Kettingbreuken

Het doel van dit Hoofdstuk is een inleiding te geven in de theorie van kettingbreuken, en enkele toepassingen daarvan te geven.

1.1 Eindige kettingbreuken

Een aardige manier om kettingbreuken te introduceren wordt gegeven via het verband met het algoritme van Euclides (zie bijvoorbeeld **Algoritme 4.12** in het dictaat *Ringen en Lichamen*).

1.1.1 Voorbeeld Veronderstel dat we de grootste gemene deler van 33 en 137 trachten te bepalen volgens de methode van Euclides. Dan krijgen we achtereenvolgens:

$$\begin{aligned} 137 &= 4 \cdot 33 + 5, \\ 33 &= 6 \cdot 5 + 3, \\ 5 &= 1 \cdot 3 + 2, \\ 3 &= 1 \cdot 2 + 1, \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

waaruit we zien dat de grootste gemene deler 1 is. Maar delen we in elk van de bovenstaande regels van de vorm

$$a = q \cdot b + r$$

door b, dan krijgen we

$$\begin{aligned}\frac{137}{33} &= 4+\frac{5}{33},\\ \frac{33}{5} &= 6+\frac{3}{5},\\ \frac{5}{3} &= 1+\frac{2}{3},\\ \frac{3}{2} &= 1+\frac{2}{1},\\ \frac{2}{1} &= 2+\frac{0}{1}.\end{aligned}$$

Omdat de breuk rechts steeds de omgekeerde is van de breuk links op de volgende regel, krijgen we hieruit door substitutie

$$\frac{137}{33} = 4+\frac{5}{33} = 4+\frac{1}{6+\frac{3}{5}} = 4+\frac{1}{6+\frac{1}{1+\frac{2}{3}}} = 4+\frac{1}{6+\frac{1}{1+\frac{1}{1+\frac{1}{2}}}}.$$

Het zal duidelijk zijn waarom de uitdrukking rechts een kettingbreuk genoemd wordt, en ook waarom we de minder papierverslindende schrijfwijze $[0;4,6,1,1,2]$ zullen invoeren.

1.1.2 Definitie Een *eindige kettingbreuk* $[a_0;a_1,a_2,\ldots,a_n]$ is een herhaalde breuk van de vorm

$$[a_0;a_1,a_2,\ldots,a_n] = a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{\ddots\,\cfrac{1}{a_n}}}},$$

voor gehele getallen a_i met de condities dat $a_i \geq 1$ als $i \geq 1$, en $a_n \geq 2$. De getallen a_i heten de *wijzergetallen* van de kettingbreuk. De kettingbreuk $[a_0;a_1,a_2,\ldots,a_n]$ bepaalt een rationaal getal p/q, dat we de *waarde* ervan zullen noemen. De rationale getallen

$$[a_0;\ ],[a_0;a_1],[a_0;a_1,a_2],\ldots,[a_0;a_1,\ldots a_n],$$

heten de *convergenten* van $[a_0;a_1,a_2,\ldots,a_n]$. Het getal n is de *lengte* van de kettingbreuk.

1.1.3 Opmerking We kunnen de waarde p/q terugvinden door de kettingbreuk van rechts 'op te rollen' (alsof we het Euclidische algoritme teruglezen). De naam convergent zal straks duidelijk worden; we zullen voor de teller en de noemer ervan de standaardnotatie p_k/q_k invoeren: $p_k/q_k = [a_0;a_1,a_2,\ldots,a_k]$ voor $0 \leq k \leq n$, met natuurlijk $p_0/q_0 = a_0/1 \in \mathbb{Z}$ en $p_n/q_n = p/q$.

Merk op dat de eisen $a_i \geq 1$ als $i \geq 1$, en $a_n \geq 2$ logisch volgen wanneer we kijken naar het algoritme van Euclides. Ook los daarvan ligt de eis dat het laatste wijzergetal groter dan 1 moet zijn voor de hand, omdat een kettingbreuk die met $a_n = 1$ eindigt direct ingekort kan worden door het vorige wijzergetal op te hogen:

$$a_{n-1} + \frac{1}{1} = a_{n-1} + 1.$$

De kettingbreuken die we net hebben ingevoerd worden wel *regelmatige* kettingbreuken genoemd; *half-regelmatige* kettingbreuken bestaan uit de generalisatie

$$[a_0; \epsilon_1 a_1, \epsilon_2 a_2, \ldots, \epsilon_n a_n] = a_0 + \cfrac{\epsilon_1}{a_1 + \cfrac{\epsilon_2}{a_2 + \cfrac{\epsilon_3}{\ddots \cfrac{\epsilon_n}{a_n}}}},$$

met $\epsilon_i \in \{\pm 1\}$, en condities op a_i en ϵ_j. Deze kunnen bijvoorbeeld ook verkregen worden door herschrijven van reguliere kettingbreuken waarin *negatieve* wijzergetallen worden toegelaten. Zie ook opgave ??.

1.1.4 Stelling *Elk rationaal getal p/q bepaalt een unieke eindige kettingbreuk.*

Bewijs Bij gegeven p/q kunnen we als boven met het algoritme van Euclides altijd een eindige kettingbreuk $[a_0; a_1, a_2, \ldots, a_n]$ vinden.

Merk op dat voor $t = [0; a_1, a_2, \ldots, a_n]$ geldt: $0 \leq t < 1$ (met altijd ongelijkheid rechts omdat $a_n > 1$), en daarom is $a_0 \leq [a_0; a_1, a_2, \ldots, a_n] < a_0 + 1$.

Veronderstel nu dat we voor p/q een andere eindige kettingbreuk $p/q = [b_0; b_1, \ldots b_k]$ hebben. Dan moet $a_0 = \lfloor p/q \rfloor = b_0$ omdat $\lfloor p/q \rfloor$ het unieke gehele getal is met $\lfloor p/q \rfloor \leq p/q < \lfloor p/q \rfloor + 1$.

Bekijk nu

$$\frac{1}{[a_1; a_2, \ldots, a_n]} = [0; a_1, a_2, \ldots, a_n] = \frac{p}{q} - \lfloor p/q \rfloor = [0; b_1, \ldots b_k] = \frac{1}{[b_1; b_2, \ldots, b_k]},$$

dan zien we dat $[a_1; a_2, \ldots, a_n] = [b_1; b_2, \ldots, b_k]$, dus $a_1 = b_1$ als boven, enzovoorts.

Wanneer we het algoritme van Euclides loslaten zien we aan het voorbeeld $p/q = 33/137$ gemakkelijk hoe we in het algemeen de kettingbreuk *vinden* voor gegeven p/q: neem eerst het gehele deel a_0 en trek dat van de breuk af; neem van het resultaat de reciproke en herhaal het proces. Met andere woorden, we itereren de operatie

$$x_{k+1} = \frac{1}{x_k - \lfloor x_k \rfloor} \tag{1.1}$$

met $x_0 = p/q$ totdat $x_k - \lfloor x_k \rfloor$ de waarde 0 heeft gekregen. Steeds is $a_k = \lfloor x_k \rfloor$. Dit heet wel de *eindige kettingbreukalgoritme*.

Het vinden van de convergenten gaat als volgt. Per definitie is $p_0/q_0 = [a_0;\ ] = a_0/1$. Dan is

$$\frac{p_1}{q_1} = a_0 + \frac{1}{a_1} = \frac{a_1 a_0 + 1}{a_1},$$

en

$$\frac{p_2}{q_2} = a_0 + \frac{1}{a_1 + \dfrac{1}{a_2}} = a_0 + \frac{a_2}{a_2a_1+1} = \frac{a_2a_1a_0 + a_2 + a_0}{a_2a_1+1}.$$

Natuurlijk is die uit de voorgaande te verkrijgen door a_1 te vervangen door $a_1 + 1/a_2$. Net zo vinden we hieruit

$$\frac{p_3}{q_3} = \frac{(a_2 + \frac{1}{a_3})a_1a_0 + a_2 + \frac{1}{a_3} + a_0}{(a_2 + \frac{1}{a_3})a_1 + 1} = \frac{a_3(a_2a_1a_0 + a_2 + a_0) + a_1a_0 + 1}{a_3(a_2a_1 + 1) + a_1}$$

en dan is met inductie eenvoudig in te zien dat algemeen de volgende Stelling geldt, waarin de kettingbreuk als het ware voorwaarts opgerold wordt.

1.1.5 Stelling *Voor de convergent p_k/q_k van een rationaal getal p/q geldt:*

$$\frac{p_k}{q_k} = \frac{a_kp_{k-1} + p_{k-2}}{a_kq_{k-1} + q_{k-2}}. \tag{1.2}$$

voor $1 \le k \le n$, als we definiëren dat $p_{-1} = 1, q_{-1} = 0$.

1.1.6 Voorbeeld We vatten de wijzergetallen en convergenten uit ons eerste voorbeeld in een tabel samen:

n :	-1	0	1	2	3	4	5
a_n :		0	4	6	1	1	2
p_n :	1	0	1	6	7	13	33
q_n :	0	1	4	25	29	54	137

1.1.7 Lemma *Voor de convergenten p_k/q_k van een rationaal getal p/q geldt dat $|p_k| \ge |p_{k-1}|$ en $q_k \ge q_{k-1}$ voor $k \ge 1$ en zelfs:*

$$|p_k| > |p_{k-1}|, \quad (k \ge 3), \text{ en} \qquad q_k > q_{k-1}, \quad (k \ge 2),$$

en bovendien

$$p_{k-1}q_k - p_kq_{k-1} = (-1)^k.$$

Bewijs Gebruik de vergelijking 1.2:

$$\begin{aligned}\frac{p_{k-1}q_k - p_kq_{k-1}}{q_{k-1}q_k} &= \frac{p_{k-1}}{q_{k-1}} - \frac{p_k}{q_k} = \frac{p_{k-1}}{q_{k-1}} - \frac{a_kp_{k-1} + p_{k-2}}{a_kq_{k-1} + q_{k-2}} = \\ &= \frac{(-1)(p_{k-2}q_{k-1} - p_{k-1}q_{k-2})}{q_{k-1}(a_kq_{k-1} + q_{k-2})},\end{aligned}$$

hetgeen met inductie gelijk is aan

$$\frac{(-1)^k(p_{-1}q_0 - p_0q_{-1})}{q_{k-1}(a_kq_{k-1} + q_{k-2})} = \frac{(-1)^k}{q_{k-1}(a_kq_{k-1} + q_{k-2})}.$$

Dus is $p_{k-1}q_k - p_kq_{k-1} = (-1)^k$ en in het bijzonder zijn p_k en q_k onderling ondeelbaar. Ook is $q_k = a_kq_{k-1} + q_{k-2} > q_{k-1}$ voor $k \ge 2$ met inductie, omdat $a_k \ge 1$, en $q_{k-1} > 0$ voor $k \ge 1$. Ook is $|p_k| = a_k|p_{k-1}| + |p_{k-2}| > |p_{k-1}|$, voor $k \ge 3$ omdat $|p_{k-2}| > 0$ voor $k \ge 3$.

1.1.8 Stelling *Voor de convergenten $p_k/q_k, p_{k+1}/q_{k+1}$ van een rationaal getal p/q geldt voor $k \geq 0$ dat:*

$$\frac{p_{k-1}}{q_{k-1}} - \frac{p_k}{q_k} = \frac{(-1)^k}{q_{k-1}q_k},$$

en

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \cdots < \frac{p}{q} = \frac{p_n}{q_n} < \cdots < \frac{p_3}{q_3} < \frac{p_1}{q_1} < \frac{p_{-1}}{q_{-1}};$$

bovendien is

$$\left|\frac{p}{q} - \frac{p_k}{q_k}\right| < \left|\frac{p}{q} - \frac{p_{k-1}}{q_{k-1}}\right|$$

voor $0 \leq k \leq n$.

Bewijs De eerste bewering volgt direct uit het Lemma. Dat zegt ook dat de rij van q_i's strikt stijgt, en dus worden de verschillen tussen twee opeenvolgende convergenten steeds kleiner. Daaruit volgt de tweede bewering. Voor de laatste bewering merken we eerst het volgende op voor positieve reële getallen a, b en $0 \leq k \leq n$:

$$\begin{aligned} \frac{ap_{k-1} + p_{k-2}}{aq_{k-1} + q_{k-2}} \leq \frac{bp_{k-1} + p_{k-2}}{bq_{k-1} + q_{k-2}} \quad &\Longleftrightarrow \\ 0 \leq (a-b)(p_{k-2}q_{k-1} - p_{k-1}q_{k-2}) = (a-b)(-1)^{k-1} \quad &\Longleftrightarrow \\ k \text{ oneven en } b \leq a, \quad \text{of} \quad k \text{ even en } a \leq b. & \end{aligned}$$

Voor oneven $k < n$ geldt dat

$$\frac{p_{k-1}}{q_{k-1}} < \frac{p_{k+1}}{q_{k+1}} < \frac{p}{q} < \frac{p_k}{q_k},$$

en passen we het bovenstaande toe met $b = a_{k+1} \geq 1$ en $a = 1$, dan:

$$\frac{p}{q} > \frac{p_{k+1}}{q_{k+1}} = \frac{a_{k+1}p_k + p_{k-1}}{a_{k+1}q_k + q_{k-1}} \geq \frac{p_k + p_{k-1}}{q_k + q_{k-1}};$$

maar dan is

$$\begin{aligned} \frac{p}{q} - \frac{p_{k-1}}{q_{k-1}} &> \frac{p_{k+1}}{q_{k+1}} - \frac{p_{k-1}}{q_{k-1}} \geq \frac{p_k + p_{k-1}}{q_k + q_{k-1}} - \frac{p_{k-1}}{q_{k-1}} = \frac{-(p_{k-1}q_k - p_kq_{k-1})}{q_{k-1}(q_k + q_{k+1})} = \\ &= \frac{1}{q_{k-1}(q_k + q_{k+1})} > \frac{1}{q_k(q_k + q_{k+1})} = \frac{-(p_{k-1}q_k - p_kq_{k-1})}{q_k(q_k + q_{k+1})} = \\ &= \frac{p_k}{q_k} - \frac{p_k + p_{k-1}}{q_k + q_{k-1}} \geq \frac{p_k}{q_k} - \frac{a_{k+1}p_k + p_{k-1}}{a_{k+1}q_k + q_{k-1}} = \frac{p_k}{q_k} - \frac{p_{k+1}}{q_{k+1}} > \frac{p_k}{q_k} - \frac{p}{q}. \end{aligned}$$

Het geval k is even gaat net zo.

1.1.9 Toepassing (Tandwielen) Huygens gebruikte convergenten van kettingbreuken in zijn constructie van een planetarium. Met een enkele aandrijfstang en tandwielen met de juiste overbrengingsverhouding moesten in een model alle (toen bekende) planeten in een redelijk accurate omwenteling rond de centrale zon gebracht worden. Die verhouding moest corresponderen

met de verhouding tussen de lengte van het jaar op de betreffende planeet en die op aarde. Omdat de tandwielen daadwerkelijk gemaakt moesten worden, mochten aantallen tanden noch te groot noch te klein worden. Voor de binnenste planeet, Mercurius, vond Huygens bijvoorbeeld een verhouding van 25335/105190. Dat getal heeft kettingbreuk $[0; 4, 6, 1, 1, 2, 1, 1, 1, 1, 7, 1, 2]$ en aanvankelijk gebruikte Huygens de vijfde convergent $[0; 4, 6, 1, 1, 2] = \frac{33}{137}$. Later ontdekte hij dat de negende convergent zelf weliswaar te veel tanden zou vergen: $[0; 4, 6, 1, 1, 2, 1, 1, 1, 1] = \frac{204}{847}$, maar omdat $204 = 12 \cdot 17$ en $847 = 7 \cdot 121$ is die betere benadering als verhouding te realiseren door vier tandwielen met $12, 17, 7$, en 121 tanden, waarvan er twee op dezelfde as zitten.

1.1.10 Toepassing (Oplossen van lineaire vergelijkingen) De eigenschap dat twee opeenvolgende convergenten voldoen aan $p_{k-1}q_k - p_k q_{k-1} = \pm 1$ kunnen we gebruiken om de oplossingen te bepalen van de vergelijking

$$ax - by = 1, \quad a, b \in \mathbb{Z}_{\geq 1}$$

in gehele getallen x, y. Merk op dat $\gcd(a, b) = 1$ moet gelden anders zijn er geen oplossingen.

Ontwikkel de breuk b/a in een kettingbreuk en beschouw de laatste twee convergenten: p_{n-1}/q_{n-1} en $p_n/q_n = b/a$. Dan geldt volgens Lemma 1.1.7 dat

$$p_{n-1}q_n - p_n q_{n-1} = p_{n-1}a - q_{n-1}b = (-1)^n,$$

zodat, afhankelijk van de pariteit van n een oplossing wordt gegeven door $(x_0, y_0) = (p_{n-1}, q_{n-1})$ of door $(x_0, y_0) = (-p_{n-1}, -q_{n-1})$. Wensen we uitsluitend positieve oplossingen dan kunnen we ook de lengte n van de kettingbreuk even *maken*, door het laatste wijzergetal a_n te vervangen door $a_{n-1}, 1$.

We vinden de *algemene* oplossing van de vergelijking uit een particuliere oplossing (x_0, y_0) simpelweg uit $(x, y) = (x_0 + zb, y_0 + za)$: het is duidelijk dat al deze paren oplossingen geven, en anderzijds geldt dat een tweede oplossing (x_1, y_1) voldoet aan

$$ax_1 - by_1 = 1 = ax_0 - by_0$$

zodat

$$a(x_1 - x_0) = b(y_1 - y_0).$$

Omdat a, b onderling ondeelbaar zijn, moet a een deler zijn van $y_1 - y_0$ en b van $x_1 - x_0$. Het resultaat volgt direkt.

Om de vergelijking $ax + by = \pm 1$ op te lossen passen we het volgende toe. Als voorheen ontwikkel je eerst b/a in een kettingbreuk om een particuliere oplossing (x_0, y_0) van $ax - by = \pm 1$ te vinden, dan is $(x_0, -y_0)$ een oplossing van $ax + by = \pm 1$ en de algemene oplossing wordt gegeven door $(x_0 + bz, -y_0 - az)$.

Om vergelijkingen van de vorm $ax \pm by = c$ met $|c| > 1$ op te lossen vermenigvulidigt men de oplossing voor $ax \pm by = 1$ met c.

1.1.11 Voorbeeld Vind alle oplossingen van de vergelijking

$$34 \cdot x + 49 \cdot y = -13.$$

De kettingbreuk van $49/34$ is $[1;2,3,1,3]$. De aanpassing hiervan met oneven lengte is $[1;2,3,1,2,1]$ geeft een oplossing van

$$34 \cdot x + 49 \cdot y = -1$$

via de voorlaatste convergent uit de rij

$$\frac{1}{1}, \frac{3}{2}, \frac{10}{7}, \frac{13}{9}, \frac{36}{25}, \frac{49}{34},$$

want $36 \cdot 34 - 25 \cdot 49 = -1$. De gevraagde algemene oplossing is dan $x = 13 \cdot 36 + 49z$, $y = 13 \cdot (-25) - 34z$.

1.1.12 Toepassing (Stambreuken) Stambreuken of *Egyptische breuken* zijn breuken met teller 1. De Egyptenaren schreven hun breuken (met uitzondering van $2/3$) als sommen van zulke stambreuken met verschillende noemers. Er zijn verschillende algoritmen om een breuk als som van stambreuken te schrijven (zie ook de opgaven), en daarbij doen zich twee vragen voor: hoe groot worden de benodigde noemers, en hoe lang is de ontwikkeling?

De volgende methode, die van kettingbreuken gebruik maakt, levert zowel tamelijk korte ontwikkelingen als kleine noemers. Preciezer gezegd: voor een breuk p/q levert dit algoritme een som van niet meer dan p stambreuken met noemers kleiner dan of gelijk aan $q(q-1)$.

Laat $0 < p/q < 1$ gegeven zijn, met $\gcd(p,q) = 1$. Laat de kettingbreuk voor p/q zijn: $p/q = [0; a_1, a_2, \ldots, a_n]$. We definiëren de ontwikkeling in stambreuken als volgt met inductie naar de lengte van de kettingbreuk. Als $n = 1$, dan is $p/q = 1/a_1$ en zijn we klaar. Veronderstel nu dat we voor breuken met kettingbreuk ter lengte $< n$ klaar zijn, dan gaan we als volgt te werk. Als n oneven is, dan is $p_{n-1}/q_{n-1} < p_n/q_n = p/q$, en

$$\frac{p}{q} - \frac{p_{n-1}}{q_{n-1}} = \frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{p_n q_{n-1} - p_{n-1} q_n}{q_{n-1} q_n} = \frac{1}{q_{n-1} q_n},$$

zodat we klaar zijn. Als n even is, dan is $p_{n-2}/q_{n-2} < p/q$ en gebruiken we de medianten:

$$\frac{p_{n-2}}{q_{n-2}} < \frac{p_{n-2} + p_{n-1}}{q_{n-2} + q_{n-1}} < \cdots < \frac{p_{n-2} + a_n p_{n-1}}{q_{n-2} + a_n q_{n-1}} = \frac{p_n}{q_n} = p/q.$$

Omdat

$$\frac{p_{n-2} + j p_{n-1}}{q_{n-2} + j q_{n-1}} - \frac{p_{n-2} + (j-1) p_{n-1}}{q_{n-2} + (j-1) q_{n-1}} = \frac{1}{(q_{n-2} + (j-1) q_{n-1})(q_{n-2} + j q_{n-1})}$$

kunnen we schrijven

$$\frac{p}{q} = \frac{p_{n-2}}{q_{n-2}} + \sum_{j=1}^{a_n} \frac{1}{(q_{n-2} + (j-1) \cdot q_{n-1})(q_{n-2} + j \cdot q_{n-1})},$$

en zijn we weer klaar met inductie. In totaal hebben we ook niet meer dan $1 + a_2 + \cdots + a_{n'}$ stambreuken nodig, waar n' het grootste even getal kleiner dan of gelijk aan n is.

Er is een aanpassing van dit algoritme dat werkt door de medianten in groepjes bij elkaar te nemen, maar dat is enigszins ingewikkeld omdat vermeden moet worden dat twee termen gelijk worden.

1.1.13 Toepassing (Sommen van kwadraten) Laat p een priemgetal zijn. Het is welbekend dat de multiplicatieve groep $\mathbb{F}_p^*$ van het eindige lichaam $\mathbb{F}_p$ cyclisch is: er is een geheel getal g zodat de machten van g modulo p alle $p-1$ niet-nul restklassen geven. Natuurlijk is $g^{p-1} \equiv 1 \bmod p$. De vergelijking $x^2 - 1 = 0$ heeft in $\mathbb{F}_p$ dan de oplossingen 1 en $-1 \equiv g^{(p-1)/2} \bmod p$; en de vergelijking $x^2 + 1 = 0$ heeft in $\mathbb{F}_p$ dan afhankelijk van p géén oplossingen (als $p \equiv 3 \bmod 4$), één oplossing (als $p = 2$) of de twee verschillende oplossingen $\pm g^{(p-1)/4} \bmod p$ (als $p \equiv 1 \bmod 4$).

We gebruiken dit om te proberen p als som van twee kwadraten te schrijven; omdat dit voor $p = 2$ een triviaal probleem is, nemen we aan dat p oneven is. We zoeken a, b zodat $p = a^2 + b^2$. Als $p \equiv 3 \bmod 4$ bestaan zulke a, b niet, want anders is $(ab^{-1})^2 \equiv -1 \bmod p$ in tegenstelling met het boven beweerde.

Het volgende vindt nu voor elke $p \equiv 1 \bmod 4$ een oplossing voor $p = a^2 + b^2$. Veronderstel dat we w met $w^2 \equiv -1 \bmod p$ hebben gevonden, dan bepalen we a, b uit w met behulp van kettingbreuken als volgt. (Zie ook verderop ...). Kies eerst $w \in \mathbb{Z}$ zo dat $w^2 \equiv -1 \bmod p$ en $0 < w < p/2$; ontwikkel vervolgens p/w in een kettingbreuk, dan blijkt dat

$$\frac{p}{w} = [a_0; a_1, \ldots, a_m, a_m, \ldots, a_1, a_0];$$

de oplossing is te vinden uit de convergenten $p_{m-1}/q_{m-1} = [a_0; a_1, \ldots, a_{m-1}]$ en $p_m/q_m = [a_0; a_1, \ldots, a_m]$; namelijk, $a = p_{m-1}$ en $b = p_m$ voldoen.

Bijvoorbeeld, voor $p = 9973$ hebben we $2798^2 \equiv -1 \bmod p$, en de kettingbreuk van $9973/2798$ is

$$[3; 1, 1, 3, 2, 1, 1, 2, 3, 1, 1, 3].$$

Daaruit vinden we de convergenten

$$\frac{3}{1}, \frac{4}{1}, \frac{7}{2}, \frac{25}{7}, \frac{57}{16}, \frac{82}{23}, \frac{139}{39}, \frac{360}{101}, \frac{1219}{342}, \frac{1579}{443}, \frac{2798}{785}, \frac{9973}{2798}.$$

De tellers van de twee convergenten vlak voor het midden geven de representatie $57^2 + 82^2 = 9973$.

De reden dat dit algoritme werkt zien we wanneer we het uitgebreide algoritme van Euclides uitwerken; in dit voorbeeld doorlopen we de stappen:

$$\begin{aligned}
1 \cdot 9973 &+ 0 \cdot 2798 &&= 9973;\\
0 \cdot 9973 &+ 1 \cdot 2798 &&= 2798;\\
1 \cdot 9973 &- 3 \cdot 2798 &&= 1579;\\
-1 \cdot 9973 &+ 4 \cdot 2798 &&= 1219;\\
2 \cdot 9973 &- 7 \cdot 2798 &&= 360;\\
-7 \cdot 9973 &+ 25 \cdot 2798 &&= 139;\\
16 \cdot 9973 &- 57 \cdot 2798 &&= 82;\\
-23 \cdot 9973 &+ 82 \cdot 2798 &&= 57;\\
39 \cdot 9973 &- 139 \cdot 2798 &&= 25;\\
-101 \cdot 9973 &+ 360 \cdot 2798 &&= 7;\\
342 \cdot 9973 &- 1219 \cdot 2798 &&= 4;\\
-443 \cdot 9973 &- 1579 \cdot 2798 &&= 3;\\
785 \cdot 9973 &- 2798 \cdot 2798 &&= 1.
\end{aligned}$$

Rij $n+1$ wordt hier steeds verkregen uit de rijen n en $n-1$ door deling met rest in de linkerkolom toe te passen; de quotiënten zijn telkens de wijzergetallen. De symmetrie tussen de rij coëfficiënten in de tweede kolom en de derde kolom wordt veroorzaakt door de eigenschap dat $2798^2 \equiv -1 \bmod 9973$: neem elke rij modulo $p = 9973$ en vermenigvuldig met -2798. We vinden de onderste helft van het schema dus eenvoudig uit de bovenste. We kunnen ophouden zodra in de rechterkolom een getal kleiner dan $\sqrt{p}$ verschijnt, en de gezochte a en b staan dan als coëfficiënt in de tweede en in de derde kolom.

1.2 Oneindige kettingbreuken

We verruimen nu onze blik, en laten willekeurige reële getallen x toe bij het bepalen van kettingbreuken: dat wil zeggen, we passen de iteratie uit 1.1 nu toe op $x_0 = x \in \mathbb{R}$. We krijgen dan

$$\begin{aligned} x_0 &= a_0 + \frac{1}{x_1}, \\ x_1 &= a_1 + \frac{1}{x_2}, \end{aligned}$$

enzovoorts, en het is duidelijk dat dit een oneindige rij $[a_0; a_1, a_2, \ldots]$ van wijzergetallen definieert, tenzij $x = x_0$ rationaal is. Als voorheen bepaalt dit een rij (die nu oneindig mag zijn) van convergenten

$$\frac{p_{-1}}{q_{-1}} = \frac{1}{0}, \frac{p_0}{q_0} = \frac{a_0}{1}, \frac{p_1}{q_1}, \frac{p_2}{q_2}, \cdots .$$

Het is met inductie ook eenvoudig in te zien dat voor $n \geq 0$

$$x = \frac{x_{n+1}p_n + p_{n-1}}{x_{n+1}q_n + q_{n-1}}; \tag{1.3}$$

immers voor $n = 0$ staat er

$$x = \frac{x_1 a_0 + 1}{x_1} = a_0 + \frac{1}{x_1} = x_0,$$

en er geldt dat

$$\begin{aligned} \frac{x_{n+1}p_n + p_{n-1}}{x_{n+1}q_n + q_{n-1}} &= \frac{x_{n+1}(a_n p_{n-1} + p_{n-2}) + p_{n-1}}{x_{n+1}(a_n q_{n-1} + q_{n-2}) + q_{n-1}} = \frac{(a_n p_{n-1} + p_{n-2}) + \frac{p_{n-1}}{x_{n+1}}}{(a_n q_{n-1} + q_{n-2}) + \frac{q_{n-1}}{x_{n+1}}} \\ &= \frac{(a_n + \frac{1}{x_{n+1}})p_{n-1} + p_{n-2}}{(a_n + \frac{1}{x_{n+1}})q_{n-1} + q_{n-2}} = \frac{x_n p_{n-1} + p_{n-2}}{x_n q_{n-1} + q_{n-2}}, \end{aligned}$$

waar we de recursieve relatie voor tellers en noemers van convergenten uit 1.2 gebruiken (het bewijs met inductie werkt natuurlijk ook voor oneindige kettingbreuken).

Verderop formuleren en gebruiken we een soort omkering van 1.3.

Net als in het bewijs van 1.1.8 zien we voor oneindige kettingbreuken dat de convergenten steeds betere rationale benaderingen geven, afwisselend van boven en beneden, voor x, en dat twee opeenvolgende convergenten op afstand $(q_{k-1}q_k)^{-1}$ liggen. Uit Stelling 1.1.8 volgt onmiddellijk dat

$$x = \lim_{n\to\infty} \frac{p_n}{q_n}.$$

1.2.1 Stelling *Voor de convergenten p_k/q_k van een irrationaal getal x geldt:*

$$\frac{1}{2q_kq_{k+1}} < \frac{1}{q_k(q_k+q_{k+1})} < \left|x - \frac{p_k}{q_k}\right| < \frac{1}{q_kq_{k+1}} < \frac{1}{q_k^2},$$

voor $k \geq 1$.

Bewijs Uit 1.3 volgt

$$\left|x - \frac{p_k}{q_k}\right| = \left|\frac{x_{k+1}p_k + p_{k-1}}{x_{k+1}q_k + q_{k-1}} - \frac{p_k}{q_k}\right| = \left|\frac{(-1)^k}{q_k(q_kx_{k+1} + q_{k-1})}\right|.$$

Omdat $a_{k+1} < x_{k+1} < a_{k+1} + 1$ is $q_{k+1} < q_kx_{k+1} + q_{k-1} < q_{k+1} + q_k$, dus

$$\frac{1}{q_k(q_k+q_{k+1})} < \left|x - \frac{p_k}{q_k}\right| < \frac{1}{q_kq_{k+1}}.$$

De overige ongelijkheden volgen uit $q_k < q_{k+1}$.

1.2.2 Stelling *Voor twee opeenvolgende convergenten $p_{k-1}/q_{k-1}, p_k/q_k$ van een irrationaal getal x geldt:*

$$\left|x - \frac{p_{k-1}}{q_{k-1}}\right| < \frac{1}{2q_{k-1}^2} \quad \textit{of} \quad \left|x - \frac{p_k}{q_k}\right| < \frac{1}{2q_k^2}.$$

Bewijs Uit

$$\left|\frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}}\right| = \left|x - \frac{p_k}{q_k}\right| + \left|x - \frac{p_{k-1}}{q_{k-1}}\right|$$

en de veronderstelling dat de bewering niet klopt zou volgen:

$$\frac{1}{q_{k-1}q_k} = \left|\frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}}\right| \geq \frac{1}{2q_k^2} + \frac{1}{2q_{k-1}^2}$$

hetgeen equivalent is met

$$(q_k - q_{k-1})^2 \leq 0;$$

een tegenspraak, omdat $q_k > q_{k-1}$ voor $k \geq 2$.

1.2.3 Stelling *Als de breuk p/q voor een convergent p_k/q_k van x voldoet aan $0 < q \leq q_k$ dan geldt*

$$\frac{p}{q} \neq \frac{p_k}{q_k} \quad \Rightarrow \quad \left|x - \frac{p}{q}\right| > \left|x - \frac{p_k}{q_k}\right|.$$

BEWIJS Zonder beperking mogen we veronderstellen dat p en q onderling ondeelbaar zijn. Als $q = q_k$ dan

$$\left|\frac{p}{q} - \frac{p_k}{q_k}\right| > \frac{1}{q_k}$$

maar

$$\left|x - \frac{p_k}{q_k}\right| < \frac{1}{2q_k}$$

zodat

$$\left|x - \frac{p_k}{q_k}\right| < \left|x - \frac{p}{q}\right|.$$

Veronderstel nu, zonder beperking der algemeenheid, dat $q_{k-1} < q < q_k$; laat de gehele getallen e, f gedefinieerd zijn door

$$e = (qp_{k-1} - pq_{k-1}), \quad f = (pq_k - qp_k),$$

dan is $f \neq 0$ en

$$\begin{aligned} ep_k + fp_{k-1} = p(p_{k-1}q_k - p_kq_{k-1}) &= \pm p, \\ eq_k + fq_{k-1} = q(p_{k-1}q_k - p_kq_{k-1}) &= \pm q, \end{aligned}$$

zodat we eventueel door het teken van e en f te veranderen mogen aannemen dat rechts +tekens staan. Omdat $eq_k + fq_{k-1} = q < q_k$ hebben e en f tegengesteld teken, evenals $p_k - q_kx$ en $p_{k-1} - q_{k-1}x$. Maar dan hebben $e(p_k - q_kx)$ en $f(p_{k-1} - q_{k-1}x)$ juist weer hetzelfde teken. Bovendien is

$$p - qx = e(p_k - q_kx) + f(p_{k-1} - q_{k-1}x)$$

en als $|f| = 1$ dan is $e \neq 0$ omdat $q > q_{k-1}$, zodat

$$|p - qx| > |p_{k-1} - q_{k-1}x|.$$

Uit Stelling 1.2.1 volgt

$$|p_{k-1} - q_{k-1}x| > q_{k-1}\frac{1}{q_{k-1}(q_{k-1} + q_k)} \geq \frac{1}{q_{k+1}} > q_k\left|\frac{p_k}{q_k} - x\right| = |p_k - q_kx|.$$

Dus $|p - qx| > |p_k - q_kx|$ en de bewering volgt bij deling door q links en door $q_k > q$ rechts.

1.2.4 Stelling *Als de breuk p/q voldoet aan*

$$\left|x - \frac{p}{q}\right| < \frac{1}{2q^2}$$

dan is

$$\frac{p}{q} = \frac{p_k}{q_k}.$$

voor een convergent p_k/q_k van x.

BEWIJS Ontwikkel p/q in een eindige kettingbreuk van oneven lengte n; dan is $p/q = p_n/q_n$ en

$$\frac{p_n}{q_n} - x = \frac{\delta}{q_n^2}, \quad \delta < \frac{1}{2}.$$

Er bestaat een $y > 0$ zodat

$$x = \frac{yp_n + p_{n-1}}{yq_n + q_{n-1}},$$

en dan is

$$\frac{\delta}{q_n^2} = \frac{p_n}{q_n} - x = \frac{p_n q_{n-1} - p_{n-1}q_n}{q_n(yq_n + q_{n-1}} = \frac{(-1)^{n+1}}{q_n(yq_n + q_{n-1}}),$$

en dus

$$\delta = \frac{q_n}{yq_n + q_{n-1}}$$

waaruit volgt dat

$$y = \frac{1}{\delta} - \frac{q_{n-1}}{q_n} > 1.$$

Volgens Lemma 1.2.5, hieronder, zijn p_{n-1}/q_{n-1} en $p_n/q_n = p/q$ dan opeenvolgende convergenten van x.

1.2.5 Lemma *Als*

$$x = \frac{py + r}{qy + s},$$

met $y \in \mathbb{R}$ *en* $p, q, r, s \in \mathbb{Z}$ *zodanig dat*

$$y > 1, \quad q > s > 0, \quad ps - qr = \pm 1,$$

dan bestaat er een $n \geq 0$ *zodat*

$$y = x_{n+1}, \quad \frac{p}{q} = \frac{p_n}{q_n}, \quad \frac{r}{s} = \frac{p_{n-1}}{q_{n-1}},$$

als $x = [a_0; a_1, \ldots]$, $x_i = [a_i; a_{i+1}, \ldots]$ *en* $p_i/q_i = [a_0; a_1, \ldots, a_i]$ *voor* $i \geq 0$.

BEWIJS Ontwikkel p/q in een kettingbreuk $p/q = [A_0; A_1, \ldots, A_n] = v_n/w_n$, en laat $v_{n-1}/w_{n-1} = [A_0; A_1, \ldots, A_{n-1}]$. Hier hebben we de kettingbreuk zo aangepast dat voor de lengte n geldt dat $(-1)^{n+1} = v_n w_{n-1} - v_{n-1}w_n = ps - qr = \pm 1$. Dan is

$$v_n w_{n-1} - v_{n-1}w_n = v_n s - v_n r,$$

en volgt $v_n(w_{n-1} - s) = w_n(v_{n-1} - r)$ en dus (omdat v_n, w_n onderling ondeelbaar zijn en $v_n > v_{n-1}$) dat $s = w_{n-1}$ en $r = v_{n-1}$. Maar de kettinbreukontwikkeling van

$$\frac{v_n y + v_{n-1}}{w_n y + w_{n-1}} = [A_0; A_1, \ldots, A_n, y]$$

(vergelijk 1.3) en dus is $[A_0; A_1, \ldots, A_n]$ het beginstuk van de kettingbreuk voor x en y de staart: $[A_0; A_1, \ldots, A_n] = [a_0; a_1, \ldots, a_n]$ en $y = [A_{n+1}; A_{n+2}, \ldots] = [a_{n+1}; a_{n+2}, \ldots]$ de staart.

Twee reële getallen die zoals in het eerdere Lemma via een unimodulaire transformatie met elkaar in verband staan, hebben op mogelijk een verschillend beginstuk na dezelfde kettingbreukontwikkeling. We noemen twee zulke reële getallen x, y, waarvoor dus geldt:

$$x = \frac{ay+b}{cy+d}, \quad \text{met} \quad ad - bc = \pm 1,$$

equivalent.

1.2.6 Stelling *Twee irrationale getallen x, y met kettingbreukontwikkelingen $x = [a_0; a_1, \ldots]$, $y = [b_0; b_1, \ldots]$ zijn equivalent dan en slechts dan als er gehele getallen $m, n \geq 0$ bestaan zodat*

$$x_{n+1} = [a_{n+1}; a_{n+2} \ldots] = [b_{m+1}; b_{m+2}, \ldots] = y_{m+1}.$$

Bewijs Veronderstel dat

$$x = \frac{ay+b}{cy+d};$$

en dat $(cy+d) > 0$. Gebruik 1.3 om te schrijven:

$$x = \frac{a(\frac{y_{m+1}p_m+p_{m-1}}{y_{m+1}q_m+q_{m-1}})+b}{c\frac{y_{m+1}p_m+p_{m-1}}{y_{m+1}q_m+q_{m-1}}+d} = \frac{(ap_m+bq_m)y_{m+1}+(ap_{m-1}+bq_{m-1})}{(cp_m+dq_m)y_{m+1}+(cp_{m-1}+dq_{m-1})} = \frac{\alpha y_{m+1}+\beta}{\gamma y_{m+1}+\delta}.$$

Als m groot genoeg is, is

$$cp_m + dq_m > cp_{m-1} + dq_{m-1} > 0.$$

Maar dan is

$$x = \frac{\alpha y_{m+1}+\beta}{\gamma y_{m+1}+\delta}$$

met $\gamma > \delta > 0$ en

$$\begin{aligned} \alpha\delta - \gamma\beta &= (ap_m+bq_m)(cp_{m-1}+dq_{m-1}) - (cp_m+dq_m)(ap_{m-1}+bq_{m-1}) \\ &= (ad-bc)(p_mq_{m-1} - p_{m-1}q_m) = \pm 1. \end{aligned}$$

Dit kan alleen maar als y_{m+1} gelijk is aan x_{n+1}, voor zekere $n \geq 1$, volgens Lemma 1.2.5.

Omgekeerd, als $x_{n+1} = [a_{n+1}; a_{n+2} \ldots] = [b_{m+1}; b_{m+2}, \ldots]$, dan is

$$x = [a_0; a_1, \ldots, a_n, b_{m+1}; b_{m+2}, \ldots] = \frac{p_nx_{n+1}+p_{n-1}}{q_nx_{n+1}+q_{n-1}} = \frac{p_ny_{m+1}+p_{n-1}}{q_ny_{m+1}+q_{n-1}}$$

zodat x en y_{m+1} equivalent zijn. Omdat ook y en y_{m+1} equivalent zijn, volgt equivalentie van x en y uit het feit dat equivalentie een equivalentierelatie is (zie opgave).

We richten ons nu op het eenvoudigste soort oneindige kettingbreuken, namelijk de repeterende. Het zal blijken dat die precies corresponderen met kwadratisch irrationale getallen, maar voordat we dat bewijzen, geven we eerst een voorbeeld.

1.2.7 Voorbeeld (wortel) We bepalen de kettingbreuk voor $\sqrt{77}$. Het is belangrijk om op te merken dat we hiervoor alleen maar hoeven te weten dat $8^2 < 77 < 9^2$ en dus $8 < \sqrt{77} < 9$.

$$x_0 = x = \sqrt{77},\ \text{dus } a_0 = \lfloor x_0 \rfloor = 8.$$

Dan

$$x_1 = \frac{1}{x_0 - a_0} = \frac{1}{\sqrt{77} - 8} = \frac{\sqrt{77}+8}{77-64},\ \text{dus } a_1 = \lfloor x_1 \rfloor = 1.$$

Vervolgens

$$x_2 = \frac{1}{x_1 - a_1} = \frac{1}{\frac{\sqrt{77}-5}{13}} = \frac{\sqrt{77}+5}{\frac{77-25}{13}} = \frac{\sqrt{77}+5}{4},\ \text{dus } a_2 = \lfloor x_2 \rfloor = 3.$$

Daarna

$$x_3 = \frac{1}{x_2 - a_2} = \frac{1}{\frac{\sqrt{77}-7}{4}} = \frac{\sqrt{77}+7}{\frac{77-49}{4}} = \frac{\sqrt{77}+7}{7},\ \text{dus } a_3 = \lfloor x_3 \rfloor = 2,$$

en

$$x_4 = \frac{1}{x_3 - a_3} = \frac{1}{\frac{\sqrt{77}-7}{7}} = \frac{\sqrt{77}+7}{\frac{77-49}{7}} = \frac{\sqrt{77}+7}{4},\ \text{dus } a_4 = \lfloor x_4 \rfloor = 3,$$

waaruit volgt

$$x_5 = \frac{1}{x_4 - a_4} = \frac{1}{\frac{\sqrt{77}-5}{4}} = \frac{\sqrt{77}+5}{\frac{77-25}{4}} = \frac{\sqrt{77}+5}{13},\ \text{dus } a_5 = \lfloor x_5 \rfloor = 1.$$

Tenslotte is

$$x_6 = \frac{1}{x_5 - a_5} = \frac{1}{\frac{\sqrt{77}-8}{13}} = \frac{\sqrt{77}-8}{\frac{77-64}{13}} = \frac{\sqrt{77}+8}{1},\ \text{dus } a_6 = \lfloor x_6 \rfloor = 16,$$

zodat

$$x_7 = \frac{1}{x_6 - a_6} = \frac{1}{\sqrt{77} - 8} = x_1,$$

en de kettingbreuk repeteert vanaf hier:

$$x + [8; \overline{1, 3, 2, 3, 1, 16}]$$

waar de overstreping oneindige herhaling van dat blok wijzergetallen aangeeft.

1.2.8 Definitie Een oneindige kettingbreuk $[a_0; a_1, a_2, \ldots]$ heet *periodiek met periodelengte* m als er een $N \geq 0$ bestaat zodanig dat voor alle $n \geq N$ geldt dat $a_n = a_{n+m}$ en er geen kleinere $m \geq 1$ met die eigenschap bestaat. De wijzergetallen $a_0, \ldots, a_{N-1}$ vormen dan de *preperiode*, de (zich steeds herhalende) $a_N, \ldots, a_{N+m-1}$ de *periode*. Een kettingbreuk heet *zuiver periodiek* als hij periodiek is en $N = 0$ genomen kan worden, dat wil zeggen, er is geen preperiode.

Om alle identiteiten in onderstaande bewijzen ook te laten gelden wanneer $N = 0$, is het handig de (teller en noemer van de) convergent met index -2 te definiëren door $p_{-2} = 0$, en $q_{-2} = 1$. De gebruikelijke recursies (zoals $p_k = a_k p_{k-1} + p_{k-2}$) blijven dan ook geldig voor $k = 0$.

1.2.9 Stelling (Euler) *Een irrationaal getal x met een periodieke kettingbreuk is een element van $\mathbb{Q}(\sqrt{d})$ voor een $d \in \mathbb{Z}_{\geq 1}$, waar d geen kwadraat is.*

Bewijs Veronderstel dat $x = [a_0; a_1, \ldots, a_{N-1}, \overline{a_N, \ldots, a_{N+m-1}}]$, en gebruik nu dat $x_N = x_{N+m}$ met relatie 1.3:

$$x = \frac{x_N p_{N-1} + p_{N-2}}{x_N q_{N-1} + q_{N-2}} = \frac{x_{N+m} p_{N+m-1} + p_{N+m-2}}{x_{N+m} q_{N+m-1} + q_{N+m-2}},$$

dan is

$$-\frac{x q_{N-2} - p_{N-2}}{x q_{N-1} - p_{N-1}} = x_N = x_{N+m-1} = -\frac{x q_{N+m-2} + p_{N+m-2}}{x q_{N+m-1} + p_{N+m-1}},$$

en daarom

$$\begin{aligned} 0 &= (q_{N-2}q_{N+m-1} - q_{N-1}q_{N+m-2})x^2 + \\ &+ (p_{N-1}q_{N+m-2} - p_{N-2}q_{N+m-1} + p_{N+m-2}q_{N-1} - p_{N+m-1}q_{N-2})x + \\ &+ p_{N-2}p_{N+m-1} - p_{N-1}p_{N+m-2}. \end{aligned} \tag{1.4}$$

Dit is een kwadratische vergelijking die niet ontaard is; immers de kopcoëfficiënt kan alleen nul zijn wanneer

$$q_{N-2}q_{N+m-1} = q_{N-1}q_{N+m-2},$$

maar omdat q_{N+m-2} en q_{N+m-1} onderling ondeelbaar zijn kan dat alleen indien q_{N-m+2} een deler is van q_{N-2}, hetgeen in tegenspraak is met $q_{N-m+2} > q_{N-2}$.

1.2.10 Definities Als $x \in \mathbb{Q}(\sqrt{d})$ dan bestaan er $a, b \in \mathbb{Q}$ zodat $x = a + b\sqrt{d}$, en we noemen het element $\bar{x} = a - \sqrt{d}$ de *geconjugeerde* van x. Omdat eenvoudig is in te zien dat de geconjugeerde van de som, resp. het product van twee elementen van $\mathbb{Q}(\sqrt{d})$ de som, resp. het product van de geconjugeerden is, en de geconjugeerde van een element van $\mathbb{Q}$ het element zelf is, volgt dat $\bar{x}$ aan dezelfde kwadratische vergelijking over $\mathbb{Q}$ voldoet als x:

$$ax^2 + bx + c = 0 \quad \Rightarrow \quad a\bar{x}^2 + b\bar{x} + c = 0.$$

voor $a, b, c \in \mathbb{Q}$.

Wanneer x kwadratisch irrationaal is, zullen we in het vervolg P, Q, d willen kiezen zodat $x = (P + \sqrt{d})/Q$, zodanig dat $P, Q, d \in \mathbb{Z}$, met $d > 0$ geen kwadraat en Q een deler van $P^2 - d$. Dat kan altijd, omdat voor zekere a, b, c geldt dat $ax^2 + bx + c = 0$, en volgens de 'wortelformule' kunnen we dan $P = -b$ nemen, $Q = 2a$ en $d = b^2 - 4ac$.

Een element x van $\mathbb{Q}(\sqrt{d})$ heet *gereduceerd* als $x > 1$ en $-1 < \bar{x} < 0$.

1.2.11 Stelling (Lagrange) *Als x irrationaal is en $x \in \mathbb{Q}(\sqrt{d})$ met $d \in \mathbb{Z}_{\geq 1}$ dan is de kettingbreuk van x periodiek.*

BEWIJS Schrijf $x = x_0 = (P_0 + \sqrt{d})/Q_0$, met $Q_0 \,|\, P^2 - d$. Met $a_0 = \lfloor x_0 \rfloor$ krijgen we

$$x_1 = \frac{1}{x_0 - a_0} = \frac{1}{\frac{(P_0 - a_0 Q_0) + \sqrt{d}}{Q_0}} = \frac{(P_0 - a_0 Q_0) - \sqrt{d}}{\frac{(P_0 - a_0 Q_0)^2 - d}{Q_0}} = \frac{(a_0 Q_0 - P_0) + \sqrt{d}}{\frac{d - P_0^2}{Q_0} + 2a_0 P_0 - a_0^2 Q_0}$$

hetgeen gelijk is aan

$$\frac{P_1 + \sqrt{d}}{Q_1},$$

als we schrijven

$$P_1 = a_0 Q_0 - P_0, \quad Q_1 = \frac{d - P_0^2}{Q_0} + 2a_0 P_0 - a_0^2 Q_0 = \frac{d - P_1^2}{Q_0};$$

dit is opnieuw van onze standaardvorm, daar duidelijk $Q_1 \,|\, d - P_1^2$. Dus is, met inductie, voor $k \geq 1$, te schrijven $x_k = (P_k + \sqrt{d})/Q_k$, waar

$$P_k = a_{k-1} Q_{k-1} - P_{k-1}, \quad Q_k = \frac{d - P_{k-1}^2}{Q_{k-1}} + 2a_{k-1} P_{k-1} - a_{k-1}^2 Q_{k-1} = \frac{d - P_k^2}{Q_{k-1}},$$

met $Q_k \,|\, d - P_k^2$. We leiden een aantal ongelijkheden af, waaruit allereerst volgt dat er maar eindig veel verschillende mogelijkheden zijn voor (P_k, Q_k), maar waarvan we ook later nog gebruik zullen maken. Conjugeren we de gelijkheid

$$x = x_0 = \frac{x_k p_{k-1} + p_{k-2}}{x_k q_{k-1} + q_{k-2}},$$

dan krijgen we voor de geconjugeerde

$$\bar{x}_0 = \frac{\bar{x}_k p_{k-1} + p_{k-2}}{\bar{x}_k q_{k-1} + q_{k-2}},$$

zodat

$$\bar{x}_k = -\frac{\bar{x}_0 q_{k-2} - p_{k-2}}{\bar{x}_0 q_{k-1} - p_{k-1}} = -\frac{q_{k-2}}{q_{k-1}} \left(\frac{\bar{x}_0 - \frac{p_{k-2}}{q_{k-2}}}{\bar{x}_0 - \frac{p_{k-1}}{q_{k-1}}} \right),$$

maar omdat p_k/q_k convergeert naar $x_0 \neq \bar{x}_0$, en $q_{k-2} < q_{k-1}$ is voor k groot genoeg $-1 < \bar{x}_k < 0$ terwijl $x_k > 1$ (dus x_k is gereduceerd, voor k groot genoeg). Maar dan is

$$\frac{2\sqrt{d}}{Q_k} = x_k - \bar{x}_k > 0, \quad \text{dus} \quad Q_k > 0$$

en

$$\frac{2P_k}{Q_k} = x_k + \bar{x}_k > 0, \quad \text{dus} \quad P_k > 0.$$

Bovendien is

$$-1 < \bar{x}_k = \frac{P_k - \sqrt{d}}{Q_k} < 0$$

zodat

$$P_k < \sqrt{d} \quad \text{en} \quad \sqrt{d} - P_k < Q_k,$$

en

$$\frac{P_k+\sqrt{d}}{Q_k} = x_k > 1 \quad \text{dus} \quad Q_k < P_k + \sqrt{d},$$

en daarom

$$0 < P_k < \sqrt{d} \quad \text{en} \quad 0 < Q_k < 2\sqrt{d}. \tag{1.5}$$

Dat voltooit het bewijs. Merk nog wel op dat

$$\sqrt{d} < x_k = \frac{P_k+\sqrt{d}}{Q_k} \quad \Rightarrow \quad P_k > \sqrt{d}(Q_k - 1)$$

zodat (omdat $P_k < \sqrt{d}$) de ongelijkheid $x_k > \sqrt{d}$ precies optreedt wanneer $Q_k = 1$. In het bijzonder is

$$a_k < \sqrt{d} \quad \text{tenzij} \quad Q_k = 1, \text{ en dan } a_k < 2\sqrt{d}. \tag{1.6}$$

1.2.12 Stelling (Galois) *Een kwadratisch irrationaal getal x heeft een zuiver periodieke kettingbreuk dan en slechts dan als x gereduceerd is. Bovendien heeft in dat geval $-\frac{1}{\bar{x}}$ de omgekeerde periode:*

$$x = [\overline{a_0; a_1, \ldots, a_{m-1}}], \quad \textit{en} \quad -\frac{1}{\bar{x}} = [\overline{a_{m-1}; a_{m-2}, \ldots, a_0}].$$

Bewijs Veronderstel dat x zuiver periodieke kettingbreuk heeft; dan is $a_0 = a_m \geq 1$ en dus is $x = x_0 > 1$. Beschouw nu het kwadratische polynoom uit 1.4 waarvan x nulpunt is, in het huidige geval $N = 0$ (met de in Definitie 1.2.8 ingevoerde conventies voor p_{-2} en q_{-2}):

$$f(X) = q_{m-1}X^2 + (q_{m-2} - p_{m-1})X - p_{m-2};$$

dan geldt $f(0) = -p_{m-2} < 0$ terwijl $f(-1) = q_{m-1} - q_{m-2} + p_{m-1} - p_{m-2} > 0$ en dus heeft f een nulpunt tussen -1 en 0 dat dan wel $\bar{x}$ moet zijn. Dan is x juist gereduceerd.

Is, omgekeerd, x gereduceerd kwadratisch, dus $-1 < \bar{x} < 0$ en $x > 1$, dan is

$$x_0 = a_0 + \frac{1}{x_1}, \quad \text{en} \quad \bar{x}_0 = a_0 + \frac{1}{\bar{x}_1},$$

zodat

$$\frac{1}{\bar{x}_1} = -a_0 + \bar{x}_0 < -a_0 \leq -1,$$

vanwaar $-1 < \bar{x}_1 < 0$. Dan met inductie $-1 < \bar{x}_k < 0$ voor $k \geq 0$. Nemen we aan dat x geen zuiver periodieke kettingbreuk heeft (die wel periodiek is met periode m zeg, want x is kwadratisch), dan is er een N zodat $a_{N-1} \neq a_{N+m-1}$ maar $x_N = x_{N+m}$ en we krijgen

$$0 \neq x_{N-1} - x_{N+m-1} = a_{N-1} + \frac{1}{x_N} - (a_{N+m-1} + \frac{1}{x_{N+m}}) = a_{N-1} - a_{N+m-1} \in \mathbb{Z},$$

en dan ook $0 \neq \bar{x}_N - \bar{x}_{N+m} \in \mathbb{Z}$ terwijl zowel $\bar{x}_N$ als $\bar{x}_{N+m}$ tussen -1 en 0 ligt: een tegenspraak.

De laatste bewering volgt door te kijken naar

$$x_0 = a_0 + \frac{1}{x_1}, x_1 = a_1 + \frac{1}{x_1}, \ldots, x_{m-2} = a_{m-2} + \frac{1}{x_{m-1}}, x_{m-1} = a_{m-1} + \frac{1}{x_0},$$

en de geconjugeerden

$$\bar{x}_0 = a_0 + \frac{1}{\bar{x}_1}, \bar{x}_1 = a_1 + \frac{1}{\bar{x}_1}, \ldots, \bar{x}_{m-2} = a_{m-2} + \frac{1}{\bar{x}_{m-1}}, \bar{x}_{m-1} = a_{m-1} + \frac{1}{\bar{x}_0},$$

omdat, in omgekeerde volgorde lezend,

$$-\frac{1}{\bar{x}_0} = a_{m-1} - \bar{x}_{m-1}, -\frac{1}{\bar{x}_{m-1}} = a_{m-2} - \bar{x}_{m-2}, \ldots, -\frac{1}{\bar{x}_1} = a_0 - \bar{x}_0.$$

Omdat x_n gereduceerd is voor $n \geq 0$, is $0 < -\bar{x}_n < 1$ en daarom staat hier de kettingbreukontwikkeling van $-1/\bar{x}_0$: $[a_{m-1}; a_{m-2}, \ldots, a_0, a_{m-1}, \ldots]$.

1.2.13 Stelling *De kettingbreuk van $\sqrt{d}$, voor $d \in \mathbb{Z}_{\geq 1}$ (geen kwadraat) heeft de vorm*

$$[a_0; \overline{a_1, a_2, \ldots, a_2, a_1, 2a_0}\ ].$$

Bewijs Laat de periodelengte van de kettingbreuk voor $x_0 = \sqrt{d}$ eens m zijn, en de preperiode lengte N hebben:

$$\sqrt{d} = [a_0; a_1, \ldots, a_{N-1}, \overline{a_N, \ldots, a_{N+m-1}}].$$

Dan is

$$x_0 = \sqrt{d} = \lfloor \sqrt{d} \rfloor + \frac{1}{x_1}$$

en

$$x_1 = \frac{1}{\sqrt{d} - \lfloor \sqrt{d} \rfloor} > 1.$$

Bovendien is

$$\bar{x}_1 = \frac{1}{-\sqrt{d} - \lfloor \sqrt{d} \rfloor} = \frac{-1}{\sqrt{d} + \lfloor \sqrt{d} \rfloor} > -1$$

zodat $-1 < \bar{x}_1 < 0$. Dus is x_1 gereduceerd, en heeft deze volgens de vorige Stelling een zuiver periodieke kettingbreuk $x_1 = [\overline{a_1; a_2, \ldots, a_m}]$, terwijl

$$\sqrt{d} + \lfloor \sqrt{d} \rfloor = -\frac{1}{\bar{x}_1} = [\overline{a_m; a_{m-1}, \ldots, a_1}] = [a_m; \overline{a_{m-1}, \ldots, a_1, a_m}].$$

Anderzijds is

$$\sqrt{d} + \lfloor \sqrt{d} \rfloor = x_0 + a_0 = [2a_0; \overline{a_1, a_2, \ldots, a_m}],$$

en het resultaat volgt.

1.2.14 Opmerking Uit wat we al bewezen hebben over P_k en Q_k volgt onmiddellijk dat de periodelengte m van $\sqrt{d}$ (en daarmee van elk kwadratisch irrationaal getal) begrensd is door $2d$; een scherpe bovengrens is van de orde $\sqrt{d} \log d$.

Ook is eenvoudig te bewijzen dat in de kettingbreuk van $\sqrt{d}$ geldt dat

$$Q_k = 1 \quad \Longleftrightarrow \quad m | k.$$

1.2.15 Toepassing (Pell) De Pell-vergelijking is de vergelijking $x^2 - dy^2 = 1$, met $d \in \mathbb{Z}_{\geq 2}$ geen kwadraat; er worden niet-negatieve gehele oplossingen voor x, y gezocht. We betrekken ook de vergelijking $x^2 - dy^2 = -1$ direct mee in de beschouwing. Omdat

$$x^2 - dy^2 = (x - y\sqrt{d})(x + y\sqrt{d}) = (x - \sqrt{d})^2 + 2y\sqrt{d},$$

zien we dat voor oplossingen (x, y) van de vergelijkingen geldt

$$0 < \left| \frac{x}{y} - \sqrt{d} \right| < \frac{1}{2y^2\sqrt{d}} < \frac{1}{2y^2}.$$

Volgens Stelling 1.2.4 geldt dan dat x/y een convergent van $\sqrt{d}$ moet zijn. Dus alle oplossingen van de vergelijkingen $x^2 - dy^2 = \pm 1$ zijn te vinden onder de convergenten van $\sqrt{d}$.

Om alle oplossingen te bepalen gebruiken we weer de relatie

$$x = \frac{x_{n+1}p_n + p_{n-1}}{x_{n+1}q_n + q_{n-1}},$$

met $x = \sqrt{d}$ en $x_{n+1} = (P_{n+1} + \sqrt{d})/Q_{n+1}$. Hieruit volgt

$$(q_{n-1}Q_{n+1} + q_nP_{n+1} - p_n)\sqrt{d} = p_nP_{n+1} + p_{n-1}Q_{n+1} - q_nd,$$

en dat kan alleen als links en rechts nul staat, dus

$$p_n = q_{n-1}Q_{n+1} + q_nP_{n+1}, \quad \text{en} \quad q_nd = p_{n-1}Q_{n+1} + p_nP_{n+1}.$$

Maar dan is

$$\begin{aligned} p_n^2 - q_n^2 d &= p_n(q_{n-1}Q_{n+1} + q_nP_{n+1}) - q_n(p_{n-1}Q_{n+1} + p_nP_{n+1}) = \\ &= (p_nq_{n-1} - p_{n-1}q_n)Q_{n+1} = (-1)^{n+1}Q_{n+1}. \end{aligned}$$

Volgens de voorgaande opmerking kan dat laatste alleen ± 1 zijn indien $n+1$ een veelvoud is van de periodelengte m van de kettingbreuk voor $\sqrt{d}$. Is die periodelengte m *even*, dan zijn voor $k = 0, 1, 2, 3, \ldots$ de tellers en noemers (p_{km-1}, q_{km-1}) van de convergenten van $\sqrt{d}$ dus precies alle oplossingen van de vergelijking $x^2 - dy^2 = 1$ en zijn er geen oplossingen voor de vergelijking met -1; is de periodelengte oneven, dan zijn beide vergelijkingen oplosbaar en vormen (p_{km-1}, q_{km-1}) voor $k = 1, 3, 5, \ldots$ alle oplossingen voor $x^2 - dy^2 = -1$ en (p_{km-1}, q_{km-1}) voor $k = 0, 2, 4, \ldots$ alle oplossingen voor $x^2 - dy^2 = 1$.

1.2.16 Toepassing (factorisatie) Een aantal van de beste methoden om een gegeven getal N in factoren te ontbinden is gebaseerd op het idee dat wanneer je twee gehele getallen x en y hebt met $0 < x < y < N$ zodat modulo N geldt $x^2 \equiv y^2$, dan zal $\text{ggd}(N, x - y)$ een factor voor N opleveren omdat dan N een deler is van $x^2 - y^2 = (x - y)(x + y)$. Die factor kan triviaal zijn, wanneer $x \equiv -y \bmod N$, (een geval dat wel op moet treden wanneer N priem is), maar als N minstens twee verschillende priemdelers heeft kan het zijn dat sommige

priemfactoren in $x+y$ zitten en andere in $x-y$ zodat we een niet-triviale factor detecteren.

Het grote probleem is natuurlijk om x en y te *vinden*. Fermat probeerde $x^2-y^2=N$ op te lossen door systematisch te zoeken, beginnend bij $x=\lfloor\sqrt{N}\rfloor$, en x telkens met 1 ophogend, naar een kwadraat van de vorm x^2-N. Dit werkt aardig wanneer N het product is van twee priemgetallen die heel dicht bij elkaar liggen, maar hopeloos als de twee ver uiteen lopen, bijvoorbeeld $p\approx\sqrt[3]{N}$.

Een succesvolle (en tot in de jaren 1980 veel gebruikte) aanpassing maakt gebruik van kettingbreuken, als volgt. We gebruiken de in het vorige voorbeeld gevonden identiteit $p_n^2-Nq_n^2=(-1)^{n+1}Q_{n+1}$, voor de convergenten p_n/q_n van $\sqrt{N}$, met $x_n=(P_n+\sqrt{N})/Q_n$, voor $n\geq 0$, en de ongelijkheid $Q_{n+1}<2\sqrt{N}$. Het nut is gelegen in de congruentie $p_n^2\equiv(-1)^{n+1}Q_{n+1} \bmod N$. Om ook rechts een kwadraat te krijgen vereist wat veel geluk, maar we kunnen wel congruenties proberen te *combineren* tot een kwadraat, en daarvoor willen we Q_{n+1} klein hebben om deze te kunnen ontbinden in factoren. Het idee is als volgt: leg een lijst van kleine priemgetallen aan (te beginnen met $-1,2,3,5,\cdots$, zie echter onder), voer een stap in de kettingbreukontwikkeling van N uit, en zie (via deling met rest door de priemen) of Q_{n+1} te ontbinden is met behulp van uitsluitend de priemen uit de lijst. Bepaal dan de exponenten k_i in

$$Q_{n+1}=(-1)^{k_0}p_1^{k_1}\cdots p_r^{k_r},$$

en herhaal dit proces. Het doel is om zo een matrix met als rijen de gevonden exponenten modulo 2 op te bouwen en in deze matrix een afhankelijheid tussen de rijen te vinden: zo'n afhankelijkheid modulo 2 betekent namelijk dat er een product van overeenkomstige Q's bestaat waarvan de exponenten in de factorisatie bij alle p_i en bij -1 even zijn. Met andere woorden, dit product is een kwadraat! Omtrent de *factor basis* (de lijst van priemgetallen tot een te kiezen grens B) is het nuttig op te merken dat natuurlijk eerst gekeken wordt of N door één van die kleine p_i deelbaar is, maar ook dat slechts ongeveer de helft van de priemgetallen van nut zijn. Immers, een priemgetal p dat een Q_{n+1} deelt, deelt $p_n^2-Nq_n^2$, dus $N\equiv(p_n/q_n)^2 \bmod p$. Met andere woorden, N moet een kwadraatrest modulo p zijn, een eigenschap die eenvoudig te verifiëren is. Het kan zijn dat de periodelengte van de kettingbreuk van $\sqrt{N}$ klein is, en in dat geval treden maar weinig verschillende waarden Q_{n+1} op. Een manier om dat te verhelpen is door naar de kettingbreuk van $\sqrt{kN}$ voor kleine veelvouden van N te kijken. Niet alleen kan de periode zo groter worden, maar k kan ook nog eens zo geselecteerd worden dat kN kwadraatrest is voor veel van de priemgetallen tot B.