m_1$.
Er geldt : $\Delta_{m-1} = Q_{m-2}(Q_{m-1}\alpha - P_{m-1}) - Q_{m-1}(Q_{m-2}\alpha - P_{m-2})$,
dus $p^{m_2} \mid \Delta_{m-1}$, en $p^{m_2+1} \mid \Delta_{m-1}$ alleen als $p \mid Q_{m-1}$
Maar als $p \mid Q_{m-1}$, dan volgt $p \mid P_{m-1}$, in tegenspraak met $\text{ggd}(P_{m-1}, Q_{m-1}) = 1$.
Dus : $\text{ord}_p(\Delta_{m-1}) = m_2$, en analoog volgt :
$\text{ord}_p(\Delta_m) = m_1$.
Dan : $\text{ord}_p(a_m) = m_1 - m_2 \geq 1$.
(ii) triviaal. qed.

Voorbeeld : $\alpha = 337 \in \mathbb{Q}_5$

m	-1	0	1	2	3	4	5	6
P_m	1	0	1	6	31	91	-59	337
Q_m	0	1	-2	13	-37	93	-232	1
Δ_m	-	1	-1	5^2	-5^3	$2\cdot5^4$	$\cdot -5^5$	5^6
δ_m	-	-2	-6	5^2	-5^3	$-3\cdot5^4$	$-2\cdot5^5$	-
a_m	-	1	25	25	10	$5/2$	5	-
b_m	-	-2	6	1	1	$-3/2$	2	-

dus $337 = \left[\frac{1}{-2}\right] + \left[\frac{25}{6}\right] + \left[\frac{25}{1}\right] + \left[\frac{10}{1}\right] + \left[\frac{5/2}{-3/2}\right] + \left[\frac{5}{2}\right]$.
De 'tellers' kunnen weggewerkt worden :

$$337 = \left[0, -2, \frac{6}{25}, 1, \frac{1}{10}, -6, \frac{1}{10}\right].$$

HOOFDSTUK 7 : EEN CRITERIUM VOOR BESTE BENADERINGEN.

Voordat we in hoofdstuk 8 een nieuw algoritme presenteren om beste benaderingen te vinden van p-adische getallen, behandelen we eerst een criterium voor p-adische beste benaderingen. We beschouwen in dit hoofdstuk slechts beste benaderingen t.a.v. de vierkante norm.
In het reële geval geldt : $\frac{p}{q}$ is een beste benadering van $x \in \mathbb{R}$ als $|x - \frac{p}{q}| < \frac{1}{2q^2}$. (stelling 3.10.)
Een analoog resultaat geldt voor p-adische benaderingen.

<u>Stelling 7.1.</u> Zij $\alpha \in \mathbb{Q}_p$, gehéél. Zij (P, Q) een benadering van α met ggd (P, Q) een macht van p, zodat $0 \neq |Q\alpha - P|_p < \frac{1}{2 \cdot \max(|P|, |Q|)^2}$.

Dan is (P, Q) een beste benadering van α.

<u>bewijs</u> : Zij $m \in \mathbb{Z}$ gegeven door $|Q\alpha - P|_p = p^{-m}$.

Er geldt : $|Q\alpha - P|_p < \frac{1}{2 \cdot \max(|P|, |Q|)^2} \iff \max(|P|, |Q|) < \frac{p^{\frac{1}{2}m}}{\sqrt{2}}$.

Zij (P', Q') een benadering van α met $|Q'\alpha - P'|_p \leq p^{-m}$ en ggd (P', Q') een macht van p.

Als $PQ' = P'Q$, dan is $(P, Q) = p^k (P', Q')$ voor zekere $k \in \mathbb{Z}$.

Omdat dan $p^{-m} \geq |Q'\alpha - P'|_p = p^k \cdot |Q\alpha - P|_p = p^{k-m}$, is $k \leq 0$, en $\max(|P'|, |Q'|) \geq \max(|P|, |Q|)$.

Gelijkheid treedt alleen op als $k = 0$, maar dan is $(P, Q) = (P', Q')$.

Stel $P'Q \neq PQ'$; er volgt uit $p^m \mid Q\alpha - P$ en $p^m \mid Q'\alpha - P'$ dat $p^m \mid Q'(Q\alpha - P) - Q(Q'\alpha - P') = QP' - Q'P$, en dus $p^m \leq |QP' - Q'P| \leq |Q| \cdot |P'| + |Q'| \cdot |P| \Rightarrow$

$$\Rightarrow p^m \leq 2 \cdot \max(|P|, |Q|) \cdot \max(|P'|, |Q'|).$$

Dan volgt: $\max(|P'|, |Q'|) \geqslant \dfrac{p^m}{2 \max(|P|, |Q|)}$,

en omdat $\dfrac{p^{\frac{1}{2}m}}{\sqrt{2}} > \max(|P|, |Q|)$, krijgen we

$$\max(|P'|, |Q'|) > \max(|P|, |Q|).$$

Samenvattend: voor iedere breuk (P', Q') met $|Q'\alpha - P'|_p \leq |Q\alpha - P|_p$ geldt $\max(|P'|, |Q'|) > \max(|P|, |Q|)$, tenzij $(P', Q') = (P, Q)$. Maar dan is (P, Q) een beste benadering van α. qed.

Lang niet alle beste benaderingen voldoen aan het criterium $|Q\alpha - P|_p < \dfrac{1}{2 \cdot \max(|P|, |Q|)^2}$, wel aan $|Q\alpha - P|_p \leq \dfrac{1}{\max(|P|, |Q|)^2}$, zie st. 4.4.

Voor $\alpha = |01| \in \mathbb{Q}_5$ bijvoorbeeld hebben we de volgende beste benaderingen:

(P, Q)	$\lvert Q\alpha - P\rvert_p$	$\lvert Q\alpha - P\rvert_p \cdot \max(\lvert P\rvert, \lvert Q\rvert)^2$	
$(1, 1)$	5^{-1}	0,20	
$(-1, 4)$	5^{-2}	0,64	*
$(4, 9)$	5^{-3}	0,65	*
$(17, 7)$	5^{-4}	0,46	
$(-48, 17)$	5^{-5}	0,74	*
$(-59, 86)$	5^{-6}	0,47	
$(101, 1)$	0	0	

* betekent: $|Q\alpha - P|_p \geqslant \dfrac{1}{2 \max(|P|, |Q|)^2}$.

Wel is stelling 7.1. scherp in deze zin, dat er geen $c < 2$ bestaat zodat geldt

$$|Q\alpha - P|_p < \frac{1}{c \cdot \max(|P|, |Q|)^2} \Rightarrow (P, Q) \text{ is beste benadering van } \alpha.$$

We zullen dat aantonen door een rij $\{\alpha_n\} \subset \mathbb{Q}_p$ te construeren, met een rij benaderingen $\{(P_n, Q_n)\}$, zodat (P_n, Q_n) géén beste benadering is van α_n, en toch

$$\lim_{n \to \infty} |Q_n \alpha_n - P_n|_p \cdot \max(|P_n|^2, |Q_n|^2) = \tfrac{1}{2}.$$

Als $p = 2$ kunnen we $\alpha_n = 2^n - 1 \in \mathbb{Q}_2$ kiezen, $n = 1, 2, 3, \ldots$.
We gaan algorithme 6.3. toepassen met $m = 2n - 1$.
We moeten de kettingbreuk van $\frac{2^n - 1}{2^{2n-1}}$ uitrekenen, deze blijkt te zijn:

$$\frac{2^n - 1}{2^{2n-1}} = [0, 2^{n-1}, 1, 1, 2^{n-1} - 1]$$

(bv. voor $n = 7$: $\frac{127}{8192} = [0, 64, 1, 1, 63]$.).

We vinden als benaderingen:

R_k:	1	0	1	1	2
Q_k:	0	1	2^{n-1}	$2^{n-1}+1$	$2^n+1 > 2^{n-\frac{1}{2}} = p^{\frac{1}{2}m}$
P_k:			-2^{n-1}	$2^{n-1}-1$	

Er blijkt: $(-2^{n-1}, 2^{n-1})$ is een beste benadering;
$(P_n, Q_n) = (2^{n-1} - 1, 2^{n-1} + 1)$ is géén beste benadering.

We vinden nu:

$$|Q_n\alpha_n - P_n|_p \cdot \max(|P_n|, |Q_n|)^2 = |(2^{n-1}+1)(2^n-1) - (2^{n-1}-1)|_2 \cdot (2^{n-1}+1)^2$$
$$= 2^{-(2n-1)} \cdot (2^{n-1}+1)^2 =$$
$$= \frac{1}{2} + \frac{1}{2^{n-1}} + \frac{1}{2^{2n-1}},$$

en dus $\lim_{n\to\infty} |Q_n\alpha_n - P_n|_p \cdot \max(|P_n|, |Q_n|)^2 = \frac{1}{2}$.

(bv. voor $n=7$ is $\alpha_n = 127$, $(P_n, Q_n) = (63, 65)$ en
$|65 \cdot 127 - 63|_2 \cdot \max(63, 65)^2 = \frac{1}{1,939}$).

Met $p=2$ zijn meer van zulke rijtjes te vinden, bv.
$\alpha_n = 2^n + 1$, $(P_n, Q_n) = (-2^{n-1}-1, 2^{n-1}-1)$ is geen beste benadering van α_n, en
$|Q_n\alpha_n - P_n|_p \cdot \max(|P_n|, |Q_n|)^2 = \frac{1}{2} + \frac{1}{2^{n-1}} + \frac{1}{2^{2n-1}}$.
(bv. voor $n=7$ is $\alpha_n = 129$, $(P_n, Q_n) = (-65, 63)$, en
$|63 \cdot 129 + 65|_2 \cdot \max(63, 65)^2 = \frac{1}{1,939}$).

Of: $\alpha_n = 2^n - 3$, $(P_n, Q_n) = (-2^{n-1}-3, 2^{n-1}+1)$ is geen beste benadering van α_n, en
$|Q_n\alpha_n - P_n|_p \cdot \max(|P_n|, |Q_n|)^2 = \frac{1}{2} + \frac{3}{2^{n-1}} + \frac{9}{2^{2n-1}}$.
($n=7$: $\alpha_7 = 125$, $(P_7, Q_7) = (-67, 65)$, en
$|65 \cdot 125 + 67|_2 \cdot \max(67, 65) = \frac{1}{1,825}$).

Voor $p \geq 3$ heb ik niet zulke simpele rijtjes kunnen vinden. We gaan daarom in dat geval wat anders te werk.

We zoeken P, Q, α met $|Q\alpha - P|_p = p^{-m}$ en
$p^{-m} \cdot \max(|P|, |Q|)^2 \approx \frac{1}{2}$, en (P, Q) géén beste benadering van α.

Stel we hebben $Q\alpha - P = p^m$, dan ook $(Q+1)\alpha - (P+\alpha) = p^m$.
Als we nu $\alpha \in \mathbb{Z} \cap \mathbb{Q}_p$ kiezen, en P zo dat $|P| \approx |P+\alpha|$, ofwel $P \approx -\frac{1}{2}\alpha$, dan hebben we twee benaderingen van α, nl. (P, Q) en $(P+\alpha, Q+1)$, met $\max(|P|, |Q|) \approx$ $\approx \max(|P+\alpha|, |Q+1|)$. Eén van deze twee zal dan geen beste benadering zijn in het algemeen.
Het ligt voor de hand om $|P| \approx |Q|$ te kiezen.
De voorwaarde $\max(|P|, |Q|)^2 \approx \frac{1}{2} p^m$ leidt dan tot
$\alpha \approx \sqrt{2} \cdot p^{\frac{1}{2}m}$, $P \approx -\frac{1}{2}\sqrt{2} \cdot p^{\frac{1}{2}m}$, $Q \approx \frac{1}{2}\sqrt{2}\, p^{\frac{1}{2}m}$.

Bijvoorbeeld: $p=5$, $m=9$ geeft $\sqrt{2} \cdot p^{\frac{1}{2}m} = 1976{,}42\cdots$.
Met $\alpha = 1976$ kunnen we kiezen $(P, Q) = (-837, 909)$ en $(P+\alpha, Q+1) = (1139, 909)$. Dan weten we dat $(1139, 909)$ geen beste benadering is van $1976 \in \mathbb{Q}_5$, en we vinden $|909 \cdot 1976 - 1139|_5 \cdot 1139^2 = \frac{1139^2}{5^9} = \frac{1}{1{,}506}$.

Met $\alpha' = \alpha - 2 = 1974$ en $Q' = Q + 1 = 909$ vinden we
$P' = Q'\alpha' - p^m = 909 \cdot 1974 - 5^9 = -839$, dus
$(P', Q') = (-839, 909)$ en $(P'+\alpha', Q'+1) = (1135, 990)$.
Ook $(1135, 990)$ is dus geen beste benadering, en
$|990 \cdot 1974 - 1135|_5 \cdot 1135^2 = \frac{1135^2}{5^9} = \frac{1}{1{,}516}$, al iets beter.
We kunnen op deze manier verder gaan:
De volgende tabel geeft voor gegeven α en Q de bijbehorende P zodat $Q\alpha - P = p^m$. De tabel is gebaseerd op de observaties dat als $Q\alpha - P = p^m$, dan ook
$(Q+1)\alpha - (P+\alpha) = p^m$ en $Q(\alpha-1) - (P-Q) = p^m$.

$\downarrow Q$ $\xrightarrow{\alpha}$	1970	1971	1972	1973	1974	1975	1976	1977
987								-1826
988						-1825	-837	151
989				-1828	-839	150	1139	
990		-1835	-845	145	1135			
991	-855	136	1127					
992	1115							

Als we de tabel naar linksonder voortzetten, vinden we:

$\downarrow Q$ $\xrightarrow{\alpha}$	1959	1960
996	-1961	-965
997	-2	995

We zien dat $(995, 997)$ geen beste benadering is van $1960 \in \mathbb{Q}_5$, immers $(-965, 996)$ is wel iets beter.
En: $|997 \cdot 1960 - 995|_5 \cdot 997^2 = \frac{997^2}{59} = \frac{1}{1{,}965}$

Op eenzelfde manier kunnen we voor iedere $p \geq 3$ en $m \geq 3$, een α, P, Q vinden, zodat $|Q\alpha - P|_p = p^{-m}$, (P, Q) is geen beste benadering van α, en $|Q\alpha - P|_p \cdot \max(|P|, |Q|) \to \frac{1}{2}$ als $m \to \infty$. Zij dus $p \geq 3$ priem, en $m \geq 3$.

<u>Algorithme 7.2.</u>

i) bereken $\alpha_0^* = [\sqrt{2} \cdot p^{\frac{1}{2}m}]$, $Q_0^* = [p^m / \alpha_0^*]$ en $P_0^* = Q_0^* \alpha_0^* - p^m$.

ii) bereken $P_0' = P_0^* + \alpha_0^*$, $Q_0' = Q_0^* + 1$

iii) als $P_0' \geq Q_0'$, zet dan $P_0 = P_0'$, $Q_0 = Q_0'$, $\alpha_0 = \alpha_0^*$

als $P_0' \leq Q_0' - 1$, zet dan $P_0 = P_0' + Q_0'$,
$Q_0 = Q_0'$, $\alpha_0 = \alpha_0^* + 1$.

iv) bereken $P_1 = P_0 - 2Q_0 + \alpha_0 - 2$,
$X_0 = \frac{1}{4}(P_1 - P_0 + 1) + \frac{1}{4}\sqrt{(P_1 - P_0 + 1)^2 + 8(P_0 - Q_0)}$,
en $n_0 \in \mathbb{Z}$ zo dat $X_0 \leq n_0 < X_0 + 1$.

v) bereken $\alpha_{n_0} = \alpha_0 - 2n_0$, $Q_{n_0} = Q_0 + n_0$,
$P_{n_0} = Q_{n_0}\alpha_{n_0} - p^m$.

Stelling 7.3. (i) (P_{n_0}, Q_{n_0}) is geen beste benadering van α_{n_0}.
(ii) $|Q_{n_0}\alpha_{n_0} - P_{n_0}|_p \cdot \max(|P_{n_0}|, |Q_{n_0}|)^2 = \frac{1}{2} + \frac{c}{p^{\frac{1}{4}m}}$,
waarbij c een van p en m onafhankelijke constante is.

Lemma 7.4. Na stap iii) van algoritme 7.2. geldt:
(i) $Q_0\alpha_0 - P_0 = p^m$
(ii) $\frac{1}{2}\sqrt{2}\, p^{\frac{1}{2}m} < Q_0 < \frac{1}{2}\sqrt{2}\, p^{\frac{1}{2}m} + 1{,}58$
(iii) $0 < Q_0 \leq P_0 < \sqrt{2}\, p^{\frac{1}{2}m} + 2{,}16$
(iv) $\sqrt{2}\, p^{\frac{1}{2}m} - 1 < \alpha_0 < \sqrt{2}\, p^{\frac{1}{2}m} + 1$

bewijs: (i) als $P_0' \geq Q_0'$, dan is $Q_0\alpha_0 - P_0 = Q_0'\alpha_0^* - P_0' =$
$= (Q_0^* + 1)\alpha_0^* - (P_0^* + \alpha_0^*) = Q_0^*\alpha_0^* - P_0^* = p^m$;
als $P_0' \leq Q_0' + 1$, dan is $Q_0\alpha_0 - P_0 = Q_0'(\alpha_0^* + 1) - (P_0' + Q_0') =$
$= Q_0'\alpha_0^* - P_0' = p^m$ als boven.

(iv) triviaal

(ii) Uit de definitie van Q_0^* volgt:
$$\frac{p^m}{\alpha_0^*} - 1 < Q_0^* \leq \frac{p^m}{\alpha_0^*}.$$

Omdat $\sqrt{2}\, p^{\frac{1}{2}m} - 1 < \alpha_0^* \leq \sqrt{2}\, p^{\frac{1}{2}m}$, volgt:

$$\tfrac{1}{2}\sqrt{2}\,p^{\frac{1}{2}m} - 1 < Q_0^* < \frac{p^m}{\sqrt{2}\,p^{\frac{1}{2}m}-1} = \tfrac{1}{2}\sqrt{2}\,p^{\frac{1}{2}m} + \frac{\frac{1}{2}\sqrt{2}}{\sqrt{2}-p^{-\frac{1}{2}m}},$$

en omdat $p^{\frac{1}{2}m} \geq 3\sqrt{3}$, volgt $\frac{\frac{1}{2}\sqrt{2}}{\sqrt{2}-p^{-\frac{1}{2}m}} < 0{,}58$.

Uit $Q_0 = Q_0^* + 1$ volgt het gevraagde.

(iii) als $P_0' \geq Q_0'$, dan is $Q_0 = Q_0' \leq P_0' = P_0$, en

$$P_0 = P_0^* + \alpha_0^* = Q_0^*\alpha_0^* - p^m + \alpha_0^* \leq \alpha_0^* \leq \sqrt{2}\,p^{\frac{1}{2}m}.$$

als $P_0' \leq Q_0' - 1$, dan is $P_0 - Q_0 = P_0' + Q_0' - Q_0' = P_0' =$

$$= P_0^* + \alpha_0^* = Q_0^*\alpha_0^* - p^m + \alpha_0^* > 0 \quad \text{(uit def. } Q_0^*\text{)}.$$

en: $P_0 = P_0' + Q_0' \leq 2Q_0' - 1 = 2Q_0 - 1 <$

$$< \sqrt{2}\,p^{\frac{1}{2}m} + 2{,}16$$

ged.

lemma 7.5. Zij, voor $n = 0, 1, 2, 3, \cdots$, $\alpha_n = \alpha_0 - 2n$, $Q_n = Q_0 + n$, en $P_n = Q_n\alpha_n - p^m$. Dit komt overeen met de definities van $P_0, Q_0, \alpha_0, P_1, P_{n_0}, Q_{n_0}, \alpha_{n_0}$ in algorithme 7.2. Verder geldt:

(i) $P_n = P_{n-1} - 2Q_{n-1} + \alpha_{n-1} - 2$

(ii) $P_n = -2n^2 + (P_1 - P_0 + 2)\cdot n + P_0$

(iii) $-6 \leq P_1 - P_0 \leq -2$.

bewijs: dat de definities overeenstemmen is triviaal.

(i) Omdat $Q_n = Q_{n-1} + 1$ en $\alpha_n = \alpha_{n-1} - 2$, is

$$P_n = Q_n\alpha_n - p^m = (Q_{n-1}+1)(\alpha_{n-1}-2) - p^m =$$

$$= Q_{n-1}\alpha_{n-1} - p^m - 2Q_{n-1} + \alpha_{n-1} - 2.$$

(ii) Met inductie: voor $n-1$ is het triviaal;

stel het klopt voor $n-1$, dan:

$$P_n = P_{n-1} - 2Q_{n-1} + \alpha_{n-1} - 2 =$$

$$= -2(n-1)^2 + (P_1 - P_0 + 2)(n-1) + P_0 - 2(Q_0 + n - 1) + \alpha_0 - 2n - 1$$

$$= -2n^2 + (P_1 - P_0 + 2)\cdot n + P_0 + X, \text{ en}$$

$$X = 2n^2 - 2(n-1)^2 - (P_1 - P_0 + 2) - 2(Q_0 + n - 1) + \alpha_0 - 2n - 1 =$$
$$= -P_1 + P_0 - 2Q_0 + \alpha_0 - 2 = 0.$$

(iii) $P_1 - P_0 = -2Q_0 + \alpha_0 - 2$; volgens lemma 7.4. (ii), (iv) :

$P_1 - P_0 < -\sqrt{2}\, p^{\frac{1}{2m}} + \sqrt{2}\, p^{\frac{1}{2m}} + 1 - 2 = -1$, en

$P_1 - P_0 > -\sqrt{2}\, p^{\frac{1}{2m}} - 3{,}16 + \sqrt{2}\, p^{\frac{1}{2m}} - 1 - 2 = -6{,}16$,

dus $-6{,}16 < P_1 - P_0 < -1$, maar $P_1 - P_0 \in \mathbb{Z}$, dus

$-6 \leq P_1 - P_0 \leq -2$. q.e.d.

<u>bewijs</u> van stelling 7.3. :

Zij voor $x \in \mathbb{R}$ $P_x = -2x^2 + (P_1 - P_0 + 2)\cdot x + P_0$ en $Q_x = Q_0 + x$.

Deze definitie stemt overeen met de definitie van P_n en Q_n voor $n \in \mathbb{Z}$.

We gaan oplossen : $P_x = Q_x$, $x > 0$.

$$P_x = Q_x \iff 2x^2 - (P_1 - P_0 + 1)\cdot x - P_0 + Q_0 = 0$$
$$\iff x = \tfrac{1}{4}(P_1 - P_0 + 1) \pm \tfrac{1}{4}\sqrt{(P_1 - P_0 + 1)^2 + 8(P_0 - Q_0)}\,.$$

Omdat $P_0 - Q_0 \geq 0$, zijn er twee reële oplossingen van $P_x = Q_x$, de eis $x > 0$ leidt tot de keuze $x = x_0$, met x_0 als in algoritme 7.2. : $x_0 = \tfrac{1}{4}(P_1 - P_0 + 1) + \tfrac{1}{4}\sqrt{(P_1 - P_0 + 1)^2 + 8(P_0 - Q_0)}$

Het maximum van P_x wordt aangenomen bij $x = \tfrac{1}{4}(P_1 - P_0 + 2) \leq 0$.

Dus, vanwege $x_0 > 0$, is P_x dalend voor $x \geq x_0$, en dus:

$$(1) \qquad P_{n_0} \leq P_{x_0} = Q_{x_0} \leq Q_{n_0}\,.$$

We lossen voorts op : $P_x = 0$, $x > 0$.

$$P_x = 0 \iff 2x^2 - (P_1 - P_0 + 2)\cdot x - P_0 = 0$$
$$\iff x = \tfrac{1}{4}(P_1 - P_0 + 2) \pm \tfrac{1}{4}\sqrt{(P_1 - P_0 + 2)^2 + 8P_0}\,.$$

Er geldt dus :

$P_x > 0$ als $0 \le x < x_1 = \frac{1}{4}(P_1 - P_0 + 2) + \frac{1}{4}\sqrt{(P_1 - P_0 + 2)^2 + 8P_0}$

We willen aantonen: $P_{n_0} > 0$.

Stel $P_{n_0} \le 0$, dan $n_0 \ge x_1$, en er volgt:

$x_0 + 1 > n_0 \ge x_1$, en dus:

$$1 + \frac{1}{4}(P_1 - P_0 + 1) + \frac{1}{4}\sqrt{(P_1 - P_0 + 1)^2 + 8(P_0 - Q_0)} > \frac{1}{4}(P_1 - P_0 + 2) + \frac{1}{4}\sqrt{(P_1 - P_0 + 2)^2 + 8P_0} \Rightarrow$$

$$3 + \sqrt{(P_1 - P_0 + 1)^2 + 8(P_0 - Q_0)} > \sqrt{(P_1 - P_0 + 2)^2 + 8P_0}.$$

Kwadrateren geeft:

$$9 + 6\sqrt{(P_1 - P_0 + 1)^2 + 8(P_0 - Q_0)} + (P_1 - P_0 + 1)^2 + 8(P_0 - Q_0) > (P_1 - P_0 + 2)^2 + 8P_0 \Rightarrow$$

$$6\sqrt{(P_1 - P_0 + 1)^2 + 8(P_0 - Q_0)} \ge 2(P_1 - P_0) + 8Q_0 - 6.$$

Nogmaals kwadrateren:

$$0 > -36(P_1 - P_0 + 1)^2 - 288(P_0 - Q_0) + 4(P_1 - P_0)^2 + 64Q_0^2 + 36 + 32(P_1 - P_0)Q_0 - 24(P_1 - P_0) - 96Q_0 \ge$$

$$\ge -36 \cdot 25 - 288P_0 + 288Q_0 + 16 + 64Q_0^2 + 36 - 192Q_0 + 48 - 96Q_0 =$$

$$= -288P_0 + 64Q_0^2 - 800 > -288\sqrt{2}\,p^{\frac{1}{2}m} + 64 \cdot (\tfrac{1}{2}\sqrt{2}\,p^{\frac{1}{2}m})^2 - 800 \Rightarrow$$

$$\Rightarrow \quad 32p^m - 408p^{\frac{1}{2}m} - 800 < 0$$

$$\Rightarrow \quad p^m < \tfrac{1}{64}(408 + \sqrt{408^2 + 4 \cdot 32 \cdot 800}) < 210$$

$\Rightarrow$ $p^m = 3^3, 3^4$ of 5^3 Ook in deze gevallen geldt echter $P_{n_0} > 0$.

Samen met (1) geeft dit:

(2) $\max(|P_{n_0}|, Q_{n_0}) = Q_{n_0}$.

We gaan vervolgens n_0 afschatten:

Er geldt: $n_0 < x_0 + 1 = 1 + \frac{1}{4}(P_1 - P_0 + 1) + \frac{1}{4}\sqrt{(P_1 - P_0 + 1)^2 + 8(P_0 - Q_0)} <$

$< \frac{3}{4} + \frac{1}{4}\sqrt{25 + 8(P_0 - Q_0)}$, omdat $-6 \leq P_1 - P_0 \leq -2$.

Uit lemma 7.4.: $P_0 - Q_0 < \frac{1}{2}\sqrt{2}\, p^{\frac{1}{2}m} + 2{,}16$, dus

omdat $p^{\frac{1}{2}m} \geq 3\sqrt{3}$, volgt:

$$25 + 8(P_0 - Q_0) < 42{,}28 + 4\sqrt{2}\, p^{\frac{1}{2}m} \leq$$

$$\leq \left(\frac{42{,}28}{3\sqrt{3}} + 4\sqrt{2}\right) p^{\frac{1}{2}m} < 13{,}80\, p^{\frac{1}{2}m}, \quad \text{dus:}$$

(3) $\quad n_0 < 0{,}75 + 0{,}93\, p^{\frac{1}{4}m}$.

Zij $P_{n_0}^* = P_{n_0} - \alpha_{n_0}$ en $Q_{n_0}^* = Q_{n_0} - 1$, dan

$Q_{n_0}^* \alpha_{n_0} - P_{n_0}^* = p^m$.

We willen aantonen dat $(P_{n_0}^*, Q_{n_0}^*)$ een betere benadering van α_{n_0} is dan (P_{n_0}, Q_{n_0}).

Er geldt: $P_{n_0}^* - Q_{n_0}^* = P_{n_0} - \alpha_{n_0} - Q_{n_0} + 1 <$

$< -\alpha_0 + 2n_0 + 1 <$

$< -\sqrt{2}\, p^{\frac{1}{4}m} + 1 + 1{,}50 + 1{,}96\, p^{\frac{1}{4}m} + 1 < 0$

als $p^{\frac{1}{4}m} > \dfrac{1{,}96 + \sqrt{1{,}96^2 + 4 \cdot 1{,}41 \cdot 3{,}50}}{2 \cdot 1{,}41} \iff p^m > 31{,}42$.

De enige uitzondering is $p^m = 3^3$, ook dan is $P_{n_0}^* - Q_{n_0}^* < 0$. Dus:

(4) $\quad P_{n_0}^* < Q_{n_0}^*$

Voorts: $-P_{n_0}^* - Q_{n_0}^* = -P_{n_0} + \alpha_{n_0} - Q_{n_0} + 1 =$

$= \alpha_{n_0} - Q_{n_0} + 1 - P_{n_0-1} + 2Q_{n_0-1} - \alpha_{n_0-1} + 2 =$

$= -P_{n_0-1} + Q_{n_0-1}$.

Als we nu weten dat $P_{n_0-1} > P_{x_0}$, dan volgt:

$$-P_{n_0}^* - Q_{n_0}^* = -P_{n_0-1} + Q_{n_0-1} < -P_{x_0} + Q_{n_0-1} = -Q_{x_0} + Q_{n_0-1} =$$
$$= -x_0 + n_0 - 1 < 0 \quad , \text{ en dus, samen met (4):}$$

(5) $\quad |P_{n_0}^*| < Q_{n_0}^* .$

Welnu, als $x > \frac{1}{4}(P_1 - P_0 + 2)$, dan daalt P_x, dus
als $n_0 - 1 \geq \frac{1}{4}(P_1 - P_0 + 2)$, dan volgt $P_{x_0} < P_{n_0-1}$
uit $x_0 > n_0 - 1$.
Stel $n_0 - 1 < \frac{1}{4}(P_1 - P_0 + 2)$, dan : $n_0 - 1 < 0 \Rightarrow n_0 \leq 0$.
Ook geldt : $n_0 \geq x_0 > 0$, tegenspraak.

We combineren nu (2) en (5) tot :

$$\max(|P_{n_0}^*|, Q_{n_0}^*) < \max(|P_{n_0}|, Q_{n_0})$$

immers : $\max(|P_{n_0}^*|, Q_{n_0}^*) = Q_{n_0}^* = Q_{n_0-1} < Q_{n_0} =$
$= \max(|P_{n_0}|, Q_{n_0})$.
Met andere woorden : (P_{n_0}, Q_{n_0}) is geen beste benadering van α_{n_0}.

Tenslotte : $|Q_{n_0}\alpha_{n_0} - P_{n_0}|_p \cdot \max(|P_{n_0}|, |Q_{n_0}|)^2 =$
$= \frac{1}{p^m} \cdot Q_{n_0}^2$, en, uit (3) en lemma 7.4. :

$$Q_{n_0} = Q_0 + n_0 < \tfrac{1}{2}\sqrt{2}\, p^{\frac{1}{2}m} + 1{,}58 + 0{,}75 + 0{,}93\, p^{\frac{1}{4}m}$$
$$< \tfrac{1}{2}\sqrt{2}\, p^{\frac{1}{2}m} + 1{,}96\, p^{\frac{1}{4}m} \qquad (\text{gebruik } p^m \geq 3^3)$$
$$\Rightarrow Q_{n_0}^2 < \tfrac{1}{2} p^m + 4{,}46\, p^{\frac{3}{4}m}, \text{ en dus}$$

$$|Q_{n_0}\alpha_{n_0} - P_{n_0}|_p \cdot \max(|P_{n_0}|, |Q_{n_0}|)^2 < \tfrac{1}{2} + \frac{4{,}46}{p^{\frac{1}{4}m}} \qquad \text{q.e.d.}$$

We hebben in het voorgaande bewijs de gevallen $p^m = 3^3$, 3^4 en 5^3 apart moeten behandelen. Bij wijze van voorbeeld zijn 3^3 en 5^3 wat verder uitgewerkt:

$p=3$, $m=3$: stap i): $\alpha_0^* = 7$; $(P_0^*, Q_0^*) = (-6, 3)$

ii): $(P_0', Q_0') = (1, 4)$

iii): $\alpha_0 = 8$; $(P_0, Q_0) = (5, 4)$

iv): $P_1 = 3$; $x_0 = 0{,}5$; $n_0 = 1$

v): $\alpha_1 = 6$; $(P_1, Q_1) = (3, 5)$

en: $(P_1^*, Q_1^*) = (-3, 4)$

$p=5$, $m=3$: stap i): $\alpha_0^* = 15$; $(P_0^*, Q_0^*) = (-5, 8)$

ii): $(P_0', Q_0') = (10, 9)$

iii): $\alpha_0 = 15$; $(P_0, Q_0) = (10, 9)$

iv): $P_1 = 5$; $x_0 = 0{,}22$; $n_0 = 1$

v): $\alpha_1 = 13$; $(P_1, Q_1) = (5, 10)$

en: $(P_1^*, Q_1^*) = (-8, 9)$.

Een laatste voorbeeld:

$p = 11$, $m = 7$, $11^7 = 19\,487\,171$, leidt tot $n_0 = 13$, en

$\alpha_{13} = 6217$; $(P_{13}, Q_{13}) = (3124, 3135)$ en

$(P_{13}^*, Q_{13}^*) = (-3093, 3134)$.

Dus: $(3124, 3135)$ is geen beste benadering van $\alpha_{13} = 6217 \in Q_{11}$, maar er geldt wel:

$$|Q_{13}\alpha_{13} - P_{13}|_{11} \cdot \max(|P_{13}|, |Q_{13}|)^2 = \frac{3135^2}{117} = \frac{1}{1{,}983}.$$

HOOFDSTUK 8: EEN ALGORITHME MET BASISREDUKTIE

In hoofdstuk 4 hebben we gezien dat de $(P,Q) \in \mathbb{Z} \times \mathbb{Z}$ met $|Q\alpha - P|_p \leq p^{-m}$ voor zekere m en $\alpha \in \mathbb{Q}_p$, een rooster Γ_m vormen. Een beste benadering van α is een roosterpunt dat het dichtst bij $(0,0)$ ligt, t.o.v. een gegeven norm.
Ieder roosterpunt in Γ_m, dus ook een beste benadering, kan geschreven worden als een $\mathbb{Z}$-lineaire combinatie van twee basis-punten. Omdat een beste benadering het dichtst bij $(0,0)$ ligt, ligt het voor de hand dat er een basis is met die beste benadering als één van de basispunten. Op deze gedachten zijn de algorithmes in dit hoofdstuk gebaseerd.
We gaan dus, gegeven een rooster $\Gamma_m \subset \mathbb{Z} \times \mathbb{Z}$, een basis zoeken van dit rooster, die een beste benadering bevat.
We doen dat door eerst een basis van Γ_m te berekenen, en dan vanuit deze basis een andere basis te berekenen, die voldoet. Deze tweede stap heet 'basisreduktie'.
We zullen eerst twee algorithmes voor basisreduktie geven: één voor de vierkante norm $\Phi(X,Y) = \max(|X|,|Y|)$, en één voor de euclidische norm $\Phi(X,Y) = \sqrt{X^2+Y^2}$.

Zij $\alpha \in \mathbb{Q}_p$ gehéél, $\alpha \neq 0$, en $m \in \mathbb{N}$, $m \geq 0$.
Zij $\Gamma_m = \{(P,Q) \in \mathbb{Z} \times \mathbb{Z} : |Q\alpha - P|_p \leq p^{-m}\}$, het rooster.

Uit stelling 4.2. weten we: $\{(X,Y),(Z,U)\}$ is een basis van Γ_m dan en slechts dan als $XU - YZ = \pm p^m$.

Zij $\{(X,Y),(Z,U)\}$ een basis van Γ_m. Hier volgt dan het basisreduktie algorithme voor de norm $\Phi(X,Y) = \max(|X|,|Y|)$.

Algorithme 8.1. i) als $\max(|X|,|Y|) < \max(|Z|,|U|)$, verwissel dan (X,Y) en (Z,U).

ii) als $Z=0$, zet dan $k = Y/U$
als $U=0$, zet dan $k = X/Z$
als Z en U het zelfde teken hebben,
zet dan $k = \dfrac{X+Y}{Z+U}$

als Z en U verschillend teken hebben,
zet dan $k = \dfrac{X-Y}{Z-U}$.

iii) bereken $(X',Y') = (X,Y) - [k](Z,U)$
$(X'',Y'') = (X,Y) - ([k]+1)(Z,U)$
en zet (X,Y) van deze twee die met de kleinste $\max(|X|,|Y|)$.

iv) als $\max(|X|,|Y|) \geq \max(|Z|,|U|)$, dan stop,
als $\max(|X|,|Y|) < \max(|Z|,|U|)$,
verwissel dan (X,Y) en (Z,U) en ga naar ii).

Voor het gemak zullen we twee punten (X,Y) en (Z,U) nog wel eens weergeven als een matrix: $\begin{pmatrix} X & Y \\ Z & U \end{pmatrix}$.

Stap iii) van algoritme 8.1. komt neer op het vermenigvuldigen van $\begin{pmatrix} X & Y \\ Z & U \end{pmatrix}$ met $T_n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$:

$$T_n \cdot \begin{pmatrix} X & Y \\ Z & U \end{pmatrix} = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} X & Y \\ Z & U \end{pmatrix} = \begin{pmatrix} X+nZ & Y+nU \\ Z & U \end{pmatrix}.$$

met $n = -[k]$ of $n = -[k]-1$.

Stap i) en iv) komen neer op het vermenigvuldigen van $\begin{pmatrix} X & Y \\ Z & U \end{pmatrix}$ met $S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$:

$$S \cdot \begin{pmatrix} X & Y \\ Z & U \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} X & Y \\ Z & U \end{pmatrix} = \begin{pmatrix} Z & U \\ X & Y \end{pmatrix}.$$

Voorbeeld : $(X, Y) = (-1428, 1337)$

$(Z, U) = (-571, 617)$

ii) : $k = \frac{-1428 - 1337}{-571 - 617} = 2,33$

iii) : $(X', Y') = (-1428, 1337) - 2 \cdot (-571, 617) = (-286, 103)$

$(X'', Y'') = (-1428, 1337) - 3 \cdot (-571, 617) = (285, -514)$

dus $(X, Y) = (-286, 103)$

iv) : $(X, Y) = (-571, 617)$

$(Z, U) = (-286, 103)$

ii) : $k = \frac{-571 - 617}{-286 - 103} = 3,05$

iii) : $(X', Y') = (-571, 617) - 3 \cdot (-286, 103) = (287, 308)$

$(X'', Y'') = (-571, 617) - 4 \cdot (-286, 103) = (573, 205)$

dus $(X, Y) = (287, 308)$

iv) : Stop.

lemma 8.2. $\{(X,Y),(Z,U)\}$ blijft gedurende het doorlopen van algorithme 8.1. steeds een basis van Γ_n

bewijs: de determinant $\begin{vmatrix} X & Y \\ Z & U \end{vmatrix}$ blijft steeds gelijk op het teken na, want $-\det(S) = \det(T_n) = 1$. qed.

lemma 8.3. de functie $f(c) = \max(|X+cZ|, |Y+cU|)$ heeft op $\mathbb{R}$ een minimum bij $c = k$, met:

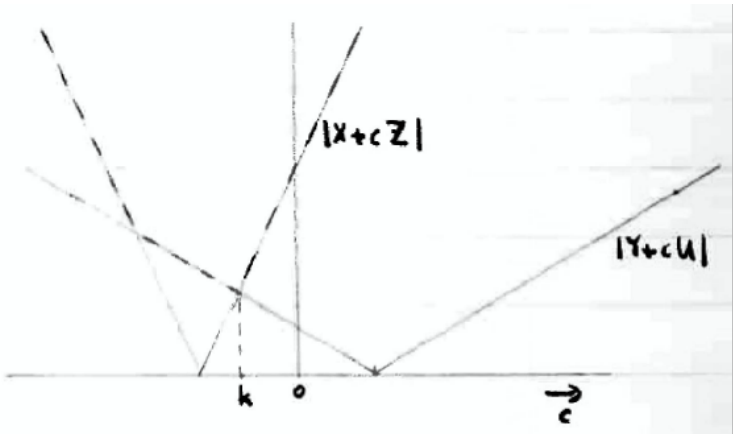
$k = -Y/U$ als $Z = 0, U \neq 0$

$k = -X/Z$ als $U = 0, Z \neq 0$

$k = -\frac{X-Y}{Z-U}$ als Z en U verschillend teken hebben

$k = -\frac{X+Y}{Z+U}$ als Z en U hetzelfde teken hebben.

bewijs: vrijwel triviaal, vergelijk de nevenstaande figuur.



Gevolg: Zij $f(c) = \max(|X+cZ|, |Y+cU|)$ gedefinieerd op $\mathbb{Z}$. Dan bereikt f een minimum bij $c = [k]$ of $c = [k]+1$, met k als in lemma 8.3.

Stelling 8.4. Zij $\{(X',Y'),(Z',U')\}$ een basis van Γ_n. Pas hierop algorithme 8.1. toe, en zij $\{(X,Y),(Z,U)\}$ de uitkomst. Dan is (Z,U) een n-e orde bijna-beste benadering van α, t.a.v. $\Phi(X,Y) = \max(|X|,|Y|)$.

<u>bewijs</u>. Volgens lemma 8.2. is $XU - YZ = \pm p^m$.
Er geldt : $\max(|X|,|Y|) \geq \max(|Z|,|U|)$ volgens stap iv) van algoritme 8.1., en het gevolg op lemma 8.3. leert ons : $\max(|X|,|Y|) \leq \max(|X+cZ|, |Y+cU|)$ $\forall c \in \mathbb{Z}$.
Ik beweer : $\max(|Z|,|U|) \leq p^{\frac{1}{2}m}$. Namelijk :

- als $X = 0$, $Y \neq 0$, dan : $p^m = |YZ| = \max(|X|,|Y|)\cdot|Z| \geq$
$\geq \max(|Z|,|U|)\cdot|Z| \geq |Z|^2 \Rightarrow |Z| \leq p^{\frac{1}{2}m}$.
als $|U| \leq |Z|$ zijn we klaar;
als $|U| > |Z|$, hebben we $|U| \leq |Y| = \max(|X|,|Y|)$;
er is een $k \in \{-1,1\}$ met $|Y+kU| < |Y|$. Dan:
$|Y| = \max(|X|,|Y|) \leq \max(|X+kZ|, |Y+kU|) =$
$= \max(|Z|, |Y+kU|) < |Y|$, tegenspraak.
- als $Y=0$, $X \neq 0$ redeneren we analoog.
- als $Z=0$, $U \neq 0$ en $|U| \leq |X|$, is $p^m = |XU| \geq |U|^2 \Rightarrow |U| \leq p^{\frac{1}{2}m}$;
als $|U| > |X|$, is $|X| < |U| = \max(|Z|,|U|) \leq \max(|X|,|Y|)$
en dus $|Y| = \max(|X|,|Y|)$; er is een $k \in \{-1,1\}$ met
$|Y+kU| < |Y|$, en a volgt : $|Y| = \max(|X|,|Y|) \leq$
$\leq \max(|X+kZ|, |Y+kU|) = \max(|X|, |Y+kU|) < |Y|$, onzin.
- als $U=0$, $Z \neq 0$ redeneren we analoog.
- Zij $XYZU \neq 0$. Zonder beperking kunnen we aannemen : $U \geq Z > 0$;
- als X en Y hetzelfde teken hebben, is er een $k \in \{-1,1\}$ met
$|X+kZ| < \max(|X|,|Z|) \leq \max(|X|,|Y|,|Z|,|U|) = \max(|X|,|Y|)$
én $|Y+kU| < \max(|Y|,|U|) \leq \max(|X|,|Y|,|Z|,|U|) = \max(|X|,|Y|)$
in tegenspraak met $\max(|X|,|Y|) \leq \max(|X+kZ|, |Y+kU|)$;
- als X en Y verschillend teken hebben, en $|X| \geq |Y|$, dan
is $p^m = |XU - YZ| = |XU| + |YZ| \geq |XU| =$
$= \max(|X|,|Y|)\cdot\max(|Z|,|U|) \geq \max(|Z|,|U|)^2$;
- als X en Y verschillend teken hebben, en $|X| < |Y|$,

veronderstel dan dat $|U| = \max(|Z|,|U|) > p^{\frac{1}{2}m}$.

Ook: $|Y| = \max(|X|,|Y|) \geq |U| > p^{\frac{1}{2}m}$.

Er geldt: $p^m = |XU| + |YZ| > p^{\frac{1}{2}m}(|X|+|Z|)$, en dus

$$|X|+|Z| < p^{\frac{1}{2}m} < |U|.$$

De functie $f(c) = \max(|X+cZ|, |Y+cU|)$ bereikt z'n minimum bij $c = -\frac{X+Y}{Z+U}$. Omdat $\{(X,Y),(Z,U)\}$ de uitkomst van algorithme 8.1. is, geldt $\left|\frac{X+Y}{Z+U}\right| < 1$, en dus $|Y|-|X| = |X+Y| < |Z+U| = |Z|+|U|$, $\Rightarrow$

$$|Y|-|U| < |X|+|Z| < |U|.$$

Er is een $k \in \{-1, 1\}$ zodat $|X+kZ| = |X|+|Z|$, én $|Y+kU| = |Y|-|U|$, en dus volgt:

$$\max(|X|,|Y|) \leq \max(|X+kZ|, |Y+kU|) < |U| \leq \max(|Z|,|U|) \leq \max(|X|,|Y|),$$ tegenspraak.

Dus altijd geldt: $\max(|Z|,|U|) \leq p^{\frac{1}{2}m}$.

Zij $(aX+bZ, aY+bU) \in \Gamma_m$, $a,b \in \mathbb{Z}$ en $(a,b) \neq (0,0)$.

Als $a=0$, is $|b| \geq 1$, en $\max(|aX+bZ|, |aY+bU|) =$

$$= |b| \cdot \max(|Z|,|U|) \geq \max(|Z|,|U|).$$

Als $|a|=1$, is volgens lemma 8.3.: $\max(|Z|,|U|) \leq$

$$\leq \max(|X|,|Y|) \leq \max(|X+bZ|, |Y+bU|).$$

We zullen aantonen dat, als $(aX+bZ, aY+bU)$ een betere benadering van α is dan (Z,U), dan is $|a| \leq 1$.

Laat $f(c) = \max(|X+cZ|, |Y+cU|)$ een minimum aannemen bij $c=k$. Veronderstel $\max(|aX+bZ|, |aY+bU|) < \max(|Z|,|U|)$.

Als $Z=0$, is $\max(|Z|,|U|) > |a| \cdot \max(|X+\frac{b}{a}Z|, |Y+\frac{b}{a}U|) \geq$

$$\geq |a| \max(|X|, |Y+kU|) = |a| \max(|X|, |Y - \tfrac{Y}{U} \cdot U|) = |a||X|.$$

Omdat $p^m = |XU - YZ| = |XU|$, en $|U| = \max(|Z|,|U|) \leq p^{\frac{1}{2}m}$, volgt $|X| \geq p^{\frac{1}{2}m}$, en dus $|a| < \frac{\max(|Z|,|U|)}{|X|} \leq \frac{p^{\frac{1}{2}m}}{p^{\frac{1}{2}m}} = 1$.

Als $U=0$, redeneren we analoog.

Als $UZ \neq 0$, dan: $\max(|Z|,|U|) > |a| \cdot \max(|X+\frac{b}{a}Z|, |Y+\frac{b}{a}U|)$

$\geq |a| \cdot \max(|X+kZ|, |Y+kU|) = |a| \cdot \frac{|XU-YZ|}{|Z \pm U|} = \frac{|a|\, p^m}{|Z \pm U|}$,

en er volgt $|a| < p^{-m} \cdot \max(|Z|,|U|) \cdot |Z \pm U| \leq$

$\leq p^{-m} \cdot 2 \cdot \max(|Z|,|U|)^2 \leq 2$. Uit $|a|<2$

en $a \in \mathbb{Z}$ volgt: $|a| \leq 1$. qed.

We kunnen algoritme 6.1. simpel aanpassen om beste benaderingen te vinden, door, in geval van $\max(|X|,|Y|) = \max(|Z|,|U|)$, $|Y\alpha - X|_p$ en $|U\alpha - Z|_p$ te vergelijken, en eventueel ook $(X \pm Z, Y \pm U)$ na te gaan als $|\alpha|_p = p^{\frac{1}{2}m}$. (vgl. stelling 4.6, 4.7 en algoritme 6.3.).

We schakelen nu over naar de euclidische norm $\phi(X,Y) = \sqrt{X^2+Y^2}$.
Zij weer $\{(X,Y),(Z,U)\}$ een basis van Γ_m.

<u>Algoritme 6.5.</u>

i) als $X^2+Y^2 < Z^2+U^2$, verwissel dan (X,Y) en (Z,U).

ii) bereken $k = \frac{XZ+YU}{Z^2+U^2}$

iii) zij $K \in \mathbb{Z}$ zo dat $|K-k| \leq \frac{1}{2}$, en
zet $(X,Y) = (X,Y) - K \cdot (Z,U)$

iv) als $X^2+Y^2 \geq Z^2+U^2$, dan stop.
als $X^2+Y^2 < Z^2+U^2$, verwissel dan (X,Y) en (Z,U), en ga naar ii).

Voorbeeld: $(X,Y) = (-1128, 1337)$ $\quad X^2+Y^2 = 3826753$

$(Z,U) = (-571, 617)$ $\quad Z^2+U^2 = 706730$

ii) $k = 2,32$

iii) $K = 2$, $(X,Y) = (-206, 103)$, $X^2+Y^2 = 92405$

iv) $(X,Y) = (-571, 617)$

$(Z,U) = (-206, 103)$

ii) $k = 2,46$

iii) $K = 2$, $(X,Y) = (1, 411)$, $X^2+Y^2 = 168922$ stop.

<u>lemma 8.6.</u> De funktie $f(c) = (X + cZ)^2 + (Y + cU)^2$ bereikt z'n minimum bij $k = -\frac{XZ+YU}{Z^2+U^2}$, mits $(Z,U) \neq (0,0)$.

<u>bewijs</u>: als $(Z,U) \neq (0,0)$ is $f(c)$ een kwadratisch polynoom. Er geldt: $f'(c) = 2Z(X+cZ) + 2U(Y+cU)$ en

$$f'(c) = 0 \iff c = -\frac{XZ+YU}{Z^2+U^2}.$$

qed.

<u>Gevolg</u>: De funktie $f(c) = (X+cZ)^2 + (Y+cU)^2$ op $\mathbb{Z}$ bereikt z'n minimum bij $K \in \mathbb{Z}$ met $|K-k| \leq \frac{1}{2}$, met k als in lemma 8.6.

<u>Stelling 8.7.</u> Zij $\{(X',Y'), (Z',U')\}$ een basis van Γ_m. Pas hierop algoritme 8.5. toe, en zij $\{(X,Y), (Z,U)\}$ de uitkomst. Dan is $\{(X,Y), (Z,U)\}$ een basis van Γ_m, en (Z,U) is een m-e orde bijna-beste benadering van α t.a.v. $\Phi(X,Y) = \sqrt{X^2+Y^2}$.

<u>bewijs</u>: dat $\{(X,Y), (Z,U)\}$ een basis van Γ_m is, is triviaal. Uit het algoritme volgt: $X^2+Y^2 \geq Z^2+U^2$, en $f(c) = (X+cZ)^2 + (Y+cU)^2$ heeft z'n minimum op $\mathbb{Z}$

bij $c=0$; of wel, volgens lemma 2.6.: $\frac{|Xz+Yu|}{z^2+u^2} \leq \frac{1}{2}$.

Zonder beperking in te voeren nemen we aan dat $Xz+Yu \geqslant 0$.

Zij $(aX+bz,\ aY+bu) \in \Gamma_m$, dus $a,b \in \mathbb{Z}$, en $(a,b) \neq (0,0)$.

Te bewijzen: $(aX+bz)^2 + (aY+bu)^2 \geqslant z^2+u^2$.

We maken gebruik van de identiteit

$$(aX+bz)^2 + (aY+bu)^2 = a^2(X^2+Y^2) + b^2(z^2+u^2) + 2ab(Xz+Yu).$$

Als $ab=0$ is $(aX+bz,\ aY+bu)$ een veelvoud van (X,Y) of (z,u), en dus niet beter.

Als $ab>0$, dan is, vanwege $a^2, b^2 \geqslant 1$:

$$a^2(X^2+Y^2) + b^2(z^2+u^2) + 2ab(Xz+Yu) \geqslant$$
$$\geqslant X^2+Y^2+z^2+u^2 > z^2+u^2.$$

Als $ab<0$, dan is $(aX+bz)^2 + (aY+bu)^2 =$

$$= a^2(X^2+Y^2) + b^2(z^2+u^2) - 2|ab|(Xz+Yu) \geqslant$$
$$\geqslant a^2(X^2+Y^2) + b^2(z^2+u^2) - |ab|(z^2+u^2) \geqslant$$
$$\geqslant (a^2+b^2-|ab|)(z^2+u^2),$$ waarbij we gebruikten dat $|Xz+Yu| \leq \frac{1}{2}(z^2+u^2)$.

Er geldt: $a^2+b^2-|ab| \geqslant |ab| \geqslant 1$. qed.

Deze stelling is in essentie bewezen in Mahler (1940), m.b.v. modulaire transformaties.

Nu we weten hoe we vanuit de ene basis van Γ_m een andere maken kunnen, die een bijna-beste benadering bevat, blijft het probleem om een of andere basis van Γ_m te berekenen. Dat is niet zo moeilijk. Immers, als $\alpha \in \mathbb{Q}_p$ met $\alpha = a_0 + a_1 p + a_2 p^2 + \cdots$

als p-adische ontwikkeling, en $\alpha_m = a_0 + a_1 p + \cdots + a_{m-1} p^{m-1}$, dan is $\{(p^m, 0), (\alpha_m, 1)\}$ een basis van Γ_m.
Immers: $|0 \cdot \alpha - p^m|_p = p^{-m}$, en $|1 \cdot \alpha - \alpha_m|_p = |a_m p^m + a_{m+1} p^{m+1} + \cdots|_p \leq$ $\leq p^{-m}$, dus beide punten liggen in Γ_m; en hun determinant is p^m.
Als we algorithme 8.1. toepassen op deze basis, doen we in feite hetzelfde als in algorithme 6.3. Daar berekenen we immers $R_{-1} = 1$, $Q_{-1} = 0$, $P_{-1} = -p^m$; $R_0 = 0$, $Q_0 = 1$, $P_0 = \alpha_m$, en $(P_k, Q_k) = b_k (P_{k-1}, Q_{k-1}) + (P_{k-2}, Q_{k-2})$, met b_k zo gekozen dat $|P_k| < |P_{k-1}|$.

Voorbeeld: $\alpha = 60 \in \mathbb{Q}_7$, $m = 3$, volgens algorithme 6.3.:

$\frac{60}{343} = [0, 5, 1, 2, 1, 1, 8]$

b_k:		0	5	1	2	1	1	8
R_k:	1	0	1	1	3	4	7	60
Q_k:	0	1	5	6	17	23	40	343
P_k:	-343	60	-43	17	-9	8	-1	0

en volgens algorithme 8.1.:

$$\begin{pmatrix} 343 & 0 \\ 60 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 343 - 6 \cdot 60 & 0 - 6 \cdot 1 \\ 60 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 60 & 1 \\ -17 & -6 \end{pmatrix} \longrightarrow$$

$$\longrightarrow \begin{pmatrix} 60 + 3 \cdot -17 & 1 + 3 \cdot -6 \\ -17 & -6 \end{pmatrix} = \begin{pmatrix} 9 & -17 \\ -17 & -6 \end{pmatrix}.$$

Algorithme 8.1. slaat zelfs nog een stapje over, zo lijkt het, nl. $(-43, 5)$. Dat is echter schijn: in stap iii) van het algorithme wordt immers gekozen tussen twee benaderingen, in dit geval $(+43, -5)$ en $(-17, -6)$.

We constateren dat algorithme 8.1. toegepast op de basis $\{(p^m, 0), (\alpha_m, 1)\}$ ons niets nieuws leert.

Er is een andere manier om een basis van Γ_m te vinden, namelijk vanuit een gegeven basis van Γ_{m-1}. We kunnen dan starten met $\{(1,0),(0,1)\}$ als basis van Γ_0, en achtereenvolgens bases berekenen van $\Gamma_1, \Gamma_2, \ldots$. Als we ook nog na iedere stap het basisreductie-algoritme 8.1. of 8.5. toepassen, verkrijgen we zo een rij beste benaderingen van α.

Zij $\alpha \in \mathbb{Q}_p$ geheel, en $m \in \mathbb{Z}$, $m \geq 0$. Zij $\{(P_m, Q_m), (P_m', Q_m')\}$ een basis van Γ_m. Zij $\alpha = a_0 + a_1 p + a_2 p^2 + \cdots$ de p-adische ontwikkeling van α, en zij $\alpha_i = a_0 + a_1 p + \cdots + a_{i-1} p^{i-1}$, $i = 1, 2, 3, \ldots$

<u>Algorithme 8.8.</u>

i) bereken R_m, R_m' uit
$$Q_m \alpha_{m+1} - P_m = R_m p^m$$
$$Q_m' \alpha_{m+1} - P_m' = R_m' p^m$$

ii) als $p \mid R_m'$, verwissel dan P_m, Q_m, R_m met resp. P_m', Q_m', R_m'.
bereken $S_m \in \mathbb{Z}$ uit $R_m' S_m \equiv R_m \bmod p$
en $|S_m| \leq \frac{1}{2} p$

iii) bereken $P_{m+1}' = p \cdot P_m'$, $Q_{m+1}' = p \cdot Q_m'$,
$P_{m+1} = P_m - S_m P_m'$, $Q_{m+1} = Q_m - S_m Q_m'$.

<u>Stelling 8.9.</u> De m.b.v. algorithme 8.8. berekende (P_{m+1}, Q_{m+1}) en (P_{m+1}', Q_{m+1}') vormen een basis van Γ_{m+1}.

bewijs: Er geldt: $R_m, R_m' \in \mathbb{Z}$, en $p^m(Q_m R_m' - Q_m' R_m) =$
$= Q_m(Q_m' \alpha_{m+1} - P_m') - Q_m'(Q_m \alpha_{m+1} - P_m) =$
$= -(Q_m P_m' - P_m Q_m') = \pm p^m$,
dus $Q_m R_m' - Q_m' R_m = \pm 1$, en $\text{ggd}(R_m, R_m') = 1$.
Na eventuele verwisseling in stap ii) geldt dan zeker $p \nmid R_m'$, dus S_m kan berekend worden.

(P_{m+1}, Q_{m+1}) en (P_{m+1}', Q_{m+1}') liggen in Γ_{m+1}, want
$Q_{m+1}' \alpha_{m+1} - P_{m+1}' = p(Q_m' \alpha_{m+1} - P_m') = p^{m+1} R_m$
en $Q_{m+1} \alpha_{m+1} - P_{m+1} = Q_m \alpha_{m+1} - P_m - S_m(Q_m' \alpha_{m+1} - P_m') =$
$= p^m(R_m - S_m R_m')$, en $p \mid (R_m - S_m R_m')$ vanwege de keuze voor S_m.

Tenslotte: (P_{m+1}, Q_{m+1}) en (P_{m+1}', Q_{m+1}') vormen een basis van Γ_{m+1}, want:
$P_{m+1} Q_{m+1}' - P_{m+1}' Q_{m+1} = p(P_m - S_m P_m') Q_m' - p P_m'(Q_m - S_m Q_m')$
$= p(P_m Q_m' - P_m' Q_m) = \pm p^{m+1}$, want (P_m, Q_m) en (P_m', Q_m') vormen een basis van Γ_m. qed.

Algoritme 8.8 en, naar keuze 8.1. of 8.5, kunnen nu aan elkaar gekoppeld worden:

Zij $\alpha \in \mathbb{Q}_p$ geheel, $\alpha = a_0 + a_1 p + a_2 p^2 + \cdots$ en $\alpha_m = a_0 + a_1 p + \cdots + a_{m-1} p^{m-1}$.

Algoritme 8.10. i) zet $m=0$, $(P_0, Q_0) = (1,0)$, $(P_0', Q_0') = (0,1)$
ii) bereken m.b.v. algoritme 8.8. een basis $\{(P_{m+1}^*, Q_{m+1}^*), (P_{m+1}^{*1}, Q_{m+1}^{*1})\}$ van Γ_{m+1} uit $\{(P_m, Q_m), (P_m', Q_m')\}$.
iii) bereken m.b.v. algoritme 8.1. of 8.5. uit

$\{(P_{m+1}^*, Q_{m+1}^*), (P_{m+1}^{*1}, Q_{m+1}^{*1})\}$ een basis $\{(P_{m+1}, Q_{m+1}), (P_{m+1}', Q_{m+1}')\}$ van Γ_{m+1} met (P_{m+1}', Q_{m+1}') een beste benadering van α.

iv) zet $m = m+1$ en ga naar ii).

Merk op dat de grootte orde van (P_m, Q_m) en (P_m', Q_m'), gemeten in $\Phi(X,Y) = \max(|X|,|Y|)$ of $\Phi(X,Y) = \sqrt{X^2+Y^2}$, ongeveer $p^{\frac{1}{2}m}$ zal zijn. De grootte orde van $(P_{m+1}^{*1}, Q_{m+1}^{*1})$ wordt dus $p^{\frac{1}{2}m+1}$, en ook (P_{m+1}^*, Q_{m+1}^*) heeft dezelfde orde van grootte, door de eis $|S_m| \leq \frac{1}{2}p$. De reduktie in stap iii) is dus een reduktie van grootteorde $p^{\frac{1}{2}m+1}$ naar $p^{\frac{1}{2}(m+1)}$, m.a.w. met een faktor $\sqrt{p}$. Het ziet er daarom naar uit dat één of twee keer alle stappen van algorithme 8.1. of 8.5 doorlopen, in de meeste gevallen voldoende is.

Voorbeeld: $\alpha = 411 \in \mathbb{Q}_7$, $\alpha = 5 + 2\cdot 7 + 1\cdot 7^2 + 1\cdot 7^3$.

$a_1 = 5$, $\begin{pmatrix} P_0 & Q_0 \\ P_0' & Q_0' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\begin{matrix} R_0 = -1 \\ R_0' = 5 \end{matrix}$, $S_0 = -3$.

$$\begin{pmatrix} P_1^* & Q_1^* \\ P_1^{*1} & Q_1^{*1} \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 0 & 7 \end{pmatrix} \to \begin{pmatrix} 1 & 3 \\ -2 & 1 \end{pmatrix}$$

$a_2 = 19$, $\begin{pmatrix} P_1 & Q_1 \\ P_1' & Q_1' \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ -2 & 1 \end{pmatrix}$, $\begin{matrix} R_1 = 8 \\ R_1' = 3 \end{matrix}$, $S_1 = -2$.

$$\begin{pmatrix} P_2^* & Q_2^* \\ P_2^{*1} & Q_2^{*1} \end{pmatrix} = \begin{pmatrix} -3 & 5 \\ -14 & 7 \end{pmatrix} \to \begin{pmatrix} -8 & -3 \\ -3 & 5 \end{pmatrix}$$

$a_3 = 68$, $\begin{pmatrix} P_2 & Q_2 \\ P_2' & Q_2' \end{pmatrix} = \begin{pmatrix} -8 & -3 \\ -3 & 5 \end{pmatrix}$, $\begin{matrix} R_2 = -4 \\ R_2' = 7 \end{matrix}$, verwisselen, en $S_2 = 0$,

$$\begin{pmatrix} P_3^* & Q_3^* \\ P_3^{*1} & Q_3^{*1} \end{pmatrix} = \begin{pmatrix} -3 & 5 \\ -56 & -21 \end{pmatrix} \to \begin{pmatrix} -44 & -41 \\ -3 & 5 \end{pmatrix}$$

$\alpha_4 = 411$, $\begin{pmatrix} P_3 & Q_3 \\ P_3' & Q_3' \end{pmatrix} = \begin{pmatrix} -444 & -411 \\ -3 & 5 \end{pmatrix}$, $R_3 = -49$, $R_3' = 6$, $S_3 = 0$

$\begin{pmatrix} P_4^* & Q_4^* \\ P_4^{*\prime} & Q_4^{*\prime} \end{pmatrix} = \begin{pmatrix} -444 & -411 \\ -21 & 35 \end{pmatrix}$

$\alpha_5 = 411$, $\begin{pmatrix} P_4 & Q_4 \\ P_4' & Q_4' \end{pmatrix} = \begin{pmatrix} -444 & -411 \\ -21 & 35 \end{pmatrix}$, $R_4 = -7$, $R_4' = 6$, $S_4 = 0$

$\begin{pmatrix} P_5^* & Q_5^* \\ P_5^{*\prime} & Q_5^{*\prime} \end{pmatrix} = \begin{pmatrix} -444 & -411 \\ -147 & 245 \end{pmatrix} \longrightarrow \begin{pmatrix} -191 & 2044 \\ -444 & -411 \end{pmatrix}$

$\alpha_6 = 411$, $\begin{pmatrix} P_5 & Q_5 \\ P_5' & Q_5' \end{pmatrix} = \begin{pmatrix} -191 & 2044 \\ -444 & -411 \end{pmatrix}$ $R_5 = 5$, $R_5' = -1$, $S_5 = 2$

$\begin{pmatrix} P_6^* & Q_6^* \\ P_6^{*\prime} & Q_6^{*\prime} \end{pmatrix} = \begin{pmatrix} -103 & 286 \\ -308 & -287 \end{pmatrix} \longrightarrow$

$\alpha_7 = 411$, $\begin{pmatrix} P_6 & Q_6 \\ P_6' & Q_6' \end{pmatrix} = \begin{pmatrix} -308 & -287 \\ -103 & 286 \end{pmatrix}$ $R_6 = -1$, $R_6' = 1$, $S_6 = -1$

$\begin{pmatrix} P_7^* & Q_7^* \\ P_7^{*\prime} & Q_7^{*\prime} \end{pmatrix} = \begin{pmatrix} -411 & -1 \\ -721 & 2002 \end{pmatrix} \longrightarrow \begin{pmatrix} -1954 & 1999 \\ -411 & -1 \end{pmatrix}$

We vinden dus de volgende nij beste benaderingen:
$(-2, 1)$, $(-3, 5)$, $(-21, 35)$, $(-444, -411)$, $(-103, 286)$, $(-411, -1)$.
Waren we alleen geïnteresseerd geweest in een beste benadering met bv. orde 5, dan hadden we $(444, 411)$ veel sneller gevonden.
De keus voor algorithme 6.3. of 8.10. zal dus gemaakt moeten worden op grond van het doel dat men zich stelt. Is men alleen geïnteresseerd in een n-e orde beste benadering voor één vaste n, biedt algorithme 6.3. voordelen. Als er benaderingen voor meerdere n gewenst zijn, is algorithme 8.10. geschikter.

LITERATUUR

Agrawal, M.K.; J.H. Coates; D.C. Hunt; A.J. van der Poorten — Elliptic Curves of Conductor 17, Math. Comp. 35 (1980), 991-6.

Bundschuh, P. — p-adische Kettenbrüche und Irrationalität p-adischer Zahlen, El. Math. 32 (1977), 36-40

Hardy, G.H.; E.M. Wright — An Introduction to the Theory of Numbers, Oxford (1930/1979)

Koblitz, N. — P-adic Numbers, P-adic analysis and Zeta-functions, New York (1977)

Mahler, K. — Zur Approximation p-adischer Irrationalzahlen, Nw. Arch. Wisk. II-18 (1934), 22-34

Mahler, K. — On a geometrical representation of p-adic numbers, Ann. Math. 41 (1940), 8-56

Mahler, K. — Lectures on Diophantine Approximations I, g-adic numbers and Roth's Theorem, Univ. of Note Dame (1961)

Mahler, K. — Introduction to p-adic numbers and their functions, Cambridge (1973)

Perron, O. — Die Lehre von den Kettenbrüchen, Leipzig (1913)/ Stuttgart (1954)

Schneider, Th. — Über p-adische Kettenbrüche, Symp. Math. IV (1970), 181-189.