Devoir Surveillé n°2

Préliminaires

1. (Question de cours) Inégalité triangulaire (démonstration).
2. (Question de cours) Mettre $\cos(nx)$ sous la forme d'une fonction polynomiale en $\cos(x)$.
3. Montrer que $\text{Arctan}\left(\frac{1}{2}\right) + \text{Arctan}\left(\frac{1}{3}\right) = \frac{\pi}{4}$.
4. Simplifier l'expression suivante là où elle a un sens : $\text{Arccos}(-x) + \text{Arccos}(x)$.

Exercice - Nombres pseudo - premiers par rapport à a

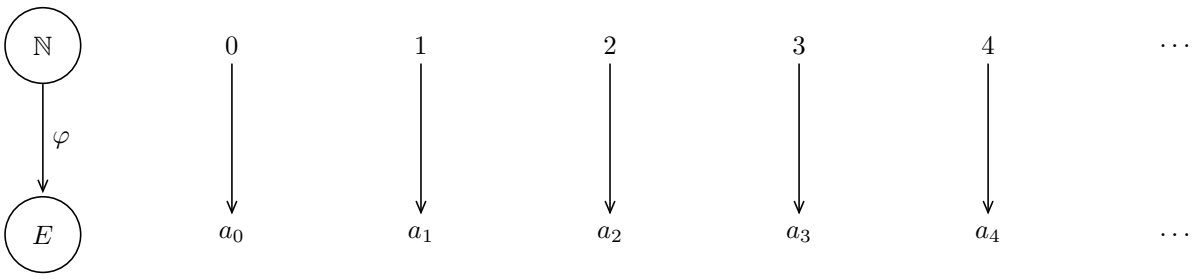
On se donne dans tout l'exercice un entier $a > 1$ ainsi qu'un nombre premier p impair qui ne divise pas $a^2 - 1$. Enfin, on pose

$$m = \frac{a^{2p} - 1}{a^2 - 1}$$

1. Justifier qu'il existe une infinité de nombres premiers p qui conviennent, et justifier que m est un entier (on pourra utiliser la factorisation de $x^n - y^n$, avec x, y et n bien choisis).
2. Prouver que $a^{2p} \equiv 1[m]$.
3. Justifier que $(a^2 - 1) \times (m - 1) = a\left(a^{p-1} - 1\right)(a^p + a)$.
4. (a) Justifier que $a^{p-1} - 1$ est divisible par p.
   (b) En se souvenant que $p - 1$ est pair et en utilisant la factorisation de $x^n - y^n$, montrer que $a^{p-1} - 1$ est aussi divisible par $a^2 - 1$. En déduire que $a^{p-1} - 1$ est divisible par $p(a^2 - 1)$.
   (c) Prouver également que $a^p + a$ est divisible par 2.
5. Déduire de la question précédente et de la question 3 que $2p$ divise $m - 1$.
6. Prouver que $a^{m-1} \equiv 1[m]$.

Problème - Dénombrabilité de $\mathbb{Q}$

On dit qu'un ensemble E est dénombrable lorsqu'il est en bijection avec $\mathbb{N}$. Intuitivement, un ensemble est dénombrable lorsqu'on peut le mettre « face à face avec $\mathbb{N}$ » (rappelons qu'en anglais, une bijection est parfois appelée « one to one function »), lorsqu'on peut « dénombrer » ses éléments, c'est-à-dire lorsqu'on peut écrire ses éléments sous la forme $a_0, a_1, \ldots$ (i.e. sous forme de suite) :



Le but du problème est donc de prouver (de plusieurs façons différentes) que $\mathbb{Q}$ est dénombrable.

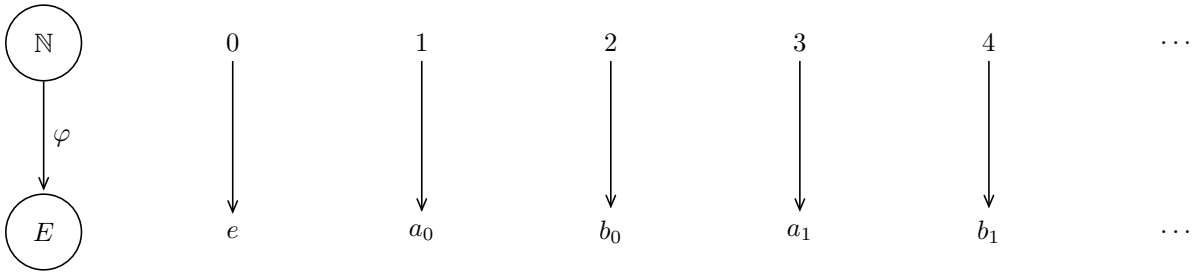
Ce résultat, assez simple (il est au programme de deuxième année et on en verra une autre démonstration au chapitre 17), est tout de même très riche d'un point de vue mathématique, et se trouve (on va le voir) au cœur de nombreux domaines des mathématiques (théorie des ensembles évidemment, mais aussi arithmétique, fractions continuées, etc.).

On pourra, dans tout le problème, utiliser sans démonstration le théorème de Cantor-Bernstein [1] : si E et F sont deux ensembles tels qu'il existe une injection de E dans F et une injection de F dans E, alors il existe une bijection de E dans F.

1. Démontré dans le chapitre 4 (mais non traité en classe) et dans le DS n° 2 de l'an dernier.

Partie I - Préliminaires

1. Prouver que $\mathbb{N}^*$ est dénombrable. Évidemment, on n'affirmera pas sans preuve qu'une fonction est bijective... Illustrer par un dessin du même type que celui de l'introduction.
2. Justifier qu'il suffit de prouver qu'il existe une injection de $\mathbb{Q}$ dans $\mathbb{N}$ ou dans $\mathbb{N}^*$ pour affirmer que $\mathbb{Q}$ est dénombrable. On prouverait de même (et donc on l'admettra) qu'il suffit d'une injection de $\mathbb{Q}_+^*$ dans $\mathbb{N}$ ou dans $\mathbb{N}^*$ pour prouver que $\mathbb{Q}_+^*$ est dénombrable.
3. La fonction
$$f : \begin{cases} \mathbb{N} \times \mathbb{N}^* \longrightarrow \mathbb{Q} \\ (p,q) \longmapsto \dfrac{p}{q} \end{cases}$$
est-elle injective ? surjective ?
4. (a) On suppose dans cette question que A et B sont disjoints et dénombrables et on se donne un élément e qui n'appartient pas à A ni à B. On se donne donc $f : \mathbb{N} \to A$ et $g : \mathbb{N} \to B$ bijectives. Prouver que la fonction
$$h : \begin{cases} \mathbb{N} \longrightarrow & A \cup \{e\} \cup B \\ n \longmapsto \begin{cases} e & \text{si } n = 0 \\ f\left(\dfrac{n-1}{2}\right) & \text{si } n \text{ est impair} \\ g\left(\dfrac{n-2}{2}\right) & \text{si } n \text{ est pair} \end{cases} \end{cases}$$
est une bijection de $\mathbb{N}$ dans $E = A \cup \{e\} \cup B$. Ainsi, $A \cup \{e\} \cup B$ est dénombrable, ce qui se voit bien sur le dessin suivant (avec des notations transparentes pour A et B) :



   (b) En déduire qu'il suffit de prouver que $\mathbb{Q}_+^*$ est dénombrable pour affirmer que $\mathbb{Q}$ est dénombrable.

Partie II - Première preuve

1. Montrer que l'application
$$f : \begin{cases} \mathbb{Q} \longrightarrow & \mathbb{N} \\ r = \dfrac{p}{q} \longmapsto \begin{cases} 3^p \times 5^q & \text{si } r \geq 0 \\ 2 \times 3^{-p} \times 5^q & \text{si } r < 0 \end{cases} \end{cases}$$
où p/q est l'écriture **irréductible** du rationnel r (c'est-à-dire avec $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$ premiers entre eux), est bien définie.
2. Montrer que f injective : cela prouve donc, cf. question 2 de la partie I, que $\mathbb{Q}$ est dénombrable.
3. Est-elle bijective ?

Partie III - En passant par $\mathbb{N}^2$

1. (a) Montrer par récurrence [2] que, pour tout $n \in \mathbb{N}^*$, il existe un couple $(p,q) \in \mathbb{N}^2$ tel que $n = 2^p(2q+1)$.
   (b) Soit $n \in \mathbb{N}$. Justifier que le couple (p,q), dont l'existence a été prouvée à la question précédente, est unique. Il n'est pas nécessaire de faire une récurrence dans cette question.

2. Il est demandé explicitement de faire une récurrence dans cette question, même si on pourrait s'en passer : cf. question 1.(c).

(c) Sans récurrence, mais avec des arguments arithmétiques, prouver une seconde fois, pour tout $n \in \mathbb{N}^*$, l'existence d'un couple $(p, q) \in \mathbb{N}^2$ tel que $n = 2^p(2q + 1)$. Il n'est pas demandé de prouver l'unicité.

(d) En déduire une bijection de $\mathbb{N}^2$ dans $\mathbb{N}^*$.

2. Montrer que l'application

$$f : \begin{cases} \mathbb{Q}_+^* & \longrightarrow & \mathbb{N}^2 \\ r = \dfrac{p}{q} & \longmapsto & (p, q) \end{cases}$$

où p/q est toujours l'écriture irréductible du rationnel r, est injective. Est-elle surjective ?

3. Conclure.

Partie IV - Arbre de Calkin-Wilf (2000) et théorème de Newman (2003)

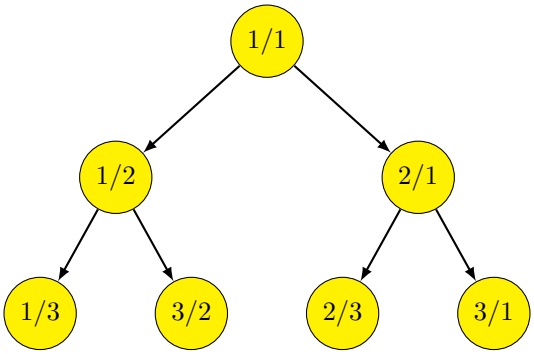
Nous définissons dans cette partie l'arbre binaire de Calkin-Wilf de la façon suivante :

- 1 se trouve au sommet (la racine).
- Chaque nœud x a deux fils : son fils gauche est $\dfrac{x}{x+1}$ et son fils droit est $x + 1$.

On prouverait par une récurrence immédiate (et donc on l'admettra) que, pour tout n, les nombres apparaissant à la ligne n sont des rationnels strictement positifs. On peut donc reformuler la définition de cet arbre de la façon suivante :

- $\dfrac{1}{1}$ se trouve au sommet (la racine).
- Chaque nœud de la forme $\dfrac{i}{j}$ (avec $i, j \geq 1$) a deux fils : son fils gauche est $\dfrac{i}{i+j}$ et son fils droit est $\dfrac{i+j}{j}$.

Les trois premières lignes de cet arbre sont donc :



1. Donner la quatrième ligne de l'arbre.
2. Montrer par récurrence que, pour tout n, si un rationnel r/s apparaît à la n-ième ligne, alors r et s sont premiers entre eux. On en déduit donc que toutes les fractions de l'arbre sont sous forme irréductible.
3. Le but de la question est de montrer, par récurrence forte sur $r + s \geq 2$, que toute fraction irréductible de la forme r/s apparaît au plus une fois dans l'arbre, c'est-à-dire que, pour tout $n \geq 2$, toute fraction irréductible de la forme r/s avec $r + s = n$ apparaît au plus une fois dans l'arbre.

   (a) Soit r/s une fraction irréductible de l'arbre qui ne soit pas la racine (donc qui ait un père). Justifier que $r \neq s$ et en déduire que le résultat est vrai au rang $n = 2$.

   (b) On fixe dans la suite de cette question un entier $n \geq 2$, on suppose le résultat vrai aux rangs $2, \ldots, n$ et on se donne une fraction irréductible r/s telle que $r + s = n + 1$. Justifier que $s > r$ ou $r > s$. On supposera dans la suite (raisonnement analogue dans l'autre cas) que $s > r$.

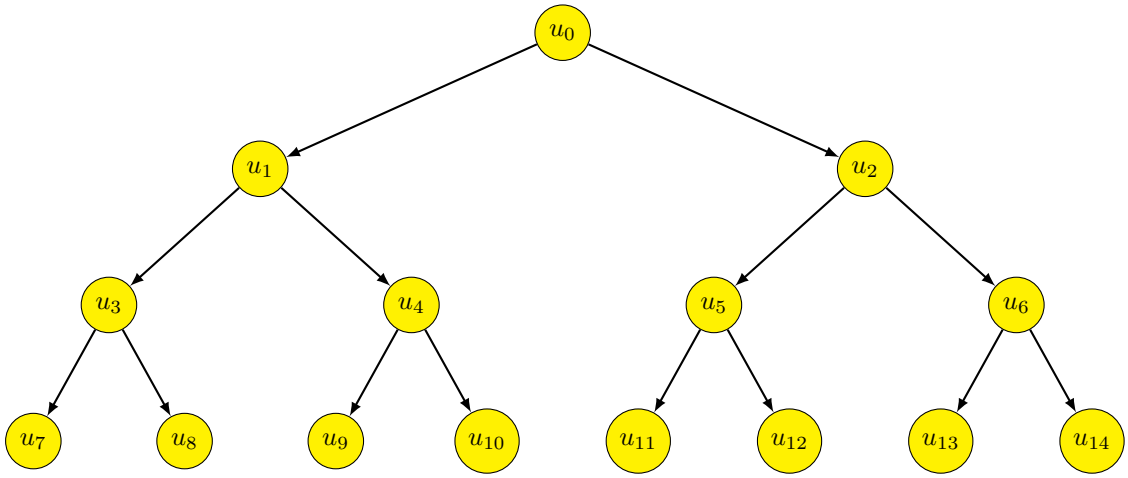
   (c) On suppose que la fraction r/s apparaît deux fois. Montrer que les deux pères de r/s sont égaux et donner leur expression (commune) en fonction de r et s. On rappelle (cf. cours) que l'écriture irréductible d'un rationnel est unique [3], c'est-à-dire que si $a/b = c/d$ sont deux fractions irréductibles, alors $a = c$ et $b = d$.

   (d) Conclure.

4. Montrer de même que toute fraction irréductible (strictement positive) apparaît dans l'arbre. On a donc prouvé que l'arbre contient exactement une fois tout rationnel strictement positif (et qu'il apparaît sous sa forme irréductible).

Numérotons les éléments de l'arbre de la façon suivante : on note $u_0 = 1$, puis $u_1 = 1/2, u_2 = 2/1$ puis $u_3 = 1/3, u_4 = 3/2, u_5 = 2/3, u_6 = 3/1$ etc. Plus précisément : on parcourt successivement chaque ligne de gauche à droite, et cela nous donne une suite $(u_n)_{n\in\mathbb{N}}$.

3. On dira « par unicité d'une fraction irréductible ». Si je lis le mot « identification », je brûle la copie.



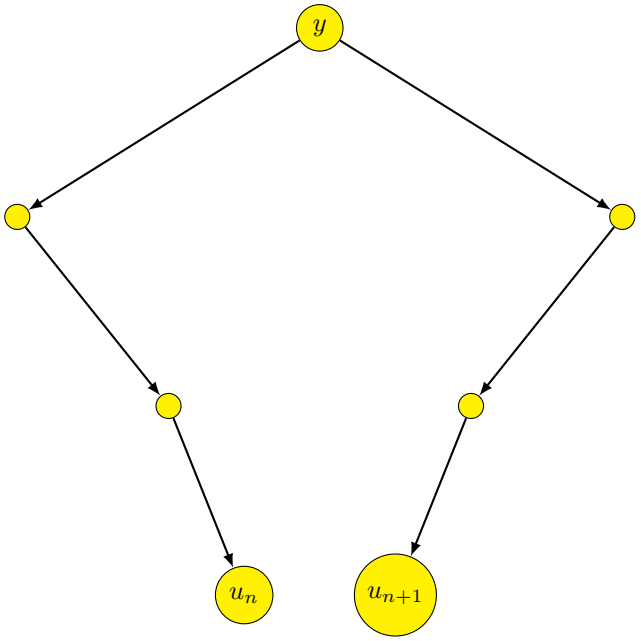
On vient de prouver que chaque rationnel strictement positif apparaît exactement une fois dans les termes de la suite. Une suite étant une fonction définie sur $\mathbb{N}$, on vient donc de prouver l'existence d'une bijection de $\mathbb{N}$ dans $\mathbb{Q}_+^*$: on a vu que cela suffisait pour prouver que $\mathbb{Q}$ est dénombrable.

Le but de la fin de la partie est de trouver une relation simple entre un terme de la suite et son successeur : en d'autres termes, pour tout n, peut-on trouver une relation reliant u_{n+1} et u_n ?

On se donne dans la suite un entier $n \in \mathbb{N}$. On admettra (ce n'est pas très difficile à voir mais un peu ennuyeux à rédiger proprement) que :

- u_n et u_{n+1} ont un plus proche ancêtre commun noté y.
- u_n est obtenu à partir de y en prenant une fois le fils gauche, puis k fois (pour un certain k) fois le fils droit.
- u_{n+1} est obtenu à partir de y en prenant une fois le fils droit, puis k fois (pour un certain k) fois le fils gauche.

Par exemple, pour u_8 et u_9, leur plus proche ancêtre commun y est u_1, et $k = 1$ (fils gauche puis 1 fils droit pour u_8, et fils droit puis 1 fils gauche pour u_9). Si on prend u_{10} et u_{11}, alors leur plus proche ancêtre commun est u_0, et $k = 2$: fils gauche puis 2 fils droits pour u_{10}, un fils droit et 2 fils gauches pour u_{11}. Remarquons que $k = 0$ si u_n est un fils gauche, et u_{n+1} le fils droit associé (par exemple u_3 et u_4, alors $y = u_1$ comme plus proche ancêtre commun) : ainsi, ce résultat est toujours valable.



5. (a) Exprimer le k-ième fils gauche d'un nœud x (i.e. le nœud obtenu en prenant k fois uniquement le fils gauche de x), ainsi que son k-ième fils droit. Les « par récurrence immédiate » seront acceptés, mais si votre formule est fausse, il ne faudra pas venir pleurer !

   (b) En déduire une expression de u_n et de u_{n+1} en fonction de y et de k.

6. En remarquant que $0 \leq \dfrac{y}{y+1} < 1$, justifier que $k = \lfloor u_n \rfloor$.

7. Prouver finalement que :

$$u_{n+1} = \frac{1}{2\lfloor u_n \rfloor - u_n + 1}$$

On a donc prouvé le (magnifique) résultat suivant, prouvé par Moshe Newman en 2003 : la suite (u_n) définie par

$$u_0 = 1 \qquad \text{et} \qquad \forall n \in \mathbb{N}, \qquad u_{n+1} = \frac{1}{2\lfloor u_n \rfloor - u_n + 1}$$

est une énumération des rationnels strictement positifs, et contient exactement une fois chaque rationnel (strictement positif).

Partie V - Fraction continuée d'un rationnel

On se donne dans toute cette partie un rationnel strictement positif r qu'on écrit sous sa forme irréductible p/q (donc avec p et q premiers entre eux). On définit deux familles d'entiers de la façon suivante :

- $x_0 = r$.
- $a_0 = \lfloor x_0 \rfloor$.
- Si $a_0 = x_0$, on s'arrête. Sinon, on pose $x_1 = \dfrac{1}{x_0 - a_0}$ et $a_1 = \lfloor x_1 \rfloor$.
- Si $a_1 = x_1$, on s'arrête. Sinon, on pose $x_2 = \dfrac{1}{x_1 - a_1}$ et $a_2 = \lfloor x_2 \rfloor$.
- Soit $n \geq 2$. Supposons x_n et a_n construits. Si $a_n = x_n$, on s'arrête là, sinon on pose $x_{n+1} = \dfrac{1}{x_n - a_n}$ et $a_{n+1} = \lfloor x_{n+1} \rfloor$.
- On s'arrête dès qu'un des a_i est égal au x_i correspondant, c'est-à-dire dès qu'un des x_i est un entier (relatif).

1. Appliquer cet algorithme à $r = 2/7$.
2. Il est immédiat que tous les x_i (tant qu'ils sont bien définis, évidemment) sont rationnels, et donc on l'admettra. Pour tout i, notons $x_i = p_i/q_i$ avec p_i et q_i premiers entre eux. Justifier que, pour tout i tel que x_i existe, $0 \leq p_i - a_i \times q_i < q_i$. En déduire que, si x_{i+1} est bien défini, $q_{i+1} < q_i$ et $a_{i+1} \geq 1$. Attention, on rappelle que la fraction p_{i+1}/q_{i+1} doit être irréductible !
3. Prouver que l'algorithme termine. On note n le dernier rang des familles (x_i) et (a_i), c'est-à-dire que $a_n = x_n$.
4. On suppose que $n \geq 1$. Montrer par récurrence que, pour tout $i \in [\![1 ; n]\!]$,

$$r = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \; + \cfrac{1}{a_{i-2} + \cfrac{1}{a_{i-1} + \cfrac{1}{x_i}}}}}}$$

Pour gagner du temps, on pourra utiliser (dans cette partie et la suivante) la notation $[a_0; a_1; \ldots; a_{i-1}; x_i]$ pour désigner le membre de droite ci-dessus. En particulier (il n'est pas demandé de le prouver : cela découle de la récurrence précédente pour $i = n$) :

$$r = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \; + \cfrac{1}{a_{n-2} + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}}} = [a_0; a_1; \ldots; a_{n-1}; a_n]$$

Partie VI - Écriture d'un entier en base 2 et familles admissibles

On rappelle (cf. cours) que tout entier $n \in \mathbb{N}^*$ s'écrit de façon unique comme une somme de puissances de 2 distinctes, c'est-à-dire qu'il existe $k \geq 0$ et $(a_k, \ldots, a_0) \in \{0;1\}^{k+1}$ uniques tels que $a_k = 1$ et

$$n = a_k 2^k + \cdots + a_1 2^1 + a_0 2^0$$

Cette écriture s'appelle le développement en base 2 de n, que l'on notera plus simplement $n = \overline{a_k \cdots a_1 a_0}^2$. Par exemple, $13 = 8 + 4 + 1 = \overline{1101}^2$ et $24 = 16 + 8 = \overline{11000}^2$.

1. Donner l'écriture en base 2 de 100.

Écrivons tout entier n sous cette forme et mettons en évidence les suites de 1 et de 0 consécutifs de cette écriture :

$$n = \overline{\underbrace{1\ldots1}_{a_{2m}} \underbrace{0\ldots0}_{a_{2m-1}} \underbrace{1\ldots1}_{a_{2m-2}} \cdots \underbrace{1\ldots1}_{a_2} \underbrace{0\ldots0}_{a_1} \underbrace{1\ldots1}_{a_0}}^2$$

On désigne par a_0 la longueur de la suite de 1 la plus à droite (qui vaut 0 si n est pair), par a_1 la longueur de la suite de 0 qui la précède (a_1 est donc la longueur de la première suite de 0, même si n est pair et donc termine par un 0), etc. Le chiffre le plus à gauche de l'écriture de n étant un 1, cette série de longueurs se termine par un certain a_{2m} et, de a_0 à a_{2m}, contient un nombre impair de termes (il n'est pas demandé de le prouver). De plus, toutes les longueurs sont strictement positives (sauf peut-être a_0).

Désignons par φ l'application qui à n associe la suite $s = (a_0, a_1, \dots, a_{2m})$ (on fera attention au fait que a_0 est à gauche et a_{2m} à droite, contrairement à l'écriture de n en base 2). Par exemple, $\varphi(13) = (1, 1, 2)$ et $\varphi(24) = (0, 3, 2)$.

2. Donner $\varphi(100)$, et donner les antécédents de (1) et de $(0, 3, 1, 1, 2)$.

Dans la suite, on appelle « famille admissible » toute famille constituée d'un nombre impair d'éléments notée $s = (a_0, \dots, a_{2m})$ vérifiant l'une des deux conditions suivantes :

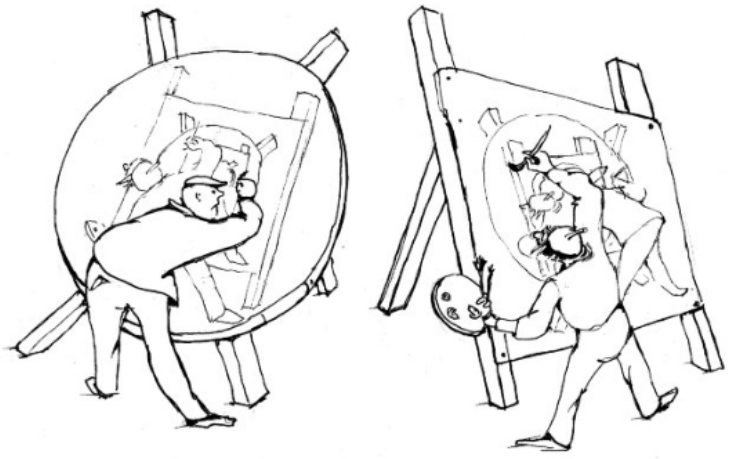
- soit $m = 0$ et $a_0 \in \mathbb{N}^*$.
- soit $m \geq 1$ et $a_0 \in \mathbb{N}, a_1, \dots, a_{2m} \in \mathbb{N}^*$.

3. Justifier rapidement que $\varphi(n)$ est une bijection de $\mathbb{N}^*$ dans l'ensemble des familles admissibles.

On associe maintenant à toute suite admissible s un rationnel $r(s) > 0$ défini de la façon suivante : si $m = 0$ et $s = (a_0)$, $r(s) = a_0$, et si $m \geq 1$ et $s = (a_0, \dots, a_{2m})$, alors :

$$r(s) = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \; a_{2m-2} + \cfrac{1}{a_{2m-1} + \cfrac{1}{a_{2m}}}}}} = [a_0; a_1; \dots; a_{2m-1}; a_{2m}]$$

4. Calculer $r(1, 2, 2)$ et $r(0, 3, 1, 1, 2)$.
5. Montrer que r est surjective (en tant qu'application de l'ensemble des familles admissibles dans $\mathbb{Q}_+^*$). On pourra utiliser la partie précédente et prouver que, si r admet un développement en fraction continuée de longueur paire $[a_0; \dots; a_n]$, alors soit $a_n > 1$, et alors $a_n = a_n - 1 + \frac{1}{1}$, soit $a_n = 1$, et alors $a_{n-1} + 1/a_n = a_{n-1} + 1$.
6. Le but de cette question est de prouver que r est injective. On se donne donc $s = (a_0, \dots, a_{2m})$ et $s' = (b_0, \dots, b_{2p})$ deux familles admissibles telles que $r(s) = r(s')$. Attention, les nombres $a_0, \dots, a_{2m}$ ne sont pas les mêmes que dans la partie précédente ! Tout ce qu'on sait est qu'ils vérifient les propriétés données dans la définition d'une famille admissible.
   (a) Justifier que, si $m \neq 0$ (i.e. la famille s contient au moins 3 éléments), alors $r(s) \notin \mathbb{N}$. En déduire que, si $m = 0$ et $r(s) = r(s')$ alors $s = s'$. Dans la suite de la question, on suppose donc $m \geq 1$.
   (b) Justifier que $a_0 = \lfloor r(s) \rfloor$. En déduire que $a_0 = b_0$.
   (c) On appelle s_1 et ${s_1}'$ les familles $(a_2, \dots, a_{2m})$ et $(b_2, \dots, b_{2p})$, c'est-à-dire les familles obtenues supprimant les deux premiers éléments de s et de s'. Montrer que s_1 et ${s_1}'$ sont encore des familles admissibles.
   (d) Vérifier que $a_1 + \frac{1}{r(s_1)} = b_1 + \frac{1}{r({s_1}')}$. Vérifier aussi que $r(s_1)$ et $r({s_1}')$ sont supérieurs ou égaux à 1 et que si l'inégalité est stricte pour l'un, elle l'est aussi pour l'autre. En déduire que, dans tous les cas, $a_1 = b_1$ et $r(s_1) = r({s_1}')$.
   (e) Prouver que r est injective.
7. Conclure encore une fois que $\mathbb{Q}$ est dénombrable.



Cantor and Bernstein en train de peindre.