CHAPITRE 1 : DIVISIBILITÉ ET PREMIERS

1. Minimums et récurrence

Une propriété très importante de l'ensemble des nombres naturels $\mathbb{N}$ est la suivante :

Propriété 1.1. *Tout sous-ensemble non vide S de $\mathbb{N}$ contient un plus petit membre* (*ou* minimum). On dit "$\mathbb{N}$ est *bien ordonné*."

Cette propriété 1.1 de "bon ordre" est très particulière de $\mathbb{N}$. Les ensembles ordonnés $\mathbb{Z}$, $\mathbb{Q}$, ou $\mathbb{R}$ contiennent tous des sous-ensembles non vides sans plus petit membre. Même dans $\mathbb{R}_{\geq 0} = \{x \in \mathbb{R} \mid x \geq 0\}$ il y a des parties comme $S = \{x \in \mathbb{R} \mid x > 1\}$ sans minimum (ce sont des sous-ensemble S avec un infimum qui n'appartient pas à S).

Une première conséquence de cette propriété de bon ordre est

Théorème 1.2. *Toute suite strictement décroissante $n_1 > n_2 > n_3 > \cdots$ dans $\mathbb{N}$ est finie.*

L'algorithme d'Euclide et beaucoup d'autres algorithmes terminent à cause de cette propriété de $\mathbb{N}$.

Preuve. Soit $S = \{n_1, n_2, n_3, \ldots\}$ l'ensemble de membres de la suite. Le sous-ensemble $S \subset \mathbb{N}$ a un minimum n_k par la propriété 1.1 (si la suite n'est pas vide). On montre que la suite termine en n_k.

Supposons le contraire. Alors n_k a un successeur n_{k+1} dans la suite. Comme la suite est strictement décroissante, on a $n_k > n_{k+1}$. Mais comme n_{k+1} est dans la suite, et n_k est le plus petit membre de la suite, on a $n_k \leq n_{k+1}$. Contradiction.

Donc la suite $n_1 > n_2 > n_3 > \cdots$ termine en $\cdots > n_{k-1} > n_k$ et est finie. □

Une deuxième conséquence de la propriété de minimums dans $\mathbb{N}$ est la validité des démonstrations par récurrence. Supposons qu'on a un énoncé $\mathcal{P}(n)$ qui dépend d'une variable entière $n \geq 1$. Par exemple

$$\mathcal{P}(n): \qquad 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

$$\mathcal{P}(n): \qquad \text{Si } n \geq 2, \text{ alors } n \text{ est un produit de nombres premiers.}$$

Il y a plusieurs formes variantes de la récurrence.

La récurrence simple. *Si on montre*

$$\mathcal{P}(1) \qquad \textit{et} \qquad \forall n \geq 2 \quad \mathcal{P}(n-1) \Longrightarrow \mathcal{P}(n)$$

alors on a montré $\mathcal{P}(n)$ pour tout $n \geq 1$.

La récurrence d'ordre 2. *Si on montre*

$$\mathcal{P}(1) \qquad \textit{et} \qquad \mathcal{P}(2) \qquad \textit{et} \qquad \forall n \geq 3 \quad \mathcal{P}(n-2) \textit{ et } \mathcal{P}(n-1) \Longrightarrow \mathcal{P}(n)$$

alors on a montré $\mathcal{P}(n)$ pour tout $n \geq 1$.

La récurrence forte. *Si on montre*

$$\mathcal{P}(1) \qquad \textit{et} \qquad \forall n \geq 2 \quad \big(\mathcal{P}(k) \text{ VRAI } \textit{pour tout } k \textit{ avec } 1 \leq k < n\big) \Longrightarrow \mathcal{P}(n)$$

alors on a montré $\mathcal{P}(n)$ *pour tout* $n \geq 1$.

Il y a d'autres variations, surtout des récurrences sur tout $n \geq 0$ ou tout $n \geq 2$, etc., ou des récurrences d'ordre 3, etc. Toutes les formes de la récurrence marchent pour la même raison : la propriété des minimums dans $\mathbb{N}$. Démontrons par exemple la validité de la récurrence simple.

Preuve de la récurrence simple. Supposons qu'on a montré que $\mathcal{P}(1)$ est VRAI, et que pour tout $n \geq 2$, on a montré $\mathcal{P}(n-1) \Rightarrow \mathcal{P}(n)$. Considérons le sous-ensemble

$$S = \{n \in \mathbb{N} \mid n \geq 1, \text{ et } \mathcal{P}(n) \text{ est FAUX}\} \subset \mathbb{N}.$$

Si S n'est pas vide, il a un plus petit membre s_0 par la propriété 1.1. Montrons par l'absurde que c'est impossible.

Donc supposons au contraire que S est non vide et contient un plus petit membre s_0. Comme on a montré que $\mathcal{P}(1)$ est VRAI, on a $1 \notin S$ et donc $s_0 \neq 1$. Donc on doit avoir $s_0 \geq 2$.

Mais alors on a $s_0 - 1 \geq 1$. On a aussi $s_0 - 1 \notin S$ car il est plus petit que le plus membre s_0 de S. Vue la définition de S, la combinaison $s_0 - 1 \geq 1$ et $s_0 - 1 \notin S$ implique que $\mathcal{P}(s_0 - 1)$ est VRAI. Mais vu que $\mathcal{P}(n-1) \Rightarrow \mathcal{P}(n)$ pour tout $n \geq 2$, on déduit que $\mathcal{P}(s_0)$ est VRAI aussi. Cela implique $s_0 \notin S$. Mais s_0 est le plus petit membre de S. Contradiction.

On conclut que S est vide, et donc que $\mathcal{P}(n)$ est VRAI pour tout $n \geq 1$. □

Faisons quelques démonstrations par récurrence.

Exercice 1.3. *Montrer par une récurrence simple pour tout* $n \geq 1$ *on a*

$$\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}.$$

Solution. Appelons la formule $\mathcal{P}(n)$. Il suffit de montrer $\mathcal{P}(1)$ et de montrer que pour tout $n \geq 2$ on a $\mathcal{P}(n-1) \Longrightarrow \mathcal{P}(n)$.

$\boxed{\mathcal{P}(1)}$ La formule $\mathcal{P}(1)$ dit que $\frac{1}{1\cdot 2} = \frac{1}{2}$ est égal à $\frac{1}{1+1} = \frac{1}{2}$, qui est VRAI.

$\boxed{\mathcal{P}(n) \text{ pour } n \geq 2}$ Soit $n \geq 2$, et supposons que $\mathcal{P}(n-1)$ est VRAI. Cela signifie qu'on a

$$\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \cdots + \frac{1}{(n-1)n} = \frac{n-1}{n}.$$

Ajoutons $\frac{1}{n(n+1)}$ aux deux membres de cette équation, puis traitons le membre de droite :

$$\begin{aligned}\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \cdots + \frac{1}{(n-1)n} + \frac{1}{n(n+1)} &= \frac{n-1}{n} + \frac{1}{n(n+1)} \\ &= \frac{(n-1)(n+1)}{n(n+1)} + \frac{1}{n(n+1)} = \frac{(n^2-1)+1}{n(n+1)} = \frac{n\cdot n}{n(n+1)} = \frac{n}{n+1}.\end{aligned}$$

Donc $\mathcal{P}(n)$ est VRAI aussi.

On a ainsi démontré notre formule par une récurrence simple. □

Exercice 1.4. *Définissons une suite par*

$$u_1 = -1, \qquad u_2 = 1, \qquad u_n = 5u_{n-1} - 6u_{n-2} \textit{ pour } n \geq 3.$$

Montrer par récurrence d'ordre 2 *que pour tout* $n \geq 1$ *on a* $u_n = 3^n - 2^{n+1}$.

Solution. Soit $\mathcal{P}(n)$ l'énoncé $u_n = 3^n - 2^{n+1}$. Démontrons cet énoncé par récurrence en montrant $\mathcal{P}(1)$ et $\mathcal{P}(2)$ et que pour $n \geq 3$ on a $\big(\mathcal{P}(n-2)$ et $\mathcal{P}(n-1)\big) \Longrightarrow \mathcal{P}(n)$.

$\boxed{\mathcal{P}(1)}$ On a $u_1 = -1$ et $3^1 - 2^{1+1} = 3 - 4 = -1$.

$\boxed{\mathcal{P}(2)}$ On a $u_2 = 1$ et $3^2 - 2^{2+1} = 9 - 8 = 1$.

$\boxed{\mathcal{P}(n) \text{ pour } n \geq 3}$ Supposons que $\mathcal{P}(n-2)$ et $\mathcal{P}(n-1)$ sont vrais, c'est à dire qu'on a

$$u_{n-1} = 3^{n-1} - 2^n, \qquad u_{n-2} = 3^{n-2} - 2^{n-1}.$$

On a alors

$$\begin{aligned} u_n = 5u_{n-1} - 6u_{n-2} &= 5(3^{n-1} - 2^n) - 6(3^{n-2} - 2^{n-1}) \\ &= (5 \cdot 3^{n-1} - 6 \cdot 3^{n-2}) - (5 \cdot 2^n - 6 \cdot 2^{n-1}). \end{aligned}$$

(On met les puissances de 3 côte à côte et les puissances de 2 côte à côte parce que cela nous aidera à simplifier.) Comme on a $3^{n-1} = 3 \cdot 3^{n-2}$ et $2^n = 2 \cdot 2^{n-1}$, cela donne

$$u_n = (5{\cdot}3{\cdot}3^{n-2} - 6{\cdot}3^{n-2}) - (5{\cdot}2{\cdot}2^{n-1} - 6{\cdot}2^{n-1}) = 9{\cdot}3^{n-2} - 4{\cdot}2^{n-1} = 3^2{\cdot}3^{n-2} - 2^2{\cdot}2^{n-1} = 3^n - 2^{n+1}.$$

Donc $\mathcal{P}(n)$ est vrai aussi. □

2. Divisibilité et l'algorithme d'Euclide

Définition 2.1. Soit a et b entiers. On dit que a *divise* b s'il existe un entier s avec $as = b$. On dit aussi que a est un *diviseur* de b, et que b est *divisible par* a. On le note $a \mid b$.

Si $a \mid b$ et $a \mid c$, alors a est dit un *diviseur commun* de b et c.

Quand a ne divise pas c, on le note $a \nmid c$.

Les propriétés faciles de la divisibilité sont les suivantes.

Propriétés 2.2. Pour a, b, c, m, n entiers :

(a) $1 \mid a$ et $a \mid a$ et $a \mid 0$.
(b) Si $a \mid b$ et $b \mid c$, alors $a \mid c$.
(c) Si $a \mid b$ et $a \mid c$, alors $a \mid bm + cn$.
(d) $a \mid 1$ si et seulement si $a = \pm 1$.
(e) $a \mid b$ et $b \mid a$ si et seulement si $a = \pm b$.
(f) Pour $m \neq 0$ on a $ma \mid mb$ si et seulement si $a \mid b$.
(g) Si $a \mid b$ et $a > 0$ et $b > 0$, alors $a \leq b$.

Théorème 2.3 (Division euclidienne)**.** *Soit a et b entiers avec $b \geq 1$. Alors il existe des entiers uniques q et r avec*

$$a = bq + r, \qquad 0 \leq r < b \tag{1}$$

Preuve. Existence. On cherche un entier r de la forme $r = a - bq$ avec $q \in \mathbb{Z}$ qui vérifie $r \geq 0$ et $r < b$.

L'ensemble des entiers de la forme $a - bm$ avec $m \in \mathbb{Z}$ contient bien des membres positifs : il suffit de prendre $m = -N$ avec N très grand et positif. Donc le sous-ensemble

$$S = \{a - bm \mid m \in \mathbb{Z} \text{ et } a - bm \geq 0\} \subset \mathbb{N}$$

est non vide. Par la propriété 1.1, il contient un plus petit membre r, que l'on peut écrire sous la forme $r = a - bq$ avec $q \in \mathbb{Z}$. On a $r \in S \subset \mathbb{N}$ donc $r \geq 0$. De plus, $r - b$ est plus petit que

le plus petit membre r de S, et donc on a $r - b = a - b(q + 1) \notin S$. Vue la définition de S, cela implique qu'on a $r - b = a - b(q + 1) < 0$. Et cela donne $r < b$.

Unicité. Si on a $a = bq + r$ avec $0 \leq r < b$, et $a = bq' + r'$ avec $0 \leq r' < b$, alors on a $bq + r = bq' + r'$ et donc $bq - bq' = r' - r$ et finalement $b(q - q') = r' - r$. Or on a $0 \leq r' < b$ et $-b < -r \leq 0$, et en faisant la somme, $-b < r' - r < b$. Donc on a $-b < b(q - q') < b$. Comme on a $b > 0$ on peut diviser par b sans changer le sens des inégalités. Donc on a $-1 < q - q' < 1$. Comme $q - q'$ est entier, cela force $q - q' = 0$. Donc on a $q = q'$ et $r = a - bq = a - bq' = r'$. □

On peut étendre (1) à tous les $b \neq 0$ (positifs et négatifs) sous la forme

$$a = bq + r, \qquad 0 \leq r < |b| \tag{2}$$

Quand on a une telle division entière avec reste, on notera

$$\text{QUOT}(a, b) = q, \qquad \text{RESTE}(a, b) = r. \tag{3}$$

L'algorithme efficace pour faire la division euclidienne est celui qu'on a appris à l'école primaire, la longue division utilisant l'écriture décimale des entiers.

Définition 2.4. Le *plus grand diviseur commun* ou *pgcd* de $a_1, a_2, \ldots, a_r$ est un entier d tel que

(i) d est un diviseur commun de $a_1, a_2, \ldots, a_r$

(ii) tout diviseur commun de $a_1, a_2, \ldots, a_r$ divise d.

Par exemple, les diviseurs de 10 sont ± 1, ± 2, ± 5, ± 10. Les diviseurs de 26 sont ± 1, ± 2, ± 13, ± 26. Les diviseurs communs de 10 et 26 sont donc ± 1 et ± 2. Les diviseurs communs divisibles par tous les autres sont ± 2. Donc ± 2 sont les pgcd de 10 et 26. Normalement on choisit le pgcd positif et écrit $\text{pgcd}(10, 26) = 2$.

Il y a plusieurs algorithmes pour calculer le pgcd de deux entiers. Le plus classique est l'algorithme d'Euclide. Pour calculer le pgcd de 26 et 10, on divise 26 par 10, trouvant un reste. Puis on divise 10 par ce reste, trouvant un deuxième reste. On divise le premier reste par le deuxième, trouvant un troisième reste. On continue, en divisant chaque reste par son prédécesseur :

$$\begin{aligned} 26 &= 2 \cdot 10 + 6, \\ 10 &= 1 \cdot 6 + 4, \\ 6 &= 1 \cdot 4 + 2, \\ 4 &= 2 \cdot 2 + 0. \end{aligned}$$

Quand on arrive au reste 0, on s'arrête, parce qu'on ne peut pas diviser par 0. Le pgcd est le dernier reste non nul 2. Donc on devrait avoir $\text{pgcd}(10, 26) = 2$ selon l'algorithme.

Mais pourquoi 2 est-il réellement le pgcd de 10 et 26 ? Considérons la suite de restes successifs 26, 10, 6, 4, 2, 0 calculés dans l'algorithme. A cause des équations ci-dessus, chaque fois qu'un entier divise deux membres consécutifs de la suite des restes, il divise tous les membres de la suite des restes. Par exemple, 2 divise 0 et 2, donc il divise aussi $4 = 2 \cdot 2 + 0$, puis $6 = 1 \cdot 4 + 2$, puis $10 = 1 \cdot 6 + 4$ et enfin $26 = 2 \cdot 10 + 6$. Donc 2 est bien un diviseur commun de 10 et 26. Et tout d divisant 26 et 10 divise aussi $6 = 26 - 2 \cdot 10$ et $4 = 6 - 1 \cdot 2$ et $2 = 6 - 1 \cdot 4$ et $0 = 4 - 2 \cdot 2$. Donc tout diviseur commun de 10 et 26 divise 2 aussi. Donc 2 est bien le pgcd de 10 et 26.

Pour calculer le pgcd de 4147 et 10672, on fait

$$\begin{aligned} 10672 &= 2 \cdot 4147 + 2378, \\ 4147 &= 1 \cdot 2378 + 1769, \\ 2378 &= 1 \cdot 1769 + 609, \\ 1769 &= 2 \cdot 609 + 551, \\ 609 &= 1 \cdot 551 + 58, \\ 551 &= 9 \cdot 58 + 29, \\ 58 &= 2 \cdot 29 + 0. \end{aligned}$$

On trouve $\operatorname{pgcd}(4147, 10672) = 29$.

L'algorithme d'Euclide. *Pour calculer le pgcd de u et v, on pose d'abord $u_{-2} = u$ et $u_{-1} = v$. Pour $i = 0, 1, 2, \dots$, tant que $u_{i-1} \neq 0$, on pose $u_i = \text{RESTE}(u_{i-2}, u_{i-1})$. Quand on arrive à $u_N = 0$, on sort $\operatorname{pgcd}(u, v) = u_{N-1}$, le dernier reste non nul.*

Donc on calcule

$$\begin{aligned} u &= a_0 v + u_0, \\ v &= a_1 u_0 + u_1, \\ u_0 &= a_2 u_1 + u_2, \\ &\vdots \\ u_{N-3} &= a_{N-1} u_{N-2} + u_{N-1}, \\ u_{N-2} &= a_N u_{N-1} + 0, \end{aligned} \tag{4}$$

avec les a_i et u_i entiers. Et vu que dans la division euclidienne (2) le diviseur b et le reste r vérifient $0 \leq r < |b|$, on a

$$|v| > u_0 > u_1 > \cdots > u_{N-1} > 0. \tag{5}$$

Théorème 2.5. *L'algorithme d'Euclide* (4) *calculant le pgcd de u et v termine, et son dernier reste non nul vérifie $u_{N-1} = \operatorname{pgcd}(u, v)$.*

Démonstration. La suite de restes successifs $|v| > u_0 > u_1 > \cdots$ est une suite strictement décroissante dans $\mathbb{N}$, et donc est finie par le théoréme 1.2. Par conséquent l'algorithme doit s'arrêter dans un temps fini, ce qu'il ne peut faire qu'en trouvant un $u_N = 0$.

Pour montrer que u_{N-1} est bien le pgcd de u et v, on montre d'abord que tout d divisant deux membres consécutifs de la suite des restes u_{-2}, u_{-1}, $u_0, \dots, u_{N-1}, u_N$ divise tous les membres de la suite. Cela se montre par les équations (4) comme on a fait pour 10 et 26, mais par une récurrence formelle omise ici. Ainsi u_{N-1}, qui divise les deux derniers restes u_{N-1} et $u_N = 0$, divise tous les membres de la suite dont $u_{-2} = u$ et $u_{-1} = v$. Donc u_{N-1} est un diviseur commun de u et v. Egalement, tout diviseur commun d des deux premiers membres de la suite $u = u_{-2}$ et $v = u_{-1}$ divise aussi l'avant-dernier membre u_{N-1}. Donc u_{N-1} est un diviseur commun de u et v divisible par tous leurs diviseurs communs, et par définition il est leur pgcd. □

Théorème 2.6. *Tout systéme fini d'entiers $a_1, a_2, \dots, a_r$ a un pgcd, qui est unique à signe près, et il vérifie*

$$\operatorname{pgcd}(a_1, a_2, \dots, a_r) = \operatorname{pgcd}\big(a_1, \operatorname{pgcd}(a_2, \dots, a_r)\big).$$

Preuve. Unicité. Supposons que d et d' sont des pgcd de $a_1, \dots, a_{r-1}, a_r$. Alors d est un diviseur commun de $a_1, \dots, a_{r-1}, a_r$ et donc divise leur pgcd d', et vice-versa. Ainsi $d \mid d'$ et $d' \mid d$. Mais cela entraîne $d = \pm d'$.

Existence. On va par récurrence sur r. Le pgcd d'un entier est $\text{pgcd}(a_1) = a_1$. Pour deux entiers $\text{pgcd}(a_1, a_2)$ est le dernier reste non nul de l'algorithme d'Euclide par le théorème 2.5. Supposons alors $r \geq 3$ et que le pgcd d'un système de s entiers existe tant qu'on a $1 \leq s \leq r-1$. En particulier $d = \text{pgcd}\big(a_1, \text{pgcd}(a_2, \dots, a_r)\big)$ existe. Il suffit de montrer que d est le pgcd de $a_1, a_2, \dots, a_r$.

...(à compléter) □

3. Le lemme de Bezout et l'algorithme d'Euclide étendu

Lemme de Bezout. *Soit u, v entiers et $d = \text{pgcd}(u, v)$. Alors il existe des entiers x et y avec $ux + vy = d$.*

Une *relation de Bezout* est une équation de la forme $ux + vy = d$ avec u, v, d, x, y entiers et $d = \text{pgcd}(u, v)$. On peut avoir plusieurs relations de Bezout pour les mêmes u, v, d. Par exemple, pour $u = 5$ et $v = 2$ et $d = 1$, on a des relations de Bezout avec $(x, y) = (1, -2)$ ou $(x, y) = (-1, 3)$ ou $(x, y) = (-2m + 1, 5m - 2)$ pour n'importe quel $m \in \mathbb{Z}$.

On donne un algorithme qui calcule un x et un y explicitement. Cet algorithme n'est pas identique aux calculs faits en "remontant l'algorithme d'Euclide", mais c'est très apparenté. Cet algorithme sera réutilisé dans le prochain chapitre pour calculer les réduites d'une fraction continue.

Algorithme d'Euclide étendu. *On a deux entiers u, v en entrées. On pose*

$$\begin{aligned} u_{-2} &= u, & u_{-1} &= v, \\ p_{-2} &= 0, & p_{-1} &= 1, \\ q_{-2} &= 1, & q_{-1} &= 0. \end{aligned} \tag{6}$$

Pour $i = 0, 1, 2, \dots$, tant que $u_{i-1} \neq 0$, on pose

$$\begin{aligned} a_i &= \text{QUOT}(u_{i-2}, u_{i-1}), & p_i &= a_i p_{i-1} + p_{i-2}, \\ u_i &= \text{RESTE}(u_{i-2}, u_{i-1}), & q_i &= a_i q_{i-1} + q_{i-2}. \end{aligned} \tag{7}$$

Quand on arrive à $u_N = 0$, on sort $d = u_{N-1}$ et $q = q_{N-1}$ et $p = p_{N-1}$.

Théorème 3.1. *Les d, p, et q sortis par l'algorithme d'Euclide étendu vérifient $d = \text{pgcd}(u, v)$ et $uq - vp = (-1)^{N-1} d$.*

Donc on trouve la relation de Bezout $ux + vy = d$ en changeant quelques signes.

Regardons quelques exemples. Les deux premières colonnes et la première ligne sont des décorations. On remplit les troisième et quatrième colonnes avec (6) et les colonnes plus à droite par (7).

		+	−	+	−	+	−
	a_i			2	1	1	2
	u_i	26	10	6	4	2	0
−10	p_i	0	1	2	3	5	13
26	q_i	1	0	1	1	2	5

On a toujours $26q_i - 10p_i = (-1)^i u_i$. (C'est la signification des -10, 26, $+$ et $-$ dans les premières ligne et colonne.)

$$26 \cdot 1 - 10 \cdot 0 = 26, \qquad 26 \cdot 1 - 10 \cdot 2 = 6, \qquad 26 \cdot 2 - 10 \cdot 5 = 2,$$
$$26 \cdot 0 - 10 \cdot 1 = -10, \qquad 26 \cdot 1 - 10 \cdot 3 = -4, \qquad 26 \cdot 5 - 10 \cdot 13 = 0.$$

		+	−	+	−	+	−	+	−	+
	a_i			2	1	1	2	1	9	2
	u_i	10672	4147	2378	1769	609	551	58	29	0
−4147	p_i	0	1	2	3	5	13	18	175	368
10672	q_i	1	0	1	1	2	5	7	68	143

Cette fois on a $10672q_i - 4147p_i = (-1)^i u_i$. En particulier on trouve $10672 \cdot 68 - 4147 \cdot 175 = -29$, qui est la relation de Bezout à signe près.

Lemme 3.2. *Dans l'algorithme d'Euclide étendu d'équations* (6) *et* (7)*, on a* $uq_i - vp_i = (-1)^i u_i$ *pour tout* i *avec* $-2 \le i \le N$.

Le théorème 3.1 est le cas particulier $i = N - 1$ du lemme.

Preuve. On fait une récurrence "par deux". Les cas initiaux sont $i = -2$ et $i = -1$, où on a bien $u \cdot 1 - v \cdot 0 = u$ et $u \cdot 0 - v \cdot 1 = -v$, respectivement.

Donc supposons qu'on a un i avec $0 \le i \le N$, et que la formule du lemme est vrai au niveaux $i - 1$ et $i - 2$:

$$uq_{i-1} - vp_{i-1} = (-1)^{i-1} u_{i-1},$$
$$uq_{i-2} - vp_{i-2} = (-1)^{i-2} u_{i-2}.$$

On multiplie la première équation par a_i, et on l'ajoute à la seconde, donnant

$$\begin{aligned} u(a_i q_{i-1} + q_{i-2}) - v(a_i p_{i-1} + p_{i-2}) &= (-1)^{i-1} a_i u_{i-1} + (-1)^{i-2} u_{i-2} \\ &= (-1)^i (u_{i-2} - a_i u_{i-1}). \end{aligned}$$

Le fait que a_i et u_i sont le quotient et le reste de la division de u_{i-2} par u_{i-1} signifie qu'on a $u_{i-2} = a_i u_{i-1} + u_i$, et donc $u_i = u_{i-2} - a_i u_{i-1}$. Substituant cela et les formules $q_i = a_i q_{i-1} + q_{i-2}$ et $p_i = a_i p_{i-1} + p_{i-2}$ du (7) dans l'équation ci-dessus donne bien $uq_i - vp_i = (-1)^i u_i$. □

Quand on a $\operatorname{pgcd}(a, b) = 1$, on dit que a est *premier avec* b, ou que a et b sont *premiers entre eux*.

Quelques autre propriétés des pgcd :

Propriétés 3.3. (a) On a $\operatorname{pgcd}(ma, mb) = m \operatorname{pgcd}(a, b)$.

(b) Pour d un diviseur commun de a et b, on a $\operatorname{pgcd}(\frac{a}{d}, \frac{b}{d}) = \frac{\operatorname{pgcd}(a,b)}{d}$.

(c) En particulier $\frac{a}{\operatorname{pgcd}(a,b)}$ et $\frac{b}{\operatorname{pgcd}(a,b)}$ sont premiers entre eux.

(d) Il existe x et y entiers avec $ax + by = 1$ si et seulement si a et b sont premiers entre eux.

(e) Si a est premier avec b et c, il est aussi premier avec bc. (C'est parce que pour a premier avec b et c il existe des entiers x, y, t, u avec $ax + by = 1$ et $at + cu = 1$ et donc $ax + by(at + cu) = a(x + byt) + bc(yu) = 1$ d'où a est premier avec bc.)

(f) On a $\operatorname{pgcd}(a, b) = \operatorname{pgcd}(a, Na + b) = \operatorname{pgcd}(a, Na - b)$. (C'est parce que les diviseurs communs de a et b sont les mêmes que les diviseurs communs de a et $Na \pm b$.) En particulier a et $Na \pm 1$ sont toujours premiers entre eux.

4. Les nombres premiers

Définition 4.1. Un nombre naturel p est *premier* si $p \geq 2$ et les seuls diviseurs (positifs) de p sont 1 et p.

Un nombre naturel n est *composé* si $n \geq 2$ et n n'est pas premier.

Les plus petits nombres premiers sont 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 43, 47. La liste de tous les premiers $\leq N$ se calcule par un procédé appelé la *crible d'Eratosthène*.

Théorème 4.2. (a) (Le lemme de Gauss) *Si $a \mid bc$ et* $\operatorname{pgcd}(a,b) = 1$*, alors $a \mid c$.*

(b) *Soit p un premier et b entier. Alors soit $p \mid b$ soit* $\operatorname{pgcd}(p,b) = 1$.

(c) *Si p et premier et $p \mid bc$, alors $p \mid b$ ou $p \mid c$.*

(d) *Si p est premier et $p \mid b_1 b_2 \cdots b_r$, alors p divise un des b_i.*

Preuve. (a) Par le lemme de Bezout il existe des entiers x et y avec $ax + by = 1$. Alors $c = 1 \cdot c = (ax + by)c = acx + bcy$. Comme $a \mid a$ et $a \mid bc$, on trouve $a \mid acx + bcy = c$.

(b) Comme $\operatorname{pgcd}(p,b)$ est un diviseur de p, il est soit p soit 1 car ce sont les seuls diviseurs positifs du premier p. Si $\operatorname{pgcd}(p,b) = p$ on a $p \mid b$. Sinon on a $\operatorname{pgcd}(p,b) = 1$.

(c) Par le (b) on a soit $p \mid b$ soit $\operatorname{pgcd}(p,b) = 1$. Dans le deuxième cas, le lemme de Gauss implique qu'on a $p \mid c$.

(d) Appliquer le (c) et la récurrence. □

Le théorème de factorisation unique. *Tout entier $n \geq 2$ est un produit de nombres premiers. De plus, l'écriture $n = p_1 p_2 \cdots p_r$ comme un produit de nombres premiers est unique à l'ordre des facteurs près.*

Preuve. Existence. On utilise une récurrence forte. Le cas initial est $n = 2$, qui est un nombre premier, et est le produit de 1 nombre premier 2.

Maintenant considérons $n \geq 3$, et supposons que tout k avec $2 \leq k \leq n-2$ est un produit de nombres premiers. Alors n est soit premier soit composé. Si n est premier, il est le produit de 1 nombre premier n, et ça va. Si n est composé, alors $n = ab$ avec $2 \leq a \leq n-2$ et $2 \leq b \leq n-1$. Par l'hypothèse de récurrence, on peut écrire $n = q_1 \cdots p_r$ et $b = q_1 \cdots q_s$ comme des produits de premiers. Alors $n = p_1 \cdots p_r q_1 \cdots q_s$ est aussi un produit de premiers. Conclusion : que n soit premier ou composé, il est un produit de premiers.

Unicité. Supposons qu'on a deux écritures $n = p_1 p_2 \ldots p_r$ et $n = q_1 q_2 \ldots q_s$ d'un nombre comme produits de premiers. On montre par récurrence simple sur $r \geq 1$ que les deux écritures sont les mêmes à ordre près.

Dans le cas initial $r = 1$, le nombre $n = p_1$ est premier, mais il s'écrit aussi $n = q_1 \ldots q_s$. Comme un nombre premier n'est pas un produit de 2 entiers (ou plus) qui sont ≥ 2, il faut que $s = 1$ et $n = q_1$. Ainsi les écritures sont les mêmes.

Maintenant considérons le cas $r \geq 2$ en supposant le cas $r - 1 \geq 1$. On a deux factorisation en premiers $n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$. Alors p_1 est premier et $p_1 \mid q_1 q_2 \cdots q_s$. On déduit alors du théorème 4.2(d) que p_1 divise un des q_i. En modifiant l'ordre des q_i si nécessaire, on peut supposer que $p_1 \mid q_1$. Or les seuls diviseurs positifs du premier q_1 sont 1 et q_1, et $p_1 \neq 1$ car il est premier. Donc on a $p_1 = q_1$. De plus on a deux écritures $\frac{n}{p_1} = p_2 \cdots p_r$ et $\frac{n}{p_1} = q_2 \cdots q_s$ d'un même nombre comme un produit de $r-1$ et $s-1$ premiers. Par l'hypothèse de récurrence, les deux écritures pour $\frac{n}{p_1}$ sont les mêmes à l'ordre des facteurs près. On déduit que les écritures $n = p_1 p_2 \cdots p_r$ et $n = p_1 q_2 \cdots q_s = q_1 q_2 \cdots q_s$ sont les mêmes à l'ordre des facteurs près. □

Théorème 4.3 (Euclide)**.** *Il y a une infinité de nombres premiers.*

Démonstration. Supposons au contraire qu'il n'y a qu'un nombre fini de premiers $p_1, p_2, \dots, p_r$. Alors le nombre $n = p_1 p_2 \cdots p_r + 1$ n'est divisible par aucun des p_i. Mais n est soit un premier soit un produit de premiers. Donc il y a un premier différent de $p_1, p_2, \dots, p_r$. □

L'*écriture standard* d'un entier $n \geq 2$ comme un produit de premiers est une écriture $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ où $p_1 < p_2 < \cdots < p_r$ sont des premiers distincts en ordre croissant, et les puissances vérifient $e_i \geq 1$. Par exemple

$$600 = 2^3 3^1 5^2, \qquad 10\,! = 3628800 = 2^8 3^4 5^2 7^1$$

Cette écriture standard est unique.

5. Les ppcm

Définition 5.1. Le *plus petit multiple commun* ou *ppcm* de $a_1, \dots, a_r$ est un entier m qui (a) est un multiple commun de $a_1, \dots, a_r$ et (b) divise tout multiple commun de $a_1, \dots, a_r$.

Comme le pgcd, le ppcm de plusieurs entiers se calcule itérativement parce qu'on a

$$\operatorname{ppcm}(a_1, a_2, a_3, \dots, a_r) = \operatorname{ppcm}(\operatorname{ppcm}(a_1, a_2), a_3, \dots, a_r).$$

Théorème 5.2. *Pour des entiers $m \geq 1$ et $n \geq 1$, on a*

$$\operatorname{ppcm}(m, n) = \frac{mn}{\operatorname{pgcd}(m, n)}.$$

Par exemple on a

$$\operatorname{ppcm}(10, 26) = \frac{10 \cdot 26}{\operatorname{pgcd}(10, 26)} = \frac{260}{2} = 130,$$
$$\operatorname{ppcm}(4147, 10672) = \frac{4147 \cdot 10672}{29} = 1\,526\,096.$$

Preuve du théorème 5.2. Soit $d = \operatorname{pgcd}(m, n)$ et notons $m' = \frac{m}{d}$ et $n' = \frac{n}{d}$. Remarquons que m' et n' sont premiers entre eux par la propriété 3.3(c).

Alors $\frac{mn}{d} = m'n'd$ est bien un multiple commun de m et n car il s'écrit $m'n'd = mn' = nm'$. Un multiple commun général $N = ma = nb$ s'écrit $N = dm'a = dn'b$. On a alors $m'a = n'b$. Comme m' et n' sont premiers entre eux, et $n' \mid m'a$ on a $n' \mid a$ par le lemme de Gauss (théorème 4.2). Donc il y a un entier s avec $a = n's$, et on a $N = dm'n's$. Donc tout multiple commun N de m et n est un multiple de $m'n'd$. Ainsi $m'n'd = \frac{mn}{d}$ vérifie la définition du pppcm de m et n. □

Chapitre 2 : Fractions continues

6. Fractions continues finies

Une *fraction continue finie* est une fraction itérée du genre

$$1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2}}}}}, \qquad -1 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{5 + \cfrac{1}{7 + \cfrac{1}{9}}}}}$$

La forme générale est

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \cfrac{}{a_{N-1} + \cfrac{1}{a_N}}}}} \tag{8}$$

Les a_i sont les *quotients partiels* ou parfois tout simplement les *quotients* de la fraction continue.

Nous nous intéressons aux fractions continues dites *simples* où tous les numérateurs sont des 1, les quotients partiels a_i sont entiers, et en plus $a_i \geq 1$ pour $i \geq 1$. (Mais a_0 est un entier de signe quelconque.)

Mais il est convenable parfois de permettre les a_i à être des réels ou des variables ou des fonctions ou autre chose.

La notation ci-dessus n'est pas très compacte, et parfois elle est remplacée par

$$a_0 + \frac{1}{a_1+}\,\frac{1}{a_2+}\,\cdots\,\frac{1}{a_{N-1}+}\,\frac{1}{a_N} \qquad \text{ou} \qquad [a_0, a_1, a_2, \ldots, a_{N-1}, a_N]$$

ou des variations. Dans le dernier système de notations, les deux fractions continues tout en haut sont $[1, 2, 1, 2, 1, 2]$ et $[-1, 1, 3, 5, 7, 9]$.

7. Evaluation d'une fraction continue finie

On évaluera la fraction continue $[a_0, a_1, a_2, \ldots, a_N]$ de (8) en trouvant une formule récursive évaluant ses troncations

$$a_0, \qquad a_0 + \frac{1}{a_1}, \qquad a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2}}, \qquad \text{etc.}$$

Théorème 7.1. *Définissons*

$$\begin{aligned} p_{-2} &= 0, & p_{-1} &= 1, & p_n &= a_n p_{n-1} + p_{n-2} \quad \textit{pour } n \geq 0, \\ q_{-2} &= 1, & q_{-1} &= 0, & q_n &= a_n q_{n-1} + q_{n-2} \quad \textit{pour } n \geq 0, \end{aligned}$$

Alors pour tout $n \geq 0$ on a

$$\frac{p_n}{q_n} = [a_0, a_1, \ldots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots \cfrac{}{a_{n-1} + \cfrac{1}{a_n}}}}.$$

Définition 7.2. Les fractions $\frac{p_0}{q_0}, \frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots$ s'appellent les *réduites* de la fraction continue $[a_0, a_1, a_2, \ldots]$. En anglais on dit "*convergents*".

Exemple 7.3. Pour évaluer les fractions continues $[1,2,1,2,1,2]$ et $[-1,1,3,5,7,9]$ ci-dessus, on utilise les tableaux suivants, qui ressemblent à ceux de l'algorithme d'Euclide étendu.

a_i			1	2	1	2	1	2
p_i	0	1	1	3	4	11	15	41
q_i	1	0	1	2	3	8	11	30

a_i			-1	1	3	5	7	9
p_i	0	1	-1	0	-1	-5	-36	-329
q_i	1	0	1	1	4	21	151	1380

Donc on a $[1,2,1,2,1,2] = \frac{41}{30}$ et ses réduites sont $1, \frac{3}{2}, \frac{4}{3}, \frac{11}{8}, \frac{15}{11}, \frac{41}{30}$, c'est à dire

$$1 = 1, \qquad 1 + \frac{1}{2} = \frac{3}{2}, \qquad 1 + \cfrac{1}{2 + \cfrac{1}{1}} = \frac{4}{3}, \qquad 1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2}}} = \frac{11}{8},$$

$$1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1}}}} = \frac{15}{11}, \qquad 1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2}}}}} = \frac{41}{30}.$$

On a $[-1,1,3,5,7,9] = -\frac{329}{1380}$, et ses réduites sont $-1, 0, -\frac{1}{4}, -\frac{5}{21}, -\frac{36}{151}, -\frac{329}{1380}$.

Preuve du théorème 7.1. On fait une récurrence d'ordre 2 sur n.

Pour $n = 0$ on a $\frac{p_0}{q_0} = \frac{a_0}{1} = a_0$.

Pour $n = 1$ on a $\frac{p_1}{q_1} = \frac{a_1 a_0 + 1}{a_1} = a_0 + \cfrac{1}{a_1}$.

Donc les deux cas initiaux sont vérifiés.

Maintenant supposons $n \geq 2$, et qu'on a $\frac{p_{n-2}}{q_{n-2}} = [a_0, \ldots, a_{n-2}]$ et $\frac{p_{n-1}}{q_{n-1}} = [a_0, \ldots, a_{n-2}, a_{n-1}]$ quelquesoit les valeurs de $a_0, \ldots, a_{n_1}$. Or la fraction continue

$$[a_0, \ldots, a_{n-2}, a_{n-1}, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots \cfrac{}{a_{n-1} + \cfrac{1}{a_n}}}}$$

s'obtient en prenant

$$[a_0, \ldots, a_{n-2}, a_{n-1}] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots\ a_{n-1}}}$$

et en remplaçant a_{n-1} par $a_{n-1}+\frac{1}{a_n}$. C'est à dire on a

$$\begin{aligned}
[a_0,\dots,a_{n-2},a_{n-1},a_n] &= [a_0,\dots,a_{n-2},a_{n-1}+\frac{1}{a_n}] \\
&= \frac{p_{n-1}(a_0,\dots,a_{n-2},a_{n-1}+\frac{1}{a_n})}{q_{n-1}(a_0,\dots,a_{n-2},a_{n-1}+\frac{1}{a_n})} \\
&= \frac{(a_{n-1}+\frac{1}{a_n})p_{n-2}+p_{n-3}}{(a_{n-1}+\frac{1}{a_n})q_{n-2}+q_{n-3}} \\
&= \frac{a_{n-1}p_{n-2}+p_{n-3}+\frac{1}{a_n}p_{n-2}}{a_{n-1}q_{n-2}+q_{n-3}+\frac{1}{a_n}q_{n-2}} \\
&= \frac{p_{n-1}+\frac{1}{a_n}p_{n-2}}{q_{n-1}+\frac{1}{a_n}q_{n-2}} \\
&= \frac{a_np_{n-1}+p_{n-2}}{a_nq_{n-1}+q_{n-2}} = \frac{p_n}{q_n}.
\end{aligned}$$

□

Théorème 7.4. (a) *On a* $p_nq_{n-1}-p_{n-1}q_n=(-1)^{n-1}$ *pour* $n\geq 0$.
(b) *On a* $p_nq_{n-2}-p_{n-2}q_n=(-1)^n a_n$ *pour* $n\geq 1$.

Preuve. (a) Pour $n=0$ c'est $p_0q_{-1}-q_0p_{-1}=a_0\cdot 0-1\cdot 1=-1$. Pour $n\geq 1$, on suppose par récurrence qu'on a $p_{n-1}q_{n-2}-p_{n-2}q_{n-1}=(-1)^{n-2}$, et on trouve

$$\begin{aligned}
p_nq_{n-1}-p_{n-1}q_n &= (a_np_{n-1}+p_{n-2})q_{n-1}-p_{n-1}(a_nq_{n-1}+q_{n-2}) \\
&= p_{n-2}q_{n-1}-p_{n-1}q_{n-2} = -(-1)^{n-2} = (-1)^{n-1}.
\end{aligned}$$

(b) En utilisant le (a), on a

$$\begin{aligned}
p_nq_{n-2}-p_{n-2}q_n &= (a_np_{n-1}+p_{n-2})q_{n-2}-p_{n-2}(a_nq_{n-1}+q_{n-2}) \\
&= a_n(p_{n-1}q_{n-2}-p_{n-2}q_{n-1}) = (-1)^n a_n.
\end{aligned}$$

□

Théorème 7.5. *Supposons qu'on a une fraction continue* $[a_0,a_1,a_2,\dots]$ simple*, c'est à dire que* a_0 *est entier, et* $a_i\geq 1$ *est entier et strictement positif pour* $i\geq 1$*. Alors dans chaque fraction* $\frac{p_n}{q_n}=[a_0,\dots,a_n]$*, le numérateur* p_n *et le dénominateur* q_n *sont des entiers premiers entre eux. De plus la suite des dénominateurs* $1=q_0\leq q_1<q_2<q_3<\cdots$ *est strictement croissante après* q_1*, et on a*

$$\frac{p_n}{q_n}-\frac{p_{n-1}}{q_{n-1}}=\frac{(-1)^{n-1}}{q_nq_{n-1}}, \qquad \frac{p_n}{q_n}-\frac{p_{n-2}}{q_{n-2}}=\frac{(-1)^n a_n}{q_nq_{n-2}},$$

Preuve. Il est clair des formules de récurrence que si les a_n sont tous entiers, alors les p_n et q_n sont entiers aussi. La formule $p_nq_{n-1}-p_{n-1}q_n=(-1)^{n-1}$ donne alors une relation de Bezout montrant que p_n et q_n sont premiers entre eux. En utilisant les relations $q_0=1$, $q_1=a_1$, et $q_n=a_nq_{n-1}+q_{n-2}$ pour $n\geq 2$, on montre par récurrence qu'on a $q_n\geq 1$ pour tout $n\geq 0$. Puis on a $q_n\geq q_{n-1}+q_{n-2}>q_{n-1}$ pour tout $n\geq 2$. Les valeurs de $\frac{p_n}{q_n}-\frac{p_{n-1}}{q_{n-1}}$ et de $\frac{p_n}{q_n}-\frac{p_{n-2}}{q_{n-2}}$ se calculent en utilisant le théorème 7.4. □

8. La fraction continue d'un rationnel

Pour ξ un réel, on définit une suite de réels ξ_n et une suite d'entiers a_n par récurrence $\xi_0 = \xi$, et pour $n \geq 0$

$$\xi_n = \begin{cases} a_n & \text{si } \xi_n \text{ est entier,} \\ a_n + \dfrac{1}{\xi_{n+1}} & \text{avec } a_n \text{ entier et } \xi_{n+1} > 1, \text{ sinon.} \end{cases} \tag{9}$$

C'est à dire, on a $a_n = [\xi_n]$, la partie entière de ξ_n, et $\frac{1}{\xi_{n+1}} = \xi_n - [\xi_n]$, la partie fractionnelle de ξ_n, tant que ceci est non nulle. On a

$$\xi = a_0 + \frac{1}{\xi_1} = a_0 + \frac{1}{a_1 + \dfrac{1}{\xi_2}} = a_0 + \frac{1}{a_1 + \dfrac{1}{a_2 + \dfrac{1}{\xi_3}}} = \cdots$$

et en général

$$\xi = [a_0, a_1, \ldots, a_{n-1}, \xi_n]. \tag{10}$$

Si un ξ_n est entier, on s'arrête avec $\xi_n = a_n$. Sinon, on continue.

Les *réduites* de ξ sont les réduites de la fraction continue finie ou infinie $[a_0, a_1, a_2, \ldots]$.

Exemple 8.1. Les fractions continues des rationnels $\frac{31}{22}$ et $-\frac{4}{15}$ se calculent comme suit :

$$\begin{aligned} \xi_0 &= \frac{31}{22} = 1 + \frac{9}{22}, \\ \xi_1 &= \frac{22}{9} = 2 + \frac{4}{9}, \\ \xi_2 &= \frac{9}{4} = 2 + \frac{1}{4}, \\ \xi_3 &= \frac{4}{1} = 4. \end{aligned} \qquad \begin{aligned} \xi_0 &= -\frac{4}{15} = -1 + \frac{11}{15}, \\ \xi_1 &= \frac{15}{11} = 1 + \frac{4}{11}, \\ \xi_2 &= \frac{11}{4} = 2 + \frac{3}{4}, \\ \xi_3 &= \frac{4}{3} = 1 + \frac{1}{3}, \\ \xi_4 &= \frac{3}{1} = 3. \end{aligned}$$

Donc on a

$$\frac{31}{22} = 1 + \frac{1}{2 + \dfrac{1}{2 + \dfrac{1}{4}}}, \qquad -\frac{4}{15} = -1 + \frac{1}{1 + \dfrac{1}{2 + \dfrac{1}{1 + \dfrac{1}{3}}}}.$$

Quand ξ est rationnel, on peut écrire $\xi = \dfrac{u}{v}$ avec u et $v > 0$ entiers. L'algorithme (9) donne

$$\begin{aligned}
\xi_0 &= \frac{u}{v} = a_0 + \frac{u_0}{v} && \text{avec } 0 \le u_0 < v,\\
\xi_1 &= \frac{v}{u_0} = a_1 + \frac{u_1}{u_0} && \text{avec } 0 \le u_1 < u_0,\\
&\vdots\\
\xi_{N-1} &= \frac{u_{N-3}}{u_{N-2}} = a_{N-1} + \frac{u_{N-1}}{u_{N-2}} && \text{avec } 0 \le u_{N-1} < u_{N-2},\\
\xi_N &= \frac{u_{N-2}}{u_{N-1}} = a_N.
\end{aligned}$$

Si on multiplie chaque équation par le dénominateur des fractions, on retrouve les équations $u = a_0 v + u_0$, $v = a_1 u_0 + u_1$, …, etc., de l'algorithme d'Euclide. Donc quand on applique l'algorithme (9) à un rationnel $\frac{u}{v}$, on fait l'algorithme d'Euclide, sauf que les sorties de l'algorithme sont les quotients entiers a_i des divisions successives, qui deviennent les quotients partiels de la fraction continue de $\frac{u}{v}$.

Théorème 8.2. *Pour u et $v > 0$ entiers, l'algorithme d'Euclide étendu calcule les quotients partiels de la fraction continue de $\frac{u}{v} = [a_0, a_1, \dots, a_N]$ et les réduites $\frac{p_0}{q_0}, \frac{p_1}{q_1}, \dots, \frac{p_N}{q_N}$ de cette fraction continue.*

En particulier, on a $\frac{p_N}{q_N} = \frac{u}{v}$ mais avec $\operatorname{pgcd}(p_N, q_N) = 1$. C'est à dire, $\frac{p_N}{q_N}$ est la forme réduite (ou simplifiée) de $\frac{u}{v}$.

9. Fractions continues infinies

Supposons qu'on a une fraction continue infinie

$$[a_0, a_1, a_2, a_3, \dots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots}}}}$$

La suite de ses réduites

$$\frac{p_0}{q_0} = [a_0], \qquad \frac{p_1}{q_1} = [a_0, a_1], \qquad \dots \qquad \frac{p_n}{q_n} = [a_0, a_1, \dots, a_n], \qquad \dots$$

est convergente, selon le théorème suivant. La *valeur* de la fraction continue infinie est cette limite.

Théorème 9.1. *Soit a_0 un entier relatif, et $a_1, a_2, \dots$ des entiers strictement positifs. Alors la suite de réduites $\frac{p_0}{q_0}, \frac{p_1}{q_1}, \frac{p_2}{q_2}, \dots$ de la fraction continue infinie $[a_0, a_1, a_2, \dots]$ a les propriétés suivantes.*

(a) *La sous-suite des réduites paires $\frac{p_0}{q_0}, \frac{p_2}{q_2}, \dots, \frac{p_{2n}}{q_{2n}}, \dots$ est strictement croissante.*

(b) *La sous-suite des réduites impaires $\frac{p_1}{q_1}, \frac{p_3}{q_3}, \dots, \frac{p_{2n+1}}{q_{2n+1}}, \dots$ est strictement décroissante.*

(c) *Toute réduite paire est plus petite que toute réduite impaire.*

(d) *Si la suite des réduites est infinie, elle a une limite ξ.*

On peut écrire (a)(b)(c) sous la forme

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \cdots < \cdots < \frac{p_5}{q_5} < \frac{p_3}{q_3} < \frac{p_1}{q_1}$$

Par exemple, les premières réduites de $[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, \dots]$ sont

$$\begin{aligned}
\frac{1}{1} &= 1.00000000000000000000000000 \\
\frac{3}{2} &= 1.50000000000000000000000000 \\
\frac{8}{5} &= 1.60000000000000000000000000 \\
\frac{21}{13} &= 1.61538461538461538461538461 \\
\frac{55}{34} &= 1.61764705882352941176470588 \\
\frac{144}{89} &= 1.61797752808988764044943820 \\
&\vdots \\
\text{limite } \alpha = \frac{1+\sqrt{5}}{2} &= 1.61803398874989484820458683 \\
&\vdots \\
\frac{233}{144} &= 1.61805555555555555555555555 \\
\frac{89}{55} &= 1.61818181818181818181818181 \\
\frac{34}{21} &= 1.61904761904761904761904761 \\
\frac{13}{8} &= 1.62500000000000000000000000 \\
\frac{5}{3} &= 1.66666666666666666666666666 \\
\frac{2}{1} &= 2.00000000000000000000000000
\end{aligned}$$

Preuve. (a) (b) Selon le théorème 2.5, on a

$$\frac{p_{2n}}{q_{2n}} - \frac{p_{2n-2}}{q_{2n-2}} = \frac{a_{2n}}{q_{2n}q_{2n-2}} > 0, \qquad \frac{p_{2n+1}}{q_{2n+1}} - \frac{p_{2n-1}}{q_{2n-1}} = -\frac{a_{2n+1}}{q_{2n+1}q_{2n-1}} < 0.$$

Donc on a toujours $\frac{p_{2n-2}}{q_{2n-2}} < \frac{p_{2n}}{q_{2n}}$ et $\frac{p_{2n-1}}{q_{2n-1}} > \frac{p_{2n+1}}{q_{2n+1}}$

(c) Selon le même théorème pour tout entier impair $2n-1$ on a

$$\frac{p_{2n-1}}{q_{2n-1}} - \frac{p_{2n-2}}{q_{2n-2}} = \frac{1}{q_{2n-1}q_{2n-2}} > 0, \qquad \frac{p_{2n}}{q_{2n}} - \frac{p_{2n-1}}{q_{2n-1}} = -\frac{1}{q_{2n}q_{2n-1}} < 0.$$

Donc on a $\frac{p_{2n-1}}{q_{2n-1}} > \frac{p_{2n-2}}{q_{2n-2}}$ et $\frac{p_{2n-1}}{q_{2n-1}} > \frac{p_{2n}}{q_{2n}}$. Chaque réduite impaire est plus grande que les réduites paires l'entourant immédiatement.

Or soit $\frac{p_{2m}}{q_{2m}}$ une réduite paire quelconque. On a soit $2m \leq 2n-2$ soit $2m \geq 2n$. Dans le premier cas, on a $\frac{p_{2m}}{q_{2m}} \leq \frac{p_{2n-2}}{q_{2n-2}} < \frac{p_{2n-1}}{q_{2n-1}}$. Dans le deuxième cas on a $\frac{p_{2n-1}}{q_{2n-1}} \geq \frac{p_{2m-1}}{q_{2m-1}} > \frac{p_{2m}}{q_{2m}}$. Dans les deux cas on a $\frac{p_{2n-1}}{q_{2n-1}} > \frac{p_{2m}}{q_{2m}}$.

(d) La suite des réduites paires est strictement croissante et bornée supérieurement par toutes les réduites impaires. Elle a donc une limite $\frac{p_{2n}}{q_{2n}} \to \xi_{\text{pair}}$ vérifiant $\xi_{\text{pair}} < \frac{p_{2n-1}}{q_{2n-1}}$ pour tout impair $2n-1$. Similairement la suite des réduites est décroissante et bornée inférieurement par toutes les réduites paires, donnant une limite $\frac{p_{2n-1}}{q_{2n-1}} \to \xi_{\text{impair}}$ avec $\frac{p_{2n}}{q_{2n}} < \xi_{\text{impair}}$ pour tout pair $2n$. Comme ces limites sont le suprémum des réduites paires et l'infimum des réduites impaires, on a aussi $\xi_{\text{pair}} \leq \xi_{\text{impair}}$. On a donc

$$\frac{p_{2n}}{q_{2n}} < \xi_{\text{pair}} \leq \xi_{\text{impair}} < \frac{p_{2n-1}}{q_{2n-1}}.$$

On a donc

$$|\xi_{\text{impair}} - \xi_{\text{pair}}| \leq \left| \frac{p_{2n-1}}{q_{2n-1}} - \frac{p_{2n}}{q_{2n}} \right| = \frac{1}{q_{2n-1}q_{2n}} \leq \frac{1}{(2n-1)(2n)} \to 0$$

quand $n \to \infty$, car on a $q_m \geq m$ pour tout m. Donc on a $\xi_{\text{pair}} = \xi_{\text{impair}}$, et la suite a une limite. □

Dans la direction opposée, on peut associer une fraction continue à un irrationnel ξ par le même **algorithme de fractions continues** que pour les rationnels. On pose $\xi_0 = \xi$, puis pour tout $n = 0, 1, 2, \ldots$ on pose

$$a_n = [\xi_n] \text{ la partie entière}, \qquad \xi_{n+1} = \frac{1}{\xi_n - a_n} \iff \xi_n = a_n + \frac{1}{\xi_{n+1}}. \tag{11}$$

Pour ξ irrationnel, tous les ξ_n sont tous irrationnels, donc la suite $a_0, a_1, a_2, \ldots$ est infinie. On a toujours $0 \leq \xi_n - a_n < 1$ d'où $0 < \frac{1}{\xi_{n+1}} < 1$ et $\xi_{n+1} > 1$ et $a_{n+1} = [\xi_{n+1}] \geq 1$. Donc tous les a_n sont strictement positifs sauf peut-être a_0. Donc associé à ξ on a une fraction continue infinie $[a_0, a_1, a_2, \ldots]$ comme dans le théorème 9.1.

Lemme 9.2. *Soit ξ un réel, soit $\xi_0, \xi_1, \xi_2, \ldots$ la suite de réels et $a_0, a_1, a_2, \ldots$ la suite d'entiers associés à ξ par la procédure* (11) *ci-dessus, et soit $\frac{p_0}{q_0}, \frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots$ la suite de réduites de la fraction continue $[a_0, a_1, a_2, \ldots]$. Alors on a*

$$\xi = \frac{p_n\xi_{n+1} + p_{n-1}}{q_n\xi_{n+1} + q_{n-1}}, \qquad \frac{p_n}{q_n} - \xi = \frac{(-1)^n}{q_n(q_n\xi_{n+1} + q_{n-1})}. \tag{12}$$

Preuve. Parce qu'on a

$$\xi = \xi_0 = a_0 + \frac{1}{\xi_1}, \qquad \xi_1 = a_1 + \frac{1}{\xi_2}, \qquad \ldots \qquad \xi_n = a_n + \frac{1}{\xi_{n+1}},$$

On a

$$\xi = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_n + \cfrac{1}{\xi_{n+1}}}}} = [a_0, a_1, \ldots, a_n, \xi_{n+1}]$$

Donc si on applique les formules qui calculent les réduites à la fraction continue $[a_0, a_1, \dots, a_n, \xi_{n+1}]$, ses réduites sont $\frac{p_0}{q_0}, \frac{p_1}{q_1}, \dots, \frac{p_n}{q_n}$ et

$$\xi = \frac{\overline{p}_{n+1}}{\overline{q}_{n+1}} = \frac{p_n\xi_{n+1} + p_{n-1}}{q_n\xi_{n+1} + q_{n-1}}.$$

Ceci démontre la première formule. Pour la deuxième on a par le théorème 2.5

$$\xi - \frac{p_n}{q_n} = \frac{\overline{p}_{n+1}}{\overline{q}_{n+1}} - \frac{p_n}{q_n} = \frac{(-1)^{n-1}}{q_n\overline{q}_{n+1}} = \frac{(-1)^{n-1}}{q_n(q_n\xi_{n+1} + q_{n-1})}.$$ □

Théorème 9.3. *Soit ξ un réel, $[a_0, a_1, a_n, \dots]$ sa fraction continue associée par la procédure (11), et $\frac{p_0}{q_0}, \frac{p_1}{q_1}, \frac{p_2}{q_2}, \dots$ les réduites de la fraction continue. Alors on a*

$$\left|\frac{p_n}{q_n} - \xi\right| \leq \frac{1}{q_nq_{n+1}} < \frac{1}{a_{n+1}q_n^2} \leq \frac{1}{q_n^2}.$$

En particulier, si ξ est irrationnel, on a $\frac{p_n}{q_n} \to \xi$ quand $n \to \infty$; les réduites de la fraction continue de ξ tendent vers ξ.

Preuve. En appliquant le lemme on a

$$\left|\frac{p_n}{q_n} - \xi\right| = \frac{1}{q_n(\xi_{n+1}q_n + q_{n-1})}.$$

Mais on a $\xi_{n+1} \geq a_{n+1}$ et $q_n > 0$ et $q_{n-1} > 0$ et $a_{n+1} \geq 1$, d'où

$$\xi_{n+1}q_n + q_{n-1} \geq a_{n+1}q_n + q_{n-1} = q_{n+1} > a_{n+1}q_n \geq q_n.$$

En multipliant ces inégalités par q_n et en prenant les réciproques, on trouve les inégalités du théorème. Finalement, comme on a $q_n \geq n$ pour tout n, on a $\left|\frac{p_n}{q_n} - \xi\right| < \frac{1}{n^2} \to 0$ pour $n \to \infty$. □

Par exemple le début de la fraction continue de π est $[3, 7, 15, 1, 292, 1, 1, 1, 2, \dots]$. Ses premières réduites sont

$$\frac{3}{1} = 3.00000000000000000000000000, \qquad \frac{3}{1} - \pi = -0.14159265358979323846264338 32,$$
$$\frac{333}{106} = 3.14150943396226415094339622 6, \qquad \frac{333}{106} - \pi = -0.00008321962752908751924715684090,$$
$$\frac{103993}{33102} = 3.14159265301190260407226149 4, \qquad \frac{103993}{33102} - \pi = -0.00000000057789063439038188 84,$$
$$\pi = 3.14159265358979323846264338 3,$$
$$\frac{355}{113} = 3.14159292035398230088495575 2, \qquad \frac{355}{113} - \pi = 0.00000026676418906242231236890825 93,$$
$$\frac{22}{7} = 3.14285714285714285714285714 2, \qquad \frac{22}{7} - \pi = 0.00126448926734961868021375958 8,$$

La formule $\left|\frac{p_n}{q_n} - \pi\right| < \frac{1}{q_n^2}$ siginife que quand $q_n \approx 10^r$, alors les représentations décimales de $\frac{p_n}{q_n}$ et de π coïncident pendant $2r$ chiffres après le virgule. On voit cela bien avec $\frac{333}{106}$ (4 chiffres) et $\frac{103993}{33102}$ (9 chiffres). Mais l'inégalité raffinée $\left|\frac{p_n}{q_n} - \pi\right| < \frac{1}{a_{n+1}q_n^2}$ indique que le l'approximation est particulièrement bonne quand le prochain quotient partiel est grand. On voit cela d'abord

pour $\frac{22}{7}$ où l'erreur est plus proche de $\frac{1}{1000}$ que de $\frac{1}{50}$, et surtout pour $\frac{355}{113}$, où l'erreur est plus proche de 10^{-6} que de 10^{-4}.

On a aussi $\xi_{n+1} < a_{n+1} + 1$ et $q_{n-1} \leq q_n$, d'où

$$\xi_{n+1}q_n + q_{n-1} < (a_{n+1}+1)q_n + q_{n-1} = q_{n+1} + q_n \leq (a_{n+1}+2)q_n$$

et donc des minorations

$$\left|\frac{p_n}{q_n} - \xi\right| > \frac{1}{q_n(q_{n+1}+q_n)} \geq \frac{1}{(a_{n+1}+2)q_n^2}.$$

Donc pour qu'une réduite $\frac{p_n}{q_n}$ de ξ soit exceptionnellement proche de ξ, il faut et il suffit que le prochain quotient partiel a_{n+1} soit exceptionnellement grand.

Théorème 9.4. *Soit ξ un réel et $[a_0, a_1, a_2, \dots]$ sa fraction continue obtenue par l'algorithme (11).*

Si ξ est irrationnel, alors $[a_0, a_1, a_2, \dots]$ est la seule fraction continue de valeur ξ.

Si ξ est rationnel, alors $[a_0, a_1, \dots, a_{N-1}, a_N]$ et $[a_0, a_1, \dots, a_{N-1}, a_N - 1, 1]$ sont les deux seules fractions continues de valeur ξ.

La preuve est par récurrence, et utilise sur deux lemmes.

Lemme 9.5. *Soit $[a_0, a_1, a_2, \dots]$ une fraction continue de valeur ξ. Si ξ n'est pas entier, alors $a_0 = [\xi]$. Si $\xi = m$ est entier, alors $[a_0, a_1, \dots]$ est $[m]$ ou $[m-1, 1]$.*

Preuve. La fraction continue peut avoir 4 formes : $[a_0]$, $[a_0, 1]$, $[a_0, a_1]$ avec $a_1 \geq 2$, et $[a_0, a_1, a_2, \dots]$.

Dans les deux premiers cas, $\xi = m$ est entier, et la fraction continue et $[m]$ ou $[m-1, 1]$.

Dans le troisième cas, on a $\xi = a_0 + \frac{1}{a_1}$ avec $a_1 \geq 2$, d'où un encadrement $a_0 < \xi \leq a_0 + \frac{1}{2} < a_0 + 1$. Donc ξ est non entier et $[\xi] = a_0$.

Dans le quatrième cas, par le théorème 9.1 toutes les réduites paires sont plus petites que ξ, et toutes les réduites impaires sont plus grandes que ξ, avec égalité seulement quand ξ est rationnel et la réduite est la dernière et vaut ξ. Or dans ce cas $\frac{p_0}{q_0}$ et $\frac{p_1}{q_1}$ ne sont pas les dernières réduites, donc on a $a_0 = \frac{p_0}{q_0} < \xi < \frac{p_1}{q_1} = a_0 + \frac{1}{a_1} \leq a_0 + 1$. D'où ξ est encore non entier, et $[\xi] = a_0$. □

Lemme 9.6. *Soit $[a_0, a_1, a_2, \dots]$ une fraction continue de valeur ξ, et soit $\frac{p_0}{q_0}, \frac{p_1}{q_1}, \frac{p_2}{q_2}, \dots$ ses réduites. Soit ξ_{n+1} l'unique réel avec $\xi = \frac{p_n\xi_{n+1}+p_{n-1}}{q_n\xi_{n+1}+q_{n-1}}$. Alors $[a_{n+1}, a_{n+2}, a_{n+3}, \dots]$ est de valeur ξ_{n+1}.*

Preuve. Pour une fractions continue finie

$$a_0 + \cfrac{1}{\ddots \cfrac{1}{a_n + \cfrac{1}{\boxed{a_{n+1} + \cfrac{1}{\ddots + \cfrac{1}{a_{n+m}}}}}}} \tag{13}$$

on peut traiter la partie emboîtée comme un seul nombre $[a_{n+1}, \dots, a_{n+m}] = \frac{h_m}{k_m}$. On a donc

$$\frac{p_{n+m}}{q_{n+m}} = [a_0, \dots a_{n+m}] = [a_0, \dots, a_n, \frac{h_m}{k_m}] = \frac{\frac{h_m}{k_m} p_n + p_{n-1}}{\frac{h_m}{k_m} q_n + q_{n-1}} \tag{14}$$

On peut résoudre l'équation $\xi = \frac{p_n \xi_{n+1} + p_{n-1}}{q_n \xi_{n+1} + q_{n-1}}$ et l'équation (14) pour trouver

$$\xi_{n+1} = -\frac{q_{n-1}\xi - p_{n-1}}{q_n \xi - p_n} \qquad\qquad \frac{h_m}{k_m} = -\frac{q_{n-1}\frac{p_{n+m}}{q_{n+m}} - p_{n-1}}{q_n \frac{p_{n+m}}{q_{n+m}} - p_n} \tag{15}$$

Comme les réduites $\frac{p_{n+m}}{q_{n+m}}$ de $[a_0, a_1, \dots]$ tendent vers ξ, les réduites $\frac{h_m}{k_m}$ de $[a_{n+1}, a_{n+2}, a_{n+3}, \dots]$ tendent vers ξ_{n+1}. □

Preuve du théorème 9.4. On distingue deux cas : ξ irrationnel et ξ rationnel.

D'abord traitons le cas d'un ξ irrationnel. Supposons que $[b_0, b_1, b_2, \dots]$ est aussi de valeur ξ. Montrons que $a_n = b_n$ pour tout n. C'est vrai pour $n = 0$ car on a $[\xi] = a_0 = b_0$ par le lemme 9.5. Supposons maintenant que $a_i = b_i$ pour tout $0 \leq i \leq n$. Alors on a $[b_0, b_1, \dots] = [a_0, \dots, a_n, b_{n+1}, b_{n+2}, \dots]$. Par le lemme 9.6, on voit que $[a_{n+1}, a_{n+2}, \dots]$ et $[b_{n+1}, b_{n+2}, \dots]$ sont tous les deux de valeur ξ_{n+1}. Comme ξ_{n+1} est irrationnel, le lemme 9.5 dit qu'on a $[\xi_{n+1}] = a_{n+1} = b_{n+1}$. Donc on a la récurrence montrant qu'on a $a_n = b_n$ pour tout n.

Maintenant traitons le cas d'un ξ rationnel dont la fraction continue donnée par l'algorithme (11) est $[a_0, \dots, a_m]$. Soit $[b_0, \dots, b_k]$ une autre fraction continue de valeur ξ. Les mêmes arguments que dans le cas irrationnel marchent tant que les $\xi_{n+1} = [a_{n+1}, \dots, a_m]$ sont non entiers. Donc on a $[a_0, \dots, a_{m-1}, a_m] = [a_0, \dots, a_{m-1}, b_m, \dots, b_k]$, et on a $\xi_m = a_m = [b_m, \dots, b_k]$ entier. Par le lemme 9.5 on a donc soit $[b_m, \dots, b_k] = [a_m]$ soit $[b_m, \dots, b_k] = [a_m - 1, 1]$. □

10. Fractions continues périodiques

Définition 10.1. Un *irrationnel quadratique* est un nombre réel de la forme $a + b\sqrt{D}$ avec $D \geq 2$ un entier non carré, et a et $b \neq 0$ rationnels. On dit aussi un *nombre quadratique réel.*

Par exemple,

$$\sqrt{2}, \qquad\qquad \frac{1+\sqrt{5}}{2}, \qquad\qquad \frac{2+\sqrt{14}}{5}$$

sont des irrationnels quadratiques. Les nombres quadratiques réels sont les solutions réelles mais irrationnelles des équations du second degré $ax^2 + bx + c = 0$ avec a, b, c rationnels (ou entiers). Pour trouver l'équation du second degré dont $\frac{2+\sqrt{14}}{5}$ est la solution, on écrit $x = \frac{2+\sqrt{14}}{5}$ puis on isole le radical

$$5x - 2 = \sqrt{14}.$$

Maintenant on élève les deux membres de l'équation au carré, puis on met tous les termes d'un côté.

$$(5x-2)^2 = \left(\sqrt{14}\right)^2 = 14, \qquad 25x^2 - 20x + 4 = 14, \qquad 25x^2 - 20x - 10 = 0.$$

Comme les trois coefficients 25, -20, -10 ont un pgcd non trivial 5, on peut diviser par lui et trouver l'équation plus jolie

$$5x^2 - 4x - 2 = 0.$$

Cette procédure trouve une équation du second degré $ax^2 + bx + c = 0$ avec a, b, c entiers, $a > 0$ et $\text{pgcd}(a, b, c) = 1$ pour tout irrationnel quadratique.

Le grand théorème sur les fractions continues et les irrationnels quadratiques est le suivant.

Théorème 10.2. *La fraction continue d'un réel ξ est ultimement périodique si et seulement si ξ est un irrationnel quadratique.*

Une fraction continue ultimement périodique est notée avec une barre au dessus de la période, comme pour les décimaux. Par exemple $[1, 1, \overline{2, 1, 4}]$ signifie $[1, 1, 2, 1, 4, 2, 1, 4, 2, 1, 4, \dots]$.

Commençons d'abord avec une fraction continue périodique dès son début, par exemple $[\overline{1}] = [1, 1, 1, 1, \dots]$. Essentiellement, si on a

$$x = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{\ddots}}}},$$

alors on a

$$x = 1 + \frac{1}{x}.$$

Cela se résout en écrivant $x = \frac{x+1}{x}$ puis $x^2 = x + 1$ puis $x^2 - x - 1 = 0$. Or cette équation du second degré a une solution positive $\frac{1+\sqrt{5}}{2}$ et une solution négative $\frac{1-\sqrt{5}}{2}$. Comme notre nombre est positif — sa partie entière est $[x] = a_0 = 1$ — on a $x = \frac{1+\sqrt{5}}{2}$.

Similairement si on a

$$y = 1 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{\ddots}}}}}} = [\overline{1, 2, 3}],$$

alors on a

$$y = 1 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{y}}} = [1, 2, 3, y].$$

On évalue le membre de droite par l'algorithme des réduites

a_i	$-$	1	2	3	y
p_i	1	1	3	10	$10y + 3$
q_i	0	1	2	7	$7y + 2$

Donc on a

$$y = \frac{10y + 3}{7y + 2}, \qquad y(7y + 2) = 7y^2 + 2y = 10y + 3, \qquad 7y^2 - 8y - 3 = 0$$

$$y = \frac{8 \pm \sqrt{8^2 + 4 \cdot 7 \cdot 3}}{2 \cdot 7} = \frac{8 \pm \sqrt{148}}{14} = \frac{4 \pm \sqrt{37}}{7}.$$

Pour les fractions continues qui sont périodiques dèpuis leur début avec des quotients partiels strictement positif $a_i > 0$, il y a toujours une racine positive et une racine négative de l'équation du second degré, et notre nombre est la racine positive $y = \frac{4+\sqrt{37}}{7}$.

(La raison pour laquelle les racines sont de signes opposés est que l'équation est de la forme

$$q_n x^2 - (p_n - q_{n-1})x - p_{n-1} = 0 \qquad \text{ou} \qquad x^2 - \frac{p_n - q_{n-1}}{q_n}x - \frac{p_{n-1}}{q_n} = 0.$$

Les deux solutions α, β d'une telle équation vérifient $\alpha + \beta = \frac{p_n - q_{n-1}}{q_n}$ et $\alpha\beta = -\frac{p_{n-1}}{q_n} < 0$. Donc une est positive et une est négative.)

Si la fraction continue n'est pas périodique depuis le début mais seulement plus tard, on calcule d'abord la partie périodique. Par exemple pour $z = [1, 1, \overline{1, 2, 3}]$ on écrit

$$z = [1, 1, y] \qquad y = [\overline{1, 2, 3}] = [1, 2, 3, y].$$

On calcule d'abord $y = \frac{4+\sqrt{37}}{7}$ comme ci-dessus. Puis on utilise l'algorithme des réduites pour calculer z

a_i	$-$	1	1	y
p_i	1	1	2	$2y+1$
q_i	0	1	1	$y+1$

$$z = \frac{2y+1}{y+1} = \frac{2 \cdot \frac{4+\sqrt{37}}{7} + 1}{\frac{4+\sqrt{37}}{7} + 1} \cdot \frac{7}{7} = \frac{15 + 2\sqrt{37}}{11 + \sqrt{37}} \cdot \frac{11 - \sqrt{37}}{11 - \sqrt{37}} = \frac{81 + 7\sqrt{37}}{84}.$$

Un autre exemple : pour calculer $x = [1, 2, 3, 3, 3, \dots] = [1, 2, \overline{3}]$, on écrit $x = [1, 2, y]$ et $y = [\overline{3}] = [3, y]$. On a les tableaux

$y \to$

a_i	$-$	3	y
p_i	1	3	$3y+1$
q_i	0	1	y

$x \to$

a_i	$-$	1	2	y
p_i	1	1	3	$3y+1$
q_i	0	1	2	$2y+1$

Donc on a

$$y = \frac{3y+1}{y}, \qquad y^2 = 3y + 1, \qquad y^2 - 3y - 1 = 0, \qquad y = \frac{3 + \sqrt{13}}{2},$$

$$x = \frac{3y+1}{2y+1} = \frac{3 \cdot \frac{3+\sqrt{13}}{2} + 1}{2 \cdot \frac{3+\sqrt{13}}{2} + 1} \cdot \frac{2}{2} = \frac{11 + 3\sqrt{13}}{8 + 2\sqrt{13}} \cdot \frac{8 - 2\sqrt{13}}{8 - 2\sqrt{13}} = \frac{10 + 2\sqrt{13}}{12} = \frac{5 + \sqrt{13}}{6}.$$

Pour trouver la fraction continue d'un irrationnel quadratique ξ avec une étape de préparation que j'expliquerai en bas, on applique l'algorithme standard, mais en gardant la liste $a_0, a_1, a_2, \dots$ des quotients partiels, mais aussi la liste $\xi_0, \xi_1, \xi_2, \dots$ des restes partiels. Quand on trouve une répétition $\xi_i = \xi_{i+n}$, on sait qu'on aura ensuite

$$\begin{aligned} a_i &= [\xi_i] = [\xi_{i+n}] = a_{i+n}, \\ \xi_{i+1} &= \frac{1}{\xi_i - a_i} = \frac{1}{\xi_{i+n} - a_{i+n}} = \xi_{i+n+1}, \\ a_{i+1} &= [\xi_{i+1}] = [\xi_{i_{n+1}}] = a_{i+n+1}, \\ &\dots \end{aligned}$$

Donc on aura $a_k = a_{k+n}$ pour tout $k \geq i$ et la fraction continue est

$$\xi = [a_0, a_1, \dots, a_{i-1}, \overline{a_i, \dots, a_{i+n-1}}].$$

Par exemple, pour $\xi = \sqrt{7}$, on trouve

$$\begin{aligned}
\xi_0 &= \sqrt{7},\\
a_0 &= \lfloor \sqrt{7} \rfloor = 2,\\
\xi_1 &= \frac{1}{\sqrt{7}-2} \cdot \frac{\sqrt{7}+2}{\sqrt{7}+2} = \frac{\sqrt{7}+2}{3},\\
a_1 &= \left\lfloor \frac{\sqrt{7}+2}{3} \right\rfloor = 1,\\
\xi_2 &= \left(\frac{\sqrt{7}-1}{3} \right)^{-1} = \frac{3}{\sqrt{7}-1} \cdot \frac{\sqrt{7}+1}{\sqrt{7}+1} = \frac{3(\sqrt{7}+1)}{6} = \frac{\sqrt{7}+1}{2},\\
a_2 &= \left\lfloor \frac{\sqrt{7}+1}{2} \right\rfloor = 1,\\
\xi_3 &= \frac{2}{\sqrt{7}-1} = \frac{\sqrt{7}+1}{3},\\
a_3 &= \left\lfloor \frac{\sqrt{7}+1}{3} \right\rfloor = 1,\\
\xi_4 &= \frac{3}{\sqrt{7}-2} = \sqrt{7}+2,\\
a_4 &= \lfloor \sqrt{7}+2 \rfloor = 4,\\
\xi_5 &= \frac{1}{\sqrt{7}-2} = \frac{\sqrt{7}+2}{3} = \xi_1.
\end{aligned}$$

et on a $\sqrt{7} = [2, \overline{1,1,1,4}]$.

On voit un phénomène apparaît. Tous nos ξ_n sont de la forme

$$\xi_n = \frac{\sqrt{D}+U_n}{V_n} \qquad \text{avec } V_n \text{ divisant } D - U_n^2. \tag{16}$$

Quand on a cela, on a

$$\xi_n - a_n = \frac{\sqrt{D} + (U_n - a_n V_n)}{V_n} = \frac{\sqrt{D} - U_{n+1}}{V_n}$$

pour $U_{n+1} = a_n V_n - U_n$. Or V_n qui divise $D - U_n^2$ divise aussi $D - U_{n+1}^2 = D - (U_n - a_n V_n)^2$. Donc on a

$$\xi_{n+1} = \frac{1}{\xi_n - a_n} = \frac{V_n}{\sqrt{D} - U_{n+1}} = \frac{\sqrt{D}+U_{n+1}}{V_{n+1}}$$

avec $V_n V_{n+1} = D - U_{n+1}^2$. Donc dès qu'on a ξ_n sous la forme (16), on pose

$$a_n = \left\lfloor \frac{\sqrt{D}+U_n}{V_n} \right\rfloor, \quad U_{n+1} = a_n V_n - U_n, \quad V_{n+1} = \frac{D - U_{n+1}^2}{V_n}, \quad \xi_{n+1} = \frac{\sqrt{D}+U_{n+1}}{V_{n+1}}. \tag{17}$$

Et comme V_{n+1} divise $D - U_{n+1}^2$, on peut continuer, jusqu'à ce qu'on voit une répétition.

Il est toujours possible de réécrire un irrationnel quadratique sous la forme (16). Par exemple, si on a $\xi = \frac{1}{2} - \frac{\sqrt{2}}{3}$:

– On écrit tout un dénominateur commun : $\xi = \frac{3}{6} - \frac{2\sqrt{2}}{6} = \frac{-2\sqrt{2}+3}{6}$.

– Si le signe devant le terme avec le radical est négatif, on le fait entrer dans le dénominateur : $\xi = \frac{2\sqrt{2}-3}{-6}$.
– S'il y a un entier devant le radical comme dans $2\sqrt{2}$, on fait entrer son carré sous le radical $\sqrt{8}$. Cela donne $\xi = \frac{\sqrt{8}-3}{-6}$.
– On a maintenant un $\frac{\sqrt{d}+u}{v}$. Si v ne divise pas $d-u^2$, on multiplie numérateur et dénominateur par $w = \frac{|v|}{\operatorname{pgcd}(v,d-u^2)}$. On a $\frac{\sqrt{d}+u}{v} = \frac{\sqrt{dw^2}+uw}{vw}$ avec vw divisant $(d-u^2)w^2$. Maintenant on a ce qu'il faut. Dans notre cas, on trouve $\xi = \frac{\sqrt{8\cdot 36}-18}{-36} = \frac{\sqrt{288}-18}{-36}$.

Maintenant on fait les calculs (17) en prenant compte de l'encadrement $16 < \sqrt{288} < 17$.

$$\begin{aligned}
\xi_0 &= \frac{\sqrt{288}-18}{-36}, & a_0 &= 0, & \xi_0 - a_0 &= \frac{\sqrt{288}-18}{-36},\\
\xi_1 &= \frac{-36}{\sqrt{288}-18} = \frac{\sqrt{288}+18}{1}, & a_1 &= 34, & \xi_1 - a_1 &= \frac{\sqrt{288}-16}{1}\\
\xi_2 &= \frac{1}{\sqrt{288}-16} = \frac{\sqrt{288}+16}{32}, & a_2 &= 1, & \xi_2 - a_2 &= \frac{\sqrt{288}-16}{32}\\
\xi_3 &= \frac{32}{\sqrt{288}-16} = \frac{\sqrt{288}+16}{1} & a_3 &= 32, & \xi_3 - a_3 &= \frac{\sqrt{288}-16}{1}\\
\xi_4 &= \frac{1}{\sqrt{288}-16} = \frac{\sqrt{288}+16}{32} = \xi_2
\end{aligned}$$

Donc $\frac{1}{2} - \frac{\sqrt{2}}{3} = [0, 34, \overline{1, 32}]$.

Théorème 10.3. *Pour $N \geq 2$ un entier naturel non carré, la fraction continue de $[\sqrt{N}]+\sqrt{N}$ est périodique depuis le début.*

Donc les fractions continues de $1+\sqrt{2}$, $1+\sqrt{3}$, $2+\sqrt{5}$, $2+\sqrt{6}$, $2+\sqrt{7}$, $2+\sqrt{8}$, $3+\sqrt{10}$, $3+\sqrt{11}$, …, sont périodiques depuis le début. Si la fraction continue de $[\sqrt{N}]+\sqrt{N}$ est $[\overline{2a_0, a_1, \ldots, a_n}]$, alors celle de $\sqrt{N}$ est $[a_0, \overline{a_1, \ldots, a_n, 2a_0}]$.

Références. Il y a essentiellement deux démonstrations de la périodicité ultime de la fraction continue d'un irrationel quadratique ξ : une [2, 3, 6] qui démontre que dans les équations du second degré $A_n\xi_n^2 + B_n\xi_n + C_n = 0$ vérifiées par les ξ_n, les A_n, B_n, C_n sont bornés, donc il faut que dans la suite infinie des ξ_n il y a des répétitions de ces équations. L'autre [4, 7, 8] démontre que les conjugués $\overline{\xi}_n$ sont ultimement négatifs, donnant des bornes $0 < V_n < D$ et $|U_n| < \sqrt{D}$ pour $n \gg 0$, donc il faut encore des répétitions.

Dans [8, Theorem 7.20] on trouve une caractérisation des ξ dont la fraction continue est périodique (non seulement ultimement). La caractérisation est équivalente à ce que ξ soit de la forme $\alpha + \sqrt{\beta}$ avec β un rationnel positif non carré, et α un rationnel vérifiant $|\sqrt{\beta}-1| < \alpha < \sqrt{\beta}$. Les nombres $[\sqrt{N}]+\sqrt{N}$ sont de ce genre, d'où le théorème 10.3.

Pour certains nombres, dont les $[\sqrt{N}]+\sqrt{N}$, les périodes sont symétriques, et la fraction continue de la forme $[\overline{a_0, a_1, a_2, a_3, \ldots, a_3, a_2, a_1}]$. Je n'ai pas trouvé de référence expliquant ce phénomène connu, mais je pense que c'est pour les $\alpha + \sqrt{\beta}$ comme ci-dessus avec α entier ou demi-entier.

Références

[1] Michel Demazure. *Cours d'algèbre : Primalité. Divisibilité. Codes.* Nouvelle Bibliothèque Mathématique, 1. Cassini, Paris, 1997.

[2] G.H. Hardy and E.M. Wright. *An introduction to the theory of numbers. Transl. from the English by François Sauvageot, introduction by Catherine Goldstein. (Introduction à la théorie des nombres.)*. Paris : Vuibert ; Paris : Springer. xxxiv, 568 p., 2007.

[3] A. Ya. Khinchin. *Continued fractions.* Dover Publications Inc., Mineola, NY, 1997. Traduit du russe. Réédition de la traduction américaine de 1964 [University of Chicago Press, Chicago].

[4] Donald E. Knuth. *The Art of Computer Programming. Vol. 2 : Seminumerical Algorithms.* Boston : Addison-Wesley, 3rd edition, 1998.

[5] H. W. Lenstra, Jr. Solving the Pell equation. *Notices Amer. Math. Soc.*, 49(2) :182–192, 2002.

[6] William Judson LeVeque. *Topics in number theory. Vol. I, II.* Dover Publications Inc., Mineola, NY, 2002. Reprint of the 1956 original [Addison-Wesley Publishing Co., Reading, Mass.].

[7] Ivan Niven. *Irrational numbers.* The Carus Mathematical Monographs, No. 11. The Mathematical Association of America. Distributed by John Wiley and Sons, Inc., New York, N.Y., 1956.

[8] Ivan Niven and Herbert S. Zuckerman. *An introduction to the theory of numbers.* John Wiley & Sons, New York-Chichester-Brisbane, 4th edition, 1980.

[9] André Weil. *Number theory for beginners.* Springer-Verlag, New York, 1979. Avec la collaboration de Maxwell Rosenlicht.