# Sur la densité du chiffre 1 dans l'écriture binaire d'un nombre algébrique

Colin Faverjon

3 juillet 2009

## 1 Introduction

Les nombres réels peuvent être regroupés dans différents ensembles. $\mathbb{N}$ est l'ensemble des entiers naturels, $\mathbb{Z}$ l'ensemble des entiers relatifs, $\mathbb{Q}$ l'ensemble des rationnels et enfin $\mathbb{R}$ l'ensemble de tous les réels. Nous nous intéresserons ici à l'ensemble $\mathbb{R}\backslash\mathbb{Q}$, c'est à dire l'ensemble des nombres réel qui ne peuvent pas s'écrire sous la forme d'une fraction irréductible, l'ensemble des irrationnels. Ces nombres ont une infinité de chiffres non nuls après la virgule dans leur développement binaire (ainsi que dans n'importe quelle base), et ne sont pas ultimement périodiques, contrairement aux nombres rationnels. Par exemple

$$(\sqrt{2})_2 = 1.011\,010\,100\,000\,1\cdots \in \mathbb{R}\backslash\mathbb{Q}$$

$$\left(\frac{1}{7}\right)_2 = 0.001\,001\,001\,001\cdots = 0.(001)^\omega \notin \mathbb{R}\backslash\mathbb{Q}.$$

Aux nombres rationnels, qui ont un développement assez "simple", on peut opposer les nombres normaux. Un nombre est dit simplement normal si chaque chiffre apparait avec une même fréquence dans une base donnée. On dit qu'il est normal si il est simplement normal dans toutes les bases entières. Émile Borel a prouvé que "presque tous" les nombres sont normaux (au sens de la théorie de la mesure de Lesbegue).

On peut aussi séparer les nombres irrationnels en deux sous-ensembles : l'ensemble des nombres algébriques et l'ensemble des nombres transcendants. On dit qu'un nombre est algébrique s'il existe un polynôme à coefficients entiers dont il est racine, sinon on dit qu'il est transcendant. Le polynôme minimal de $x$, un nombre algébrique, est le polynôme annulateur de $x$, non nul, à coefficients entiers, premiers entre eux, de degré minimal et tel que le coefficient de plus haut degré est positif. On appelle degré de $x$ le degré de son polynôme minimal. Historiquement, on connait l'existence des nombres algébriques depuis l'antiquité alors que les premières preuves de transcendance ($\pi$, $e$) datent du XIX$^{ième}$ siècle.

Concernant le développement d'un nombre algébrique dans une base entière, on s'attend généralement au résultat suivant.

**Conjecture 1.1.** *Tout nombre irrationnel algébrique est normal.*

De façon surprenante, on ne dispose que de résultats extrêment partiels en direction de cette conjecture. Dans cette étude nous allons nous concentrer essentiellement sur l'écriture en base 2 des nombres irrationnels algébriques. On notera pour le développement binaire d'un nombre algébrique irrationnel $x$ :

$$x = a_{-k}a_{-k+1}...a_{-1}a_0.a_1a_2a_3....,$$

où les $a_n$ vérifient

$$x = \sum_{n=-k}^{\infty} \frac{a_n}{2^n} \ , \ a_n \in \{0;1\} \ \forall \ n \geq -k.$$

Cette écriture est unique si l'on considère qu'un nombre ne peut pas se terminer par une infinité de 1.
Notre travail s'appuie sur un article de H. Bailey, J. Borwein, E. Crandall et C. Pomerance [1] qui démontre le résultat suivant.

**Théorème 1.2.** *Soient $x$ un nombre algébrique de degré $D > 1$, $A_D$ le coefficient de degré $D$ du polynôme minimal de $x$, et $\epsilon$ un nombre strictement positif. Posons $C := \frac{1}{(2+\epsilon)A_D}$. Alors, le nombre de 1 parmi les $N$ premiers chiffres (après la virgule) de l'écriture binaire de $x$, noté $\#(|x|, N)$, vérifie*

$$\#(|x|, N) > CN^{1/D}$$

*pour $N$ assez grand.*
Cette minoration est une avancée dans le sens de la conjecture 1.1. Cependant la démonstration donnée par les quatre mathématiciens donne un résultat ineffectif, c'est à dire qu'elle prouve que l'inégalité est vraie pour $N$ assez grand, mais elle ne permet pas de savoir à partir de quand précisement. Dans la démonstration que nous allons présenter, nous avons rendu le théorème effectif.

**Théorème 1.3.** *Soient $x$ un nombre algébrique irrationnel de degré $D > 1$, $A_D$ le coefficient de degré $D$ du polynôme minimal de $x$, et $H(x)$ la hauteur du polynôme minimal de $x$, c'est à dire plus grand de ses coefficients en valeur absolue. Posons $C := \left(\frac{7D-2}{16D^2A_D}\right)^{1/D}$. Alors,*

$$\#(|x|, N) > CN^{1/D}$$

*pour tout entier $N \geq (8H(x)D^3)^D$.*

Le théorème sous sa forme effective permet de mieux connaître certains nombres algébriques dont le polynôme minimal est connu. Prenons l'exemple de $\sqrt{2}$ dont l'irrationnalité est célèbre, et qui a pour polynôme minimal $X^2 - 2$. Dès que l'on regarde $N > 17\,000$ chiffres après la virgule dans son développement binaire, le théorème 1.3 dit que l'on a plus de $0,94\sqrt{N}$ fois le chiffre 1.

La preuve du théorème 1.2 utilise comme ingrédient essentiel un résultat célèbre sur l'approximation des nombres algébriques par des nombres rationnels : le théorème de Roth. Dans la preuve du théorème 1.3, nous avons choisi de lui substituer

1. "On the binary expansions of algebraic numbers" - Journal de Théorie des Nombres de Bordeaux 16 (2004)

le théorème de Liouville pour plusieurs raisons. Tout d'abord, la démonstration du théorème de Roth est longue et difficile, alors que la preuve du théorème de Liouville est courte et n'utilise pas de résultats plus complexes que le théorème des accroissements finis. Ensuite, l'intérêt du théorème de Liouville est qu'il donne un résultat effectif contrairement au théorème de Roth. L'utilisation du théorème de Liouville presente toutefois quelques inconvénients ; il donne par exemple une moins bonne constante $C$ dans le théorème 1.3 que dans le théorème 1.2.

Avant d'entamer la preuve du théorème 1.3, nous allons définir certaines notions de théorie additive des nombres, et démontrer quelques résultats qui nous serviront dans la preuve du théorème 1.3.

# 2 Quelques notions de théorie additive des nombres

Soit $x$ un nombre réel. Comme $x$ n'a qu'un nombre fini de chiffres à gauche de la virgule, on peut, sans pertes de généralité, supposer $x$ compris entre 1 et 2 puisque nous ne considérons dans le théorème 1.3 que les chiffres apparaissant après la virgule. Nous verrons plus tard l'intérêt d'une telle restriction.
Regardons l'écriture binaire de $x$ :

$$x = x_0.x_1x_2x_3\cdots \text{ avec } x_n \in \{0;1\}\ \forall\ n \geq 0.$$

On note

$$\mathcal{P} = \{p \mid x_p = 1\}$$

l'ensemble des positions du chiffre 1.
Pour $d \in \mathbb{N}^*$ on définit

$$r_d(x,n) = \#\left\{(p_1...p_d) \in \mathcal{P}^d \mid p_1 + p_1 + ... + p_d = n\right\}.$$

En posant $d = 1$ on a donc : $r_1(x,p) = 1 \Leftrightarrow p \in \mathcal{P}$.
On remarque alors qu'on a la relation de récurrence

$$r_d(x,n) = \sum_{i \leq n} r_{d-1}(x,i) r_1(x,n-i).$$

Une conséquence importante du choix d'un $x$ entre 1 et 2 : comme $r_1(x,0) = 1$ alors $0 \in \mathcal{P}$. Par conséquent $r_{d-1}(x,n) > 0 \Rightarrow r_d(x,n) > 0$ et surtout $r_d(x,n) = 0 \Rightarrow r_{d-1}(x,n) = 0$.
Le nombre $r_d(x,n)$ peut en fait être vu comme l'écriture du $n^{ième}$ chiffre après la virgule de $x^d$ dans une écriture particulière de $x^d$ où l'on aurait gardé les retenues succesives lors de l'élevation aux différentes puissances que l'on appellera l'écriture "brute" de $x^d$. On le comprend assez bien en faisant une récurrence.
C'est immédiat pour $d = 1$, l'écriture brute est alors identique à l'écriture binaire.
Supposons que ce soit vrai à la puissance $d-1$. Alors quand on multiplie $x^{d-1}$ par $x$ selon la méthode classique, on trouve que le $n^{ième}$ chiffre est l'addition de tous les $i^{ème}$ chiffres de l'écriture brute de $x^{d-1}$ avec les bits $n-i$ de l'écriture binaire de $x$

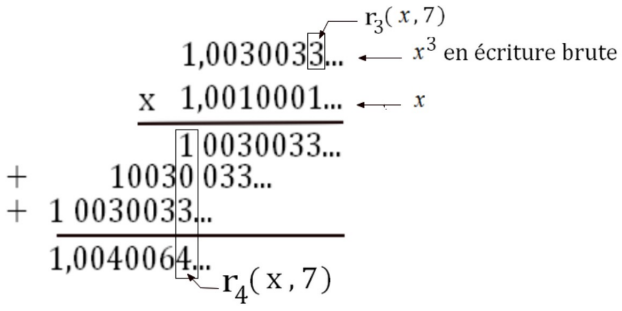


FIGURE 1 – Elevation d'un nombre binaire aux puissances succesives

c'est à dire $\sum_{i\leq n} r_{d-1}(x,i)r_1(x,n-i) = r_d(x,n)$.
Ainsi, l'écriture brute de $x^d$ permet d'obtenir l'égalité suivante :

$$x^d = \sum_{n\geq 0} \frac{r_d(x,n)}{2^n}.$$

On définit ensuite pour $R \in \mathbb{N}$ la queue du développement binaire : $T_d(x,R) = \sum_{m\geq 1} \frac{r_d(x,R+m)}{2^m}$, qui est, d'après la relation ci-dessus, $2^R$ fois une série partielle de $x^d$ écrit sous sa forme brute. C'est en fait la partie fractionnaire de $2^R x^d$ en écriture brute.
Si pour simplifier les notations on note provisoirement $a_{d,n} = r_d(x,n)$. Alors en écriture brute

$$\begin{aligned} x^d &= a_{d,0}.a_{d,1}a_{d,2}\cdots a_{d,R}a_{d,R+1}\cdots \\ T_d(x,R) &= 0.a_{d,R+1}a_{d,R+2}a_{d,R+3}\cdots \end{aligned}$$

Nous allons maintenant chercher à majorer $T_d(x,R)$ pour tout $R$ plus petit qu'un nombre $N$ donné grâce au

**Lemme 2.1.** *Soient $N$ et $d$ deux entiers et $x$ un réel dans $[1;2]$, alors pour tout entier $R$ tel que $R \leq N$, on a*

$$T_d(x,R) \leq \frac{(N+d)^d}{(d-1)!(N+1)}.$$

*Démonstration.* Tout d'abord majorons $r_d(x,n)$.

$$\begin{aligned} r_d(x,n) &= \sum_{i\leq n} r_{d-1}(x,i)r_1(x,n-i) \\ &\leq \#\{(i_1...i_d)|\sum i_j = n\} && \text{cas où l'écriture binaire n'a que des 1 jusqu'à N,} \\ &\leq \binom{n+d-1}{d-1} && \text{loi de combinaisons avec répétitions.} \end{aligned}$$

On en déduit

$$T_d(x,R) \leq \sum_{m\geq 1} 2^{-m}\binom{R+m+d-1}{d-1}.$$

Or $U_d(R) = \sum_{m\geq 1} 2^{-m}\binom{R+m+d-1}{d-1}$ vérifie la relation de récurrence :

$$U_d(R) = 2U_{d-1} + \binom{R+d-1}{d-1}.$$

En effet, en se rappelant que les coefficents binômiaux vérifient

$$\binom{n}{p} = \binom{n-1}{p-1} + \binom{n-1}{p},$$

on a

$$\begin{aligned}
U_d(R) &= \sum_{m\geq 1} 2^{-m}\binom{R+m+d-1}{d-1} \\
&= \sum_{m\geq 1} 2^{-m}\binom{R+m+d-2}{d-2} + \sum_{m\geq 1} 2^{-m}\binom{R+m+d-2}{d-1} \\
&= U_{d-1}(R) + \sum_{m\geq 2} 2^{-m}\binom{R+m+d-1}{d-1} + \frac{1}{2}\binom{R+d-1}{d-1} \\
&= U_{d-1}(R) + \frac{1}{2}\binom{R+d-1}{d-1} + \frac{1}{2}U_d(R),
\end{aligned}$$

et par conséquent

$$U_d(R) = 2U_{d-1} + \binom{R+d-1}{d-1}.$$

On en déduit la forme générale :

$$U_d(R) = \sum_{j=0}^{d-1}\binom{R+d}{j}.$$

On peut prouver cela par récurrence.
Pour d=1, ceci est trivial. Supposons que ce soit vrai au rang d-1, alors :

$$\begin{aligned}
U_d(R) &= 2U_{d-1}(R) + \binom{R+d-1}{d-1} \\
&= 2\sum_{j=0}^{d-2}\binom{R+d-1}{j} + \binom{R+d-1}{d-1} \\
&= \binom{R+d-1}{0} + \sum_{j=0}^{d-2}\left(\binom{R+d-1}{j} + \binom{R+d-1}{j+1}\right) \\
&= \sum_{j=0}^{d-1}\binom{R+d}{j}.
\end{aligned}$$

Et finalement

$$T_d(x,R) \leq U_d(R) \leq \frac{(R+d)^{d-1}}{(d-1)!}\sum_{n\geq 0}(\frac{d-1}{R+d})^n = \frac{(R+d)^d}{(d-1)!(R+1)} \leq \frac{(N+d)^d}{(d-1)!(N+1)}.$$

□

Dans la suite log désignera le logarithme de base 2.

**Lemme 2.2.** *On garde $N$ et $d$ deux entiers et $x$ un réel dans $[1;2]$. On se donne $D$ un entier et on suppose $d \leq D$. On pose alors $K = D\log N$. Alors pour $N$ assez grand*

$$\sum_{1\leq R\leq N-K} T_d(x,R) \leq \#(x,N)^d + 2$$

*Démonstration.*

$$\begin{aligned}
\sum_{1\leq R\leq N-K} T_d(x,R) &= \sum_{m\geq 1} 2^{-m} \sum_{R\leq N-K} r_d(x,R+m) \\
&\leq \sum_{m=1}^{K}\sum_{R\leq N}\frac{r_d(x,R)}{2^m} + 2^{-K}\sum_{m>K}2^{K-m}\sum_{R\leq N-K} r_d(x,R+m) \\
&\leq \sum_{R\leq N} r_d(x,R) + 2^{-K}\sum_{K\leq R\leq N} T_d(x,R) \\
&\leq \#(x,N)^d + N^{-D}\frac{(N-d\log N)(N+d)^d}{(d-1)!(N+1)} \qquad \text{d'après le lemme 2.1.}
\end{aligned}$$

On cherche donc $N$ tel que

$$N^{-D}\frac{(N-d\log N)(N+d)^d}{(d-1)!(N+1)} < 2.$$

Il suffit alors d'avoir $\left(\frac{N+D}{N}\right)^D \leq 2 \Leftrightarrow 1+\frac{D}{N} \leq 2^{1/D}$.
Il suffit donc d'avoir

$$N \geq \frac{D}{2^{1/D}-1}.$$

Or $(8H(x)D^3)^D > \frac{D}{2^{1/D}-1}\ \forall D > 1$, on a donc bien $N \geq \frac{D}{2^{1/D}-1}$ et par conséquent

$$\sum_{1\leq R\leq N-K} T_d(x,R) \leq \#(x,N)^d + 2.$$

□

Avant d'entamer la preuve du théorème principale, il nous faut rappeler l'inégalité de Liouville qui est un des premiers résultats de transcendance. L'inégalité de Liouville permet par exemple de prouver directement la transcendence du nombre $\sum_{n\geq 0}\frac{1}{2^{n!}}$. Ici, elle va nous permettre de prouver la transcendence de nombres avec une beaucoup plus grande fréquence du chiffre 1.

# 3 Inégalité de Liouville

Dans cette partie, nous allons démontrer l'inégalité de Liouville.

**Théorème 3.1.** (Liouville) *Soit $x$ un nombre irrationnel algébrique alors pour tout couple d'entiers $(p, q)$*

$$\left|x - \frac{p}{q}\right| \geq \frac{L_x}{q^D}$$

*où $D$ est le degré de $x$ et $L_x$ est une constante qui ne dépend que de $x$.*

*Démonstration.* Nous avons choisit de présenter cette démonstration en quatre étapes. On trouve ces quatre étapes dans la plupart des preuves de transcendance (c'est notament le cas de la preuve du théorème de Roth, même si chaque étape est bien plus fastidieuse).

## 3.1 Fonction auxiliaire

Soit $x$ un nombre algébrique de degré $D > 1$. On introduit comme fonction auxiliaire, le polynôme minimal de $x$ noté $P$ de degré $D$.
On pose $L_x = \left(sup_{t\in\{x-1;x+1\}}|P'(t)|\right)^{-1}$ qui est bien définit car $P$ est non constant, donc de dérivée non identiquement nulle. Supposons que l'on ait deux entiers $p$ et $q$ tels que

$$\left|x - \frac{p}{q}\right| < \frac{L_x}{q^D}.$$

## 3.2 Majoration

D'après le théorème des accroissements finis il existe $t_0$ entre $x$ et $\frac{p}{q}$ tel que

$$\left|P(x) - P\left(\frac{p}{q}\right)\right| = P'(t_0)\left|x - \frac{p}{q}\right|.$$

D'après l'hypothèse sur $p$ et $q$ on a forcément $|x - \frac{p}{q}| < 1$, et donc on a $t_0 \in \{x-1; x+1\}$. On en déduit la majoration

$$\left|P(x) - P\left(\frac{p}{q}\right)\right| \leq \frac{1}{L_x}\left|x - \frac{p}{q}\right|,$$

et comme $x$ est racine de $P$, $P(x) = 0$ donc

$$L_x\left|P\left(\frac{p}{q}\right)\right| \leq \left|x - \frac{p}{q}\right|.$$

### 3.3 Non-nullité

La troisième étape consiste a prouver que $\left|P\left(\frac{p}{q}\right)\right|$ est non nul.
Nous allons d'abord prouver que $\frac{p}{q}$ n'est pas racine de $P$. Supposons qu'il le soit, alors, on peut écrire $P$ sous la forme

$$P(X) = \left(X - \frac{p}{q}\right) Q(X)$$

où $Q$ est de degré $D-1$. Le polynôme $R = q^D Q$ serait donc un annulateur non nul de $x$, à coefficients entiers, et de degré $D-1$, ce qui contredit le fait que $P$ est le polynôme minimal de $x$. Donc $\left|P\left(\frac{p}{q}\right)\right| \neq 0$.

### 3.4 Minoration

On minore maintenant $\left|P\left(\frac{p}{q}\right)\right|$ et on va voir que l'on arrive à une contradiction.
Après réduction au même dénominateur $\left|P\left(\frac{p}{q}\right)\right|$ peut s'écrire sous la forme $\frac{A}{q^D}$, $A \in \mathbb{N}^*$. Comme $A$ est non nul, il est supérieur ou égal à 1, et on obtient

$$\left|P\left(\frac{p}{q}\right)\right| \geq \frac{1}{q^D}.$$

Par conséquent on a

$$\left|x - \frac{p}{q}\right| \geq \frac{L_x}{q^D}.$$

On aboutit à une contradiction, ce qui prouve le théorème. □

Passons maintenant à la preuve du théorème principal.

## 4 Démonstration du théorème principal

Là encore nous allons suivre les quatre étapes d'une preuve de transcendance.

### 4.1 Fonction auxiliaire

Soit $x$ un nombre algébrique irrationnel de degré $D > 1$. Pour les mêmes raisons que précedement, on va supposer sans perte de généralités qu'on a $1 < x < 2$. Raisonnons par l'absurde et supposons que $\#(x, N) \leq CN^{1/D}$ pour $N \geq (8D^3H(x))^D$. Soit $P(X) = A_D X^D + A_{D-1}X^{D-1} + ... + A_1 X + A_0$ le polynôme minimal. Quitte à remplacer $P$ par $-P$, on supposera $A_D > 0$. Soit $R \in \mathbb{N}$ , on peut écrire

$$-2^R A_0 = 2^R \sum_{d=1}^{D} A_d x^d.$$

En notant $\sum_{d=1}^{D} A_d \sum_{m\geq 0}^{R} \frac{r_d(x,m)}{2^{m-R}} =: J(x,R)$, on voit que l'on a $J(x,R) \in \mathbb{Z}$ et on obtient l'égalité

$$\begin{aligned} -2^R A_0 &= J(x,R) + \sum_{d=1}^{D} A_d \sum_{m\geq 1} \frac{r_d(x,R+m)}{2^m} \\ &= J(x,R) + \sum_{d=1}^{D} A_d T_d(x,R). \end{aligned}$$

On définit $T(x,R) := \sum_{d=1}^{D} A_d T_d(x,R)$, alors $-2^R A_0 = J(x,R) + T(x,R)$ et finalement

$$T(x,R) = -2^R A_0 - J(x,R)$$

donc $T(x,R) \in \mathbb{Z}$.

## 4.2 Majoration

On va, dans cette partie, majorer la somme $S = \sum_{R\leq N-K} |T(x,R)|$ où $K = D\log N$.

On rappelle que par définition $T(x,R) = \sum_{d=1}^{D} A_d T_d(x,R)$. Ainsi

$$\begin{aligned} \sum_{R\leq N-K} |T(x,R)| &= \sum_{R\leq N-K} \sum_{d=1}^{D} A_d T_d(x,R) \\ &= \sum_{d=1}^{D} A_d \sum_{R\leq N-K} T_d(x,R). \end{aligned}$$

Or d'après le lemme 2.2

$$\sum_{R\leq N-K} T_d(x,R) \leq \#(x,N)^d + 2.$$

On a donc

$$\begin{aligned} \sum_{R\leq N-K} |T(x,R)| &\leq \sum_{d=1}^{D} A_d(\#(x,N)^d + 2) \\ &\leq \sum_{d=1}^{D} A_d(C^d N^{d/D} + 2) \\ &\leq A_D C^D N + 2A_D + \sum_{d=1}^{D-1} |A_d|(C^d N^{\frac{d}{D}} + 2). \end{aligned}$$

Essayons d'absorber les termes en $N^{d/D},\ d \leq D-1$ dans le terme en $N$.
Pour cela cherchons $N$ tel que

$$2A_D + \sum_{d=1}^{D-1} |A_d|(C^d N^{d/D} + 2) \leq \frac{N}{8D^2}.$$

Alors en se rappelant que $H(x) := max(|A_d|)$, et comme $C \leq 1$, il suffit d'avoir

$$\begin{aligned} N &\geq 8D^2 \left(2H(x) + 2(D-1)H(x) + (D-1)H(x)N^{1-1/D}\right) \\ N^{1/D} &\geq 8D^2 \left(\frac{(D+1)H(x)}{N^{1-1/D}} + (D-1)H(x)\right). \end{aligned}$$

Si l'on choisit $N \geq ((D+1)H(x))^{D/D-1}$, on a $\frac{(D+1)H(x)}{N^{1-1/D}} \leq 1$ et il suffit de prendre

$$N^{1/D} \geq 8D^2(1 + (D-1)H(x)).$$

Comme $N \geq (8D^3H(x))^D$ on a notre majoration :

$$S = \sum_{R \leq N-K} |T(x,R)| \leq (A_D C^D + \frac{1}{8D^2})N.$$

## 4.3 Non-nullité

Comme souvent dans les preuves de transcendance, c'est cette partie de la preuve qui va nous demander le plus de travail. Nous allons compter le nombre de $T(x,R) > 0$ pour $R < N - DlogN$.
Nous aurons tout d'abord besoin du

**Lemme 4.1.** *Soient $R_1 > R_0$ deux entiers positifs tels que $T(x,R_1) > 0$ et $\forall R \in [R_0; R_1]$ $r_{D-1}(x,R) = 0$, alors $T(x,R) > 0\ \forall R \in [R_0; R_1]$*

*Démonstration.* Soit $R \in [R_0; R_1]$,

$$\begin{aligned} T(x,R-1) &= \frac{1}{2}T(x,R) + \sum_{d=1}^{D} A_d r_d(x,R) \\ &= \frac{1}{2}T(x,R) + A_D r_D(x,R) \end{aligned}$$

car $r_d(x,R) = 0\ \ \forall d < D$. On comprend ici toute l'importance du choix de $x$ entre 1 et 2 : comme $r_{D-1}(x,R) = 0$, $r_d(x,R) = 0\ \ \forall d \leq D-1$.
Donc $T(x,R-1) > 0$ si $T(x,R) > 0$, et par induction, comme $T(x,R_1) > 0$, alors $T(x,R) > 0\ \ \forall R \in [R_0; R_1]$. □

D'après notre hypothèse initiale : $\#(x,N) \leq CN^{1/D}$. Le nombre d'entiers $R \leq N$ tels que $r_{D-1}(x,R) > 0$ est donc $Q \leq C^{D-1}N^{1-1/D}$.

En effet si $r_{D-1}(R) > 0$, alors $r_{D-1}(R) \geq 1$ et donc on a

$$\begin{aligned} Q = \#\{R \leq N \mid r_{D-1}(R) > 0\} &\leq \sum_{k=1}^{N} r_{D-1}(x,k) \\ &\leq \#(x,N)^{D-1} \qquad \text{d'après la formule de récurrence} \\ &\leq C^{D-1} N^{1-1/D}. \end{aligned}$$

On notera $0 = R_1 < R_2 < ... < R_Q < R_{Q+1} := N$.
On se donne $\epsilon > 0$, soit $I := \{i \leq Q | R_{i+1} - R_i \geq \epsilon C^{1-D} N^{1/D}\}$. Alors on a

$$\begin{aligned} \sum_{i \in I} R_{i+1} - R_i &\geq \sum_{m \leq Q} (R_{m+1} - R_m) - \epsilon C^{1-D} N^{1/D} Q \\ &\geq N - \epsilon C^{1-D} N^{1/D} C^{D-1} N^{1-1/D} \\ &\geq (1-\epsilon) N. \end{aligned}$$

Nous allons minorer le nombre $m$ de $R \leq N - DlogN$ tels que $T(x,R) > 0$.
Soit i fixé, supposons que l'on ait $R' \in ]R_i; R_{i+1} - DlogN]$ tel que $r_D(x,R') > 0$. On doit s'assurer tout d'abord que $]R_i; R_{i+1} - DlogN]$ définit bien un intervalle non vide, c'est à dire on doit avoir $R_i < R_{i+1} - DlogN$. Il nous faut

$$\epsilon C^{1-D} N^{1/D} > D \log N.$$

Alors, en se rappelant que $C \leq \left(\frac{7D-2}{16D^2 A_D}\right)^{1/D}$ on a

$$N^{1/D} > \frac{D \log N}{\epsilon} \left(\frac{7D-2}{16D^2 A_D}\right)^{1-1/D}.$$

Comme $A_D > 0$ on peut simplifier l'inégalité : il suffit d'avoir

$$N^{1/D} > \frac{D^{1/D}}{\epsilon (4A_D)^{1-1/D}}.$$

On trouve donc qu'il suffit de prendre $N > \frac{D^2}{\epsilon^D 4^{D-1}}$ pour obtenir $R_i > R_{i+1} - D \log N$.
Dans la suite on choisira arbitrairement $\epsilon = \frac{1}{16}$, il suffira alors que l'on ait

$$N > D^2 4^{D+1},$$

ce qui est le cas d'après notre hypothèse sur $N$.

On va montrer que pour tout $R$ entre $R_i$ et $R'$, $T(x,R) > 0$. La première étape sera de montrer que $T(x, R'-1) > 0$.

$$\begin{aligned} T(x,R'-1) &= A_D T_D(x,R'-1) + \sum_{d=1}^{D-1} A_d T_d(x,R'-1) \\ &= A_D \sum_{m \geq 1} \frac{r_D(x,R'-1+m)}{2^m} + \sum_{d=1}^{D-1} A_d \sum_{m \geq 1} \frac{r_d(x,R'-1+m)}{2^m} \\ &\geq \frac{1}{2} A_D - \sum_{d=1}^{D-1} |A_d| \sum_{m \geq 1} \frac{r_d(x,R'-1+m)}{2^m} \end{aligned}$$

car $r_d(x,R')>0$, donc $\sum_{m\geq 1}\frac{r_D(x,R'-1+m)}{2^m}\geq\frac{1}{2}$.
Or pour $d\leq D-1$ et $m\leq R_{i+1}-R'$, $r_d(x,R'-1+m)=0$. Donc

$$\begin{aligned}
T(x,R'-1) &\geq \frac{1}{2}A_D-\sum_{d=1}^{D-1}|A_d|\sum_{m\geq R_{i+1}-R'}\frac{r_d(x,R'-1+m)}{2^m}\\
&\geq \frac{1}{2}A_D-\sum_{d=1}^{D-1}|A_d|\sum_{m\geq 1}\frac{r_d(x,R_{i+1}+m)}{2^{R_{i+1}-R'+m}}\\
&\geq \frac{1}{2}A_D-2^{R'-R_{i+1}}\sum_{d=1}^{D-1}|A_d|T_d(x,R_{i+1})\\
&\geq \frac{1}{2}A_D-N^{-D}\sum_{d=1}^{D-1}|A_d|\frac{(N+d)^d}{(d-1)!(N+1)} \qquad \text{d'après le lemme 2.1.}
\end{aligned}$$

On va chercher à partir de quand on aura :

$$N^{-D}\sum_{d=1}^{D-1}|A_d|\frac{(N+d)^d}{(d-1)!(N+1)}<\frac{1}{2}A_D.$$

Il nous suffit de prendre $N$ tel que :

$$N^{-D}(D-1)H(x)\frac{(N+D-1)^{D-1}}{N}<\frac{1}{2}$$

car $A_D\geq 1$, donc

$$N^{D+1}>2(D-1)H(x)(N+D-1)^{D-1}.$$

Dès que $N\geq D$, $(N+D-1)^{D-1}\leq(2N)^D$.
Alors comme $N\geq(8D^3H(x))^D$ on obtient $T(x,R'-1)>0$. On utilise maintenant le lemme 4.1, en posant $R_0=R_i$ et $R_1=R'-1$. Alors pour tout $R$ entre $R_i$ et $R'-1$, $T(x,R)>0$.

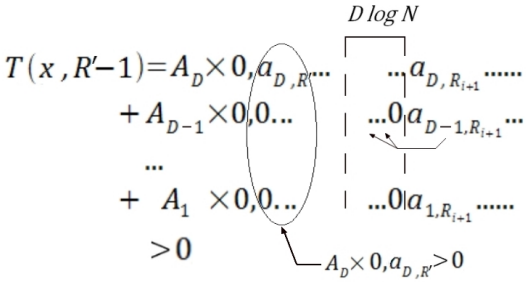


FIGURE 2 – Schéma expliquant pourquoi $T(x,R'-1)>0$

On doit maintenant s'assurer que l'on peut bien trouver un tel $R'$. Ici c'est l'inégalité de Liouville qui va nous apporter la solution. Pour tout $i$ on a :

$$\left|x-\sum_{p\in\mathcal{P},p\leq p_i}\frac{1}{2^p}\right|\leq\frac{2}{2^{p_{i+1}}}.$$

Or, $\sum_{p\in\mathcal{P},p\leq p_i}\frac{1}{2^p}=\frac{a}{2^{p_i}}$ après réduction au même dénominateur, avec $a$ entier.
Or d'après le théorème de Liouville :

$$\left|x-\frac{a}{2^{p_i}}\right|\geq\frac{L_x}{2^{Dp_i}}.$$

On a donc

$$\begin{aligned}\frac{L_x}{2^{Dp_i}} &\leq \frac{2}{2^{p_{i+1}}}\\ L_x 2^{p_{i+1}} &\leq 2^{Dp_i+1}\\ \log L_x + p_{i+1} &\leq Dp_i+1\\ p_{i+1} &\leq Dp_i+1-\log L_x\end{aligned}$$

Donc tout intervalle de la forme $\left[\frac{k+\log L_x-1}{D};k\right]$ contient un $j_i\in\mathcal{P}$ c'est à dire tel que $r_1(x,j_i)>0$.
On trouve donc qu'il existe un $j_i$ dans $\left[\frac{R_{i+1}-R_i-D\log N-1+\log L_x}{D};R_{i+1}-R_i-D\log N\right]$ tel que $r_1(x,j_i)>0$. Comme $r_{D-1}(x,R_i)>0$ on déduit de la formule de récurrence que

$$r_D(x,R_i+j_i)>0.$$

Il s'en suit que pour tout $R\in[R_i;R_i+i_j]$, $T(x,R)>0$. Le nombre de $R<N-D\log N$ tels que $T(x,R)>0$ est donc au moins

$$\begin{aligned}m &\geq \sum_{i\in I} j_i\\ &\geq \sum_{i\in I}\frac{R_{i+1}-R_i-D\log N-1+\log L_x}{D}\\ &\geq \sum_{i\in I}\frac{R_{i+1}-R_i}{D}-\sum_{i\in I}\frac{D\log N+1-\log L_x}{D}\\ &\geq \frac{1-\frac{1}{16}}{D}N-\frac{C^{D-1}N^{1-1/D}D\log N+1-\log L_x}{D}.\end{aligned}$$

Essayons d'absorber le second terme dans le terme en $N$. Pour cela cherchons à partir de quel $N$ on a :

$$\frac{C^{D-1}N^{1-1/D}(D\log N+1-\log L_x)}{D}\leq\frac{1}{2D}N.$$

Comme $C<1$, il suffit d'avoir

$$D\log N+1+\log L_x^{-1}\leq\frac{N^{1/D}}{2}.$$

Occupons nous du $\log L_x$. (On rappelle que $L_x=\left(sup_{t\in\{x-1;x+1\}}|P'(t)|\right)^{-1}$.) La dérivée de $P$ le polynôme minimal est $P'(X)=DA_DX^{D-1}+(D-1)A_{D-1}X^{D-2}+...+A_1$ et comme $x\in[1;2]$ on évalue $P'(X)$ entre 0 et 3. On a donc

$$L_x^{-1}\leq\sum_{d=1}^{D}d|A_d|3^{d-1}\leq DH(x)\sum_{d=0}^{D-1}3^d\leq\frac{3^DDH(x)}{2}.$$

Et après passage au log il suffit d'avoir $N$ tel que

$$D\log N + \log\left(3^D DH(x)\right) \leq \frac{N^{1/D}}{2}.$$

Comme $N \geq (8D^3H(x))^D$ on a bien l'inégalité $\frac{C^{D-1}N^{1-1/D}(D\log N+1-\log L_x)}{D} \leq \frac{1}{2D}N$, et on peut donc conclure :

$$m \geq \frac{1-\frac{1}{16}}{D}N - \frac{N}{2D} = \frac{7}{16D}N.$$

### 4.4 Minoration

On a minoré le nombre $m$ de $R < N - D\log N$ tels que $T(x,R) > 0$. Or $T(x,R) \in \mathbb{Z}$, donc $T(x,R) > 0 \Rightarrow T(x,R) \geq 1$. On a donc au final :

$$S = \sum_{R \leq N - D\log N} |T(x,R)| \geq \frac{7}{16D}N.$$

Alors pour $N \geq (8D^3H(x))^D$ on a

$$(A_D C^D + \frac{1}{8D^2})N \geq S \geq \frac{1}{16D}N,$$

et comme

$$C \leq \left(\frac{7D-2}{16D^2A_D}\right)^{1/D}$$

on arrive à une contradiction, ce qui termine la preuve du théorème. □

On a choisit de fixer arbitrairement $\epsilon$ dans cette preuve. On aurait pu le faire tendre vers 0 quand $N$ tend vers $+\infty$, en prenant $\epsilon = \frac{1}{\log\log N}$ par exemple, toutefois le gain aurait été très minime. En réalité, il est possible d'obtenir une meilleure constante $C$ et une inégalité valable pour un $N$ plus petit, en reprenant plus finement les calculs. Ici nous avons choisit de perdre en précision pour gagner en clarté et pour ne pas trop alourdir les calculs.

## 5 Conséquences

Ce théorème, en plus d'être une avancée dans le sens de la conjecture 1.1, permet de prouver la transcendence de nouvelles catégories de nombres irrationnels.

**Corollaire 5.1.** *Soit $x$ un nombre irrationnel tel que $x = \sum_{n\geq 0} \frac{1}{2^{f(n)}}$, avec $f$ une fonction croissante à valeurs entières pour des arguments entiers. Si l'inverse de $f$ satisfait $\forall \epsilon > 0$*

$$f^{-1}(y) = \mathcal{O}(y^\epsilon)$$

*alors $x$ est transcendant.*

*Démonstration.* Prenons $x = \sum_{n\geq 0} \frac{1}{2^{f(n)}}$ que l'on supposera algébrique de degré D $>$ 1, avec $f$ vérifiant les conditions du corollaire. Alors $N = f(n)$ est la position du n-ième 1 dans l'écriture binaire de $x$, par construction. On a donc

$$\#(x, N) = \lfloor f^{-1}(N) \rfloor.$$

Or, par hypothèse, on a $\forall\ \epsilon > 0$

$$f^{-1}(y) = \mathcal{O}(y^{\epsilon}).$$

Donc

$$\#(x, N) = \mathcal{O}(N^{\epsilon}) \quad \forall \epsilon > 0$$

ce qui est incompatible avec le fait que $\#(x, N) \geq CN^{1/D}$. On en déduit la transcendance de $x$. □

On prouve notament la transcendance des nombres $m_\alpha = \sum_{n\geq 0} \frac{1}{2^{\lfloor \alpha^n \rfloor}}$, avec $\alpha > 1$. En effet si on pose $f(n) = \lfloor \alpha^n \rfloor = N$ on a $N \leq \alpha^n \leq N+1$ d'où $\frac{lg\ N}{lg\ \alpha} \leq n \leq \frac{lg\ (N+1)}{lg\ \alpha}$ et donc on a

$$n = f^{-1}(N) = \lceil \frac{lg\ N}{lg\ \alpha} \rceil = \mathcal{O}(N^{\epsilon}).$$

En réalité, une preuve de la transcendance de $m_\alpha$, pour $\alpha > 1$, avait déjà été donnée, mais elle utilisait le théorème de Ridout, qui est un théorème plus difficile que le théorème de Roth. Ici, nous nous sommes finalement contenté d'utiliser le théorème de Liouville et quelques arguments de combinatoire assez simples pour la redémontrer.
On prouve aussi, pour la première fois, la transcendance du nombre $\sum_{n\geq 0} \frac{1}{2^{\lfloor n^{\log\log n} \rfloor}}$, avec le même raisonnement. En réalité, le théorème 1.3 permet de prouver la transcendance de tout nombre pour lequel $f$ croît plus vite que n'importe quelle puissance de $n$.

Le théorème peut aussi nous aider à minorer le degré de certains nombres irrationnels.

**Corollaire 5.2.** *Si $x = \sum_{n\geq 0} \frac{1}{2^{n^k}}$, alors le degré de $x$ est supérieur à $k$ (en prenant pour convention que le degré d'un nombre transcendant est $+\infty$).*

*Démonstration.* On a ici, avec les notations du corolaire 5.1, $f(n) = n^k$. Il en découle que $\#(x, N) = \lfloor f^{-1}(N) \rfloor = N^{1/k}$. On en déduit que le degré de $x$ ne peut pas être inférieur à $k$. □