République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université A.MIRA-BEJAIA

Faculté des Sciences Exactes
Département de Mathématiques
Laboratoire de Mathématiques Appliquées (LMA)

THÈSE

EN VUE DE L'OBTENTION DU DIPLOME DE DOCTORAT

Domaine : Mathématiques et Informatique **Filière : Mathématiques**
Spécialité : Analyse

Présentée par
M. BOUSLA Sid Ali

Thème

Estimations du plus petit commun multiple de certaines suites d'entiers

Soutenue le : 02/12/2020 **Devant le Jury composé de :**

Nom et Prénom	Grade		
Mme TAS Saâdia	Professeur	Univ. de Bejaia	Présidente
Mr FARHI Bakir	M.C.A	Univ. de Bejaia	Rapporteur
Mme MOHDEB Nadia	M.C.A	Univ. de Bejaia	Examinatrice
Mr MOUSSAOUI Abdelkrim	Professeur	Univ. de Bejaia	Examinateur
Mr DAHMANI Abdelnasser	Professeur	C. Univ. de Tamanrasset	Examinateur
Mr HERNANE Mohand Ouamar	Professeur	U.S.T.H.B	Examinateur

Année Universitaire : **2019/2020**

Remerciements

Je tiens à remercier vivement mon directeur de thèse, le professeur FARHI Bakir, de m'avoir introduit à la recherche et patiemment aidé tout au long de ce travail. Je lui suis profondément reconnaissant de m'avoir fait bénéficier de sa grande compétence, de son entière disponibilité, de son orientation depuis ma L2, de sa rigueur dans la rédaction des articles scientifiques et de ses conseils que je n'oublierai jamais. Il a été d'un soutien et d'une attention exceptionnels. Enfin, ses nombreuses relectures et corrections de mes travaux de thèse ont été très appréciables. Cette thèse lui doit beaucoup. Pour tout cela merci.

Je témoigne toute ma gratitude à tous ceux qui ont contribué à ma formation et je tiens à remercier tous les enseignants du département de mathématiques.

Je suis très honoré de la présence à mon jury de thèse et je tiens à remercier :

Madame TAS Saâdia pour m'avoir fait l'honneur de présider le jury de cette thèse.

Madame MOHDEB Nadia et Monsieur MOUSSAOUI Abdelkrim pour l'honneur qu'ils m'ont fait en acceptant d'être membres de mon jury de thèse.

Monsieur DAHMANI Abdelnasser pour l'honneur qu'il m'a fait par sa présence dans mon jury de soutenance en qualité d'examinateur de mon travail.

Monsieur HERNANE Mohand Ouamar pour l'honneur qu'il m'a fait pour avoir accepté d'examiner ce travail.

Finalement je remercie ma famille et tous mes amis pour leurs encouragements et leur soutien qui m'ont été bien utiles durant ma thèse.

BOUSLA Sid Ali

Dédicaces

Je dédie cette thèse à mes parents, à toute ma famille et mes amis et à tous ceux qui auront la patience de la lire.

BOUSLA Sid Ali

Table des matières

Principales notations et conventions

On écrit $f = O(g)$ ou d'une façon équivalente $f \ll g$, s'il existe une constante $C > 0$ telle que $|f(x)| \leq Cg(x)$, pour tout x dans un voisinage d'une certaine valeur (éventuellement infinie). La première notation est due à Landau et la seconde est due à Vinogradov. Si le rapport $f(x)/g(x)$ tend vers 1 quand x tend vers $a \in \overline{\mathbb{R}}$, on écrit $f(x) \sim_a g(x)$ et on dit que f et g sont équivalentes au voisinage de a ; de même on écrit $f = o(g)$ si le rapport $f(x)/g(x)$ tend vers zéro. Pour $t \in \mathbb{R}$, on désigne respectivement par $\lfloor t \rfloor$ et $\lceil t \rceil$ la partie entière par défaut et la partie entière par excès du nombre t. L'ensemble des nombres premiers est noté P, et dans toute la suite la lettre p avec ou sans indice désigne un élément de P. Pour deux nombres réels a et b, on note $a \mid b$ pour signifier que a divise b (i.e., le rapport b/a est un entier). On désigne par π la fonction de comptage des nombres premiers ; soit :

$$\pi(x) := \sum_{p \leq x} 1 \qquad (\forall x \in \mathbb{R}^+).$$

Les fonctions ψ et θ de Chebyshev sont définies comme suit :

$$\psi(x) := \log \operatorname{ppcm}(1, 2, \ldots, \lfloor x \rfloor) \qquad (\forall x \geq 1),$$
$$\theta(x) := \sum_{p \leq x} \log p \qquad (\forall x \in \mathbb{R}^+).$$

Les fonctions généralisées de Chebyshev sont données par :

$$\begin{aligned}\pi(x;m,k) &:= \sum_{\substack{p\leq x\\ p\equiv m \pmod k}} 1\\ \theta(x;m,k) &:= \sum_{\substack{p\leq x\\ p\equiv m \pmod k}} \log p\end{aligned} \qquad (\forall x\in\mathbb{R}^+,\ \forall m,k\in\mathbb{N}^*).$$

On désigne par φ la fonction indicatrice d'Euler qui à $n\in\mathbb{N}^*$, associe le nombre d'entiers compris entre 1 et n et premiers avec n. La fonction μ de Möbius est définie par :

$$\mu(n) := \begin{cases}(-1)^{\omega(n)} & \text{si n est sans facteur carré} > 1,\\ 0 & \text{dans le cas contraire.}\end{cases} \qquad (\forall n\in\mathbb{N}^*),$$

où $\omega(n)$ désigne le nombre de facteurs premiers distincts de n. Pour un nombre premier p donné, on désigne par ϑ_p la valuation p-adique usuelle (i.e., pour tout $n\in\mathbb{N}^*$, $\vartheta_p(n)$ est le plus grand exposant $\alpha\in\mathbb{N}$ tel que p^α divise n). Le plus petit commun multiple des entiers $a_1, a_2, \ldots, a_n$ est noté $\mathrm{ppcm}(a_1, a_2, \ldots, a_n)$ ou bien $\mathrm{ppcm}\{a_1, a_2, \ldots, a_n\}$; leurs plus grand commun diviseur est noté $\mathrm{pgcd}(a_1, a_2, \ldots, a_n)$ ou bien $\mathrm{pgcd}\{a_1, a_2, \ldots, a_n\}$. Le cardinal d'un ensemble fini $\mathcal{A}$ est noté $\#\mathcal{A}$. On désigne par $\left(\frac{\cdot}{\cdot}\right)$ le symbole de Legendre. Nous utilisons souvent l'abréviation ppcm pour alléger l'expression « plus petit commun multiple ». Certaines de ces notations sont rappelées localement.

Introduction générale

Avoir une bonne estimation du plus petit commun multiple de termes consécutifs d'une suite d'entiers est un problème difficile et important. Pour la suite usuelle de tous les entiers naturels, la fonction ψ est cruciale à la fois pour l'encadrement de Chebyshev (1852) de la fonction π et pour le théorème des nombres premiers d'Hadamard-de la Vallée Poussin (1896) selon lequel on a :

$$\pi(x) \sim_{+\infty} \frac{x}{\log x}.$$

Ce théorème possède plusieurs autres énoncés équivalents, l'un de ces énoncés est celui de Chebyshev (1852), qui est donné par :

$$\log \operatorname{ppcm}(1, 2, \ldots, n) \sim_{+\infty} n.$$

Ce qui équivaut à dire que pour tout $\varepsilon > 0$, il existe $N = N_\varepsilon \in \mathbb{N}$, tel que l'on ait :

$$(e - \varepsilon)^n \leq \operatorname{ppcm}(1, 2, \ldots, n) \leq (e + \varepsilon)^n \qquad (\forall n \geq N).$$

Par ailleurs, les résultats les plus significatifs concernant l'estimation effective des nombres $\operatorname{ppcm}(1, 2, \ldots, n)$ $(n \in \mathbb{N}^*)$, sont dus à Chebyshev (1850), Hanson (1972) et Nair (1982). Dans [12], Chebyshev exploite l'idée d'estimer le nombre $\log(n!)$ de deux façons différentes : l'une est analytique et se sert de la formule de Stirling et l'autre est arithmétique et se sert de la formule de Legendre :

$$n! = \prod_{p \text{ premier}} p^{\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots} \qquad (\forall n \in \mathbb{N}^*).$$

Cette idée l'avait conduit à l'estimation :

$$e^{-1} \cdot n^{-\frac{5}{2}} (c_1)^n \leq \operatorname{ppcm}(1, 2, \ldots, n) \leq e \cdot n^{\frac{5}{4}} e^{\frac{5}{4 \log 6} \log^2 n} (c_2)^n \qquad (\forall n \in \mathbb{N}^*),$$

avec $c_1 \simeq 2,51$ et $c_2 \simeq 3,02$. En utilisant le développement du nombre 1 en série de Sylvester, Hanson [23] a montré que $\text{ppcm}(1,2,\ldots,n) \leq 3^n$, pour tout entier $n \geq 1$; quant à Nair [39], il exploite l'intégrale $\int_0^1 x^{m-1}\,(1-x)^{n-m}\,\mathrm{d}x$ $(1 \leq m \leq n)$ pour montrer que $\text{ppcm}(1,2,\ldots,n) \geq 2^n$, pour tout entier $n \geq 7$. Bien que la minoration de Nair est plus faible que celle de Chebyshev, sa méthode d'obtention est plus brève et permet en outre d'envisager le problème différemment.

Dans le but de donner un analogue à la version explicite du théorème des nombres premiers, plusieurs auteurs se sont intéressés à l'estimation effective du ppcm de certaines suites d'entiers, comme les suites arithmétiques, les suites polynomiales et les suites à forte divisibilité. On rappelle qu'une suite d'entiers strictement positifs $\boldsymbol{a} = (a_n)_{n\geq 1}$ est dite *à divisibilité* lorsqu'elle vérifie la propriété :

$$n \mid m \Rightarrow a_n \mid a_m \qquad (\forall n, m \in \mathbb{N}^*).$$

Elle est dite *à forte divisibilité* lorsqu'elle vérifie la propriété plus forte :

$$\text{pgcd}\,(a_n, a_m) = a_{\text{pgcd}(n,m)} \qquad (\forall n, m \in \mathbb{N}^*).$$

La structure générale des suites à divisibilité a été le sujet d'intérêt de plusieurs auteurs au moins depuis la seconde moitié du 20$^{\text{ème}}$ siècle. En 1936, Ward [51] étudie les valuations p-adiques de ces suites et découvre certaines de leurs propriétés. En 1990, Bézivin et al. [4] ont établi une caractérisation complète des suites à divisibilité qui sont récurrentes linéaires. Assez récemment, Bliss et al. [6] ont montré le résultat (figurant déjà implicitement dans un article antérieur de Kimberling [32]) selon lequel « le terme général d'une suite à forte divisibilité $\boldsymbol{a} = (a_n)_{n\geq 1}$ peut toujours s'écrire sous la forme :

$$a_n = \prod_{d \mid n} u_d \qquad (\forall n \geq 1),$$

pour une certaine suite d'entiers strictement positifs $(u_n)_{n\geq 1}$ ». Ce résultat a permis aux auteurs de [6] d'établir (dans le même contexte) une expression importante de $(u_n)_{n\geq 1}$ en fonction de $(a_n)_{n\geq 1}$, différente de celle qui s'obtient via la formule d'inversion de Möbius (voir le théorème 1.17). Bien que la réciproque de leur résultat soit fausse, Bliss et al. [6]

ont réussi à établir une condition nécessaire et suffisante sur une suite $\boldsymbol{u} = (u_n)_{n\geq 1}$ pour que la suite $\boldsymbol{a}$ définie par $a_n = \prod_{d|n} u_d$ $(\forall n \geq 1)$ soit à forte divisibilité (voir le théorème 3.4). Une autre condition plus pratique, équivalente à celle-ci, a été établie tout récemment par Nowicki [40] (voir le théorème 3.5). Pour une suite à forte divisibilité $(a_n)_{n\geq 1}$, Myerson (1994) se sert dans [38] d'un lemme de Kimberling [32] pour montrer que :

$$\operatorname{ppcm}(a_1, a_2, \ldots, a_n) \ \text{ divise } \ \frac{a_1 a_2 \cdots a_n}{\left(\prod_{1\leq k\leq n/b_1} a_k\right)\left(\prod_{1\leq k\leq n/b_2} a_k\right)\left(\prod_{1\leq k\leq n/b_3} a_k\right)\cdots},$$

pour toute suite d'entiers strictement positifs $(b_n)_{n\geq 1}$ telle que : $\sum_{k\geq 1} 1/b_k = 1$. Par la suite, Farhi [17] avait établi en 2005 que pour toute suite arithmétique $(u_k)_{k\in\mathbb{N}}$, dont la raison r et le premier terme u_0 sont strictement positifs et premiers entre eux, on a :

$$\operatorname{ppcm}(u_0, u_1, \ldots, u_n) \geq u_0 (r+1)^{n-1} \qquad (\forall n \in \mathbb{N}).$$

En outre, Farhi avait conjecturé que l'exposant $(n-1)$ figurant dans cette minoration peut être remplacé par n, qui est l'exposant optimal que l'on peut obtenir. Cette conjecture a été confirmée par Hong et al. [25] en 2006. Notons que Farhi utilise dans sa démonstration l'intégrale $\int_0^1 x^{m+\frac{u_0}{r}-1}(1-x)^{n-m}\mathrm{d}x$ $(0 \leq m \leq n)$. Plusieurs d'autres améliorations ont été établies, mais uniquement pour des valeurs de n assez grandes en fonction de u_0 et r (voir par exemple [25, 26, 31]). Concernant la majoration du ppcm d'une progression arithmétique générale, aucun résultat n'est établi à ce jour et d'ailleurs, cela fait bien partie de notre recherche. La méthode de Hanson (utilisée pour majorer les nombres $\operatorname{ppcm}(1, 2, \ldots, n)$) semble non généralisable aux progressions arithmétiques. D'autre part, Farhi [17] avait obtenu des minorations non triviales pour le ppcm d'une certaine classe de suites quadratiques ; il obtient en particulier la minoration suivante :

$$\operatorname{ppcm}\left(1^2+1, 2^2+1, \ldots, n^2+1\right) \geq 0.32\,(1.442)^n \qquad (\forall n \in \mathbb{N}^*).$$

Cette dernière avait été améliorée par Oon [41] qui a montré plus généralement que pour tous $c, m, n \in \mathbb{N}^*$ tels que $m \leq \left\lceil \frac{n}{2} \right\rceil$, on a :

$$\operatorname{ppcm}\left(m^2+c, (m+1)^2+c, \ldots, n^2+c\right) \geq 2^n.$$

L'idée de Oon consiste à évaluer l'intégrale $\int_0^1 x^{m-1+\sqrt{c}i}\,(1-x)^{n-m}\,\mathrm{d}x$ $(1 \leq m \leq n)$ de deux façons différentes, généralisant ainsi la méthode de Nair [39]. Dans la continuation, Hong et al. [27] avaient réussi à étendre la méthode de Oon aux suites polynomiales $(f(n))_{n\in\mathbb{N}^*}$, où $f \in \mathbb{Z}[X]$ est un polynôme non constant à coefficients positifs. Pour ce faire, ils ont dû compléter la méthode de Oon par de nouveaux arguments de la théorie algébrique des nombres.

Dans une autre direction, plusieurs estimations asymptotiques du ppcm de certaines suites d'entiers avaient été établies par divers auteurs. Parmi ces estimations, celle de Bateman et al. [2] qui énonce que pour tous $a, b \in \mathbb{Z}$, tels que $b > 0$, $a + b > 0$ et $\mathrm{pgcd}(a, b) = 1$, on a :

$$\log \mathrm{ppcm}\,(a+b, a+2b, \ldots, a+nb) \sim_{+\infty} \left(\frac{b}{\varphi(b)} \sum_{\substack{1\leq m\leq b \\ \mathrm{pgcd}(m,b)=1}} \frac{1}{m} \right) n,$$

où φ désigne la fonction indicatrice d'Euler. Ce résultat s'obtient comme conséquence du théorème des nombres premiers pour les progressions arithmétiques, qui lui même constitue une généralisation du théorème des nombres premiers (voir par exemple [5], p. 72). En désignant par $(F_n)_{n\geq 1}$ la suite de Fibonacci usuelle, définie récursivement par : $F_1 = 1$, $F_2 = 1$ et $F_{n+2} = F_n + F_{n+1}$ $(\forall n \geq 1)$; Matiyasevich et al. [36] ont montré que :

$$\log \mathrm{ppcm}\,(F_1, F_2, \ldots, F_n) \sim_{+\infty} \frac{3}{\pi^2} n^2 \log \Phi,$$

où Φ désigne le nombre d'or $(\Phi := \frac{1+\sqrt{5}}{2})$. Ce résultat a été généralisé par Kiss et al. [33] pour les suites de Fibonacci généralisées à la place de $(F_n)_n$. Une autre estimation un peu plus complexe est due à Cilleruelo [13] qui énonce que pour tout polynôme quadratique irréductible $f \in \mathbb{Z}[X]$, on a :

$$\log \mathrm{ppcm}\,(f(1), f(2), \ldots, f(n)) = n \log n + Bn + o(n),$$

où B est une constante qui dépend de f. Cette dernière estimation entraîne, en particulier, que :

$$\log \mathrm{ppcm}\,(f(1), f(2), \ldots, f(n)) \sim_{+\infty} n \log n.$$

Pour le cas où $f(x) = x^2 + 1$, Rué et al. [45] ont amélioré le terme d'erreur de l'estimation précédente en montrant que l'on a pour tout $\alpha < \frac{4}{9}$:

$$\log \operatorname{ppcm}\left(1^2+1, 2^2+1, \ldots, n^2+1\right) = n\log n + Bn + O\left(\frac{n}{(\log n)^{\alpha}}\right).$$

Cilleruelo [13] a aussi donné une conjecture qui est ouverte à ce jour et qui généralise son estimation. Plus précisément, on a :

Conjecture 1 (Cilleruelo [13])**.** *Pour tout polynôme irréductible $f \in \mathbb{Z}[X]$ tel que* $\deg f \geq 3$*, on a :*

$$\log \operatorname{ppcm}\left(f(1), f(2), \ldots, f(n)\right) \sim_{+\infty} (\deg f - 1) n \log n.$$

En outre, Cilleruelo avait précisé que cette conjecture est équivalente à dire que pour tout polynôme irréductible de degré ≥ 3, on a :

$$\#\left\{p \text{ premier};\ n \leq p \ll n^{\deg f - 1},\ p \mid f(k),\ p \mid f(j) \text{ pour certains } 1 \leq j < k \leq n\right\} = o(n).$$

À ce stade, nous avons presque introduit tout ce qui existe en littérature à propos des estimations du ppcm de certaines suites d'entiers.

Le but de la thèse

Le but de cette thèse consiste en les trois points suivants :

1. Dans la minoration de Oon, le nombre de termes figurant dans le plus petit commun multiple $L_{c,m,n} := \operatorname{ppcm}\left(m^2 + c, (m+1)^2 + c, \ldots, n^2 + c\right)$ est strictement plus grand que $n/2$. On se propose dans cette thèse de supprimer cette contrainte, en cherchant des minorations non triviales de $L_{c,m,n}$ pour des entiers strictement positifs c, m, n quelconques (bien entendu $m \leq n$).
2. On s'intéresse aussi à estimer le ppcm de quelques suites non polynomiales, comme la suite de Fibonacci, les suites de Lucas ou plus généralement les suites à forte divisibilité. Le but ici est au moins d'effectiviser le résultat asymptotique de Matiyasevich et al. [36] et sa généralisation par Kiss et al. [33].

3. Nous cherchons également à obtenir une première majoration effective et non triviale pour le ppcm d'une progression arithmétique finie, ce qui revient à préciser et effectiviser l'estimation asymptotique de Bateman et al. [2].

Aperçu de la thèse

Cette thèse est composée de cinq chapitres que nous décrivons brièvement ci-dessous :

Dans le premier chapitre, nous présentons des généralités sur les estimations du ppcm de suites d'entiers. La partie principale de notre travail se situe donc dans les chapitres 2, 3, 4 et 5.

Le deuxième chapitre est consacré à l'étude des nombres

$$L_{c,m,n} := \mathrm{ppcm}\{m^2 + c, (m+1)^2 + c, \ldots, n^2 + c\},$$

où c, m, n sont des entiers strictement positifs tels que $m \leq n$. Plus précisément, nous utilisons des arguments d'algèbre commutative et d'analyse complexe pour obtenir un diviseur rationnel et non trivial de $L_{c,m,n}$. Comme conséquence, nous établissons des nouvelles minorations non triviales pour $L_{c,m,n}$.

Dans le troisième chapitre, nous obtenons des identités intéressantes concernant le ppcm de suites à forte divisibilité. Nous appliquons ensuite ces identités pour donner un premier encadrement effectif du ppcm d'une suite de Fibonacci généralisée ; ce qui constitue en particulier une version effective du résultat de Matyasevich et al. [36] et sa généralisation par Kiss et al. [33].

Dans le quatrième chapitre, nous établissons une première majoration effective du ppcm des termes consécutifs d'une suite arithmétique finie et nous donnons quelques conséquences de cette dernière.

Dans le dernier chapitre, nous adaptons la méthode du quatrième chapitre pour la suite $(n^2+1)_n$ et nous établissons d'une part une amélioration de la minoration de Oon (pour le cas $c = 1$) et d'autre part nous obtenons une première majoration effective du ppcm de cette suite.

CHAPITRE 1

Généralités sur les estimations du ppcm de suites d'entiers

1.1 Introduction

Ce chapitre rassemble les différents travaux réalisés dans le cadre des estimations du ppcm de certaines suites d'entiers. On se focalise notamment sur certains résultats effectifs dus à Chebyshev [12], Myerson [38], Hanson [23], Nair [39], Farhi [16, 17], Oon [41] et Hong et al. [25, 27, 28]. Nous terminons par une brève présentation de quelques résultats asymptotiques dus à Bateman et al. [2] et Cilleruelo [13].

1.2 La méthode de Chebyshev

Chebyshev fut le premier à avoir obtenu en 1850 des estimations effectives et significatives de la fonction de comptage des nombres premiers π. Ses célèbres fonctions ψ et θ (définies ci-dessous) furent les points clef de sa méthode.

Définition 1.1. *Les fonctions θ, ψ, T et χ de Chebyshev associent à tout réel positif x les réels respectifs $\theta(x)$, $\psi(x)$, $T(x)$ et $\chi(x)$ définis comme suit :*

$$\begin{aligned}
\theta(x) &:= \sum_{p\leq x} \log p,\\
\psi(x) &:= \log \operatorname{ppcm}(1,2,\ldots,\lfloor x\rfloor),\\
T(x) &:= \psi(x) + \psi\left(\frac{x}{2}\right) + \psi\left(\frac{x}{3}\right) + \ldots,\\
\chi(x) &:= T(x) + T\left(\frac{x}{30}\right) - T\left(\frac{x}{2}\right) - T\left(\frac{x}{3}\right) - T\left(\frac{x}{5}\right).
\end{aligned}$$

Remarque 1.2. *En se servant du fait que* $\operatorname{ppcm}(1,2,\ldots,\lfloor x\rfloor) = \prod_{p^\alpha\leq x} p$*, où le produit étant étendu à tous les couples (p,α), avec p premier et $\alpha\in\mathbb{N}^*$, on montre immédiatement que l'on a pour tout $x\in\mathbb{R}^+$:*

$$\psi(x) = \theta(x) + \theta(x^{1/2}) + \theta(x^{1/3}) + \ldots. \tag{1.2.1}$$

De cette identité se déduit aussi l'expression de T en fonction de θ. On a la proposition suivante :

Proposition 1.3 (Chebyshev [12])**.** *Pour tout réel positif x, on a :*

$$T(x) = \sum_{n\geq 1}\sum_{j\geq 1} \theta\left(\left(\frac{x}{n}\right)^{\frac{1}{j}}\right) = \log\left(\lfloor x\rfloor!\right). \tag{1.2.2}$$

Démonstration. La première égalité de (1.2.2) résulte immédiatement de (1.2.1). Pour montrer la seconde égalité de (1.2.2), on se sert d'une part de l'identité $\operatorname{ppcm}(1,2,\ldots,\lfloor y\rfloor) = \prod_{p^\alpha\leq y} p \quad (\forall y\geq 0)$ et d'autre part de la formule des factoriels de Legendre. En effet, pour tout $x\geq 0$, on a :

$$\begin{aligned}
\exp\left(T(x)\right) &= \prod_{j\geq 1}\prod_{n\geq 1}\left(\prod_{p^j\leq x/n} p\right) = \prod_{j\geq 1}\prod_{p^j\leq x} p^{\left\lfloor \frac{x}{p^j}\right\rfloor}\\
&= \prod_{p\leq x}\left(\prod_{\substack{j\geq 1\\ p^j\leq x}} p^{\left\lfloor \frac{x}{p^j}\right\rfloor}\right) = \prod_{p\leq x} p^{\sum_{j\geq 1}\left\lfloor \frac{x}{p^j}\right\rfloor} = \lfloor x\rfloor!.
\end{aligned}$$

Ce qui conclut à l'égalité requise et complète cette démonstration. ∎

Lemme 1.4 (Chebyshev [12]). *Pour tout réel positif x, on a :*

$$\psi(x) - \psi\left(\frac{x}{6}\right) \leq \chi(x) \leq \psi(x).$$

Démonstration. En exprimant χ en fonction de ψ, on obtient pour tout $x \geq 0$:

$$\chi(x) = A_1\psi(x) + A_2\psi\left(\frac{x}{2}\right) + \cdots + A_n\psi\left(\frac{x}{n}\right) + \ldots,$$

où les coefficients $A_1, A_2, \ldots, A_n, \ldots$ prennent les valeurs 0, 1 ou -1 selon les restes de leurs indices modulo 30. On a plus précisément :

$A_n = 1$, si $n \equiv 1, 7, 11, 13, 17, 19, 23, 29 \pmod{30}$,

$A_n = 0$, si $n \equiv 2, 3, 4, 5, 8, 9, 14, 16, 21, 22, 25, 26, 27, 28 \pmod{30}$,

$A_n = -1$, si $n \equiv 0, 6, 10, 12, 15, 18, 20, 24 \pmod{30}$.

Pour montrer ce fait, il suffit de remarquer que pour tout $i \in \{1, 2, 3, 5, 30\}$, le nombre $T\left(\frac{x}{i}\right)$ est la somme des nombres $\psi\left(\frac{x}{n}\right)$, où n parcourt l'ensemble des multiples de i. On a ainsi pour tout $x \geq 0$:

$$\chi(x) = \psi(x) - \psi\left(\frac{x}{6}\right) + \psi\left(\frac{x}{7}\right) - \psi\left(\frac{x}{10}\right) + \psi\left(\frac{x}{11}\right) - \psi\left(\frac{x}{12}\right) + \ldots.$$

Constatant que cette série est alternée et que ses termes décroissent continuellement en valeurs absolues, on peut l'encadrer entre son premier terme et la somme de ses deux premiers termes ; soit

$$\psi(x) - \psi\left(\frac{x}{6}\right) \leq \chi(x) \leq \psi(x) \quad (\forall x \geq 0).$$

Le lemme est ainsi démontré. ∎

Théorème 1.5 (Chebyshev [12]). *pour tout réel $x \geq 1$, on a :*

$$Ax - \frac{5}{2}\log x - 1 \leq \psi(x) \leq \frac{6}{5}Ax + \frac{5}{4\log 6}\log^2 x + \frac{5}{4}\log x + 1,$$

où $A := \log\left(\frac{2^{1/2}3^{1/3}5^{1/5}}{30^{1/30}}\right) \simeq 0,92129202.$

Démonstration. En posant $n = \lfloor x \rfloor$, on a l'estimation de Stirling suivante :

$$n^n e^{-n}\sqrt{2\pi n} \leq n! \leq n^n e^{-n}\sqrt{2\pi n} \cdot e^{\frac{1}{12n}}$$

(voir [35, Problème 1.15]), qui entraîne (en vertu de la proposition 1.3) que :

$$\begin{aligned} T(x) &\leq \log\left(\sqrt{2\pi}\right) + n\log n - n + \frac{1}{2}\log n + \frac{1}{12n} \\ &\leq \log\left(\sqrt{2\pi}\right) + x\log x - x + \frac{1}{2}\log x + \frac{1}{12}, \\ T(x) &\geq \log\left(\sqrt{2\pi}\right) + (n+1)\log(n+1) - (n+1) - \frac{1}{2}\log(n+1) \\ &\geq \log\left(\sqrt{2\pi}\right) + x\log x - x - \frac{1}{2}\log x. \end{aligned}$$

En utilisant ces dernières estimations de la fonction T (qui sont valables pour tout $x \geq 1$), on obtient les estimations suivantes (valables pour tout $x \geq 30$) :

$$\begin{aligned} T(x) + T\left(\frac{x}{30}\right) &\leq 2\log\left(\sqrt{2\pi}\right) + \frac{2}{12} + \frac{31}{30}x\log x - x\log\left(30^{1/30}\right) - \frac{31}{30}x + \log x - \frac{1}{2}\log 30, \\ T(x) + T\left(\frac{x}{30}\right) &\geq 2\log\left(\sqrt{2\pi}\right) + \frac{31}{30}x\log x - x\log\left(30^{1/30}\right) - \frac{31}{30}x - \log x + \frac{1}{2}\log 30, \\ T\left(\frac{x}{2}\right) + T\left(\frac{x}{3}\right) + T\left(\frac{x}{5}\right) &\leq 3\log\left(\sqrt{2\pi}\right) + \frac{3}{12} + \frac{31}{30}x\log x - x\log\left(2^{1/2}3^{1/3}5^{1/5}\right) - \frac{31}{30}x \\ &\quad + \frac{3}{2}\log x - \frac{1}{2}\log 30, \\ T\left(\frac{x}{2}\right) + T\left(\frac{x}{3}\right) + T\left(\frac{x}{5}\right) &\geq 3\log\left(\sqrt{2\pi}\right) + \frac{31}{30}x\log x - x\log\left(2^{1/2}3^{1/3}5^{1/5}\right) - \frac{31}{30}x \\ &\quad - \frac{3}{2}\log x + \frac{1}{2}\log 30. \end{aligned}$$

Il découle de ces dernières estimations et de la définition même de la fonction χ que l'on a pour tout $x \geq 30$:

$$Ax - \frac{5}{2}\log x - 1 \leq \chi(x) \leq Ax + \frac{5}{2}\log x,$$

avec $A := \log\left(\frac{2^{1/2}3^{1/3}5^{1/5}}{30^{1/30}}\right)$. D'autre part, un calcul manuel montre que cette double inégalité reste également vraie pour tout $1 \leq x \leq 30$; elle est, par conséquent, vraie pour tout $x \geq 1$. Il s'ensuit, en vertu du lemme 1.4 que l'on a pour tout $x \geq 1$:

$$\psi(x) - \psi\left(\frac{x}{6}\right) \leq Ax + \frac{5}{2}\log x, \tag{1.2.3}$$

$$\psi(x) \geq Ax - \frac{5}{2}\log x - 1. \tag{1.2.4}$$

L'estimation (1.2.4) fournit la minoration requise de $\psi(x)$. Pour montrer la majoration requise pour $\psi(x)$, on considère la fonction réelle f définie sur l'intervalle $]0, +\infty[$ par :

$$f(x) := \frac{6}{5}Ax + \frac{5}{4\log 6}\log^2 x + \frac{5}{4}\log x \quad (\forall x > 0).$$

On vérifie immédiatement que l'on a pour tout $x > 0$:

$$f(x) - f\left(\frac{x}{6}\right) = Ax + \frac{5}{2}\log x.$$

Cette égalité retranchée membre à membre de (1.2.3) donne :

$$\psi(x) - f(x) \leq \psi\left(\frac{x}{6}\right) - f\left(\frac{x}{6}\right) \qquad (\forall x > 0).$$

En réitérant cette dernière plusieurs fois, on obtient que pour tout $x > 0$ et tout $m \in \mathbb{N}^*$, on a :

$$\psi(x) - f(x) \leq \psi\left(\frac{x}{6}\right) - f\left(\frac{x}{6}\right) \leq \psi\left(\frac{x}{6^2}\right) - f\left(\frac{x}{6^2}\right) \leq \cdots \leq \psi\left(\frac{x}{6^{m+1}}\right) - f\left(\frac{x}{6^{m+1}}\right),$$

En prenant m le plus grand entier positif vérifiant $\frac{x}{6^m} \geq 1$, on aura $\frac{x}{6^{m+1}} \in [\frac{1}{6}, 1[$; de sorte que $\psi\left(\frac{x}{6^{m+1}}\right) = 0$ et $-f\left(\frac{x}{6^{m+1}}\right) \leq 1$; on obtient donc :

$$\psi(x) \leq 1 + f(x) \qquad (\forall x > 0)$$

et l'on conclut à la majoration requise pour $\psi(x)$ en substituant dans cette dernière $f(x)$ par l'expression qui la définit. Ce qui complète cette démonstration. ∎

Le corollaire suivant est immédiat.

Corollaire 1.6. *Pour tout $n \in \mathbb{N}^*$, on a :*

$$e^{-1} \cdot n^{-\frac{5}{2}} (c_1)^n \leq \operatorname{ppcm}(1, 2, \ldots, n) \leq e \cdot n^{\frac{5}{4}} e^{\frac{5}{4\log 6}\log^2 n} (c_2)^n,$$

avec $c_1 = e^A \simeq 2,51$ et $c_2 = e^{\frac{6}{5}A} \simeq 3,02$.

Le théorème 1.5 entraîne aussi un encadrement effectif pour la fonction θ de Chebyshev. Un tel encadrement est donné par le corollaire suivant :

Corollaire 1.7 (Chebyshev [12])**.** *Pour tout réel $x \geq 1$, on a :*

$$Ax - \frac{12}{5}x^{1/2} - \frac{5}{8\log 6}\log^2 x - \frac{15}{4}\log x - 3 \leq \theta(x) \leq \frac{6}{5}Ax + \frac{5}{4\log 6}\log^2 x + \frac{5}{4}\log x + 1.$$

En particulier, on a :

$$Ax + o(x) \leq \theta(x) \leq \frac{6}{5}Ax + o(x) \qquad (\forall x \geq 1), \tag{1.2.5}$$

où les termes en o sont explicites.

Démonstration. Pour $x \geq 1$, on a d'une part (d'après (1.2.1)) $\theta(x) \leq \psi(x)$, et d'autre part :

$$\theta(x) \geq \theta(x) - \left[\theta(x^{1/2}) - \theta(x^{1/3})\right] - \left[\theta(x^{1/4}) - \theta(x^{1/5})\right] - \cdots = \psi(x) - 2\psi(\sqrt{x}),$$

car les termes $\theta(x^{1/2}) - \theta(x^{1/3}), \theta(x^{1/4}) - \theta(x^{1/5}), \ldots$ sont tous positifs. On conclut au résultat requis grâce à l'encadrement du théorème 1.5. ∎

Dans ce qui suit, nous indiquons brièvement comment l'on peut obtenir un encadrement effectif de la fonction de comptage des nombres premiers π. Vu la complexité des estimations de Chebyshev, nous n'allons pas rentrer dans les détails des calculs.

Théorème 1.8 (Chebyshev [12])**.** *Pour tout réel $x \geq 2$, on a :*

$$(A + o(1))\frac{x}{\log x} \leq \pi(x) \leq \frac{x}{\log x}\left(\frac{6}{5}A + o(1)\right),$$

où les termes en o sont explicites.

Démonstration. Premièrement, on a en vertu de la formule sommatoire d'Abel (voir par exemple [35, p. 5]) :

$$\pi(x) = \frac{\theta(x)}{\log x} + \int_2^x \frac{\theta(t)}{t\log^2 t}\mathrm{d}t \quad (\forall x \geq 2). \tag{1.2.6}$$

D'après l'inégalité (1.2.5), on peut estimer l'intégrale précédente comme suit :

$$\int_2^x \frac{\theta(t)}{t\log^2 t}\mathrm{d}t \leq \frac{6}{5}A\int_2^x \frac{\mathrm{d}t}{\log^2 t} + o\left(\int_2^x \frac{\mathrm{d}t}{\log^2 t}\right).$$

Ensuite, comme on a :

$$\int_2^x \frac{\mathrm{d}t}{\log^2 t} = \int_2^{\sqrt{x}} \frac{\mathrm{d}t}{\log^2 t} + \int_{\sqrt{x}}^x \frac{\mathrm{d}t}{\log^2 t} \leq \frac{\sqrt{x}}{\log^2 2} + \frac{4x}{\log^2 x} = O\left(\frac{x}{\log^2 x}\right), \tag{1.2.7}$$

il s'ensuit que :

$$\int_2^x \frac{\theta(t)}{t\log^2 t}\mathrm{d}t = O\left(\frac{x}{\log^2 x}\right).$$

En reportant ceci dans (1.2.6) et en utilisant de nouveau l'estimation (1.2.5), on obtient :

$$\pi(x) \leq \frac{6}{5}A\frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right) = \frac{6}{5}A\frac{x}{\log x}\left(1 + o(1)\right).$$

D'autre part, on a en vertu de (1.2.5) et de (1.2.6) :

$$\pi(x) \geq \frac{\theta(x)}{\log x} \geq A\frac{x}{\log x} + o\left(\frac{x}{\log x}\right) = A\frac{x}{\log x}\left(1 + o(1)\right).$$

Ce qui complète cette démonstration. ∎

Le corollaire suivant est immédiat :

Corollaire 1.9 (Chebyshev [12])**.** *Il existe $x_0 > 0$ effectivement calculable, tel que :*

$$0,9\frac{x}{\log x} \leq \pi(x) \leq 1,2\frac{x}{\log x} \qquad (\forall x \geq x_0).$$

Remarque 1.10. *Soit $x \geq 2$. Puisque* $\operatorname{ppcm}(1, 2, \ldots, \lfloor x \rfloor) = \prod_{p^\nu \leq x} p$*, où le produit étant étendu à tous les couples (p, ν), avec p premier et $\nu \in \mathbb{N}^*$, alors on a :*

$$\psi(x) = \sum_{p^\nu \leq x} \log p.$$

Par ailleurs, pour chaque nombre premier p fixé, on a :

$$p^\nu \leq x \Longleftrightarrow \nu \leq \left\lfloor \frac{\log x}{\log p} \right\rfloor.$$

Il y a donc exactement $\left\lfloor \frac{\log x}{\log p} \right\rfloor$ valeurs de ν tels que $p^\nu \leq x$, ce qui permet d'écrire :

$$\psi(x) = \sum_{p \leq x} \left\lfloor \frac{\log x}{\log p} \right\rfloor \log p.$$

Par suite, grâce à l'encadrement $\lfloor u \rfloor \leq u \leq 2\lfloor u \rfloor$ valable pour $u \geq 1$, on a :

$$\psi(x) \leq \sum_{p \leq x} \log x = \pi(x) \log x = \sum_{p \leq x} \left(\frac{\log x}{\log p}\right) \log p \leq 2 \sum_{p \leq x} \left\lfloor \frac{\log x}{\log p} \right\rfloor \log p,$$

soit

$$\frac{\psi(x)}{\log x} \leq \pi(x) \leq 2\frac{\psi(x)}{\log x}. \tag{1.2.8}$$

Ce qui permet (via le théorème 1.5) d'obtenir un autre encadrement de $\pi(x)$ $(\forall x \geq 1)$.

Le corollaire 1.9 et la remarque 1.10 impliquent qu'il existe un réel N effectivement calculable tel que $\pi(2n-2) > \pi(n)$ pour tout entier $n \geq N$. En explicitant les termes $o(1)$ dans le théorème 1.8, Chebychev a pu prouver que cette inégalité est bien valable

pour tout entier $n > 3$, ce qui constitue une preuve d'une conjecture célèbre, connue sous le nom de « postulat de Bertrand » (datant de 1845) :

Le postulat de Bertrand : Pour tout entier $n \geq 2$, il existe au moins un nombre premier p tel que :

$$n < p < 2n.$$

Notons que l'estimation des fonctions liées aux nombres premiers (comme les fonctions de Chebyshev) pour des valeurs de x assez petites se fait généralement à la main en se servant des tables de nombres premiers ou d'un logiciel de calcul. Nous verrons dans les prochaines sections, que l'étude de certaines propriétés arithmétiques des nombres $d_n := \text{ppcm}(1, 2, \ldots, n)$ $(n \in \mathbb{N}^*)$, permet d'obtenir d'autres estimations effectives plus simples pour les fonctions ψ et π.

1.3 Un multiple du ppcm de suites à forte divisibilité

Le ppcm des n premiers termes d'une suite d'entiers naturels divise de toute évidence le produit de ces termes, mais en général ce produit est beaucoup plus grand que le ppcm en question. Dans cette section, nous présentons un multiple non trivial du nombre $\text{ppcm}(a_1, a_2, \ldots, a_n)$ pour une certaine classe de suites $a_1, a_2, \ldots$ d'entiers strictement positifs.

Définition 1.11. *Une suite d'entiers strictement positifs $(a_n)_{n\geq 1}$ est dite à divisibilité lorsqu'elle vérifie la propriété :*

$$n \mid m \Longrightarrow a_n \mid a_m \qquad (\forall n, m \in \mathbb{N}^*).$$

Elle est dite à forte divisibilité lorsqu'elle vérifie la propriété plus forte :

$$\text{pgcd}\,(a_n, a_m) = a_{\text{pgcd}(n,m)} \qquad (\forall n, m \in \mathbb{N}^*).$$

Exemples 1.12.

— *Une suite à divisibilité n'est pas forcément à forte divisibilité. En effet, la suite $(2^n)_{n\geq 1}$ est à divisibilité mais elle n'est pas à forte divisibilité, car on a par exemple :* $\text{pgcd}\,(2^2, 2^3) = 4 \neq 2^{\text{pgcd}(2,3)} = 2$.

— *La suite de tous les entiers strictement positifs* $(n)_{n\geq 1}$ *est de toute évidence à forte divisibilité.*

— *Pour tous* $m, n \in \mathbb{N}^*$, *si l'on désigne par* r *le reste de la division euclidienne de* n *sur* m, *on montre facilement que* $(2^r - 1)$ *est le reste de la division euclidienne de* $(2^n - 1)$ *par* $(2^m - 1)$. *Ce qui entraîne (via l'algorithme d'Euclide) que la suite* $(2^n - 1)_{n\geq 1}$ *est à forte divisibilité.*

— *Un autre exemple très important d'une suite à forte divisibilité est la suite de Fibonacci usuelle* $(F_n)_{n\geq 1}$ *(voir [50], p. 34) qui est définie récursivement par :* $F_1 = 1$, $F_2 = 1$ *et* $F_{n+2} = F_n + F_{n+1}$ *pour tout entier* $n \geq 1$.

— *Si deux suites* $(t_n)_{n\geq 1}$ *et* $(s_n)_{n\geq 1}$ *sont à forte divisibilité alors, les suites* $(t_n^\alpha)_{n\geq 1}$ $(\alpha \in \mathbb{N}^*)$ *et* $(t_{s_n})_{n\geq 1}$ *le sont aussi (voir [32]).*

Théorème 1.13 (Myerson [38])**.** *Soient* $(a_n)_{n\geq 1}$ *une suite à forte divisibilité et* $(b_n)_{n\geq 1}$ *une suite d'entiers strictement positifs vérifiant* $\sum_{n\geq 1} \frac{1}{b_n} \leq 1$. *Alors, on a pour tout* $n \geq 1$ *:*

$$\operatorname{ppcm}(a_1, a_2, \ldots, a_n) \quad \textit{divise} \quad \frac{a_1 a_2 \cdots a_n}{\left(\prod_{1\leq k\leq n/b_1} a_k\right)\left(\prod_{1\leq k\leq n/b_2} a_k\right)\left(\prod_{1\leq k\leq n/b_3} a_k\right)\cdots}. \tag{1.3.1}$$

Remarque 1.14. *Un exemple important d'une suite* $(b_n)_{n\geq 1}$ *vérifiant les conditions du théorème 1.13 est la suite de Sylvester, qui est définie par* $b_1 = 2$ *et* $b_{n+1} = b_1 b_2 \cdots b_n + 1$ $(\forall n \in \mathbb{N}^*)$. *On vérifie facilement que pour tout* $n \in \mathbb{N}^*$, *on a :*

$$b_{n+1} = b_n^2 - b_n + 1 \tag{1.3.2}$$

et

$$\sum_{\ell=1}^{n} \frac{1}{b_\ell} + \frac{1}{b_1 b_2 \cdots b_n} = 1. \tag{1.3.3}$$

Nous ferons appel à ces identités dans la section suivante.

Exemple 1.15. *En prenant dans le théorème 1.13* $a_n = n$ $(\forall n \geq 1)$ *et* $(b_n)_{n\geq 1}$ *la suite de Sylvester, on obtient que pour tout* $n \in \mathbb{N}^*$, *on a :*

$$\operatorname{ppcm}(1, 2, \ldots, n) \quad \textit{divise} \quad \frac{n!}{\lfloor n/2\rfloor!\lfloor n/3\rfloor!\lfloor n/7\rfloor!\lfloor n/43\rfloor!\cdots},$$

où $2, 3, 7, 43, \ldots$ *est la suite de Sylvester.*

Nous partageons la preuve du théorème 1.13 en plusieurs lemmes.

Le lemme suivant est une conséquence immédiate du principe d'inclusion-exclusion (voir Hua [30, p. 10]).

Lemme 1.16 ([30], Theorem 7.3)**.** *Soient $n \in \mathbb{N}^*$ et $S = \{x_1, x_2, \ldots, x_n\}$ un sous ensemble de $\mathbb{N}^*$. Alors, on a l'identité suivante :*

$$\prod_{i=1}^{n} x_i = \operatorname{ppcm}(S) \prod_{\substack{A \subset S \\ |A| \geq 2}} \operatorname{pgcd}(A)^{(-1)^{|A|}},$$

où $|A|$, $\operatorname{pgcd}(A)$ et $\operatorname{ppcm}(S)$ désignent respectivement le cardinal de l'ensemble A, le plus grand diviseur commun des éléments de A et le ppcm *des éléments de S.*

Fixons une suite à forte divisibilité $(a_n)_{n\geq 1}$ et considérons $u_1, u_2, \ldots$ les nombres rationnels strictement positifs définis récursivement par la formule :

$$a_n = \prod_{d|n} u_d. \tag{1.3.4}$$

D'après la formule d'inversion de Möbius (voir par exemple [48, p. 35]), on a :

$$u_n = \prod_{d|n} a_{n/d}^{\mu(d)}. \tag{1.3.5}$$

Le lemme suivant donne quelques propriétés de la suite $(u_n)_n$. Il figure déjà implicitement dans un article antérieur de Kimberling [32]. Nous donnons ici sa version explicite établie par Bliss et al. [6].

Lemme 1.17 (Bliss et al. [6])**.** *Les nombres $u_1, u_2, \ldots$ sont tous des entiers strictement positifs. De plus, si $n \in \mathbb{N}^*$ possède la factorisation primaire $n = {q_1}^{\alpha_1} {q_2}^{\alpha_2} \cdots {q_m}^{\alpha_m}$, on a :*

$$u_n = \frac{a_n}{\operatorname{ppcm}\left(a_{n/q_1}, a_{n/q_2}, \ldots, a_{n/q_m}\right)}. \tag{1.3.6}$$

Démonstration. Pour tout $\ell \in \{0, 1, \ldots, m\}$, désignons par Q_ℓ le produit de tous les a_d tels que $\frac{n}{d}$ soit le produit de ℓ nombres premiers distincts. Puisque $\mu\left(\frac{n}{d}\right) = 0$ si et seulement si $\frac{n}{d}$ possède un facteur carré > 1 (i.e., il existe un nombre premier p tel que $p^2 \mid \frac{n}{d}$), alors on a :

$$u_n = \prod_{d|n} a_d^{\mu(n/d)} = \prod_{\ell=0}^{m} Q_\ell^{(-1)^\ell}. \tag{1.3.7}$$

Par ailleurs, d'après le lemme 1.16 qu'on applique pour $x_i = a_{n/q_i}$ $(\forall i \in \{1, 2, \ldots, m\})$ et $S = \{x_1, x_2, \ldots, x_m\}$, on a :

$$Q_1 = \prod_{i=1}^{m} x_i = \operatorname{ppcm}(S) \prod_{\substack{A \subset S \\ |A| \geq 2}} \operatorname{pgcd}(A)^{(-1)^{|A|}} = \operatorname{ppcm}(S) \prod_{k=2}^{m} \prod_{\substack{A \subset S \\ |A|=k}} \operatorname{pgcd}(A)^{(-1)^k}, \quad (1.3.8)$$

où la première égalité vient de la définition de Q_1. Par suite, comme $(a_k)_{k\geq 1}$ est à forte divisibilité, on a pour tout $k \in \{2, \ldots, m\}$ et pour tous $1 \leq i_1 < i_2 < \cdots < i_k \leq m$:

$$\operatorname{pgcd}(x_{i_1}, x_{i_2}, \ldots, x_{i_k}) = a_{\operatorname{pgcd}\left(n/q_{i_1}, n/q_{i_2}, \ldots, n/q_{i_k}\right)} = a_{n/\left(q_{i_1} q_{i_2} \cdots q_{i_k}\right)}.$$

Il s'ensuit de cette dernière et de la définition de Q_k $(k \in \mathbb{N})$ que :

$$Q_k = \prod_{1 \leq i_1 < i_2 < \cdots < i_k \leq m} a_{n/\left(q_{i_1} q_{i_2} \cdots q_{i_k}\right)} = \prod_{\substack{A \subset S \\ |A|=k}} \operatorname{pgcd}(A) \qquad (\forall k \in \{2, \ldots, m\}). \quad (1.3.9)$$

En combinant (1.3.8) et (1.3.9), on obtient :

$$Q_1 = \operatorname{ppcm}(S) \prod_{k=2}^{m} Q_k^{(-1)^k}.$$

D'où l'on a (en vertu de (1.3.7)) :

$$\begin{aligned} u_n &= \frac{Q_0 \prod_{k=2}^{m} Q_k^{(-1)^k}}{Q_1} = \frac{Q_0 \prod_{k=2}^{m} Q_k^{(-1)^k}}{\operatorname{ppcm}(S) \prod_{k=2}^{m} Q_k^{(-1)^k}} = \frac{Q_0}{\operatorname{ppcm}(S)} \\ &= \frac{a_n}{\operatorname{ppcm}\left(a_{n/q_1}, a_{n/q_2}, \ldots, a_{n/q_m}\right)}, \end{aligned}$$

ce qui confirme l'identité (1.3.6). Maintenant, puisque a_n est multiple de chacun des a_{n/q_i} $(\forall i \in \{1, \ldots, m\})$ (car $(a_k)_{k\geq 1}$ est à forte divisibilité), alors a_n est multiple de $\operatorname{ppcm}\left(a_{n/q_1}, a_{n/q_2}, \ldots, a_{n/q_m}\right)$, ce qui entraîne que les nombres $u_1, u_2, \ldots$ sont tous des entiers strictement positifs. Le lemme est ainsi démontré. ∎

Définition 1.18. *Soient $m \in \mathbb{N}^*$ et p un nombre premier. On dit que m est "champion pour p" si $(m = 1$ et $\vartheta_p(a_1) > 0)$ ou $(m > 1$ et $\vartheta_p(a_m) > \vartheta_p(a_j)$ pour tout $j < m)$.*

Remarque 1.19. *Soient $m_1, m_2 \in \mathbb{N}^*$ et p un nombre premier. Si $m_1 < m_2$ sont tous les deux champions pour p, alors m_1 divise m_2. En effet, si $d = \operatorname{pgcd}(m_1, m_2)$ alors : $\vartheta_p(a_d) = \min(\vartheta_p(a_{m_1}), \vartheta_p(a_{m_2})) = \vartheta_p(a_{m_1})$, ce qui implique que $d = m_1$ (car : $d \leq m_1$ et m_1 est champion pour p).*

Lemme 1.20 (Myerson [38]). *Pour tout $m \in \mathbb{N}^*$ et tout nombre premier p, on a : $\vartheta_p(u_m) > 0$ si et seulement si m est champion pour p.*

Démonstration. Soient $m \in \mathbb{N}^*$ et p un nombre premier.

•($\Rightarrow$) : Procédons par l'absurde et supposons que $\vartheta_p(u_m) > 0$ et $\vartheta_p(a_m) \leq \vartheta_p(a_j)$ pour un certain $j < m$. D'une part, on a (en vertu de (1.3.4)) pour tout diviseur propre d' de m :

$$\vartheta_p(a_m) = \sum_{d|m} \vartheta_p(u_d) = \vartheta_p(u_m) + \sum_{d|d'} \vartheta_p(u_d) + \sum_{\substack{d|m \\ d\neq m \\ d\nmid d'}} \vartheta_p(u_d) > \sum_{d|d'} \vartheta_p(u_d) = \vartheta_p(a_{d'}),$$

(où la deuxième égalité vient du fait que tout diviseur de d' est aussi un diviseur de m), et d'autre part, pour $d' := \text{pgcd}(m, j)$ on a : $\vartheta_p(a_{d'}) = \min(\vartheta_p(a_m), \vartheta_p(a_j)) = \vartheta_p(a_m)$, ce qui contredit le fait que $d' = \text{pgcd}(m, j) < m$ est un diviseur propre de m. Ceci confirme l'implication directe du lemme.

•($\Leftarrow$) : Supposons que m est champion pour p. D'après le lemme 1.17, on a : $\vartheta_p(u_m) = \vartheta_p(a_m) - \vartheta_p(a_{m/q})$ pour un certain facteur premier q de m. Puisque $m/q < m$ et m est champion pour p, alors $\vartheta_p(a_m) > \vartheta_p(a_{m/q})$ et donc $\vartheta_p(u_m) > 0$, comme il fallait le prouver. Le lemme est ainsi démontré. ∎

Lemme 1.21 (Myerson [38]). *Pour tout entier strictement positif n, on a :*

$$\text{ppcm}(a_1, a_2, \ldots, a_n) = \prod_{m=1}^{n} u_m. \tag{1.3.10}$$

Démonstration. Il s'agit de montrer que pour tout nombre premier p, on a :

$$\vartheta_p(\text{ppcm}(a_1, a_2, \ldots, a_n)) = \vartheta_p\left(\prod_{m=1}^{n} u_m\right).$$

Soit donc p un nombre premier. Sans perte de généralité, nous supposons que p divise au moins l'un des nombres a_m, avec $1 \leq m \leq n$ (le résultat est évident dans le cas contraire). D'une part, on a :

$$\vartheta_p(\text{ppcm}(a_1, a_2, \ldots, a_n)) = \max_{1\leq i\leq n} \vartheta_p(a_i) = \vartheta_p(a_r),$$

où r est le plus grand champion pour p qui est inférieur ou égal à n. D'autre part, d'après les lemmes 1.17 et 1.20 et la remarque 1.19, on a :

$$\vartheta_p\left(\prod_{m=1}^{n} u_m\right) = \sum_{m=1}^{n} \vartheta_p(u_m) = \sum{}' \vartheta_p(u_m) = \sum_{m|r} \vartheta_p(u_m) = \vartheta_p\left(\prod_{m|r} u_m\right) = \vartheta_p(a_r),$$

où $\sum'$ est la somme étendue sur tous les champions $m \leq n$ pour p. En comparant les deux résultats, on en déduit que pour tout nombre premier p, on a :

$$\vartheta_p\left(\text{ppcm}(a_1, a_2, \ldots, a_n)\right) = \vartheta_p\left(\prod_{m=1}^{n} u_m\right).$$

Ce qui conclut au résultat du lemme et achève cette démonstration. ∎

Démonstration du théorème 1.13. Pour tout $m \in \mathbb{N}^*$, on écrit (en vertu de (1.3.4)) :

$$\prod_{1\leq j\leq m} a_j = \prod_{1\leq j\leq m} \prod_{d|j} u_d = \prod_{1\leq j\leq m} u_j^{\lfloor m/j\rfloor}.$$

Le membre de droite de (1.3.1) s'écrit donc :

$$\prod_{1\leq j\leq n} u_j^{\lfloor n/j\rfloor - \lfloor n/jb_1\rfloor - \lfloor n/jb_2\rfloor - \lfloor n/jb_3\rfloor - \ldots}.$$

Il suffit donc de montrer (en vertu du lemme 1.21) que pour tout entier strictement positif k, on a :

$$1 \leq k - \lfloor k/b_1\rfloor - \lfloor k/b_2\rfloor - \lfloor k/b_3\rfloor - \ldots,$$

(remarquer que $\lfloor\lfloor x\rfloor/n\rfloor = \lfloor x/n\rfloor$, $\forall x \in \mathbb{R}, \forall n \in \mathbb{N}^*$). Étant donné $k \in \mathbb{N}^*$, il existe $r \in \mathbb{N}^*$ tel que $k < b_{r+1}$. On a par suite :

$$\lfloor k/b_1\rfloor + \lfloor k/b_2\rfloor + \lfloor k/b_3\rfloor + \cdots \leq k/b_1 + k/b_2 + \cdots + k/b_r = k\sum_{l=1}^{r} \frac{1}{b_l} < k.$$

Ceci entraîne que le nombre $k - \lfloor k/b_1\rfloor - \lfloor k/b_2\rfloor - \lfloor k/b_3\rfloor - \ldots$ est un entier strictement positif, comme il fallait le prouver. Le théorème est démontré. ∎

Remarque 1.22. *Une étude plus profonde des suites à forte divisibilité est donnée dans le chapitre 3.*

1.4 Majoration effective du nombre $\mathrm{ppcm}(1,2,\ldots,n)$

D'après la section §1.3, on comprend bien que l'étude des propriétés arithmétiques de certains coefficients multinomiaux permet d'obtenir des majorations effectives pour le nombre $\mathrm{ppcm}(1,2,\ldots,n)$. Dans cette section, nous présentons l'estimation de Hanson [23] qui utilise la relation de l'exemple 1.15 et aboutit au théorème suivant :

Théorème 1.23 (Hanson [23]). *Pour tout entier $n \geq 1$, on a :*

$$\mathrm{ppcm}(1,2,\ldots,n) \leq 3^n.$$

D'après l'exemple 1.15, on a :

$$\mathrm{ppcm}(1,2,\ldots,n) \leq C(n) := \frac{n!}{\lfloor n/2\rfloor!\lfloor n/3\rfloor!\lfloor n/7\rfloor!\lfloor n/43\rfloor!\cdots}, \tag{1.4.1}$$

où $2,3,7,43,\ldots$ est la suite de Sylvester (déjà définie dans la partie §1.3). Notons que le choix de cette suite étant heuristique ; il s'appuie sur le fait que la somme des inverses de ses termes converge vers 1 plus vite que toute autre série de la forme $\sum_{\ell\geq 1}\frac{1}{b_\ell}$, où $(b_\ell)_\ell$ est une suite d'entiers satisfaisant aux conditions du théorème 1.13. Cela permet d'exploiter le théorème 1.13 d'une façon optimale. Dans tout ce qui suit, on désigne par $(b_\ell)_\ell$ la suite de Sylvester.

Lemme 1.24 (Hanson [23]). *Soit $n \in \mathbb{N}^*$ et désignons par k l'unique entier strictement positif vérifiant $b_k \leq n < b_{k+1}$. Alors, on a :*

$$C(n) \leq \frac{n^n}{\lfloor n/b_1\rfloor^{\lfloor n/b_1\rfloor}\lfloor n/b_2\rfloor^{\lfloor n/b_2\rfloor}\cdots\lfloor n/b_k\rfloor^{\lfloor n/b_k\rfloor}}.$$

Démonstration. Si un entier strictement positif t possède une partition sous la forme $t = t_1 + t_2 + \cdots + t_k$, avec $t_\ell \in \mathbb{N}^*$ $(\forall \ell \in \{1,\ldots,k\})$, alors on a (en vertu de la formule multinomiale) :

$$t^t = (t_1+t_2+\cdots+t_k)^t = \sum_{i_1+i_2+\cdots+i_k=t}\frac{t!}{i_1!i_2!\cdots i_k!}{t_1}^{i_1}{t_2}^{i_2}\cdots{t_k}^{i_k} \geq \frac{t!}{t_1!t_2!\cdots t_k!}{t_1}^{t_1}{t_2}^{t_2}\cdots{t_k}^{t_k}.$$

Par suite, en appliquant cette dernière inégalité pour $t := \sum_{\ell=1}^{k}\lfloor n/b_\ell\rfloor \leq n\sum_{\ell\geq 1}1/b_\ell = n$, $t_\ell := \lfloor n/b_\ell\rfloor$ $(\forall \ell \in \{1,\ldots,k\})$ et en tenant compte du fait que $\lfloor n/b_\ell\rfloor = 0$ $(\forall \ell \geq k+1)$

(car : $n < b_{k+1} < b_{k+2} < \ldots$), on aboutit à :

$$C(n) = \frac{n(n-1)\cdots(t+1)t!}{\lfloor n/b_1\rfloor!\lfloor n/b_2\rfloor!\cdots\lfloor n/b_k\rfloor!} \leq \frac{n^{n-t}t^t}{\lfloor n/b_1\rfloor^{\lfloor n/b_1\rfloor}\lfloor n/b_2\rfloor^{\lfloor n/b_2\rfloor}\cdots\lfloor n/b_k\rfloor^{\lfloor n/b_k\rfloor}}.$$

Ce qui conclut (via l'inégalité : $n^{n-t}t^t \leq n^{n-t}n^t = n^n$) à l'estimation requise par le lemme et achève cette démonstration. ∎

Lemme 1.25 (Hanson [23]). *Soient ℓ et n deux entiers strictement positifs tels que $b_\ell \leq n$. Alors, on a :*

$$\frac{(n/b_\ell)^{n/b_\ell}}{\lfloor n/b_\ell\rfloor^{\lfloor n/b_\ell\rfloor}} \leq \left(\frac{en}{b_\ell}\right)^{(b_\ell-1)/b_\ell}. \tag{1.4.2}$$

Démonstration. Pour $n = b_\ell$, le résultat est trivial. Supposons pour la suite que $n > b_\ell$ et montrons préalablement que l'on a :

$$((n-b_\ell+1)/b_\ell)^{(n-b_\ell+1)/b_\ell} \leq \lfloor n/b_\ell\rfloor^{\lfloor n/b_\ell\rfloor}. \tag{1.4.3}$$

Puisque $\lfloor n/b_\ell\rfloor > n/b_\ell - 1$, on a : $b_\ell\lfloor n/b_\ell\rfloor \geq n - b_\ell + 1$, ce qui entraîne que $\lfloor n/b_\ell\rfloor \geq (n-b_\ell+1)/b_\ell$. Maintenant, si $(n-b_\ell+1)/b_\ell \geq 1$, l'inégalité (1.4.3) découle de la croissance de la fonction $x \mapsto x^x$ sur l'intervalle $[1,+\infty[$. Par contre, si $(n-b_\ell+1)/b_\ell < 1$, alors l'inégalité (1.4.3) est évidente (puisque $n > b_\ell \Rightarrow \lfloor n/b_\ell\rfloor^{\lfloor n/b_\ell\rfloor} \geq 1$), comme il fallait le prouver. Il s'ensuit (en vertu de (1.4.3) et de l'inégalité $\left(1+\frac{1}{x}\right)^x \leq e$ $(\forall x > 0)$) que :

$$\begin{aligned}\frac{(n/b_\ell)^{n/b_\ell}}{\lfloor n/b_\ell\rfloor^{\lfloor n/b_\ell\rfloor}} &\leq \frac{(n/b_\ell)^{n/b_\ell}}{((n-b_\ell+1)/b_\ell)^{(n-b_\ell+1)/b_\ell}} \\ &= \left(1+\frac{1}{(n-b_\ell+1)/(b_\ell-1)}\right)^{((n-b_\ell+1)/(b_\ell-1))\times((b_\ell-1)/b_\ell)}\left(\frac{n}{b_\ell}\right)^{(b_\ell-1)/b_\ell} \\ &\leq \left(\frac{en}{b_\ell}\right)^{(b_\ell-1)/b_\ell}.\end{aligned}$$

Ce qui termine cette démonstration. ∎

Lemme 1.26 (Hanson [23]). *Soit n un entier ≥ 7 et k l'unique entier strictement positif vérifiant $b_k \leq n < b_{k+1}$. Alors, on a :*

$$k \leq \log_2(\log_2 n) + 2,$$

où $\log_2$ désigne le logarithme de base 2 (i.e., $\log_2 x = \frac{\log x}{\log 2}$ $(\forall x > 0)$).

Démonstration. Puisque $b_3 = 7 \leq n$, alors on a nécessairement $k \geq 3$. Par ailleurs, en se servant de (1.3.2), on montre facilement par récurrence que pour tout entier $\ell \geq 3$, on a : $b_\ell \geq 2^{2^{\ell-2}} + 1$. Il s'ensuit de cette dernière inégalité (appliquée à $\ell = k$) que :

$$k \leq \log_2 \log_2 (b_k - 1) + 2 \leq \log_2 \log_2 n + 2.$$

Le lemme est démontré. ∎

Démonstration du théorème 1.23. En utilisant un logiciel de calcul (Maple ou Mathematica par exemple), on vérifie que le résultat du théorème est valable pour tout entier $n < 4500$. Supposons pour la suite que $n \geq 4500$ et désignons par k l'unique entier strictement positif vérifiant $b_k \leq n < b_{k+1}$. D'après les lemmes 1.24 et 1.25, on a :

$$C(n) \leq \frac{n^n}{\lfloor n/b_1 \rfloor^{\lfloor n/b_1 \rfloor} \cdots \lfloor n/b_k \rfloor^{\lfloor n/b_k \rfloor}} \leq \frac{n^n (en/b_1)^{(b_1-1)/b_1} \cdots (en/b_k)^{(b_k-1)/b_k}}{(n/b_1)^{n/b_1} \cdots (n/b_k)^{n/b_k}}. \tag{1.4.4}$$

Considérons la suite $(u_\ell)_{\ell \geq 1}$ donnée par : $u_\ell := b_1^{1/b_1} b_2^{1/b_2} \cdots b_\ell^{1/b_\ell}$ $(\forall \ell \geq 1)$ et montrons préalablement que :

$$u_\ell \leq 2,952 \quad (\forall \ell \in \mathbb{N}^*). \tag{1.4.5}$$

Il est immédiat que $(u_\ell)_{\ell \geq 1}$ est strictement croissante. D'autre part, pour $\ell \in \mathbb{N}^*$, on a (en vertu de (1.3.2)) : ${b_\ell}^2 = b_{\ell+1} + b_\ell - 1 \geq b_{\ell+1} + 1 > b_{\ell+1}$ et $b_{\ell+1} = {b_\ell}^2 - b_\ell + 1 > {b_\ell}^2 - 2b_\ell + 1 = (b_\ell - 1)^2$, soit :

$$b_\ell^2 > b_{\ell+1} > (b_\ell - 1)^2 \quad (\forall \ell \in \mathbb{N}^*).$$

Cette double-inégalité entraîne que pour tout entier $\ell \geq 3$, on a :

$$\frac{\log\left(b_{\ell+1}^{1/b_{\ell+1}}\right)}{\log\left(b_\ell^{1/b_\ell}\right)} = \frac{b_\ell \log(b_{\ell+1})}{b_{\ell+1} \log(b_\ell)} < \frac{2b_\ell}{b_{\ell+1}} < \frac{2b_\ell}{(b_\ell - 1)^2} < \frac{1}{2}.$$

En combinant cela avec l'inégalité $\log\left({b_6}^{1/b_6}\right) \leq 5 \cdot 10^{-6}$, on obtient :

$$\begin{aligned}
\sum_{\ell=1}^{+\infty} \log\left(b_\ell^{1/b_\ell}\right) &= \sum_{\ell=1}^{5} \log\left(b_\ell^{1/b_\ell}\right) + \sum_{\ell=6}^{+\infty} \log\left(b_\ell^{1/b_\ell}\right) \\
&\leq 1,0824 + \log\left(b_6^{1/b_6}\right) \sum_{\ell \geq 0} \left(\frac{1}{2}\right)^\ell \\
&\leq 1,0824 + 10^{-5}.
\end{aligned}$$

D'où : $u_m \leq \lim\limits_{\ell\to+\infty} b_1^{1/b_1} b_2^{1/b_2}\cdots b_\ell^{1/b_\ell} \leq e^{1,0824+10^{-5}} \leq 2,952$ $(\forall m \in \mathbb{N}^*)$, comme nous l'avons prétendu. Par ailleurs, on a (en vertu de (1.3.3)) :

$$\frac{b_1-1}{b_1}+\frac{b_2-1}{b_2}+\cdots+\frac{b_k-1}{b_k} = k-1+\frac{1}{b_1b_2\cdots b_k} = k-1+\frac{1}{b_{k+1}-1} \tag{1.4.6}$$

et

$$\frac{1}{b_1}+\frac{1}{b_2}+\cdots+\frac{1}{b_k} = 1-\frac{1}{b_1b_2\cdots b_k} = 1-\frac{1}{b_{k+1}-1}. \tag{1.4.7}$$

En combinant les estimations (1.4.4), (1.4.5), (1.4.6), (1.4.7) et le lemme 1.26, on aboutit à :

$$\begin{aligned} C(n) &\leq \frac{n^n}{\left(n^{1/b_1+1/b_2+\cdots+1/b_k}\right)^n}\cdot\frac{(en)^{(b_1-1)/b_1+(b_2-1)/b_2+\cdots+(b_k-1)/b_k}\left({b_1}^{1/b_1}{b_2}^{1/b_2}\cdots{b_k}^{1/b_k}\right)^n}{b_1^{(b_1-1)/b_1}b_2^{(b_2-1)/b_2}\cdots b_k^{(b_k-1)/b_k}} \\ &\leq n^{n/(b_{k+1}-1)}(en)^{k-1+1/(b_{k+1}-1)}(2,952)^n \\ &\leq e^k n^{k+1}(2,952)^n \leq (en)^{\log_2(\log_2 n)+3}(2,952)^n. \end{aligned}$$

Puisque la fonction $x \mapsto (ex)^{\frac{\log_2(\log_2 x)+3}{x}}$ est décroissante sur l'intervalle $[4500,+\infty[$, il s'ensuit que :

$$(en)^{\frac{\log_2(\log_2 n)+3}{n}} \leq (4500e)^{\frac{\log_2(\log_2 4500)+3}{4500}} \leq 1.014.$$

D'où : $C(n) \leq (1.014)^n(2.952)^n \leq 3^n$. Ce qui complète cette démonstration. ∎

Le corollaire suivant est une conséquence immédiate du théorème 1.23 et de la définition de la fonction ψ de Chebyshev.

Corollaire 1.27 (Hanson [23]). *Pour tout réel $x \geq 1$, on a :*

$$\psi(x) \leq x\log 3.$$

Corollaire 1.28 (Hanson [23]). *Pour tout réel $x \geq 2$, on a :*

$$\pi(x) \leq 1,25506\frac{x}{\log x},$$

où π désigne la fonction de comptage des nombres premiers.

Démonstration. En se servant d'un logiciel de calcul (Maple ou Mathematica par exemple), on vérifie que le résultat du théorème est valable pour tout $x < 350$. Supposons pour la suite que $x \geq 350$. En utilisant successivement la formule (1.2.6), l'inégalité triviale $\theta(t) \leq \psi(t)$ $(\forall t \geq 1)$, le corollaire 1.27 et l'estimation (1.2.7), on obtient :

$$\begin{aligned}
\pi(x) &= \frac{\theta(x)}{\log x} + \int_2^x \frac{\theta(t)}{t\log^2 t}\mathrm{d}t \\
&\leq \frac{\psi(x)}{\log x} + \int_2^x \frac{\psi(t)}{t\log^2 t}\mathrm{d}t \\
&\leq \frac{x\log 3}{\log x} + \log 3\int_2^x \frac{\mathrm{d}t}{\log^2 t} \\
&\leq \frac{x\log 3}{\log x}\left(\frac{1}{\sqrt{x}\log^2 x} + \frac{4}{\log^2 x}\right) \\
&\leq 1,25506\frac{x}{\log x}.
\end{aligned}$$

Ce qui complète cette démonstration. ∎

1.5 Minoration effective du nombre $\operatorname{ppcm}(1,2,\ldots,n)$

Nous présentons ici la démonstration de Nair [39] prouvant l'estimation :

$$\operatorname{ppcm}(1,2,\ldots,n) \geq 2^n \quad (\forall n \geq 7).$$

En fait, il existe dans la littérature mathématique des minorations bien meilleures, néanmoins celles-ci ne s'obtiennent pas de façon élémentaire. Notre préférence à cette méthode réside dans sa simplicité (on exploite l'intégrale $\int_0^1 x^n(1-x)^n\mathrm{d}x$ $(n \in \mathbb{N})$).

Théorème 1.29 (Nair [39])**.** *Pour tout entier $n \geq 7$, on a :*

$$d_n := \operatorname{ppcm}(1,2,\ldots,n) \geq 2^n. \tag{1.5.1}$$

Démonstration. Soient $k \in \mathbb{N}^*$, $\ell \in \{1,2,\ldots,k\}$ et considérons l'intégrale suivante :

$$I(k,\ell) := \int_0^1 x^{\ell-1}(1-x)^{k-\ell}\mathrm{d}x.$$

On a en vertu de la formule du binôme :

$$I(k,\ell) = \sum_{r=0}^{k-\ell}(-1)^r\binom{k-\ell}{r}\frac{1}{\ell+r}.$$

Ce qui entraîne que $I(k,\ell)d_k \in \mathbb{N}^*$ $(\forall k,\ell \in \mathbb{N}^*;\ 1 \leq \ell \leq k)$. D'autre part, en intégrant successivement par parties, on obtient :

$$I(k,\ell) = \frac{(k-\ell)}{\ell}\int_0^1 x^\ell (1-x)^{k-\ell-1}\mathrm{d}x = \cdots = \frac{(k-\ell)!}{\ell(\ell+1)\cdots(k-1)}\int_0^1 x^{k-1}\mathrm{d}x = \frac{1}{\ell\binom{k}{\ell}}.$$

Ce qui implique que :

$$\ell\binom{k}{\ell} \text{ divise } d_k \quad (\forall k,\ell \in \mathbb{N}^*;\ 1 \leq \ell \leq k). \tag{1.5.2}$$

Fixons $m \in \mathbb{N}^*$. D'après la relation (1.5.2), on a :

$$m\binom{2m}{m} \mid d_{2m} \mid d_{2m+1} \quad \text{et} \quad (2m+1)\binom{2m}{m} = (m+1)\binom{2m+1}{m+1} \mid d_{2m+1}.$$

Comme $\mathrm{pgcd}(m,2m+1)=1$, il s'ensuit que :

$$\mathrm{ppcm}\left(m\binom{2m}{m},(2m+1)\binom{2m}{m}\right) = m(2m+1)\binom{2m}{m} \text{ divise } d_{2m+1}. \tag{1.5.3}$$

Par ailleurs, on a en vertu de la formule du binôme :

$$4^m = (1+1)^{2m} = \sum_{\ell=0}^{2m}\binom{2m}{\ell} \leq (2m+1)\max\left\{\binom{2m}{\ell};\ 0 \leq \ell \leq 2m\right\} = (2m+1)\binom{2m}{m}.$$

En combinant cette dernière inégalité avec (1.5.3), on en déduit que :

$$d_{2m+1} \geq m(2m+1)\binom{2m}{m} \geq m4^m \geq 2^{2m+1} \quad (\forall m \geq 2)$$

et

$$d_{2m+2} \geq d_{2m+1} \geq m4^m \geq 2^{2m+2} \quad (\forall m \geq 4).$$

L'estimation requise par le théorème découle de ces deux dernière inégalités et de l'inégalité triviale $d_8 \geq 2^8$. Le théorème est ainsi démontré. ∎

Corollaire 1.30 (Nair [39])**.** *Pour tout entier $n \geq 7$, on a :*

$$\pi(n) \geq \frac{n\log 2}{\log n}.$$

Démonstration. Le résultat découle immédiatement de (1.2.8) et du fait que l'on a (en vertu du théorème 1.29) : $\psi(n) \geq n\log 2$ $(\forall n \geq 7)$. ∎

Un autre résultat très important dû à Nair est le suivant.

Théorème 1.31 (Nair [39]). *Pour tout entier strictement positif n, on a :*

$$d_n := \mathrm{ppcm}(1,2,\ldots,n) = \mathrm{ppcm}\left(\binom{n}{1}, 2\binom{n}{2}, \ldots, n\binom{n}{n}\right).$$

Démonstration. D'après la relation (1.5.2), on a pour tout $m \in \{1,2,\ldots,n\}$: $m\binom{n}{m}$ divise d_n. Ce qui entraîne que :

$$\mathrm{ppcm}\left(\binom{n}{1}, 2\binom{n}{2}, \ldots, m\binom{n}{m}\right) \text{ divise } d_n.$$

D'autre part, puisqu'on a visiblement m divise $m\binom{n}{m}$ pour tout $m \in \{1,2,\ldots,n\}$, il s'ensuit que :

$$d_n \text{ divise } \mathrm{ppcm}\left(\binom{n}{1}, 2\binom{n}{2}, \ldots, n\binom{n}{n}\right).$$

Ce qui conclut à l'identité requise par le théorème et complète cette démonstration. ∎

Corollaire 1.32 (Nair [39]). *Pour tout entier strictement positif n, on a :*

$$d_n := \mathrm{ppcm}\,(1,2,\ldots,n) \leq 4^n. \tag{1.5.4}$$

Démonstration. On procède par récurrence sur n. Pour $n = 1$, l'inégalité (1.5.4) est triviale. Fixons $m \in \mathbb{N}^*$ et supposons que (1.5.4) est vraie pour tout entier strictement positif $n < 2m$. Nous montrons que (1.5.4) reste vraie pour $n = 2m$ et pour $n = 2m+1$, ce qui conclura au résultat requis. Premièrement, on vérifie facilement que l'on a l'identité :

$$k\binom{2m}{k}\binom{2m-k}{m-k} = k\binom{m}{k}\binom{2m}{m} \quad (\forall k \in \{1,2,\ldots,m\}). \tag{1.5.5}$$

Cette dernière entraîne que $k\binom{2m}{k}$ divise $k\binom{m}{k}\binom{2m}{m}$ $(\forall k \in \{1,2,\ldots,m\})$. D'autre part, le membre de droite de (1.5.5) est (en vertu du théorème 1.31) un diviseur de $d_m\binom{2m}{m}$. Par conséquent, on a pour tout $k \in \{1,2,\ldots,m\}$:

$$k\binom{2m}{k} \text{ divise } d_m\binom{2m}{m}. \tag{1.5.6}$$

Puisque pour tout $k \in \{m+1,\ldots,2m\}$, on a : $k\binom{2m}{k} = (2m-k+1)\binom{2m}{2m-k+1}$ et $1 \leq 2m-k+1 \leq m$, il s'ensuit que la relation (1.5.6) est valable pour tout $k \in \{1,2,\ldots,2m\}$. En combinant cela avec le théorème 1.31, on obtient que : d_{2m} divise $d_m\binom{2m}{m}$. En procédant comme ci-dessus et en utilisant l'identité suivante :

$$k\binom{2m+1}{k}\binom{2m+1-k}{m+1-k} = k\binom{m+1}{k}\binom{2m+1}{m+1} \quad (\forall k \in \{1,2,\ldots,m+1\}),$$

au lieu de (1.5.5), on obtient que : d_{2m+1} divise $d_{m+1}\binom{2m+1}{m+1}$. On a par conséquent :

$$d_{2m} \leq d_m \binom{2m}{m} \leq 4^m (1+1)^{2m} = 4^{2m}$$

et

$$d_{2m+1} \leq d_{m+1} \binom{2m+1}{m+1} \leq 4^{m+1} \frac{(1+1)^{2m+1}}{2} = 4^{2m+1}.$$

Ce qui achève cette récurrence et complète la démonstration du corollaire. ∎

1.6 Minorations effectives du ppcm d'une suite arithmétique

Dans la continuation, Farhi [17] a présenté une méthode permettant d'obtenir des minorations effectives et non triviales du ppcm d'une suite arithmétique et d'une certaine classe de suites quadratiques. Cette partie est consacrée à la démonstration de quelques résultats portant sur le ppcm d'une suite arithmétique. On parlera aussi d'une certaine estimation conjecturée dans [17] et démontrée par Hong [25].

Théorème 1.33 (Farhi [17]). *Soit $(u_k)_{k\in\mathbb{N}}$ une suite arithmétique d'entiers, de raison r et de premier terme u_0 strictement positifs et premiers entre eux. Alors, pour tout entier naturel n, on a :*

$$\operatorname{ppcm}(u_0, u_1, \ldots, u_n) \geq u_0(1+r)^{n-1}. \tag{1.6.1}$$

Si de plus n est multiple de $(r+1)$, on a :

$$\operatorname{ppcm}(u_0, u_1, \ldots, u_n) \geq u_0(1+r)^{n}. \tag{1.6.2}$$

La démonstration de ce théorème est partagée en plusieurs lemmes.

Lemme 1.34 (Farhi [17]). *Soit $(u_k)_{k\in\mathbb{N}}$ une suite d'entiers non nuls, strictement croissante. Alors, pour tout entier naturel n, le produit $u_0u_1\cdots u_n$ divise le nombre :*

$$M_n := \operatorname{ppcm}(u_0, u_1, \ldots, u_n) \cdot \operatorname{ppcm}\left\{ \prod_{\substack{0\leq i\leq n \\ i\neq j}} (u_i - u_j);\ j = 0, 1, \ldots, n \right\}.$$

Démonstration. En substituant $x = 0$ dans la décomposition en éléments simples de la fraction rationnelle $1/(x+u_0)(x+u_1)\dots(x+u_n)$, on obtient :

$$\sum_{j=0}^{n} \frac{1}{u_j} \cdot \frac{1}{\prod_{\substack{0\leq i\leq n\\ i\neq j}}(u_i - u_j)} = \frac{1}{u_0 u_1 \cdots u_n}.$$

Le résultat requis en découle en multipliant les deux membres de cette dernière identité par M_n. ∎

Lemme 1.35 (Farhi [17]). *Soit $(u_k)_{k\in\mathbb{N}}$ une progression arithmétique strictement croissante d'entiers non nuls. Alors, pour tout entier naturel n, on a :*

$$\operatorname{ppcm}(u_0, u_1, \dots, u_n) \text{ est multiple de } \frac{u_0 u_1 \cdots u_n}{n!\,(\operatorname{pgcd}(u_0, u_1))^n}.$$

Démonstration. On peut supposer que $\operatorname{pgcd}(u_0, u_1) = 1$ (quitte à remplacer la suite $(u_k)_k$ par la suite $(v_k)_k$ de terme général $v_k := u_k/\operatorname{pgcd}(u_0, u_1)$ $(\forall k \in \mathbb{N})$). D'après le lemme 1.34, le nombre $\operatorname{ppcm}(u_0, u_1, \dots, u_n)$ est multiple du nombre rationnel :

$$\frac{u_0 u_1 \cdots u_n}{\operatorname{ppcm}\left\{\prod_{\substack{0\leq i\leq n\\ i\neq j}}(u_i - u_j);\ 0 \leq j \leq n\right\}}.$$

En désignant par $r \in \mathbb{N}^*$ la raison de la suite arithmétique $(u_k)_{k\in\mathbb{N}}$, on a pour tout $j \in \{0, 1, \dots, n\}$:

$$\prod_{\substack{0\leq i\leq n\\ i\neq j}} (u_i - u_j) = (-1)^j j!(n-j)! r^n.$$

Par conséquent, on a :

$$\operatorname{ppcm}\left\{\prod_{\substack{0\leq i\leq n\\ i\neq j}} (u_i - u_j);\ 0 \leq j \leq n\right\} = r^n n!.$$

Ce qui entraîne que le nombre $\operatorname{ppcm}(u_0, u_1, \dots, u_n)$ est multiple du nombre rationnel $\frac{u_0 u_1 \cdots u_n}{r^n n!}$. Par ailleurs, puisque les entiers u_0 et u_1 sont premiers entre eux, alors r est premier avec tous les termes de la suite $(u_k)_{k\in\mathbb{N}}$, il est donc premier avec le produit $u_0 u_1 \cdots u_n$. Enfin, le lemme de Gauss permet de déduire que le nombre $\operatorname{ppcm}(u_0, u_1, \dots, u_n)$ est multiple du nombre rationnel $\frac{u_0 u_1 \cdots u_n}{n!}$. Ce qui complète cette démonstration. ∎

Dans les deux lemmes suivants, nous fixons une suite arithmétique $(u_k)_{k\in\mathbb{N}}$, ayant pour raison r et pour premier terme u_0, avec $r, u_0 \in \mathbb{N}^*$. Pour tout $n \in \mathbb{N}$, nous désignons par $(v_{n,k})_{0\leq k\leq n}$ la suite finie de nombres rationnels définie par $v_{n,k} := \frac{u_k u_{k+1}\cdots u_n}{(n-k)!}$ $(\forall k \in \{0, 1, \ldots, n\})$.

Lemme 1.36 (Farhi [17]). *Pour tout entier naturel n, la suite $(v_{n,k})_{0\leq k\leq n}$ atteint son maximum en $k_n \in \{0, 1, \ldots, n\}$, défini par :*

$$k_n := \max\left\{0, \left\lfloor \frac{n-u_0}{r+1}\right\rfloor + 1\right\}. \tag{1.6.3}$$

Démonstration. Pour tout $k \in \{0, 1, \ldots, n-1\}$, on a :

$$\frac{v_{n,k+1}}{v_{n,k}} = \frac{n-k}{u_k} = \frac{n-k}{u_0+kr};$$

d'où :

$$v_{n,k+1} \geq v_{n,k} \Longleftrightarrow k \leq \frac{n-u_0}{r+1} \Longleftrightarrow k \leq \left\lfloor \frac{n-u_0}{r+1}\right\rfloor.$$

Deux cas peuvent se présenter. Si $n < u_0$, alors la suite $(v_{n,k})_{0\leq k\leq n}$ est décroissante et elle atteint donc son maximum en $k = 0$. Si on a au contraire $n \geq u_0$, alors la suite $(v_{n,k})_{0\leq k\leq n}$ croit jusqu'au terme d'indice $\left\lfloor \frac{n-u_0}{r+1}\right\rfloor + 1$ et elle décroit au-delà de ce dernier ; elle atteint donc sont maximum en $k = \left\lfloor \frac{n-u_0}{r+1}\right\rfloor + 1$. Ce qui conclut au résultat du lemme et achève cette démonstration. ∎

Lemme 1.37 (Farhi [17]). *Pour tout $k \in \{0, 1, \ldots, n\}$, on a :*

$$v_{n,k} = \frac{r^{n-k+1}}{\int_0^1 x^{k+\frac{u_0}{r}-1}(1-x)^{n-k}\mathrm{d}x}. \tag{1.6.4}$$

Démonstration. D'après les propriétés usuelles des fonctions Γ et β d'Euler, on a :

$$\begin{aligned} v_{n,k} = \frac{u_k\cdots u_n}{(n-k)!} &= \frac{u_k(u_k+r)\cdots(u_k+(n-k)r)}{(n-k)!} \\ &= r^{n-k+1}\cdot\frac{\frac{u_k}{r}(\frac{u_k}{r}+1)\cdots(\frac{u_k}{r}+n-k)}{(n-k)!} \\ &= r^{n-k+1}\frac{\Gamma(\frac{u_k}{r}+n-k+1)}{\Gamma(\frac{u_k}{r})\cdot\Gamma(n-k+1)} \\ &= \frac{r^{n-k+1}}{\beta(\frac{u_k}{r}, n-k+1)}, \end{aligned}$$

L'identité (1.6.4) découle de la formule intégrale de la fonction β. Ce qui complète cette démonstration. ∎

Démonstration du théorème 1.33. Fixons $n \in \mathbb{N}$ et montrons l'inégalité (1.6.1) du théorème. Étant donné $k \in \{0, 1, \ldots, n\}$, le nombre $\operatorname{ppcm}(u_0, u_1, \ldots, u_n)$ est visiblement un multiple du nombre $\operatorname{ppcm}(u_k, u_{k+1}, \ldots, u_n)$, qui est lui même (d'après le lemme 1.35) multiple de $v_{n,k} := \frac{u_k u_{k+1} \cdots u_n}{(n-k)!}$. En combinant cela avec le lemme 1.36, on obtient que :

$$\operatorname{ppcm}(u_0, u_1, \ldots, u_n) \geq \max\{v_{n,k};\ 0 \leq k \leq n\} = v_{n,k_n}. \tag{1.6.5}$$

Il ne reste plus qu'à trouver une bonne minoration pour le nombre v_{n,k_n}. Pour surmonter certaines difficultés de calcul, nous allons plutôt minorer le nombre v_{n,k^*}, où $k^* := \left\lfloor \frac{n-1}{r+1} + 1 \right\rfloor \in \{0, 1, \ldots, n\}$ et on conclura au résultat requis via l'inégalité $v_{n,k_n} \geq v_{n,k^*}$. D'après le lemme 1.37, on a :

$$v_{n,k^*} = \frac{r^{n-k^*+1}}{\int_0^1 x^{k^*+\frac{u_0}{r}-1}(1-x)^{n-k^*}\mathrm{d}x}. \tag{1.6.6}$$

Par ailleurs, comme $\frac{n-1}{r+1} < k^* \leq \frac{n+r}{r+1}$, il s'ensuit que :

$$r^{n-k^*+1} \geq r^{\frac{(n-1)r}{r+1}+1}. \tag{1.6.7}$$

De même, on a pour tout $x \in [0, 1]$:

$$x^{k^*+\frac{u_0}{r}-1}(1-x)^{n-k^*} \leq x^{\frac{n-1}{r+1}+\frac{u_0}{r}-1}(1-x)^{\frac{(n-1)r}{r+1}}.$$

En intégrant les deux membres de cette dernière inégalité sur l'intervalle $[0, 1]$, on obtient :

$$\int_0^1 x^{k^*+\frac{u_0}{r}-1}(1-x)^{n-k^*}\mathrm{d}x \leq \int_0^1 \{x(1-x)^r\}^{\frac{n-1}{r+1}} x^{\frac{u_0}{r}-1}\mathrm{d}x. \tag{1.6.8}$$

L'estimation (1.6.8) avec l'inégalité $x(1-x)^r \leq \frac{r^r}{(r+1)^{r+1}}$ $(\forall x \in [0, 1])$, entraînent que :

$$\int_0^1 x^{k^*+\frac{u_0}{r}-1}(1-x)^{n-k^*}\mathrm{d}x \leq \frac{r^{\frac{(n-1)r}{r+1}}}{(r+1)^{n-1}} \cdot \frac{r}{u_0}. \tag{1.6.9}$$

En combinant les estimations (1.6.5), (1.6.6), (1.6.7) et (1.6.9), on aboutit à :

$$\operatorname{ppcm}(u_0, u_1, \ldots, u_n) \geq v_{n,k_n} \geq v_{n,k^*} \geq u_0(r+1)^{n-1},$$

comme il fallait le prouver. La minoration (1.6.2) du théorème se démontre de la même façon en travaillons cette fois-ci avec l'entier naturel $k^{**} := \frac{n}{r+1}$ au lieu de k^*. Ce qui complète cette démonstration. ■

Farhi [17] a conjecturé que l'estimation (1.6.2) est vraie pour tout $n \in \mathbb{N}$. Une démonstration de cette conjecture, établie par Hong [25], est fournie dans le théorème suivant :

Théorème 1.38 (Hong [25]). *Soit $(u_k)_{k\in\mathbb{N}}$ une suite arithmétique d'entiers, de raison $r \in \mathbb{N}^*$ et dont le premier terme u_0 est strictement positif et premier avec r. Alors, pour tout entier naturel n, on a :*

$$\operatorname{ppcm}(u_0, u_1, \ldots, u_n) \geq u_0(1+r)^n. \tag{1.6.10}$$

Démonstration. On procède par récurrence pour montrer que $v_{n,k_n} \geq u_0(1+r)^n$ ($\forall n \in \mathbb{N}$), où $k_n \in \{0, 1, \ldots, n\}$ est déjà défini dans le lemme 1.36, ce qui conclura au résultat requis (via (1.6.5)). En vertu du lemme 1.36, on a pour tout entier naturel $n \leq u_0$:

$$v_{n,k_n} \geq v_{n,0} = \frac{u_0 u_1 \cdots u_n}{n!} = u_0(u_0+r)\left(\frac{u_0}{2}+r\right)\cdots\left(\frac{u_0}{n}+r\right) \geq u_0(1+r)^n. \tag{1.6.11}$$

Ce qui montre en particulier que la propriété requise est vraie pour $n \in \{0, 1\}$ (car $u_0 \geq 1$). Soit n un entier strictement positif. Supposons que $v_{n,k_n} \geq u_0(1+r)^n$ et montrons que $v_{n+1,k_{n+1}} \geq u_0(1+r)^{n+1}$. Si $n \leq u_0$, le résultat découle de (1.43). Supposons pour la suite que $n > u_0$. On vérifie facilement (à partir de la définition de k_n) que $k_n \leq k_{n+1} \leq k_n + 1$; ce qui nous amène à distinguer les deux cas suivants :

• **<u>1er cas :</u>** (si $k_{n+1} = k_n$). Dans ce cas, on a :

$$v_{n+1,k_{n+1}} = v_{n+1,k_n} = \frac{u_{k_n} u_{k_n+1} \cdots u_{n+1}}{(n+1-k_n)!} = v_{n,k_n} \cdot \frac{u_{n+1}}{n+1-k_n}. \tag{1.6.12}$$

Par ailleurs, on vérifie facilement (en se servant de l'égalité $k_n = k_{n+1}$) que :

$$\frac{n+1-u_0}{r+1} < k_n.$$

Cette dernière entraîne que :

$$u_{n+1} - (r+1)(n+1-k_n) = u_0 - (n+1) + k_n(r+1) > 0.$$

D'où l'on tire :

$$\frac{u_{n+1}}{n+1-k_n} > (r+1). \tag{1.6.13}$$

En combinant (1.6.12), (1.6.13) et l'hypothèse de récurrence, on aboutit à :

$$v_{n+1,k_{n+1}} \geq v_{n,k_n}(r+1) \geq u_0(1+r)^n(1+r) = u_0(1+r)^{n+1},$$

comme il fallait le prouver.

• **2nd cas :** (si $k_{n+1} = k_n + 1$). Dans ce cas, on a :

$$v_{n+1,k_{n+1}} = v_{n+1,k_n+1} = \frac{u_{k_n+1}\cdots u_{n+1}}{(n-k_n)!} = v_{n,k_n}\cdot\frac{u_{n+1}}{u_{k_n}}. \tag{1.6.14}$$

Par ailleurs, on vérifie facilement (en se servant de l'égalité $k_{n+1} = k_n + 1$) que :

$$k_n \leq \frac{n+1-u_0}{r+1}.$$

Cette dernière entraîne que :

$$\begin{aligned} u_{n+1} - (r+1)u_{k_n} &= u_0 + (n+1)r - (r+1)u_0 - k_n r(r+1) \\ &\geq nr + r - u_0 r - r(n+1-u_0) = 0. \end{aligned}$$

D'où l'on tire :

$$\frac{u_{n+1}}{u_{k_n}} \geq (r+1). \tag{1.6.15}$$

En combinant (1.6.14) et (1.6.15) et l'hypothèse de récurrence, on a abouti à :

$$v_{n+1,k_{n+1}} \geq v_{n,k_n}(r+1) \geq u_0(1+r)^n(1+r) = u_0(1+r)^{n+1}.$$

Ce qui achève cette récurrence et complète la preuve du théorème. ∎

1.7 Minorations effectives du ppcm de certaines suites quadratiques

Dans cette section, nous présentons les résultats de Farhi [17] portant sur l'estimation du plus petit commun multiple d'une certaine classe de progressions quadratiques. On parlera ensuite d'une amélioration remarquable établie par Oon [41] en 2013. Notons que cette amélioration est adaptable à une généralisation importante qu'on discutera dans la section suivante.

Théorème 1.39 (Farhi [17]). *Soient $n \in \mathbb{N}$ et $(u_k)_{k\in\mathbb{N}}$ la suite d'entiers de terme général donné par :*

$$u_k := ak(k+t) + b \qquad (\forall k \in \mathbb{N}),$$

avec $a, b \in \mathbb{N}^*$, $t \in \mathbb{N}$ et $\operatorname{pgcd}(a,b) = 1$. Alors, on a :

$$\operatorname{ppcm}(u_0, u_1, \ldots, u_n) \geq \begin{cases} 2b\left(\frac{a}{4}\right)^n & \text{si } t = 0, \\ \frac{b}{t2^t}\left(\frac{a}{4}\right)^n & \text{si } t \geq 1. \end{cases} \tag{1.7.1}$$

Démonstration. D'après le lemme 1.34, le nombre $\operatorname{ppcm}(u_0, u_1, \ldots, u_n)$ est multiple du nombre rationnel :

$$R := \frac{u_0 u_1 \cdots u_n}{\operatorname{ppcm}\left\{\prod_{\substack{0\leq i\leq n \\ i\neq j}}(u_i - u_j);\ j = 0, 1, \ldots, n\right\}}.$$

D'autre part, on vérifie facilement que pour tout $j \in \{0, 1, \ldots, n\}$, on a :

$$\prod_{\substack{0\leq i\leq n \\ i\neq j}} (u_i - u_j) = \begin{cases} (-1)^j a^n \frac{(n-j)!(n+j)!}{2} & \text{si } t = 0, \\ (-1)^j a^n \frac{(n-j)!(n+j+t)!}{\Phi(j,t)} \frac{1}{2j+t} & \text{si } t \geq 1. \end{cases} \tag{1.7.2}$$

où $\Phi(j,t) := 1$ si $t = 1$ et $\Phi(j,t) := (j+1)\cdots(j+t-1)$ si $t \geq 2$. Puisque $(n-j)!(n+j+t)!$ divise $(2n+t)!$ (car $\frac{(2n+t)!}{(n-j)!(n+j+t)!} = \binom{2n+t}{n-j} \in \mathbb{N}^*$) et pour tout $t \geq 1$, $\Phi(j,t)$ est multiple de $(t-1)!$ (car $\frac{\Phi(j,t)}{(t-1)!} = \binom{j+t-1}{t-1} \in \mathbb{N}^*$), on en déduit que le produit $\prod_{\substack{0\leq i\leq n \\ i\neq j}}(u_i - u_j)$ divise l'entier strictement positif $f(t,n)$ défini par :

$$f(t,n) := \begin{cases} a^n \frac{(2n)!}{2} & \text{si } t = 0, \\ a^n \frac{(2n+t)!}{(t-1)!} & \text{si } t \geq 1. \end{cases} \tag{1.7.3}$$

Comme $f(t,n)$ est indépendant de $j \in \{0, 1, \ldots, n\}$, il s'ensuit que :

$$\operatorname{ppcm}\left\{\prod_{\substack{0\leq i\leq n \\ i\neq j}} (u_i - u_j);\ j = 0, 1, \ldots, n\right\} \quad \text{divise} \quad f(t,n).$$

Cette dernière relation entraîne que R est multiple de $\frac{u_0 u_1 \cdots u_n}{f(t,n)}$. Par conséquent, l'entier $\operatorname{ppcm}(u_0, u_1, \ldots, u_n)$ est aussi multiple de $\frac{u_0 u_1 \cdots u_n}{f(t,n)}$. Par ailleurs, puisque a^n est premier

avec tous les termes de la suite $(u_k)_{k\in\mathbb{N}}$ (car $\text{pgcd}(a,b)=1$) et $f(t,n)$ est multiple de a^n (par définition), alors (en vertu du lemme de Gauss) l'entier $\text{ppcm}\,(u_0,u_1,\ldots,u_n)$ est multiple de $a^n\frac{u_0u_1\cdots u_n}{f(t,n)}$. D'où l'on a : $\text{ppcm}\,(u_0,u_1,\ldots,u_n)\geq a^n\frac{u_0u_1\cdots u_n}{f(t,n)}$. L'estimation requise découle alors de cette dernière, des inégalités $\binom{2n}{n}\leq 2^{2n}=4^n$, $\binom{2n+t}{n}\leq 2^{2n+t}=2^t4^n$ et de l'estimation :

$$u_0u_1\cdots u_n\geq b\,(a(1+t))\,(2a(2+t))\cdots(na(n+t))=ba^n\frac{n!(n+t)!}{t!}.$$

Ce qui complète cette démonstration. ∎

Remarque 1.40. *La minoration du théorème 1.39 est non triviale dès que $a\geq 5$. À priori, en appliquant ce résultat pour la suite $(n^2+1)_{n\in\mathbb{N}^*}$, on obtient une minoration triviale sans importance. Par contre, si r est un entier ≥ 3, le théorème 1.39 donne une minoration intéressante du* ppcm *de la suite $(r^2n^2+1)_{n\geq 1}$, qui est une sous-suite de $(n^2+1)_{n\in\mathbb{N}^*}$. En fait, on a :*

$$\text{ppcm}\left(1^2+1,2^2+1,\cdots,n^2+1\right)\geq\text{ppcm}\left(r^2+1,r^22^2+1,\cdots,r^2k^2+1\right),$$

où $k:=\lfloor\frac{n}{r}\rfloor$. Ensuite, le théorème 1.39 appliqué à la suite $(r^2n^2+1)_{n\geq 1}$ entraîne :

$$\text{ppcm}\left(1^2+1,2^2+1,\cdots,n^2+1\right)\geq 2\left(\frac{r^2}{4}\right)^k>2\left(\frac{r^2}{4}\right)^{\frac{n}{r}-1}=\frac{8}{r^2}\left\{\left(\frac{r}{2}\right)^{\frac{2}{r}}\right\}^n. \qquad (1.7.4)$$

En prenant enfin dans (1.7.4) $r=5$ (qui est la valeur de r qui rend la quantité $\frac{8}{r^2}\left\{\left(\frac{r}{2}\right)^{\frac{2}{r}}\right\}^n$ maximale), on obtient le corollaire suivant :

Corollaire 1.41 (Farhi [17])**.** *pour tout entier $n\geq 1$, on a :*

$$\text{ppcm}\left(1^2+1,2^2+1,\cdots,n^2+1\right)\geq 0,32(1,442)^n.$$

Le corollaire 1.41 a été amélioré par Oon [41], qui avait établi le résultat plus fort suivant :

Théorème 1.42 (Oon [41])**.** *Soient $c,m,n\in\mathbb{N}^*$ tels que $m\leq\lceil\frac{n}{2}\rceil$. Alors, on a :*

$$L_{c,m,n}:=\text{ppcm}\left(m^2+c,(m+1)^2+c,\ldots,n^2+c\right)\geq 2^n.$$

Démonstration. Définissons le nombre $I_{c,m,n}$ comme suit :

$$I_{c,m,n} := \int_0^1 x^{m-1+\sqrt{c}i}(1-x)^{n-m}\mathrm{d}x,$$

(où i désigne le nombre complexe $\sqrt{-1}$). Nous allons évaluer $I_{c,m,n}$ par deux méthodes différentes.

• **1ère méthode :** En développant par la formule du binôme l'expression $(1-x)^{n-m}$, dans $I_{c,m,n}$, on obtient :

$$\begin{aligned} I_{c,m,n} &= \sum_{k=0}^{n-m}(-1)^k\binom{n-m}{k}\int_0^1 x^{m-1+k+\sqrt{c}i}\mathrm{d}x = \sum_{k=0}^{n-m}\frac{(-1)^k\binom{n-m}{k}}{m+k+\sqrt{c}i} \\ &= \sum_{k=0}^{n-m}\frac{(-1)^k\binom{n-m}{k}(m+k-\sqrt{c}i)}{(m+k)^2+c}. \end{aligned}$$

Cette dernière expression montre que $I_{c,m,n}L_{c,m,n}$ est un nombre complexe de la forme $x+i\sqrt{c}y$, avec $x, y \in \mathbb{Z}$. Puisque $I_{c,m,n}L_{c,m,n} \neq 0$, il s'ensuit que $|I_{c,m,n}L_{c,m,n}| = x^2+cy^2 \in \mathbb{N}^*$. Par conséquent, on a :

$$L_{c,m,n} \geq \frac{1}{|I_{c,m,n}|}. \tag{1.7.5}$$

• **2nde méthode :** D'après les propriétés usuelles des fonctions Γ et β d'Euler, on a :

$$I_{c,m,n} = \beta(m+\sqrt{c}i, n-m+1) = \frac{\Gamma(m+\sqrt{c}i)\Gamma(n-m+1)}{\Gamma(n+1+\sqrt{c}i)} = \frac{(n-m)!}{\frac{\Gamma(n+1+\sqrt{c}i)}{\Gamma(m+\sqrt{c}i)}}.$$

D'où l'on a :

$$I_{c,m,n} = \frac{(n-m)!}{\prod_{k=m}^{n}(k+\sqrt{c}i)}. \tag{1.7.6}$$

En substituant (1.7.6) dans (1.7.5), on aboutit à :

$$L_{c,m,n} \geq \frac{\prod_{k=m}^{n}\sqrt{k^2+c}}{(n-m)!} \geq \frac{\prod_{k=m}^{n}k}{(n-m)!} = m\binom{n}{m}. \tag{1.7.7}$$

Maintenant, l'estimation (1.7.7) est vraie pour tous $n, m \in \mathbb{N}^*$ tels que $m \leq n$; en particulier, on a pour $m = \lceil \frac{n}{2} \rceil$:

$$L_{c,\lceil \frac{n}{2} \rceil,n} \geq \left\lceil \frac{n}{2} \right\rceil \binom{n}{\lceil \frac{n}{2} \rceil}.$$

Par ailleurs, on montre facilement par récurrence que pour tout entier $n \geq 7$, on a :

$$\left\lceil \frac{n}{2} \right\rceil \binom{n}{\lceil \frac{n}{2} \rceil} \geq 2^n. \tag{1.7.8}$$

Ce qui entraîne que pour tous $n, m \in \mathbb{N}^*$ tels que $n \geq 7$ et $m \leq \lceil \frac{n}{2} \rceil$, on a :

$$L_{c,m,n} \geq L_{c,\lceil \frac{n}{2} \rceil,n} \geq 2^n.$$

Pour les petites valeurs de n (i.e., $n \leq 6$), on vérifie le résultat de façon calculatoire (cas par cas). Ce qui complète la démonstration du théorème. ∎

1.8 Minorations effectives du ppcm de suites polynomiales

Comme nous l'avons signalé dans la section §1.7, la méthode de Oon est adaptable à une généralisation importante. En 2013, Hong et al. [27] ont généralisé le résultat de Oon (i.e., le théorème 1.42) en montrant qu'il reste vrai en remplaçant la suite $(n^2 + c)_n$ par n'importe quelle suite polynomiale (non constante), ayant des coefficients entiers positifs. La méthode de Hong et al. utilise quelques arguments algébriques, ainsi que certaines identités binomiales que nous présenterons dans ce qui va suivre.

Théorème 1.43 (Hong et al. [27])**.** *Soient n un entier ≥ 7 et $f \in \mathbb{Z}[X]$ un polynôme non constant, à coefficients positifs. Alors, pour tout entier $0 < m \leq \lceil \frac{n}{2} \rceil$, on a :*

$$\text{ppcm}\,(f(m), f(m+1), \ldots, f(n)) \geq 2^n.$$

La preuve de ce théorème est partagée en plusieurs lemmes. Rappelons d'abord la définition d'un entier algébrique.

Définition 1.44. *Un nombre complexe α est appelé un "entier algébrique", s'il est racine d'un polynôme unitaire $f \in \mathbb{Z}[X]$.*

Lemme 1.45. *On a les propriétés suivantes :*

1. *Les entiers algébriques rationnels sont simplement les entiers rationnels.*
2. *Si $\alpha \in \mathbb{C}$ est un entier algébrique, alors il en est de même des nombres $k\alpha$ ($k \in \mathbb{Z}$).*

Démonstration.

• Montrons le point 1 du lemme. Il est immédiat que tout entier rationnel est un entier algébrique (car : si $m \in \mathbb{Z}$, alors m est racine du polynôme $(X - m) \in \mathbb{Z}[X]$). Inversement, supposons que $m \in \mathbb{Q}$ est racine d'un polynôme unitaire $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$. Il existe $a, b \in \mathbb{Z}$ tels que $b \neq 0$, $\operatorname{pgcd}(a, b) = 1$ et $m = \frac{a}{b}$. On a par suite :

$$\left(\frac{a}{b}\right)^n + a_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + a_0 = 0.$$

En multipliant les deux membres de cette dernière par b^{n-1}, on obtient :

$$\frac{a^{n-1}}{b} = -a_{n-1}a^{n-1} - a_{n-2}a^{n-1}b - \cdots - a_0 b^{n-1} \in \mathbb{Z},$$

ce qui montre que $b \mid a^{n-1}$. Comme $\operatorname{pgcd}(a, b) = 1$, alors on a forcément $b = \pm 1$ et donc $m = \pm a \in \mathbb{Z}$, comme il fallait le prouver.

• Montrons maintenant le point 2 du lemme. Supposons que α est racine d'un polynôme unitaire $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$. Puisque $f(\alpha) = 0$, alors $k^n f(\alpha) = 0$; cela entraîne que $k\alpha$ est racine du polynôme $g \in \mathbb{Z}[X]$, donné par :

$$g(X) := X^n + ka_{n-1}X^{n-1} + k^2 a_{n-2}X^{n-2} + \cdots + k^n a_0,$$

comme il fallait le prouver. Le lemme est ainsi démontré. ∎

Dans ce qui suit, nous utilisons librement les résultats du lemme 1.45, sans se référer à ce dernier.

Lemme 1.46 (Hong et al. [27])**.** *Soient s un entier strictement positif et $f(X) = \sum_{i=0}^{s} a_i X^i \in \mathbb{Z}[X]$ un polynôme de degré s. Désignons par $\alpha_1, \alpha_2, \ldots, \alpha_s$ les racines complexes de f comptées avec leurs multiplicités. Alors, pour tout $j \in \{1, 2, \ldots, s\}$, le nombre $\beta_j := a_s \left(\prod_{\substack{1 \leq i \leq s \\ i \neq j}} \alpha_i\right)$ est un entier algébrique.*

Démonstration. Pour $s = 1$, le résultat du lemme est trivial. Supposons pour la suite que $s \geq 2$. Si au moins deux racines de f sont nulles, alors $\beta_j = 0$ $(\forall j \in \{1, 2, \ldots, s\})$, ce qui conclut au résultat requis. Si une seule racine α_t (pour un certain $t \in \{1, 2, \ldots, s\}$) est nulle, alors $\beta_t = (-1)^{s-1}a_1 \in \mathbb{Z}$ et $\beta_j = 0$ $(\forall j \neq t)$, ce qui permet de conclure. Maintenant, si toutes les racines $\alpha_1, \alpha_2, \ldots, \alpha_s$ sont non nulles, alors $\beta_j = \frac{(-1)^s a_0}{\alpha_j}$ $(\forall j \in \{1, 2, \ldots, s\})$.

Il suffit donc de montrer que pour tout $j \in \{1, 2, \ldots, s\}$, le nombre $\frac{a_0}{\alpha_j}$ est un entier algébrique. Fixons $j \in \{1, 2, \ldots, s\}$. Puisque $f(\alpha_j) = 0$, il s'ensuit que :

$$\frac{a_0^{s-1}}{\alpha_j^s} f(\alpha_i) = \left(\frac{a_0}{\alpha_j}\right)^s + a_1 \left(\frac{a_0}{\alpha_j}\right)^{s-1} + \cdots + a_{s-1} a_0^{s-2} \left(\frac{a_0}{\alpha_j}\right) + a_s a_0^{s-1} = 0.$$

Par conséquent, le nombre $\frac{a_0}{\alpha_j}$ est racine du polynôme unitaire $g(X) = X^s + a_1 X^{s-1} + \cdots + a_{s-1} a_0^{s-2} X + a_s a_0^{s-1} \in \mathbb{Z}[X]$, comme il fallait le prouver. Le lemme est démontré. ∎

Lemme 1.47 (Hong et al. [27]). *Soient m et n deux entiers strictement positifs tels que $m \leq n$. Alors, pour tout $z \in \mathbb{C} \setminus \{m, m+1, \ldots, n\}$, on a :*

$$\frac{(n-m)!}{\prod_{k=m}^{n}(k-z)} = \sum_{k=m}^{n} (-1)^{k-m} \binom{n-m}{k-m} \frac{1}{k-z}. \tag{1.8.1}$$

Démonstration. Considérons le polynôme de Lagrange L, donné par :

$$L(z) := \sum_{k=m}^{n} \prod_{\substack{m \leq j \leq n \\ j \neq k}} \left(\frac{j-z}{j-k}\right) = \sum_{k=m}^{n} \frac{(-1)^{k-m}}{(k-m)!(n-k)!} \prod_{\substack{m \leq j \leq n \\ j \neq k}} (j-z).$$

On a visiblement $\deg(L-1) \leq n-m$. Puisque le polynôme $(L-1)$ s'annule en chacun des nombres $m, m+1, \ldots, n$, alors le nombre de racines de $(L-1)$ est strictement plus grand que son degré. Cela entraîne que $(L-1)$ n'est rien d'autre que le polynôme nul. Il s'ensuit que pour tout $z \in \mathbb{C} \setminus \{m, m+1, \ldots, n\}$, on a :

$$\begin{aligned}(n-m)! = (n-m)!L(z) &= \sum_{k=m}^{n} (-1)^{k-m} \binom{n-m}{k-m} \prod_{\substack{m \leq j \leq n \\ j \neq k}} (j-z) \\ &= \left\{\prod_{k=m}^{n}(k-z)\right\} \sum_{k=m}^{n} (-1)^{k-m} \binom{n-m}{k-m} \frac{1}{k-z},\end{aligned}$$

confirmant ainsi l'identité (1.8.1). La démonstration du lemme est achevée. ∎

Lemme 1.48 (Hong et al. [27]). *Soient $m, n, s \in \mathbb{N}^*$ tels que $m \leq n$ et soit $f(x) = \sum_{i=0}^{s} a_i X^i \in \mathbb{Z}[X]$ un polynôme de degré s. Si f ne s'annule en aucun entier de l'intervalle $[m, n]$, alors on a :*

$$\prod_{k=m}^{n} f(k) \quad \textit{divise} \quad a_s{}^{n-m+1} \left((n-m)!\right)^s \left(\text{ppcm}\left(f(m), f(m+1), \ldots, f(n)\right)\right)^s.$$

Démonstration. Désignons par $\alpha_1, \alpha_2, \ldots, \alpha_s$ les racines complexes de f comptées avec leurs multiplicités. Donc, on peut écrire $f(X) = a_s\,(X-\alpha_1)\,(X-\alpha_2)\cdots(X-\alpha_s)$. Soit $k \in \{m, m+1, \ldots, n\}$. Il est immédiat que le polynôme $h_k(X) := (-1)^s f(k-X)$ est dans $\mathbb{Z}[X]$, son degré est égal à s, son coefficient dominant est égal à a_s et ses racines (comptées avec leurs multiplicités) sont $k-\alpha_1, k-\alpha_2, \ldots, k-\alpha_s$. En appliquant le lemme 1.46 sur le polynôme h_k, on en déduit que $\frac{f(k)}{k-\alpha_j} = a_s \prod_{\substack{1\leq i\leq s\\ i\neq j}}(k-\alpha_i)$ est un entier algébrique $(\forall j \in \{1,2,\ldots,s\})$. Cela est aussi vrai pour tout $k \in \{m, m+1, \ldots, n\}$ (puisque k est arbitraire). Par ailleurs, on a (en vertu du lemme 1.47) :

$$\frac{(n-m)!}{\prod_{k=m}^{n}(k-\alpha_j)} = \sum_{k=m}^{n}(-1)^{k-m}\binom{n-m}{k-m}\frac{1}{k-\alpha_j} \qquad (\forall j \in \{1,2,\ldots,s\}). \tag{1.8.2}$$

En multipliant les deux membres de (1.8.2) par $\operatorname{ppcm}(f(m), f(m+1), \ldots, f(n))$ et en se servant de ce qui précède, il s'ensuit que les nombres $Q_1, Q_2, \ldots, Q_s$ donnés par :

$$Q_j := \frac{(n-m)!\operatorname{ppcm}(f(m), f(m+1), \ldots, f(n))}{\prod_{k=m}^{n}(k-\alpha_j)} \qquad (\forall j \in \{1,2,\ldots,s\}), \tag{1.8.3}$$

sont tous des entiers algébriques. Donc, leur produit $Q := \prod_{j=1}^{s} Q_j$ l'est aussi. Le résultat requis par le lemme découle du fait que tout entier algébrique rationnel est un entier rationnel (voir le point 1 du lemme 1.45) et de l'expression suivante montrant en particulier que Q est un nombre rationnel :

$$Q := \frac{{a_s}^{n-m+1}\left((n-m)!\right)^s\left(\operatorname{ppcm}(f(m), f(m+1), \ldots, f(n))\right)^s}{\prod_{k=m}^{n} f(k)} \in \mathbb{Q}.$$

Ce qui complète cette démonstration. ∎

Démonstration du théorème 1.43. Le lemme 1.48 entraîne que :

$$\begin{aligned}\operatorname{ppcm}(f(m), f(m+1), \ldots, f(n)) &\geq \operatorname{ppcm}(f(\lceil n/2\rceil), f(\lceil n/2\rceil+1), \ldots, f(n))\\ &\geq \frac{\prod_{k=\lceil n/2\rceil}^{n}|f(k)/a_s|^{\frac{1}{s}}}{(n-\lceil n/2\rceil)!} \geq \frac{\prod_{k=\lceil n/2\rceil}^{n} k}{(n-\lceil n/2\rceil)!} = \left\lceil\frac{n}{2}\right\rceil\binom{n}{\lceil\frac{n}{2}\rceil}.\end{aligned}$$

En combinant cette dernière avec (1.7.8), on a :

$$\operatorname{ppcm}(f(m), f(m+1), \ldots, f(n)) \geq 2^n \qquad (\forall n \geq 7).$$

Ce qui complète cette démonstration. ∎

1.9 Estimations asymptotiques

Dans cette section on s'intéresse à l'étude du comportement asymptotique du nombre :

$$\log \operatorname{ppcm}(f(1), f(2), \ldots, f(n)),$$

où $f \in \mathbb{Z}[X]$ et $\deg f \in \{1, 2\}$. On commencera par le résultat de Bateman et al. [2] dont on présentera une démonstration ; nous énonçons ensuite le résultat de Cilleruelo [13] sans démonstration.

Théorème 1.49 (Bateman et al. [2])**.** *Soient $a, b \in \mathbb{Z}$ tels que $b > 0$, $a + b > 0$ et $\operatorname{pgcd}(a, b) = 1$. Alors, on a :*

$$\log \operatorname{ppcm}(a + b, a + 2b, \ldots, a + nb) \sim_{+\infty} \left(\frac{b}{\varphi(b)} \sum_{\substack{1 \leq m \leq b \\ \operatorname{pgcd}(m,b)=1}} \frac{1}{m} \right) n, \tag{1.9.1}$$

où φ désigne la fonction indicatrice d'Euler.

Démonstration. Fixons $n \in \mathbb{N}^*$ et définissons :

$$\begin{aligned} T(b) &:= \{m \in \mathbb{N}^*;\ m \leq b \text{ et } \operatorname{pgcd}(m, b) = 1\}, \\ L_{a,b,n} &:= \operatorname{ppcm}(a + b, a + 2b, \ldots, a + nb), \\ S(n) &:= \{a + b, a + 2b, \ldots, a + nb\}. \end{aligned}$$

Désignons par $P(n)$ l'ensemble des facteurs premiers de $L_{a,b,n}$ et posons $M(n) := \prod_{p \in P(n)} p$. En écrivant $L_{a,b,n} = \prod_{p \in P(n)} p^{a_p}$, avec $a_p = a_p(n) := \vartheta_p(L_{a,b,n})$ $(\forall p \in P(n))$, on a : $\frac{L_{a,b,n}}{M(n)} = \prod p^{a_p - 1}$, où le produit porte sur tous les nombres premiers $p \in P(n)$ tels que p^2 divise $L_{a,b,n}$. Puisque $\max S(n) = a + nb$, il s'ensuit que : $p^{a_p - 1} \leq a + nb$ $(\forall p \in P(n))$ et $\#\{p \in P(n);\ p^2 \text{ divise } L_{a,b,n}\} \leq \sqrt{a + nb}$. On a par conséquent :

$$0 \leq \log L_{a,b,n} - \log M(n) \leq \sqrt{a + nb} \log(a + nb) \quad (\forall n \in \mathbb{N}^*).$$

Ce qui entraîne que :

$$\lim_{n \to +\infty} \frac{\log L_{a,b,n} - \log M(n)}{n} = 0.$$

Il suffit donc d'étudier $\lim_{n\to+\infty} \frac{\log M(n)}{n}$. Pour ce faire, nous caractérisons d'abord les nombres premiers de l'ensemble $P(n)$. Soit p un nombre premier tel que $\text{pgcd}(p,b)=1$. Si m désigne le reste de la division euclidienne de p par b, alors $m \in T(b)$ et $p \equiv m \pmod{b}$. Puisque $\text{pgcd}(a,b)=1$, pour un tel m il existe un unique $m' \in T(b)$ vérifiant $mm' \equiv a \pmod{b}$, on a en particulier $m'p \equiv a \pmod{b}$. Nous constatons que $m'p$ est le plus petit multiple positif de p tel que $m'p \equiv a \pmod{b}$. On en déduit que $m'p \in S(n)$ si et seulement si $m'p \leq a+nb$; ce qui revient à dire que $p \in P(n)$ si et seulement si $p \leq \frac{a+nb}{m'}$. En désignant par $U(m)$ $(\forall m \in T(b))$ l'ensemble des nombres premiers p tels que $p \equiv m \pmod{b}$ et $p \leq \frac{a+nb}{m'}$, il s'ensuit que :

$$\log M(n) = \sum_{m\in T(b)} \sum_{p\in U(m)} \log p = \sum_{m\in T(b)} \theta\left(\frac{a+nb}{m'}; m, b\right),$$

où $\theta(x;m,b)$ désigne la fonction de Chebyshev généralisée. Par ailleurs, le théorème des nombres premiers pour les progressions arithmétiques (voir par exemple [5], p. 72) montre que l'on a :

$$\theta(x;m,b) = \frac{x}{\varphi(b)} + o(x).$$

Ce qui donne :

$$\log M(n) = \sum_{m\in T(b)} \left(\frac{a+nb}{m'\varphi(b)} + o(n)\right).$$

D'où :

$$\lim_{n\to+\infty} \frac{\log M(n)}{n} = \sum_{m\in T(b)} \frac{b}{m'\varphi(b)} = \sum_{m\in T(b)} \frac{b}{m\varphi(b)},$$

où la dernière égalité est due au fait que m' parcourt l'ensemble $T(b)$ tout comme m.
Ce qui termine cette démonstration. ■

Théorème 1.50 (Cilleruelo [13]). *Pour tout polynôme irréductible $f(X) = aX^2+bX+c \in \mathbb{Z}[X]$, on a :*

$$\log \text{ppcm}\,(f(1), f(2), \ldots, f(n)) = n\log n + Bn + o(n),$$

où $B = B_f$ est la constante définie par :

$$B_f := \gamma - 1 - 2\log 2 - \sum_p \left(\frac{d}{p}\right)\frac{\log p}{p-1} + \frac{1}{\varphi(q)} \sum_{\substack{1\le r\le q \\ \operatorname{pgcd}(r,q)=1}} \log\left(1+\frac{r}{q}\right)$$
$$+ \log a + \sum_{p\mid 2aD} \log p \left(\frac{1+\left(\frac{d}{p}\right)}{p-1} - \sum_{k\ge 1} \frac{s\left(f,p^k\right)}{p^k} \right),$$

avec γ désigne la constante d'Euler, $D := b^2 - 4ac$, d est la partie sans facteur carré de D, $\left(\frac{\cdot}{\cdot}\right)$ est le symbole de Legendre, $q := \frac{a}{\operatorname{pgcd}(a,b)}$ et $s\left(f,p^k\right)$ est le nombre de solutions de la congruence $f(X) \equiv 0 \pmod{p^k}$.

La démonstration de ce théorème est un peu longue ; elle se sert de quelques résultats concernant la répartition des racines d'un polynôme quadratique modulo des puissances de nombres premiers. Pour une preuve bien détaillée, le lecteur est invité à consulter l'article [13] de Cilleruelo.

CHAPITRE 2

Minorations non triviales du ppcm de la suite $(n^2+c)_n$

2.1 Introduction

Ce chapitre (dont les résultats sont publiés dans [9]) est consacré à l'étude des nombres :

$$L_{c,m,n} := \text{ppcm}\{m^2+c, (m+1)^2+c, \ldots, n^2+c\},$$

où c, m, n sont des entiers strictement positifs tels que $m \leq n$. Plus précisément, nous utilisons des arguments d'algèbre commutative et d'analyse complexe pour établir de nouvelles minorations non triviales de $L_{c,m,n}$. Le reste de ce chapitre est organisé en quatre parties. Dans la première partie, nous donnons un lemme algébrique qui nous permet, d'une part, de redémontrer le théorème 1.42 de Oon par une méthode facile et purement algébrique, et d'autre part de reformuler le problème de minoration du nombre $L_{c,m,n}$. Dans cette reformulation, nous sommes amenés à introduire une fonction arithmétique, notée h_c, dont un multiple fournit un diviseur pour $L_{c,m,n}$. Dans les deux parties suivantes, nous étudions la fonction arithmétique h_c et nous lui trouvons un multiple simple et non trivial. Dans la dernière partie, nous utilisons le multiple obtenu de h_c pour déduire un

diviseur non trivial pour $L_{c,m,n}$. Notre nouvelle minoration non triviale pour $L_{c,m,n}$ découle alors de ce diviseur.

Étant donné un polynôme $P \in \mathbb{C}[X]$, on désigne par $\overline{P}$ le polynôme conjugué de P dans $\mathbb{C}[X]$ (i.e., le polynôme que nous obtenons en remplaçant chaque coefficient de P par son conjugué complexe). Il est connu que la conjugaison des polynômes dans $\mathbb{C}[X]$ est compatible avec l'addition et la multiplication, c'est-à-dire que pour tous $P, Q \in \mathbb{C}[X]$, on a : $\overline{P+Q} = \overline{P} + \overline{Q}$ et $\overline{P \cdot Q} = \overline{P} \cdot \overline{Q}$. Par ailleurs, on désigne par I, E_h ($h \in \mathbb{R}$) et Δ les opérateurs linéaires de $\mathbb{C}[X]$ qui représentent respectivement l'identité, l'opérateur de translation de pas h ($E_h P(X) = P(X+h)$, $\forall P \in \mathbb{C}[X]$) et l'opérateur de différence avant ($\Delta P(X) = P(X+1) - P(X)$, $\forall P \in \mathbb{C}[X]$). Pour $n \in \mathbb{N}$, l'expression de Δ^n en fonction de E_h s'obtient facilement à partir de la formule du binôme, comme suit :

$$\Delta^n = (E_1 - I)^n = \sum_{m=0}^{n} (-1)^{n-m} \binom{n}{m} E_1^m = \sum_{m=0}^{n} (-1)^{n-m} \binom{n}{m} E_m. \tag{2.1.1}$$

Enfin, nous utilisons la notation de Knuth pour la factorielle décroissante :

$$X^{\underline{n}} := X(X-1)(X-2)\cdots(X-n+1) \qquad (\forall n \in \mathbb{N}).$$

2.2 La méthode algébrique

Bien que la méthode d'obtention du résultat de Oon [41] (i.e, le théorème 1.42) est d'apparence analytique, les ingrédients qui font son succès sont, en profondeur, algébriques ! Nous allons montrer ce fait à travers le lemme algébrique fondamental suivant :

Lemme 2.1 (fondamental)**.** *Soit $\mathcal{A}$ un anneau commutatif, unitaire et intègre et soient n un entier strictement positif et $u_0, u_1, \ldots, u_n$, a, b des éléments de $\mathcal{A}$. Supposons que a et b vérifient les conditions suivantes :*

1. *Chacun des éléments $u_0, u_1, \ldots, u_n$ de $\mathcal{A}$ est un diviseur de a.*
2. *Chacun des éléments $\prod_{\substack{0 \le j \le n \\ j \neq i}} (u_i - u_j)$ $(i = 0, 1, \ldots, n)$ de $\mathcal{A}$ est un diviseur de b.*

Alors, le produit ab est multiple du produit $u_0 u_1 \cdots u_n$.

Démonstration. Lorsque les éléments $u_0, u_1, \ldots, u_n$ de $\mathcal{A}$ ne sont pas deux à deux distincts (i.e., il existe $i, j \in \{0, 1, \ldots, n\}$, avec $i \neq j$, tels que $u_i = u_j$), le résultat du lemme est immédiat puisqu'on aura $b = 0_{\mathcal{A}}$. Supposons donc, pour toute la suite que les u_i $(i = 0, 1, \ldots, n)$ sont deux-à-deux distincts.

Étant donné que $\mathcal{A}$ est commutatif, unitaire et intègre, tout polynôme non identiquement nul de $\mathcal{A}[X]$, d'un certain degré $d \in \mathbb{N}$, possède au plus d racines dans $\mathcal{A}$. C'est sur ce résultat bien connu que nous appuyons pour prouver le lemme. Comme a est multiple de chacun des éléments $u_0, u_1, \ldots, u_n$ de $\mathcal{A}$, il existe $k_0, k_1, \ldots, k_n \in \mathcal{A}$ tels que :

$$a = k_0 u_0 = k_1 u_1 = \cdots = k_n u_n. \tag{2.2.1}$$

De même, comme b est multiple de chacun des éléments $\prod_{\substack{0 \leq j \leq n \\ j \neq i}} (u_i - u_j)$ $(i = 0, 1, \ldots, n)$ de $\mathcal{A}$, alors il existe $\ell_0, \ell_1, \ldots, \ell_n \in \mathcal{A}$ tels que :

$$b = \ell_i \prod_{\substack{0 \leq j \leq n \\ j \neq i}} (u_i - u_j) \quad (\forall i \in \{0, 1, \ldots, n\}). \tag{2.2.2}$$

Considérons le polynôme $P \in \mathcal{A}[X]$ suivant :

$$P(X) := \sum_{i=0}^{n} \left[\ell_i \prod_{\substack{0 \leq j \leq n \\ j \neq i}} (X - u_j) \right] - b.$$

Il est immédiat que $\deg P \leq n$. D'autre part, on a (d'après (2.2.2)) :

$$P(u_i) = 0 \quad (\forall i \in \{0, 1, \ldots, n\}).$$

Ce qui montre que P possède au moins $(n + 1)$ racines distinctes dans $\mathcal{A}$. Il s'ensuit (en vertu du résultat signalé au début de cette démonstration) que P est identiquement nul. D'où (en particulier) $P(0) = 0$; ce qui donne :

$$b = (-1)^n \sum_{i=0}^{n} \ell_i \left(\prod_{\substack{0 \leq j \leq n \\ j \neq i}} u_j \right).$$

En multipliant les deux membres de cette dernière égalité par a, il en résulte que :

$$\begin{aligned} ab &= (-1)^n \sum_{i=0}^{n} \ell_i a \left(\prod_{\substack{0\leq j\leq n \\ j\neq i}} u_j \right) \\ &= (-1)^n \sum_{i=0}^{n} \ell_i k_i u_i \left(\prod_{\substack{0\leq j\leq n \\ j\neq i}} u_j \right) \qquad \text{(en vertu de (2.2.1))} \\ &= (-1)^n \left(\sum_{i=0}^{n} k_i \ell_i \right) u_0 u_1 \cdots u_n. \end{aligned}$$

Ce qui montre bien que ab est multiple de $u_0 u_1 \cdots u_n$. Le lemme est ainsi démontré. ∎

Remarque 2.2. *Le lemme 2.1 est inspiré du lemme 1.34 de Farhi [17] qui en devient un cas particulier lorsqu'on prend* $\mathcal{A} = \mathbb{Z}$, $a = \operatorname{ppcm}(u_0, u_1, \ldots, u_n)$ *et*

$$b = \operatorname{ppcm}\left\{ \prod_{\substack{0\leq j\leq n \\ j\neq i}} (u_i - u_j);\ i = 0, 1, \ldots, n \right\}.$$

C'est précisément ce cas particulier qui a conduit Farhi [17] à établir les premières minorations non triviales du ppcm *d'une suite arithmétique et d'un certain type de suites quadratiques (voir les théorèmes 1.33 et 1.39).*

Maintenant, nous utilisons le lemme 2.1 pour établir une nouvelle démonstration (purement algébrique) du théorème 1.42 de Oon.

Démonstration algébrique du théorème 1.42. Puisque $L_{c,m,n}$ est clairement croissant par rapport à m, alors il suffit de prouver le résultat du théorème pour $m = \left\lceil \frac{n}{2} \right\rceil$. Pour simplifier, posons $m_0 := \left\lceil \frac{n}{2} \right\rceil$. Nous devons donc démontrer que $L_{c,m_0,n} \geq 2^n$. Pour $n \in \{1, 2, \ldots, 6\}$, cela peut être facilement vérifié à la main (comme le fait Oon). Supposons pour la suite que $n \geq 7$. Il est connu que pour tout entier $r \geq 7$, on a : $\left\lceil \frac{r}{2} \right\rceil \binom{r}{\left\lceil \frac{r}{2} \right\rceil} \geq 2^r$. En vertu de cette dernière inégalité pour $r = n$, il suffit de montrer que $L_{c,m_0,n} \geq m_0 \binom{n}{m_0}$. Plus généralement, nous allons montrer que :

$$L_{c,m',n} \geq m' \binom{n}{m'} \qquad (\forall m' \in \mathbb{N}^*,\ m' \leq n). \tag{2.2.3}$$

Soit $m' \in \mathbb{N}^*$ tel que $m' \leq n$. Pour prouver (2.2.3), nous appliquons le lemme 2.1 pour $\mathcal{A} = \mathbb{Z}[\sqrt{-c}]$ en prenant à la place des u_i les éléments $m' + \sqrt{-c}, m' + 1 + \sqrt{-c}, \ldots, n + \sqrt{-c}$ de $\mathcal{A}$ et pour a et b les entiers $a = L_{c,m',n}$ et $b = (n - m')!$. Pour tout $k \in \{m', m' + 1, \ldots, n\}$, comme $L_{c,m',n}$ est clairement multiple (dans $\mathbb{Z}$, donc aussi dans $\mathcal{A} = \mathbb{Z}[\sqrt{-c}]$) de $(k^2 + c)$ et $(k^2 + c) = \left(k + \sqrt{-c}\right)\left(k - \sqrt{-c}\right)$ est multiple (dans $\mathbb{Z}[\sqrt{-c}]$) de $\left(k + \sqrt{-c}\right)$, alors $L_{c,m',n}$ est multiple (dans $\mathbb{Z}[\sqrt{-c}]$) de $\left(k + \sqrt{-c}\right)$. Cela montre que la première condition du lemme 2.1 est satisfaite. D'autre part, on a pour tout $k \in \{m', m' + 1, \ldots, n\}$:

$$\prod_{\substack{m' \leq \ell \leq n \\ \ell \neq k}} \left\{\left(k + \sqrt{-c}\right) - \left(\ell + \sqrt{-c}\right)\right\} = \prod_{\substack{m' \leq \ell \leq n \\ \ell \neq k}} (k - \ell) = (-1)^{n-k}(k - m')!(n - k)!,$$

qui divise (dans $\mathbb{Z}$, donc aussi dans $\mathbb{Z}[\sqrt{-c}]$) l'entier $(n-m')!$ (car : $\frac{(n-m')!}{(k-m')!(n-k)!} = \binom{n-m'}{k-m'} \in \mathbb{Z}$). Cela montre que la deuxième condition du lemme 2.1 est aussi satisfaite. Nous en déduisons donc (en appliquant le lemme 2.1) que $L_{c,m',n}(n - m')!$ est multiple (dans $\mathbb{Z}[\sqrt{-c}]$) de $\prod_{k=m'}^{n} \left(k + \sqrt{-c}\right)$. Il existe par conséquent $x, y \in \mathbb{Z}$ tels que :

$$L_{c,m',n}(n - m')! = \left(x + y\sqrt{-c}\right) \prod_{k=m'}^{n} \left(k + \sqrt{-c}\right). \tag{2.2.4}$$

Ainsi, en prenant les modules dans $\mathbb{C}$ des deux côtés, on obtient :

$$L_{c,m',n}(n - m')! = \sqrt{x^2 + cy^2} \prod_{k=m'}^{n} \sqrt{k^2 + c}.$$

Par suite, comme $x^2 + cy^2 \in \mathbb{N}$ et $x^2 + cy^2 \neq 0$ (car : $x^2 + cy^2 = 0 \Longrightarrow L_{c,m',n} = 0$, ce qui est faux), alors $x^2 + cy^2 \geq 1$. D'où :

$$L_{c,m',n} = \frac{\sqrt{x^2 + cy^2} \prod_{k=m'}^{n} \sqrt{k^2 + c}}{(n - m')!} \geq \frac{\prod_{k=m'}^{n} \sqrt{k^2 + c}}{(n - m')!} \geq \frac{\prod_{k=m'}^{n} k}{(n - m')!} = m' \binom{n}{m'},$$

comme il fallait le prouver. Ce qui achève la démonstration du théorème. ∎

Maintenant, il est naturel de soulever la question suivante :

> *Comment pourrait-on améliorer la minoration* $L_{c,m,n} \geq \frac{\prod_{k=m}^{n} \sqrt{k^2+c}}{(n-m)!}$, *obtenue lors de la preuve du théorème 1.42 et établie initialement par Oon [41] ?*

Pour discuter cette question, nous aurons besoin de la définition suivante du pgcd et du ppcm dans un anneau commutatif unitaire.

Définition 2.3. *Soit $\mathcal{A}$ un anneau commutatif unitaire et soient $a, b \in \mathcal{A}$. Un élément d de $\mathcal{A}$ est appelé un plus grand commun diviseur de a et b (et est désigné par $\mathrm{pgcd}_{\mathcal{A}}(a,b)$) si d divise à la fois a et b et si tout autre élément d' de $\mathcal{A}$, qui divise à la fois a et b, divise également d. De même, un élément m de $\mathcal{A}$ est appelé un plus petit commun multiple de a et b (et est désigné par $\mathrm{ppcm}_{\mathcal{A}}(a,b)$) si m est un multiple de a et b et si tout autre élément m' de $\mathcal{A}$, qui est un multiple de a et b à la fois, est également un multiple de m. Noter que $\mathrm{pgcd}_{\mathcal{A}}(a,b)$ et $\mathrm{ppcm}_{\mathcal{A}}(a,b)$ existent au moins lorsque $\mathcal{A}$ est un anneau factoriel (ce qui est le cas de l'anneau des entiers de Gauss $\mathbb{Z}[i]$) et ils sont uniques à une multiplication près par une unité.*

Maintenant, pour simplifier, supposons que $c = 1$ et soient $m, n \in \mathbb{N}^*$ tels que $m \leq n$. En vertu de la formule (2.2.4), l'entier strictement positif $L_{1,m,n}(n-m)!$ est multiple (dans $\mathbb{Z}[i]$) de l'entier de Gauss $\prod_{k=m}^{n}(k+i)$. Par suite, en prenant les conjugués (dans $\mathbb{C}$) des deux membres de (2.2.4), on obtient que $L_{1,m,n}(n-m)!$ est aussi multiple (dans $\mathbb{Z}[i]$) de l'entier de Gauss $\prod_{k=m}^{n}(k-i)$. Il résulte de ces deux faits que $L_{1,m,n}(n-m)!$ est multiple (dans $\mathbb{Z}[i]$) de :

$$\begin{aligned}\mathrm{ppcm}_{\mathbb{Z}[i]}\left\{\prod_{k=m}^{n}(k+i), \prod_{k=m}^{n}(k-i)\right\} &= \frac{\prod_{k=m}^{n}(k+i)\cdot\prod_{k=m}^{n}(k-i)}{\mathrm{pgcd}_{\mathbb{Z}[i]}\left\{\prod_{k=m}^{n}(k+i), \prod_{k=m}^{n}(k-i)\right\}} \\ &= \frac{\prod_{k=m}^{n}(k^2+1)}{\mathrm{pgcd}_{\mathbb{Z}[i]}\left\{\prod_{k=m}^{n}(k+i), \prod_{k=m}^{n}(k-i)\right\}}.\end{aligned}$$

Par conséquent, on a :

$$L_{1,m,n} \geq \frac{\prod_{k=m}^{n}(k^2+1)}{(n-m)!\left|\mathrm{pgcd}_{\mathbb{Z}[i]}\left\{\prod_{k=m}^{n}(k+i), \prod_{k=m}^{n}(k-i)\right\}\right|}. \tag{2.2.5}$$

Nous remarquons que la majoration triviale :

$$\left|\mathrm{pgcd}_{\mathbb{Z}[i]}\left\{\prod_{k=m}^{n}(k+i), \prod_{k=m}^{n}(k-i)\right\}\right| \leq \left|\prod_{k=m}^{n}(k+i)\right| \leq \prod_{k=m}^{n}\sqrt{k^2+1}$$

suffit pour établir la minoration de Oon $L_{1,m,n} \geq \frac{\prod_{k=m}^{n}\sqrt{k^2+1}}{(n-m)!}$. Par conséquent, toute majoration non triviale pour le nombre $\left|\mathrm{pgcd}_{\mathbb{Z}[i]}\left\{\prod_{k=m}^{n}(k+i), \prod_{k=m}^{n}(k-i)\right\}\right|$ entraîne immédiatement une amélioration du théorème 1.42 de Oon. D'autre part, pour $a, b \in \mathbb{Z}$

tels que $(a,b) \neq (0,0)$, on peut facilement vérifier que $\mathrm{pgcd}_{\mathbb{Z}[i]}(a+bi, a-bi)$ n'est pas trop loin de $\mathrm{pgcd}_{\mathbb{Z}}(a,b)$. Plus précisément, on a :

$$\mathrm{pgcd}_{\mathbb{Z}[i]}(a+bi, a-bi) = (\sigma + i\tau)\,\mathrm{pgcd}_{\mathbb{Z}}(a,b),$$

où $\sigma, \tau \in \{-1,0,1\}$ et $(\sigma,\tau) \neq (0,0)$. Donc, pour le cas $c=1$, on est amené à étudier la fonction arithmétique :

$$\begin{array}{rccc} h: & \mathbb{Z}[i]\setminus\{0\} & \longrightarrow & \mathbb{N}^* \\ & a+bi & \longmapsto & \mathrm{pgcd}(a,b) \end{array};$$

plus précisément, à trouver une majoration non triviale pour la quantité $h\left(\prod_{k=m}^{n}(k+i)\right)$ $(m,n \in \mathbb{N}^*,\ m \leq n)$. Pour le cas général $(c \in \mathbb{N}^*)$, la fonction arithmétique que nous devons étudier est clairement donnée par :

$$\begin{array}{rccc} h_c: & \mathbb{Z}[\sqrt{-c}]\setminus\{0\} & \longrightarrow & \mathbb{N}^* \\ & a+b\sqrt{-c} & \longmapsto & \mathrm{pgcd}(a,b) \end{array}$$

et la quantité que nous devons majorer est $h_c\left(\prod_{k=m}^{n}(k+\sqrt{-c})\right)$ $(m,n \in \mathbb{N}^*,\ m \leq n)$.

La proposition suivante a pour objectif de remplacer un langage arithmétique spécifique de l'anneau $\mathbb{Z}[\sqrt{-c}]$ par son analogue (plus simple) dans $\mathbb{Z}$.

Proposition 2.4. *Soient $c \in \mathbb{N}^*$ et $N, a, b \in \mathbb{Z}$, avec $(a,b) \neq (0,0)$. Alors, N est multiple (dans $\mathbb{Z}[\sqrt{-c}]$) de $(a+b\sqrt{-c})$ si et seulement si N est multiple (dans $\mathbb{Z}$) de $\frac{a^2+cb^2}{\mathrm{pgcd}(a,b)}$.*

Démonstration. Le résultat de la proposition est trivial pour $b=0$. Supposons pour la suite que $b \neq 0$. On a deux implications à démontrer.

•$(\Rightarrow)$: Supposons que N est multiple (dans $\mathbb{Z}[\sqrt{-c}]$) de $(a+b\sqrt{-c})$. Il existe donc $x, y \in \mathbb{Z}$ tels que :

$$N = (x+y\sqrt{-c})(a+b\sqrt{-c}).$$

En identifiant les parties réelles et imaginaires des deux côtés de cette égalité, on obtient :

$$N = ax - byc, \tag{2.2.6}$$

$$0 = bx + ay. \tag{2.2.7}$$

Posons maintenant $d := \text{pgcd}(a, b)$. Il existe donc $a', b' \in \mathbb{Z}$, avec $b' \neq 0$ et $\text{pgcd}(a', b') = 1$, tels que $a = da'$ et $b = db'$. En substituant cela dans (2.2.7), on obtient (après simplification) :

$$b'x = -a'y. \tag{2.2.8}$$

Cette dernière égalité montre que b' divise $a'y$. Puisque $\text{pgcd}(a', b') = 1$, alors (d'après le lemme de Gauss) b' divise y. Il existe donc $k \in \mathbb{Z}$ tel que $y = kb'$. En remplaçant cela dans (2.2.8), on obtient que $x = -ka'$. D'où, en substituant $x = -ka' = -k\frac{a}{d}$ et $y = kb' = k\frac{b}{d}$ dans (2.2.6), on obtient enfin :

$$N = -k\frac{a^2 + cb^2}{d} = -k\frac{a^2 + cb^2}{\text{pgcd}(a, b)},$$

ce qui montre que N est multiple (dans $\mathbb{Z}$) de $\frac{a^2+cb^2}{\text{pgcd}(a,b)}$, comme il fallait le prouver.

•($\Leftarrow$) : Inversement, supposons que N est multiple (dans $\mathbb{Z}$) de $\frac{a^2+cb^2}{\text{pgcd}(a,b)}$. Il existe donc $k \in \mathbb{Z}$ tel que :

$$N = k\frac{a^2 + cb^2}{\text{pgcd}(a, b)} = k\frac{a - b\sqrt{-c}}{\text{pgcd}(a, b)}(a+b\sqrt{-c}) = \left(\frac{ka}{\text{pgcd}(a, b)} - \frac{kb}{\text{pgcd}(a, b)}\sqrt{-c}\right)(a+b\sqrt{-c}).$$

Puisque $\left(\frac{ka}{\text{pgcd}(a,b)} - \frac{kb}{\text{pgcd}(a,b)}\sqrt{-c}\right) \in \mathbb{Z}[\sqrt{-c}]$, cette dernière égalité montre que N est multiple (dans $\mathbb{Z}[\sqrt{-c}]$) de $\left(a + b\sqrt{-c}\right)$, comme il fallait le prouver.

Ce qui complète la démonstration de la proposition. ∎

De la proposition 2.4, nous tirons le corollaire suivant, qui est la première étape clé pour obtenir les résultats de ce chapitre.

Corollaire 2.5. *Soient $c, m, n \in \mathbb{N}^*$ tels que $m \leq n$. Alors, le nombre $L_{c,m,n}(n - m)!$ est multiple (dans $\mathbb{Z}$) de l'entier strictement positif :*

$$\frac{\prod_{k=m}^{n}(k^2 + c)}{h_c\left(\prod_{k=m}^{n}\left(k + \sqrt{-c}\right)\right)}.$$

Démonstration. La formule (2.2.4) (obtenue lors de notre nouvelle preuve du théorème 1.42) montre que $L_{c,m,n}(n - m)!$ est multiple (dans $\mathbb{Z}[\sqrt{-c}]$) de $\prod_{k=m}^{n}\left(k + \sqrt{-c}\right)$. Selon la proposition 2.4, cette dernière propriété est équivalente à l'énoncé du corollaire. ∎

En vertu du corollaire 2.5, pour minorer le nombre $L_{c,m,n}$ $(c, m, n \in \mathbb{N}^*,\ m \leq n)$, il suffit de majorer la quantité $h_c\left(\prod_{k=m}^{n}(k + \sqrt{-c})\right)$. De même, pour trouver un divi-

seur (rationnel) non trivial de $L_{c,m,n}$, il suffit de trouver un multiple non trivial pour $h_c\left(\prod_{k=m}^{n}(k+\sqrt{-c})\right)$. C'est ce que nous allons faire dans la suite.

2.3 Une identité de Bézout explicite

Dans toute la suite, fixons $c \in \mathbb{N}^*$ et $k \in \mathbb{N}$ et Posons :

$$P_k(X) := (X+\sqrt{-c})(X-1+\sqrt{-c})\cdots(X-k+\sqrt{-c}) = A_k(X) + B_k(X)\sqrt{-c},$$
$$\overline{P_k}(X) := (X-\sqrt{-c})(X-1-\sqrt{-c})\cdots(X-k-\sqrt{-c}) = A_k(X) - B_k(X)\sqrt{-c},$$

où l'on sous-entend que $A_k, B_k \in \mathbb{Z}[X]$. Dans ce qui suit, nous trouvons un multiple non trivial pour l'entier strictement positif $h_c\left(P_k(n)\right) = \operatorname{pgcd}\left(A_k(n), B_k(n)\right)$. Pour ce faire, nous allons plutôt chercher deux suites polynomiales $\left(a_k(n)\right)_n$ et $\left(b_k(n)\right)_n$ de sorte que la suite polynomiale $\left(a_k(n)A_k(n) + b_k(n)B_k(n)\right)_n$ soit indépendante de n. Il est clair que cela conduit à la recherche de deux polynômes $U_k, V_k \in \mathbb{Q}[X]$ qui satisfont l'identité de Bézout :

$$U_k(X)A_k(X) + V_k(X)B_k(X) = 1.$$

Par suite, comme $A_k = \frac{P_k+\overline{P_k}}{2}$ et $B_k = \frac{P_k-\overline{P_k}}{2\sqrt{-c}}$, cela revient donc à chercher $\sigma_k, \tau_k \in \mathbb{Q}\left(\sqrt{-c}\right)[X]$ tels que :

$$\sigma_k\left(X\right)P_k\left(X\right) + \tau_k\left(X\right)\overline{P_k}\left(X\right) = 1.$$

Justifions d'abord l'existence de σ_k et τ_k. En désignant par $Z(P)$ l'ensemble de toutes les racines complexes d'un polynôme $P \in \mathbb{C}[X]$, on a clairement :

$$Z\left(P_k\right) = \{-\sqrt{-c}, 1-\sqrt{-c}, \ldots, k-\sqrt{-c}\} \text{ et } Z\left(\overline{P_k}\right) = \{\sqrt{-c}, 1+\sqrt{-c}, \ldots, k+\sqrt{-c}\},$$

donc $Z\left(P_k\right) \cap Z\left(\overline{P_k}\right) = \emptyset$; c'est-à-dire que P_k et $\overline{P_k}$ n'ont pas de racines communes dans $\mathbb{C}$. Cela implique que P_k et $\overline{P_k}$ sont premiers entre eux dans $\mathbb{C}[X]$; donc ils sont aussi premiers entre eux dans $\mathbb{Q}\left(\sqrt{-c}\right)[X]$. Il s'ensuit (en vertu du théorème de Bézout) qu'il existe $\sigma_k, \tau_k \in \mathbb{Q}\left(\sqrt{-c}\right)[X]$ tels que : $\sigma_k P_k + \tau_k \overline{P_k} = 1$, comme il fallait le prouver.

Maintenant, pour trouver explicitement de tels σ_k et τ_k, nous avons besoin de la version plus précise du théorème de Bézout suivante :

Théorème 2.6. *Soient* $\mathbb{K}$ *un corps et* P *et* Q *deux polynômes non constants de* $\mathbb{K}[X]$ *tels que* $\operatorname{pgcd}_{\mathbb{K}[X]}(P,Q)=1$. *Alors, il existe un couple unique* (U,V) *de polynômes de* $\mathbb{K}[X]$, *avec* $\deg U<\deg Q$ *et* $\deg V<\deg P$, *tel que :*

$$PU+QV=1.$$

Démonstration. Puisque $\operatorname{pgcd}_{\mathbb{K}[X]}(P,Q)=1$, alors (d'après le théorème de Bézout) il existe $U_0,V_0\in\mathbb{K}[X]$ tels que :

$$PU_0+QV_0=1.$$

Considérons la division euclidienne de U_0 par Q et la division euclidienne de V_0 par $(-P)$ dans $\mathbb{K}[X]$:

$$U_0=U_1Q+U,$$
$$V_0=V_1(-P)+V,$$

où $U_1,V_1,U,V\in\mathbb{K}[X]$, $\deg U<\deg Q$ et $\deg V<\deg(-P)=\deg P$. Donc, on a :

$$PU+QV=P(U_0-U_1Q)+Q(V_0+V_1P)=PQ(V_1-U_1)+PU_0+QV_0=PQ(V_1-U_1)+1.$$

Si $V_1-U_1\neq 0$, alors la dernière égalité implique que $\deg(PU+QV)\geq\deg(PQ)$, ce qui est impossible, car $\deg U<\deg Q$ et $\deg V<\deg P$. D'où $V_1-U_1=0$, ce qui donne $PU+QV=1$. L'existence du couple (U,V) requis par le théorème est prouvée. Il reste à prouver l'unicité de (U,V). Soit (U_*,V_*) un autre couple de polynômes de $\mathbb{K}[X]$, avec $\deg U_*<\deg Q$, $\deg V_*<\deg P$ et $PU_*+QV_*=1$ et montrons que $(U_*,V_*)=(U,V)$. On a :

$$P(UV_*-U_*V)=(PU)V_*-(PU_*)V=(1-QV)V_*-(1-QV_*)V=V_*-V,$$

ce qui montre que le polynôme (V_*-V) est multiple de P dans $\mathbb{K}[X]$. Comme $\deg(V_*-V)<\deg P$ (car : $\deg V<\deg P$ et $\deg V_*<\deg P$), on a nécessairement $V_*-V=0$; donc $V_*=V$. Il s'ensuit de cela que $PU_*=1-QV_*=1-QV=PU$. D'où $U_*=U$. On a par conséquent $(U_*,V_*)=(U,V)$, comme il fallait le prouver.
Ce qui complète la démonstration du théorème. ∎

Dans notre contexte, l'application du théorème 2.6 donne le corollaire suivant :

Corollaire 2.7. *Il existe un unique polynôme $\sigma_k \in \mathbb{C}[X]$, de degré $\leq k$, tel que :*

$$\sigma_k P_k + \overline{\sigma_k}\,\overline{P_k} = 1.$$

Démonstration. D'après le théorème 2.6 (appliqué à $\mathbb{K} = \mathbb{C}$ et $(P, Q) = \left(P_k, \overline{P_k}\right)$), il existe un unique couple (σ_k, τ_k) de polynômes de $\mathbb{C}[X]$, avec $\deg \sigma_k < \deg \overline{P_k} = k+1$ et $\deg \tau_k < \deg P_k = k+1$, tel que $\sigma_k P_k + \tau_k \overline{P_k} = 1$. En prenant les conjugués dans $\mathbb{C}[X]$ des deux côtés de cette dernière égalité, on obtient : $\overline{\sigma_k}\,\overline{P_k} + \overline{\tau_k} P_k = 1$, c'est-à-dire que $\overline{\tau_k} P_k + \overline{\sigma_k}\,\overline{P_k} = 1$. Comme $\deg \overline{\tau_k} = \deg \tau_k < k+1$ et $\deg \overline{\sigma_k} = \deg \sigma_k < k+1$, cela montre que le couple $(\overline{\tau_k}, \overline{\sigma_k})$ satisfait à la propriété caractéristique du couple (σ_k, τ_k). D'où $(\overline{\tau_k}, \overline{\sigma_k}) = (\sigma_k, \tau_k)$, ce qui revient à dire que $\tau_k = \overline{\sigma_k}$. On a par conséquent $\sigma_k P_k + \overline{\sigma_k}\,\overline{P_k} = 1$. Ce qui complète la démonstration du corollaire. ∎

Maintenant, nous allons déterminer l'expression explicite du polynôme σ_k annoncé dans le corollaire 2.7. En remplaçant dans l'identité $\sigma_k(X) P_k(X) + \overline{\sigma_k}(X)\,\overline{P_k}(X) = 1$, l'indéterminée X par les nombres $s + \sqrt{-c}$ $(s = 0, 1, \ldots, k)$, on obtient :

$$\sigma_k\left(s + \sqrt{-c}\right) = \frac{1}{P_k\left(s + \sqrt{-c}\right)} \quad (\forall s \in \{0, 1, \ldots, k\}). \tag{2.3.1}$$

(car : $\overline{P_k}\left(s + \sqrt{-c}\right) = 0$ pour $s = 0, 1, \ldots, k$). Ainsi, les valeurs de σ_k sont connues en $(k+1)$ points équidistants de distance 1. Comme $\deg \sigma_k \leq k$, cela suffit pour déterminer l'expression de $\sigma_k(X)$ en utilisant par exemple la formule d'interpolation de Newton. En procédant ainsi, on obtient :

$$\sigma_k(X) = \sum_{\ell=0}^{k} \frac{\left(\Delta^\ell \sigma_k\right)\left(\sqrt{-c}\right)}{\ell!} \left(X - \sqrt{-c}\right)^{\underline{\ell}}.$$

Puis, en utilisant (2.1.1), on obtient :

$$\begin{aligned}
\sigma_k(X) &= \sum_{\ell=0}^{k} \sum_{j=0}^{\ell} \frac{(-1)^{\ell-j}}{\ell!} \binom{\ell}{j} \sigma_k\left(j + \sqrt{-c}\right) \left(X - \sqrt{-c}\right)^{\underline{\ell}} \\
&= \sum_{\ell=0}^{k} \left\{ \frac{1}{\ell!} \sum_{j=0}^{\ell} (-1)^{\ell-j} \binom{\ell}{j} \sigma_k\left(j + \sqrt{-c}\right) \right\} \left(X - \sqrt{-c}\right)^{\underline{\ell}} \\
&= \sum_{\ell=0}^{k} \left\{ \frac{1}{\ell!} \sum_{j=0}^{\ell} (-1)^{\ell-j} \binom{\ell}{j} \frac{1}{P_k\left(j + \sqrt{-c}\right)} \right\} \left(X - \sqrt{-c}\right)^{\underline{\ell}}
\end{aligned}$$

(en vertu de (2.3.1)). Donc, en posant pour tout $\ell \in \{0, 1, \ldots, k\}$:

$$\Theta_{k,\ell} := \frac{1}{\ell!} \sum_{j=0}^{\ell} (-1)^{\ell-j} \binom{\ell}{j} \frac{1}{P_k(j + \sqrt{-c})}, \tag{2.3.2}$$

il vient que :

$$\sigma_k(X) = \sum_{\ell=0}^{k} \Theta_{k,\ell} \left(X - \sqrt{-c}\right)^{\underline{\ell}}. \tag{2.3.3}$$

Il reste à simplifier les expressions des nombres $\Theta_{k,\ell}$ $(0 \leq \ell \leq k)$. Pour ce faire, nous introduisons les fonctions rationnelles $R_{k,\ell}$ $(0 \leq \ell \leq k)$, définies par :

$$R_{k,\ell}(z) := \frac{1}{\ell!} \sum_{j=0}^{\ell} (-1)^{\ell-j} \binom{\ell}{j} \frac{1}{P_k(z + j + \sqrt{-c})}, \tag{2.3.4}$$

de sorte que l'on ait :

$$\Theta_{k,\ell} = R_{k,\ell}(0) \quad (\forall \ell \in \{0, 1, \ldots, k\}). \tag{2.3.5}$$

Le domaine commun d'holomorphie des fonctions $R_{k,\ell}$ $(0 \leq \ell \leq k)$ est visiblement la région connexe et ouverte D de $\mathbb{C}$, donnée par :

$$D := \mathbb{C} \setminus \{j - 2\sqrt{-c}\ ;\ j \in \mathbb{Z} \text{ et } -k \leq j \leq k\}.$$

En utilisant le principe du prolongement analytique (voir [46]) ainsi que la théorie des fonctions gamma et bêta (que l'on peut trouver dans [1]), nous pouvons trouver une autre expression de $R_{k,\ell}$ $(0 \leq \ell \leq k)$, qui est plus simple que celle de ci-dessus. On a la proposition suivante :

Proposition 2.8. *Pour tout $\ell \in \mathbb{N}$, avec $\ell \leq k$, et tout $z \in D$, on a :*

$$R_{k,\ell}(z) = \frac{(-1)^{k+\ell}}{z + 2\sqrt{-c}} \binom{k+\ell}{\ell} \frac{1}{\left(k - 2\sqrt{-c} - z\right)^{\underline{k}} \left(\ell + 2\sqrt{-c} + z\right)^{\underline{\ell}}}. \tag{2.3.6}$$

Démonstration. Soit $\ell \in \mathbb{N}$ tel que $\ell \leq k$. D'après le principe du prolongement analytique, il suffit de prouver la formule (2.3.6) pour $z \in \mathbb{C}$, tel que $\Re(z) > k$. Pour un tel z,

on a :

$$
\begin{aligned}
R_{k,\ell}(z) &:= \frac{1}{\ell!}\sum_{j=0}^{\ell}(-1)^{\ell-j}\binom{\ell}{j}\frac{1}{P_k(z+j+\sqrt{-c})} \\
&= \frac{1}{\ell!}\sum_{j=0}^{\ell}(-1)^{\ell-j}\binom{\ell}{j}\frac{1}{\left(z+j+2\sqrt{-c}\right)\left(z+j-1+2\sqrt{-c}\right)\cdots\left(z+j-k+2\sqrt{-c}\right)} \\
&= \frac{1}{\ell!}\sum_{j=0}^{\ell}(-1)^{\ell-j}\binom{\ell}{j}\frac{\Gamma\left(z+j-k+2\sqrt{-c}\right)}{\Gamma\left(z+j+1+2\sqrt{-c}\right)} \\
&= \frac{1}{\ell!}\sum_{j=0}^{\ell}(-1)^{\ell-j}\binom{\ell}{j}\frac{1}{k!}\beta\left(z+j-k+2\sqrt{-c},k+1\right) \\
&= \frac{1}{k!\ell!}\sum_{j=0}^{\ell}\left[(-1)^{\ell-j}\binom{\ell}{j}\int_0^1 t^{z+j-k-1+2\sqrt{-c}}(1-t)^k\mathrm{d}t\right] \\
&= \frac{1}{k!\ell!}\int_0^1 t^{z-k-1+2\sqrt{-c}}(1-t)^k\left\{\sum_{j=0}^{\ell}(-1)^{\ell-j}\binom{\ell}{j}t^j\right\}\mathrm{d}t \\
&= \frac{1}{k!\ell!}\int_0^1 t^{z-k-1+2\sqrt{-c}}(1-t)^k\left(t-1\right)^{\ell}\mathrm{d}t \\
&= \frac{(-1)^{\ell}}{k!\ell!}\int_0^1 t^{z-k-1+2\sqrt{-c}}(1-t)^{k+\ell}\mathrm{d}t \\
&= \frac{(-1)^{\ell}}{k!\ell!}\beta\left(z-k+2\sqrt{-c},k+\ell+1\right) \\
&= \frac{(-1)^{\ell}}{k!\ell!}\frac{\Gamma\left(z-k+2\sqrt{-c}\right)\Gamma\left(k+\ell+1\right)}{\Gamma\left(z+\ell+1+2\sqrt{-c}\right)} \\
&= (-1)^{\ell}\binom{k+\ell}{\ell}\frac{1}{\left(z+\ell+2\sqrt{-c}\right)\left(z+\ell-1+2\sqrt{-c}\right)\cdots\left(z-k+2\sqrt{-c}\right)} \\
&= \frac{(-1)^{k+\ell}}{z+2\sqrt{-c}}\binom{k+\ell}{\ell}\frac{1}{\left(k-2\sqrt{-c}-z\right)^{\underline{k}}\left(\ell+2\sqrt{-c}+z\right)^{\underline{\ell}}},
\end{aligned}
$$

comme il fallait le prouver. Ce qui complète cette démonstration. ∎

De la proposition 2.8, découle immédiatement une expression explicite plus simple de $\sigma_k(X)$. On a le corollaire suivant :

Corollaire 2.9. *On a :*

$$
\sigma_k(X) = \frac{1}{2\sqrt{-c}\left(k-2\sqrt{-c}\right)^{\underline{k}}}\sum_{\ell=0}^{k}\frac{(-1)^{k+\ell}\binom{k+\ell}{\ell}}{\left(\ell+2\sqrt{-c}\right)^{\underline{\ell}}}\left(X-\sqrt{-c}\right)^{\underline{\ell}}.
$$

Démonstration. Cela découle immédiatement des formules (2.3.3), (2.3.5) et (2.3.6). ∎

2.4 Multiples non triviaux de certaines valeurs de h_c

Dans cette section, nous conservons les notations de la section §2.3. Du corollaire 2.9, nous déduisons le théorème suivant :

Théorème 2.10. *Pour tous $c, n, m \in \mathbb{N}^*$, avec $m \leq n$, on a :*

$$h_c\left(\prod_{\ell=m}^{n}\left(\ell+\sqrt{-c}\right)\right) \quad \textit{divise} \quad c\prod_{\ell=1}^{n-m}(\ell^2+4c).$$

Démonstration. Soient $c, n, m \in \mathbb{N}^*$, avec $m \leq n$ et posons $k := n-m \in \mathbb{N}$ et $d := c\prod_{\ell=1}^{n-m}(\ell^2+4c) \in \mathbb{N}^*$. On a $\prod_{\ell=m}^{n}\left(\ell+\sqrt{-c}\right) = P_k(n)$; nous devons donc démontrer que $h_c\left(P_k(n)\right)$ divise d. En constatant que $2d = \sqrt{-c}\cdot 2\sqrt{-c}\left(k-2\sqrt{-c}\right)^{\underline{k}}\left(k+2\sqrt{-c}\right)^{\underline{k}}$, on obtient (en vertu du corollaire 2.9) que $2d\sigma_k \in \mathbb{Z}[\sqrt{-c}][X]$. Donc, il existe $r_k, s_k \in \mathbb{Z}[X]$ tels que :

$$2d\sigma_k\left(X\right) = r_k\left(X\right) + s_k\left(X\right)\sqrt{-c}.$$

Par suite, l'identité polynomiale $\sigma_k P_k + \overline{\sigma_k}\,\overline{P_k} = 1$ (donnée par le corollaire 2.7) implique que $2d\sigma_k \cdot P_k + \overline{2d\sigma_k}\cdot\overline{P_k} = 2d$. En substituant dans cette dernière égalité P_k par $\left(A_k + B_k\sqrt{-c}\right)$ et $2d\sigma_k$ par $\left(r_k + s_k\sqrt{-c}\right)$, on obtient (en particulier) que :

$$r_k A_k - c s_k B_k = d,$$

ce qui implique que $\mathrm{pgcd}_{\mathbb{Z}[X]}\left(A_k, B_k\right)$ divise d. On en déduit alors que $h_c\left(P_k(n)\right) = \mathrm{pgcd}_{\mathbb{Z}}\left(A_k(n), B_k(n)\right)$ divise d, comme il fallait le prouver. ∎

2.5 Nouvelles estimations pour le nombre $L_{c,m,n}$

On a le théorème suivant :

Théorème 2.11. *Soient $c, m, n \in \mathbb{N}^*$ tels que $m \leq n$. Alors :*

1. *L'entier strictement positif $L_{c,m,n}$ est multiple du nombre rationnel :*

$$\frac{\displaystyle\prod_{k=m}^{n}\left(k^2+c\right)}{c\cdot(n-m)!\displaystyle\prod_{k=1}^{n-m}\left(k^2+4c\right)}.$$

2. *On a :*

$$L_{c,m,n} \geq \lambda_1(c) \cdot m^2 \frac{n!^2}{m!^2(n-m)!^3},$$

où $\lambda_1(c) := e^{-\frac{2\pi^2}{3}c}/c$.

Démonstration. Le premier point du théorème est une conséquence immédiate du corollaire 2.5 et du théorème 2.10. Par suite, en utilisant l'inégalité $1+x \leq e^x$ $(\forall x \in \mathbb{R})$, on a :

$$\begin{aligned}
\prod_{k=1}^{n-m} \left(k^2+4c\right) &= \prod_{k=1}^{n-m} k^2 \left(1+\frac{4c}{k^2}\right) \\
&= (n-m)!^2 \prod_{k=1}^{n-m} \left(1+\frac{4c}{k^2}\right) \\
&\leq (n-m)!^2 \prod_{k=1}^{n-m} e^{\frac{4c}{k^2}} \\
&\leq (n-m)!^2 \prod_{k=1}^{+\infty} e^{\frac{4c}{k^2}} \\
&= (n-m)!^2 e^{\sum_{k=1}^{+\infty} \frac{4c}{k^2}} \\
&= (n-m)!^2 e^{\frac{2\pi^2}{3}c}.
\end{aligned}$$

D'où l'on a :

$$\begin{aligned}
\frac{\prod_{k=m}^{n}\left(k^2+c\right)}{c\cdot(n-m)!\prod_{k=1}^{n-m}\left(k^2+4c\right)} &\geq \frac{\prod_{k=m}^{n} k^2}{c\cdot(n-m)!\cdot(n-m)!^2 e^{\frac{2\pi^2}{3}c}} \\
&= \frac{m^2\left(\frac{n!}{m!}\right)^2}{c\cdot(n-m)!^3 e^{\frac{2\pi^2}{3}c}} \\
&= \frac{e^{-\frac{2\pi^2}{3}c}}{c}\cdot m^2 \frac{n!^2}{m!^2(n-m)!^3}.
\end{aligned}$$

Le second point du théorème découle alors du premier et de cette dernière minoration. Le théorème est démontré. ∎

Nous allons maintenant imposer des conditions sur m (en fonction de n) afin d'optimiser (resp. de simplifier) l'estimation du second point du théorème 2.11. Pour ce faire, nous devons d'abord nous débarrasser des factoriels figurant dans cette estimation. On a le corollaire suivant :

Corollaire 2.12. *Soient $c, n, m \in \mathbb{N}^*$ tels que $m < n$. Alors, on a :*

$$L_{c,m,n} \geq \lambda_2(c) \cdot \frac{nm}{(n-m)^{3/2}} \left(\frac{m^2}{(n-m)^3} \right)^{n-m} e^{3(n-m)}, \tag{2.5.1}$$

où $\lambda_2(c) := \frac{e^{-\frac{2\pi^2}{3}c - \frac{5}{12}}}{(2\pi)^{3/2}c}$.

Démonstration. En partant de la minoration du second point du théorème 2.11 pour $L_{c,m,n}$ et en estimant chacun des factoriels qui y figurent en se servant de la double inégalité bien connue :

$$k^k e^{-k}\sqrt{2\pi k} \leq k! \leq k^k e^{-k}\sqrt{2\pi k} e^{\frac{1}{12k}} \quad (\forall k \in \mathbb{N}^*)$$

(que l'on peut trouver dans [35, Problem 1.15]), on obtient :

$$L_{c,m,n} \geq \lambda_1(c)(2\pi)^{-3/2} \cdot \frac{nm}{(n-m)^{3/2}} \cdot \left(\frac{n}{m}\right)^{2n} \cdot \left(\frac{m^2}{(n-m)^3} \right)^{n-m} e^{n-m} \cdot e^{-\frac{1}{6m} - \frac{1}{4(n-m)}}.$$

Par suite, comme $e^{-\frac{1}{6m} - \frac{1}{4(n-m)}} \geq e^{-\frac{1}{6} - \frac{1}{4}} = e^{-\frac{5}{12}}$ et $\left(\frac{n}{m}\right)^{2n} = e^{-2n\log(\frac{m}{n})} \geq e^{-2n(\frac{m}{n}-1)} = e^{2(n-m)}$, on en déduit que :

$$L_{c,m,n} \geq \lambda_1(c)(2\pi)^{-3/2} e^{-5/12} \cdot \frac{nm}{(n-m)^{3/2}} \left(\frac{m^2}{(n-m)^3} \right)^{n-m} e^{3(n-m)},$$

comme il fallait le prouver. ∎

Dans le contexte du corollaire 2.12, en supposant que $(n-m)$ est d'un ordre de grandeur n^α pour n assez grand (où $0 < \alpha < 1$), alors la partie dominante de la minoration (2.5.1) de $L_{c,m,n}$ est $\left(\frac{m^2}{(n-m)^3} \right)^{n-m}$, qui est d'ordre de grandeur $n^{(2-3\alpha)n^\alpha}$. Ainsi, pour avoir une estimation optimale, nous devons prendre α inférieurement proche de $\frac{2}{3}$ (une étude de la fonction $\alpha \longmapsto (2-3\alpha)n^\alpha$ montre que la meilleure valeur de α est $\alpha = \frac{2}{3} - \frac{1}{\log n}$). Un résultat concret spécifiant ce raisonnement heuristique est donné par le théorème suivant :

Théorème 2.13. *Soient $c, m, n \in \mathbb{N}^*$ tels que $m \leq n - \frac{1}{2}n^{2/3}$. Alors, on a :*

$$L_{c,m,n} \geq \lambda_3(c) \cdot \left(n - \frac{1}{2}n^{2/3} \right) \cdot \left(2e^3\right)^{\left\lfloor \frac{1}{2}n^{2/3} \right\rfloor},$$

où $\lambda_3(c) := \frac{e^{-\frac{2\pi^2}{3}c - \frac{5}{12}}}{\pi^{3/2}c}$.

Démonstration. Un simple calcul montre que le résultat du théorème est vrai pour $n < 3$. Supposons pour la suite que $n \geq 3$ et posons $m_n := n - \left\lfloor \frac{1}{2}n^{2/3} \right\rfloor < n$; donc $m \leq m_n$. D'après le corollaire 2.12, on a :

$$\begin{aligned} L_{c,m_n,n} &\geq \lambda_2(c) \frac{n\left(n - \left\lfloor \frac{1}{2}n^{2/3} \right\rfloor\right)}{\left\lfloor \frac{1}{2}n^{2/3} \right\rfloor^{3/2}} \left(\frac{\left(n - \left\lfloor \frac{1}{2}n^{2/3} \right\rfloor\right)^2}{\left\lfloor \frac{1}{2}n^{2/3} \right\rfloor^3} \right)^{\left\lfloor \frac{1}{2}n^{2/3} \right\rfloor} e^{3\left\lfloor \frac{1}{2}n^{2/3} \right\rfloor} \\ &\geq \lambda_2(c) \frac{n\left(n - \frac{1}{2}n^{2/3}\right)}{\left(\frac{1}{2}n^{2/3}\right)^{3/2}} \left(\frac{\left(n - \frac{1}{2}n^{2/3}\right)^2}{\left(\frac{1}{2}n^{2/3}\right)^3} \right)^{\left\lfloor \frac{1}{2}n^{2/3} \right\rfloor} e^{3\left\lfloor \frac{1}{2}n^{2/3} \right\rfloor} \\ &= 2^{3/2}\lambda_2(c)\left(n - \frac{1}{2}n^{2/3}\right)\left[8\left(1 - \frac{1}{2n^{1/3}}\right)^2\right]^{\left\lfloor \frac{1}{2}n^{2/3} \right\rfloor} e^{3\left\lfloor \frac{1}{2}n^{2/3} \right\rfloor}. \end{aligned}$$

Comme $1 - \frac{1}{2n^{1/3}} \geq \frac{1}{2}$ (car : $n \geq 1$), on en déduit que :

$$L_{c,m_n,n} \geq 2^{3/2}\lambda_2(c)\left(n - \frac{1}{2}n^{2/3}\right)\left(2e^3\right)^{\left\lfloor \frac{1}{2}n^{2/3} \right\rfloor}.$$

Le résultat requis découle du fait que $L_{c,m,n} \geq L_{c,m_n,n}$ (car : $m \leq m_n$). ∎

Par une autre façon, nous tirons du corollaire 2.12 le théorème suivant, qui complète (d'une certaine manière) le théorème 2.13 ci-dessus.

Théorème 2.14. *Soient $c, m, n \in \mathbb{N}^*$ tels que $n - \frac{1}{2}n^{2/3} \leq m \leq n$. Alors, on a :*

$$L_{c,m,n} \geq \lambda_2(c) \cdot ne^{3(n-m)},$$

où $\lambda_2(c)$ est déjà défini dans le corollaire 2.12.

Démonstration. Le résultat du théorème est trivial pour $m = n$. Supposons pour la suite que $m < n$; donc $n \geq 2$. Maintenant, soit $f : [0, n] \longrightarrow \mathbb{R}$ la fonction définie par $f(x) = x^2 - (n - x)^3$ $(\forall x \in [0, n])$. Il est clair que f est strictement croissante. Par suite, on a :

$$\begin{aligned} f\left(n - \frac{1}{2}n^{2/3}\right) &= \left(n - \frac{1}{2}n^{2/3}\right)^2 - \left(\frac{1}{2}n^{2/3}\right)^3 \\ &= n^2 - n^{5/3} + \frac{1}{4}n^{4/3} - \frac{1}{8}n^2 \\ &= \frac{7}{8}n^2 - n^{5/3} + \frac{1}{4}n^{4/3}. \end{aligned}$$

Puisque $n^2 \geq \frac{8}{7}n^{5/3}$ (car $n \geq 2$), il s'ensuit que $f\left(n - \frac{1}{2}n^{2/3}\right) \geq \frac{1}{4}n^{4/3} > 0$. Par suite, la croissance de f assure que $f(m) > 0$ (car $m \geq n - \frac{1}{2}n^{2/3}$ par hypothèse). D'où $\frac{m^2}{(n-m)^3} > 1$ et $\frac{m}{(n-m)^{3/2}} > 1$. En combinant cela avec (2.5.1), on en déduit que :

$$L_{c,m,n} \geq \lambda_2(c) \cdot ne^{3(n-m)},$$

comme il fallait le prouver. Ce qui complète cette démonstration. ∎

2.5.1 Comparaison avec la minoration de Oon

Dans la minoration de Oon (c'est-à-dire le théorème 1.42), le nombre de termes figurant dans le plus petit commun multiple

$$L_{c,m,n} = \text{ppcm}(m^2 + c, (m+1)^2 + c, \ldots, n^2 + c)$$

est strictement plus grand que $n/2$; alors que lorsque nous mettons ensemble nos théorèmes 2.13 et 2.14, cette contrainte est éliminée. Cependant, si la condition d'application du théorème de Oon est remplie, nous obtenons alors une minoration pour $L_{c,m,n}$ plus forte que celles de nos théorèmes. Ceci dit, notre résultat clé est plutôt le point 1 du théorème 2.11 qui fournit un diviseur rationnel et non trivial de $L_{c,m,n}$. Ici, nous avons exploité ce résultat clé de manière naïve. Il est probable qu'une "procédure plus intelligente" donnerait de meilleurs résultats.

CHAPITRE 3

Identités et estimations concernant le ppcm de suites à forte divisibilité

Il est à noter que les résultats de ce chapitre sont publiés dans [8].

3.1 Introduction

L'étude des propriétés arithmétiques des coefficients binomiaux est un sujet très ancien et fascinant. À titre d'exemple, il y a plus d'un siècle que Sylvester [47] prouvait que pour tous $n, k \in \mathbb{N}^*$, tels que $n \geq 2k$, le coefficient binomial $\binom{n}{k}$ possède au moins un diviseur premier strictement supérieur à k. Assez récemment, Farhi [18] a montré l'identité $\operatorname{ppcm}\left\{\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n}\right\} = \frac{\operatorname{ppcm}(1,2,\ldots,n,n+1)}{n+1}$ $(\forall n \in \mathbb{N})$, que Guo [22] a généralisé aux coefficients q-binomiaux. Dans ce chapitre, nous présentons d'abord une démonstration de cette identité ; ensuite nous démontrons une identité plus générale relative aux suites à forte divisibilité. Cette identité générale englobe à la fois les identités de Farhi et Guo qui en deviennent des cas particuliers (voir le théorème 3.7 et la remarque 3.12). Nous en déduisons par suite deux autres identités également intéressantes (voir les corollaires 3.9 et 3.10). Comme application, nous utilisons nos identités pour établir des estimations effectives et non triviales du ppcm des termes consécutifs de certaines suites de Lucas

(voir le théorème 3.13). L'efficacité de nos estimations effectives est garantie par les estimations asymptotiques obtenues par Matiyasevich et Guy [36] et Kiss et Matyas [33] dans le même contexte.

3.2 Une identité concernant le ppcm des coefficients binomiaux usuels

Le théorème suivant est le résultat principal de l'article [18].

Théorème 3.1 (Farhi [18]). *Pour tout entier naturel n, on a :*

$$\operatorname{ppcm}\left\{\binom{n}{0},\binom{n}{1},\dots,\binom{n}{n}\right\}=\frac{\operatorname{ppcm}(1,2,\dots,n,n+1)}{n+1}. \tag{3.2.1}$$

La preuve présentée dans [18] utilise le théorème de Kummer qui donne la valuation p-adique des coefficients binomiaux. Plus précisément, on a :

Théorème 3.2 (Kummer). *Soient $k,n\in\mathbb{N}$ et p un nombre premier. Alors, la valuation p-adique du nombre $\binom{n}{k}$ est égale au nombre d'emprunts effectués lorsque l'on soustrait k de n suivant le système de numération de base p.*

Démonstration. Considérons d'abord les représentations en base p des nombres n, k et $n-k$:

$$\begin{aligned} n &= a_r p^r + a_{r-1}p^{r-1}+\cdots+a_1 p+a_0,\\ k &= b_r p^r + b_{r-1}p^{r-1}+\cdots+b_1 p+b_0,\\ n-k &= c_r p^r + c_{r-1}p^{r-1}+\cdots+c_1 p+c_0, \end{aligned}$$

où $r\in\mathbb{N}$ et $a_0,a_1,\dots,a_r,b_0,b_1,\dots,b_r,c_0,c_1,\dots,c_r\in\{0,1,\dots,p-1\}$. Les emprunts requis $(\gamma_i)_{0\le i\le r}$ pour soustraire k de n suivant le système de base p sont alors donnés par :

$$\gamma_0 := \begin{cases} 1 & \text{si } a_0<b_0\\ 0 & \text{sinon} \end{cases},$$

et pour tout $i \in \{1, 2, \ldots, r\}$:

$$\gamma_i := \begin{cases} 1 & \text{si } a_i - b_i - \gamma_{i-1} < 0 \\ 0 & \text{sinon} \end{cases}.$$

Le nombre d'emprunts non nuls (c'est-à-dire de véritables emprunts) est alors égal à $\gamma_0 + \gamma_1 + \cdots + \gamma_r$. On vérifie facilement (à partir de la définition des γ_i) que l'on a : $\gamma_r = 0$, $c_r = a_r - b_r - \gamma_{r-1}$, $c_0 = a_0 - b_0 + p\gamma_0$ et $c_i = a_i - b_i - \gamma_{i-1} + p\gamma_i$ ($\forall i \in \{1, 2, \ldots, r-1\}$). D'autre part, en désignant par $s_p(\ell)$ ($\ell \in \mathbb{N}$) la somme des chiffres de ℓ dans sa représentation en base p, on obtient (en vertu de la formule de Legendre) :

$$\begin{aligned} \vartheta_p\left(\binom{n}{k}\right) &= \vartheta_p(n!) - \vartheta_p(k!) - \vartheta_p((n-k)!) \\ &= \frac{n - s_p(n)}{p-1} - \frac{k - s_p(k)}{p-1} - \frac{(n-k) - s_p(n-k)}{p-1} \\ &= \frac{s_p(k) + s_p(n-k) - s_p(n)}{p-1}. \end{aligned}$$

D'où :

$$\begin{aligned} \vartheta_p\left(\binom{n}{k}\right) &= \frac{(b_0 + c_0 - a_0) + (b_1 + c_1 - a_1) + \cdots + (b_r + c_r - a_r)}{p-1} \\ &= \frac{p\gamma_0 + (p\gamma_1 - \gamma_0) + \cdots + (p\gamma_{r-1} - \gamma_{r-2}) - \gamma_{r-1}}{p-1} \\ &= \frac{(p-1)\gamma_0 + (p-1)\gamma_1 + \cdots + (p-1)\gamma_{r-1}}{p-1} \\ &= \gamma_0 + \gamma_1 + \cdots + \gamma_{r-1}. \end{aligned}$$

Ce qui confirme le résultat requis et complète cette démonstration. ∎

Lemme 3.3 (Farhi [18]). *Soient $n \in \mathbb{N}$ et p un nombre premier. Supposons que $n = \sum_{i=0}^{N} c_i p^i$ est la représentation de n dans le système de numération de base p, avec $N \in \mathbb{N}$, $c_i \in \{0, \ldots, p-1\}$ ($\forall i \in \{0, 1, \ldots, N\}$) et $c_N \neq 0$. Alors, on a :*

$$\max_{0 \leq k \leq n} \vartheta_p\left(\binom{n}{k}\right) = \vartheta_p\left(\binom{n}{p^N - 1}\right) = \begin{cases} 0 & \text{si } n = p^{N+1} - 1 \\ N - \min\{i;\ c_i \neq p-1\} & \text{sinon} \end{cases}.$$

Démonstration. Nous distinguons les deux cas suivants :

•**1er cas :** (si $n = p^{N+1} - 1$). Dans ce cas, on a $c_i = p - 1$ pour tout $i \in \{0, 1, \ldots, N\}$. Par conséquent, la soustraction de tout $k \in \{0, 1, \ldots, n\}$ de n suivant le système de numération de base p ne nécessite aucun emprunt. Il s'ensuit (en vertu du théorème 3.2) que : $\vartheta_p\left(\binom{n}{k}\right) = 0$ $(\forall k \in \{0, 1, \ldots, n\})$. D'où l'on a :

$$\max_{0\leq k\leq n} \vartheta_p\left(\binom{n}{k}\right) = \vartheta_p\left(\binom{n}{p^N - 1}\right) = 0,$$

comme il fallait le prouver.

•**2nd cas :** (si $n \neq p^{N+1} - 1$). Dans ce cas, il existe au moins un $i \in \{0, 1, \ldots, N\}$ tel que $c_i \neq p - 1$. Posons $i_0 := \min\{i;\ c_i \neq p - 1\}$. Nous allons montrer que $\vartheta_p\left(\binom{n}{k}\right) \leq N - i_0$ $(\forall k \in \{0, 1, \ldots, n\})$ et que $\vartheta_p\left(\binom{n}{p^N-1}\right) = N - i_0$, ce qui conclura au résultat requis. Fixons $k \in \{0, 1, \ldots, n\}$. Par définition de i_0, on a : $c_0 = c_1 = \cdots = c_{i_0-1} = p - 1$. Donc lorsqu'on soustrait k de n suivant le système de base p, les premières i_0 soustractions chiffre-par-chiffre ne nécessitent aucun emprunt. Ce qui montre que le nombre d'emprunts requis dans cette soustraction est au plus égal à $N - i_0$. D'où l'on a (en vertu du théorème 3.2) :

$$\vartheta_p\left(\binom{n}{k}\right) \leq N - i_0 \quad (\forall k \in \{0, 1, \ldots, n\}).$$

Par ailleurs, puisque $c_{i_0} < p - 1$, alors lorsqu'on soustrait $p^N - 1 = \sum_{i=0}^{N-1}(p - 1)p^i$ de n suivant le système de base p, chacune des soustractions chiffre-par-chiffre du rang i_0 au rang $N - 1$ nécessite un emprunt. Ce qui entraîne (d'après le théorème 3.2) que :

$$\vartheta_p\left(\binom{n}{p^N - 1}\right) = N - i_0$$

et complète cette démonstration. ∎

Démonstration du théorème 3.1. Pour $n = 0$, l'identité (3.2.1) est triviale. Supposons pour la suite que $n \geq 1$ et désignons respectivement par A_n et B_n les membres de gauche et de droite de (3.2.1). Nous allons montrer que $\vartheta_p(A_n) = \vartheta_p(B_n)$ pour tout nombre premier p, ce qui conclura à l'identité (3.2.1). Fixons donc un nombre premier p et soit $\sum_{i=0}^{N} c_i p^i$ la représentation de n suivant le système de base p (où $N \in \mathbb{N}$, $c_i \in \{0, 1, \ldots, p - 1\}$ et

$c_N \neq 0$). D'après le lemme 3.3, on a :

$$\vartheta_p\left(A_n\right) = \begin{cases} 0 & \text{si } n = p^{N+1} - 1 \\ N - \min\{i;\ c_i \neq p-1\} & \text{sinon} \end{cases}. \tag{3.2.2}$$

D'autre part, puisque $\vartheta_p\left(\text{ppcm}\left(1, 2, \ldots, n, n+1\right)\right)$ est le plus grand exposant $\alpha \in \mathbb{N}$ tel que $p^\alpha \leq n+1$, alors :

$$\vartheta_p\left(\text{ppcm}\left(1, 2, \ldots, n, n+1\right)\right) = \begin{cases} N+1 & \text{si } n = p^{N+1} - 1 \\ N & \text{sinon} \end{cases}. \tag{3.2.3}$$

De plus, on constate que lorsque $n \neq p^{N+1} - 1$, on a : $(n+1) = (c_{i_0} + 1)\, p^{i_0} + c_{i_0+1} p^{i_0+1} + \cdots + c_N p^N$ (avec $i_0 := \min\{i;\ c_i \neq p-1\}$). D'où :

$$\vartheta_p\left(n+1\right) = \begin{cases} N+1 & \text{si } n = p^{N+1} - 1 \\ \min\{i;\ c_i \neq p-1\} & \text{sinon} \end{cases}. \tag{3.2.4}$$

En soustrayant (3.2.4) de (3.2.3) et en comparant ensuite avec (3.2.2), on obtient que $\vartheta_p\left(A_n\right) = \vartheta_p\left(B_n\right)$, comme il fallait le prouver. Ce qui complète cette démonstration. ∎

3.3 Quelques propriétés de suites à forte divisibilité

On rappelle qu'une suite d'entiers strictement positifs $\boldsymbol{a} = \left(a_n\right)_{n\geq 1}$ est dite *à forte divisibilité* lorsqu'elle vérifie la propriété :

$$\text{pgcd}\left(a_n, a_m\right) = a_{\text{pgcd}(n,m)} \qquad (\forall n, m \in \mathbb{N}^*).$$

D'après §1.3, une telle suite $\boldsymbol{a}$ lui correspond une unique suite d'entiers strictement positifs $\left(u_n\right)_{n\geq 1}$ telle que :

$$a_n = \prod_{d|n} u_d \qquad (\forall n \geq 1). \tag{3.3.1}$$

Le théorème suivant traite la correspondance inverse. Plus précisément, il établit une condition nécessaire et suffisante sur une suite d'entiers strictement positifs $\left(u_n\right)_{n\geq 1}$ pour que la suite $\left(\prod_{d|n} u_d\right)_{n\geq 1}$ soit à forte divisibilité.

Théorème 3.4 (Bliss et al. [6]). *Soient $(u_n)_{n\geq 1}$ une suite d'entiers strictement positifs et $(a_n)_{n\geq 1}$ la suite de terme général : $a_n = \prod_{d|n} u_d$ $(\forall n \in \mathbb{N}^*)$. Alors, les propriétés suivantes sont équivalentes :*

1. *La suite $(a_n)_{n\geq 1}$ est à forte divisibilité.*
2. *Pour tous $n, m \in \mathbb{N}^*$ tels que $n \nmid m$ et $m \nmid n$, on a :* $\operatorname{pgcd}(u_n, u_m) = 1$.

Démonstration.

• $(\Rightarrow)$: Supposons que la suite $(a_n)_{n\geq 1}$ est à forte divisibilité. Soient $m, n \in \mathbb{N}^*$ tels que $n \nmid m$ et $m \nmid n$ et posons $\delta := \operatorname{pgcd}(n, m)$. Il existe donc $n', m' \in \mathbb{N}^*$ tels que $n = \delta n'$, $m = \delta m'$ et $\operatorname{pgcd}(n', m') = 1$. Puisque $n \nmid m$ et $m \nmid n$ alors $n', m' \neq 1$. Par suite, on a (puisque $(a_n)_{n\geq 1}$ est à forte divisibilité) :

$$\operatorname{pgcd}\left(\prod_{d|n, d\nmid\delta} u_d, \prod_{d|m, d\nmid\delta} u_d\right)\prod_{d|\delta} u_d = \operatorname{pgcd}\left(\prod_{d|n} u_d, \prod_{d|m} u_d\right) = \operatorname{pgcd}(a_n, a_m) = a_\delta = \prod_{d|\delta} u_d.$$

Ce qui entraîne que :

$$\operatorname{pgcd}\left(\prod_{d|n, d\nmid\delta} u_d, \prod_{d|m, d\nmid\delta} u_d\right) = 1.$$

Comme on a de toute évidence : $u_n \mid \prod_{d|n, d\nmid\delta} u_d$ et $u_m \mid \prod_{d|m, d\nmid\delta} u_d$, il en découle à fortiori que : $\operatorname{pgcd}(u_n, u_m) = 1$, comme il fallait le prouver.

• $(\Leftarrow)$: Inversement, supposons que pour tous $n, m \in \mathbb{N}^*$ tels que $n \nmid m$ et $m \nmid n$, on a : $\operatorname{pgcd}(u_n, u_m) = 1$ et montrons que $\operatorname{pgcd}(a_n, a_m) = a_{\operatorname{pgcd}(n,m)}$ $(\forall n, m \in \mathbb{N}^*)$. Fixons $n, m \in \mathbb{N}^*$ et posons $\delta := \operatorname{pgcd}(n, m)$. Il existe donc $n', m' \in \mathbb{N}^*$ tels que $n = \delta n'$, $m = \delta m'$ et $\operatorname{pgcd}(n', m') = 1$. Nous distinguons les deux cas suivants :

1er cas : (si $n' = 1$ ou $m' = 1$). Dans ce cas, on a visiblement $n = \delta$ ou $m = \delta$. Sans perte de généralité, supposons que $n = \delta$ (le cas où $m = \delta$ se traite de la même façon). Puisque tout diviseur de δ est également un diviseur de $\delta m'$, alors $\prod_{d|\delta} u_d$ divise $\prod_{d|\delta m'} u_d$. On a par conséquent :

$$\operatorname{pgcd}(a_n, a_m) = \operatorname{pgcd}(a_\delta, a_{\delta m'}) = \operatorname{pgcd}\left(\prod_{d|\delta} u_d, \prod_{d|\delta m'} u_d\right) = \prod_{d|\delta} u_d = a_\delta = a_{\operatorname{pgcd}(n,m)},$$

comme il fallait le prouver.

2nd cas : (si $n', m' \neq 1$). Dans ce cas, on a $n \nmid m$ et $m \nmid n$, donc $\operatorname{pgcd}(u_n, u_m) = 1$ (par hypothèse). De plus, on a :

$$\operatorname{pgcd}(a_n, a_m) = \operatorname{pgcd}\left(\prod_{d|n, d\nmid\delta} u_d, \prod_{d|m, d\nmid\delta} u_d\right) a_\delta. \tag{3.3.2}$$

Maintenant, on constate que si $d_1, d_2 \in \mathbb{N}^*$ vérifient : $(d_1 \mid n, d_1 \nmid \delta)$ et $(d_2 \mid m, d_2 \nmid \delta)$, alors $\operatorname{pgcd}(d_1, d_2)$ divise δ ; ce qui fait que : $\operatorname{pgcd}(d_1, d_2) \notin \{d_1, d_2\}$ et donc $d_1 \nmid d_2$ et $d_2 \nmid d_1$; d'où (par hypothèse) : $\operatorname{pgcd}(u_{d_1}, u_{d_2}) = 1$. Il découle de ce fait que :

$$\operatorname{pgcd}\left(\prod_{d|n, d\nmid\delta} u_d, \prod_{d|m, d\nmid\delta} u_d\right) = 1.$$

En substituant cette dernière dans (3.3.2), on obtient l'égalité requise :

$$\operatorname{pgcd}(a_n, a_m) = a_\delta = a_{\operatorname{pgcd}(n,m)}.$$

Ce qui complète cette démonstration. ∎

Nowicki [40] a développé la propriété 2 du théorème 3.4 de Bliss et al. et a obtenu une autre quelque part plus pratique. On a le théorème suivant :

Théorème 3.5 (Nowicki [40]). *Soient $(a_n)_{n\geq 1}$ une suite d'entiers strictement positifs et $(c_n)_{n\geq 1}$ la suite d'entiers définie par : $c_1 = a_1$ et*

$$c_n := \frac{\operatorname{ppcm}(a_1, \ldots, a_n)}{\operatorname{ppcm}(a_1, \ldots, a_{n-1})} \qquad (\forall n \geq 2).$$

Alors $(a_n)_n$ est à forte divisibilité si et seulement si l'on a :

$$a_n = \prod_{d|n} c_d \qquad (\forall n \geq 1).$$

Démonstration.

• ($\Rightarrow$) : Supposons que $(a_n)_{n\geq 1}$ est à forte divisibilité. En vertu de (3.3.1), il existe une unique suite d'entiers strictement positifs $(u_n)_{n\geq 1}$ vérifiant : $a_n = \prod_{d|n} u_d$ $(\forall n \geq 1)$. Considérons la suite $(e_n)_{n\geq 1}$ donnée par $e_1 = 1$ et $e_{n+1} = \operatorname{ppcm}(e_n, a_n)$ $(\forall n \in \mathbb{N}^*)$. Nous procédons par récurrence pour montrer que :

$$e_{n+1} = u_1 u_2 \cdots u_n \qquad (\forall n \in \mathbb{N}^*), \tag{3.3.3}$$

ce qui entraînera que $(u_n)_n$ est identique à $(c_n)_n$ et conclura au résultat requis. Pour $n = 1$, le résultat est trivial ; en effet, on a : $e_2 = \text{ppcm}\,(e_1, a_1) = a_1 = u_1$. Supposons pour la suite que $n \geq 2$ et que $e_n = u_1 u_2 \cdots u_{n-1}$. Il s'ensuit que :

$$e_{n+1} = \text{ppcm}\,(e_n, a_n) = \text{ppcm}\left(\prod_{k=1}^{n-1} u_k, \prod_{d|n} u_d\right) = \text{ppcm}\,(A \cdot B, A \cdot u_n) = A \cdot \text{ppcm}\,(B, u_n)\,,$$

avec $A := \prod_{d|n, d<n} u_d$ et $B := \prod_{d\nmid n, d<n} u_d$. Par ailleurs, on a (en vertu du théorème 3.4) : $\text{pgcd}\,(u_d, u_n) = 1$ pour tout $1 \leq d < n$ tel que $d \nmid n$. On a par conséquent : $\text{pgcd}\,(B, u_n) = 1$. Ce qui entraîne que :

$$e_{n+1} = ABu_n = \left(\prod_{k=1}^{n-1} u_k\right) \cdot u_n = u_1 u_2 \cdots u_n,$$

comme il fallait le prouver.

• ($\Leftarrow$) : Inversement, supposons que $a_n = \prod_{d|n} c_d$ ($\forall n \geq 1$). Fixons $m \in \mathbb{N}^*$ et posons :

$$U := \prod_{d|n, d<m} c_d, \quad V := \prod_{d\nmid n, d<m} c_d.$$

On a :

$$\begin{aligned} UVc_m &= \prod_{i=1}^{m} c_i = \text{ppcm}\,(a_1, \ldots, a_m) = \text{ppcm}\,(\text{ppcm}\,(a_1, \ldots, a_{m-1})\,, a_m) \\ &= \text{ppcm}\left(\prod_{i=1}^{m-1} c_i, \prod_{d|m} c_d\right) = \text{ppcm}\,(U \cdot V, U \cdot c_m) = U \cdot \text{ppcm}\,(V, c_m)\,. \end{aligned}$$

Ce qui entraîne que $V \cdot c_m = \text{ppcm}\,(V, c_m)$, donc $\text{pgcd}\,(V, c_m) = 1$. Par conséquent, on a pour tout $1 \leq d < m$ tel que $d \nmid m$: $\text{pgcd}\,(c_d, c_m) = 1$; cela revient à dire que pour tous $n, m \in \mathbb{N}^*$ tels que $n \nmid m$ et $m \nmid n$, on a : $\text{pgcd}\,(c_m, c_n) = 1$. Ce qui montre (en vertu du théorème 3.4) que $(a_n)_{n\geq 1}$ est à forte divisibilité. Le théorème est ainsi démontré. ∎

3.4 Identités concernant le ppcm de suites à forte divisibilité

Pour généraliser l'identité (3.2.1), nous allons d'abord définir les coefficients binomiaux associés à une suite à forte divisibilité. Étant donné une telle suite $\boldsymbol{a} := (a_n)_{n\geq 1}$, pour

tout entier naturel n, on désigne par $[n]_{\boldsymbol{a}}!$ l'entier strictement positif défini par :

$$[n]_{\boldsymbol{a}}! := a_1 a_2 \cdots a_n,$$

(en convenant que $[0]_{\boldsymbol{a}}! = 1$). Pour $n, k \in \mathbb{N}$, avec $n \geq k$, on désigne par $\binom{n}{k}_{\boldsymbol{a}}$ le nombre rationnel strictement positif défini par :

$$\binom{n}{k}_{\boldsymbol{a}} := \frac{a_n a_{n-1} \cdots a_{n-k+1}}{a_1 a_2 \ldots a_k} = \frac{[n]_{\boldsymbol{a}}!}{[k]_{\boldsymbol{a}}![n-k]_{\boldsymbol{a}}!}.$$

Ces nombres sont appelés les coefficients $\boldsymbol{a}$-binomiaux. Les coefficients binomiaux usuels s'obtiennent en prenant simplement $a_n = n$ ($\forall n \geq 1$). D'après la définition, on vérifie facilement que les coefficients $\boldsymbol{a}$-binomiaux vérifient les identités suivantes :

$$\binom{n}{k}_{\boldsymbol{a}} = \binom{n}{n-k}_{\boldsymbol{a}} \qquad (\forall n, k \in \mathbb{N}, n \geq k) \tag{3.4.1}$$

$$a_k \binom{n+1}{k}_{\boldsymbol{a}} = a_{n+1} \binom{n}{k-1}_{\boldsymbol{a}} \qquad (\forall n, k \in \mathbb{N}, 1 \leq k \leq n+1) \tag{3.4.2}$$

$$\binom{n}{k}_{\boldsymbol{a}} \binom{k}{l}_{\boldsymbol{a}} = \binom{n}{l}_{\boldsymbol{a}} \binom{n-l}{k-l}_{\boldsymbol{a}} \qquad (\forall n, k, l \in \mathbb{N}, l \leq k \leq n)\,. \tag{3.4.3}$$

En utilisant la représentation (3.3.1) pour le cas particulier $a_n = q^n - 1$ (où $q \geq 2$ est un nombre entier), Knuth et Wilf ont montré une formule importante pour les coefficients binomiaux de Gauss (voir [34, Equation (10)]). En fait, cette formule peut être facilement généralisée pour toute suite à forte divisibilité, comme le montre la proposition suivante :

Proposition 3.6 (Knuth [34])**.** *Soient $(u_n)_{n\geq 1}$ une suite d'entiers strictement positifs et $(a_n)_{n\geq 1}$ la suite de terme général :*

$$a_n = \prod_{d|n} u_d \qquad (\forall n \in \mathbb{N}^*)\,.$$

Alors, pour tous $n, k \in \mathbb{N}$ tels que $n \geq k$, on a :

$$\binom{n}{k}_{\boldsymbol{a}} = \prod_{d} u_d,$$

où le produit porte sur les entiers strictement positifs $d \leq n$ tels que :

$$\left\lfloor \frac{k}{d} \right\rfloor + \left\lfloor \frac{n-k}{d} \right\rfloor < \left\lfloor \frac{n}{d} \right\rfloor.$$

En particulier, les coefficients $\boldsymbol{a}$*-binomiaux* $\binom{n}{k}_{\boldsymbol{a}}$ $(n,k\in\mathbb{N},\ n\geq 1)$ *sont tous des entiers strictement positifs.*

Démonstration. Soient $n,k\in\mathbb{N}$ tels que $n\geq k$. On a (en vertu de (3.3.1)) :

$$\binom{n}{k}_{\boldsymbol{a}}:=\frac{\prod_{n-k<m\leq n}a_m}{\prod_{1\leq m\leq k}a_m}=\frac{\prod_{n-k<m\leq n}\prod_{d|m}u_d}{\prod_{1\leq m\leq k}\prod_{d|m}u_d}.$$

Comme on a :

$$\prod_{n-k<m\leq n}\prod_{d|m}u_d=\prod_{1\leq d\leq n}\prod_{\substack{n-k<m\leq n\\ m\equiv 0 \pmod d}}u_d=\prod_{1\leq d\leq n}u_d^{\left\lfloor\frac{n}{d}\right\rfloor-\left\lfloor\frac{n-k}{d}\right\rfloor}=\prod_{d\geq 1}u_d^{\left\lfloor\frac{n}{d}\right\rfloor-\left\lfloor\frac{n-k}{d}\right\rfloor}$$

et

$$\prod_{1\leq m\leq k}\prod_{d|m}u_d=\prod_{1\leq d\leq k}\prod_{\substack{1\leq m\leq k\\ m\equiv 0 \pmod d}}u_d=\prod_{1\leq d\leq k}u_d^{\left\lfloor\frac{k}{d}\right\rfloor}=\prod_{d\geq 1}u_d^{\left\lfloor\frac{k}{d}\right\rfloor},$$

il s'ensuit que :

$$\binom{n}{k}_{\boldsymbol{a}}=\prod_{d\geq 1}u_d^{\left\lfloor\frac{n}{d}\right\rfloor-\left\lfloor\frac{k}{d}\right\rfloor-\left\lfloor\frac{n-k}{d}\right\rfloor}.$$

L'identité requise de la proposition découle du fait que :

$$\left\lfloor\frac{n}{d}\right\rfloor-\left\lfloor\frac{k}{d}\right\rfloor-\left\lfloor\frac{n-k}{d}\right\rfloor\in\{0,1\}\qquad(\forall d\geq 1).$$

Ce qui complète cette démonstration. ∎

Notre résultat principal est le suivant :

Théorème 3.7. *Soit* $\boldsymbol{a}=(a_n)_{n\geq 1}$ *une suite à forte divisibilité. Alors, pour tout* $n\in\mathbb{N}$*, on a :*

$$\operatorname{ppcm}\left\{\binom{n}{0}_{\boldsymbol{a}},\binom{n}{1}_{\boldsymbol{a}},\ldots,\binom{n}{n}_{\boldsymbol{a}}\right\}=\frac{\operatorname{ppcm}(a_1,a_2,\ldots,a_n,a_{n+1})}{a_{n+1}}.\tag{3.4.4}$$

Pour démontrer le théorème 3.7, nous utiliserons le lemme de Guo [22] suivant :

Lemme 3.8 (Guo [22])**.** *Soient* n *et* d *deux entiers strictement positifs tels que* $n\geq d$*. Alors, les deux propriétés suivantes sont équivalentes :*

1. *Il existe* $k\in\{0,1,\ldots,n\}$ *tel que :* $\left\lfloor\frac{k}{d}\right\rfloor+\left\lfloor\frac{n-k}{d}\right\rfloor<\left\lfloor\frac{n}{d}\right\rfloor$.
2. *Le nombre* d *ne divise pas* $(n+1)$.

Démonstration. Supposons que la première propriété du lemme est vérifiée et désignons respectivement par a et b les restes des divisions euclidiennes de k et $(n-k)$ sur d. Notre hypothèse est alors équivalente à :

$$\left\lfloor \frac{a}{d} \right\rfloor + \left\lfloor \frac{b}{d} \right\rfloor < \left\lfloor \frac{a+b}{d} \right\rfloor .$$

Ce qui entraîne que : $1 \leq a, b \leq d-1$ et $d \leq a+b \leq 2d-2$. Puisque $n \equiv a+b \pmod{d}$, alors $n+1 \equiv a+b+1 \not\equiv 0 \pmod{d}$, comme il fallait le prouver.

Inversement, supposons que $n+1 \equiv c \pmod{d}$ pour un certain $c \in \{1, 2, \ldots, d-1\}$. Il existe donc un $q \in \mathbb{N}^*$ tel que $n+1 = c+qd$. On a par conséquent :

$$\left\lfloor \frac{c}{d} \right\rfloor + \left\lfloor \frac{n-c}{d} \right\rfloor = \left\lfloor \frac{qd-1}{d} \right\rfloor = q-1 \leq \left\lfloor \frac{n}{d} \right\rfloor - 1 < \left\lfloor \frac{n}{d} \right\rfloor .$$

On conclut à la première propriété du lemme en prenant $k = c$. Ce qui complète cette démonstration. ∎

Démonstration du théorème 3.7. Pour $n = 0$, l'identité (3.4.4) du théorème 3.7 est triviale. Supposons pour la suite que $n \geq 1$ et désignons respectivement par A_n et B_n le membre de gauche et le membre de droite de (3.4.4). Nous allons montrer que A_n divise B_n puis que B_n divise A_n, ce qui conclura que $A_n = B_n$. Puisque la suite $\boldsymbol{a}$ est à forte divisibilité, alors (d'après le théorème 3.5) on a pour tout entier $m \geq 1$:

$$a_m = \prod_{d \mid m} u_d,$$

où $(u_d)_{d \geq 1}$ est la suite d'entiers strictement positifs définie par :

$$u_1 := a_1 \quad \text{et} \quad u_d := \frac{\operatorname{ppcm}(a_1, \ldots, a_d)}{\operatorname{ppcm}(a_1, \ldots, a_{d-1})} \qquad (\forall d \geq 2) .$$

D'autre part, de la définition de $(u_d)_d$, découle immédiatement que :

$$\operatorname{ppcm}(a_1, \ldots, a_m) = \prod_{d=1}^{m} u_d \qquad (\forall m \geq 1) .$$

Maintenant, pour tout $k \in \{0, 1, \ldots, n\}$, le produit $\prod_d u_d = \binom{n}{k}_{\boldsymbol{a}}$ fourni par la proposition 3.6 porte sur les entiers d qui vérifient tous (d'après le lemme 3.8) : $1 \leq d \leq n$ et $d \nmid (n+1)$.

Cela implique que le produit :

$$\prod_{\substack{1\leq d\leq n\\ d\nmid(n+1)}} u_d = \frac{\displaystyle\prod_{1\leq d\leq n+1} u_d}{\displaystyle\prod_{d\mid(n+1)} u_d} = \frac{\operatorname{ppcm}(a_1,\ldots,a_n,a_{n+1})}{a_{n+1}} = B_n$$

est un multiple de chacun des nombres $\binom{n}{k}_{\boldsymbol{a}}$ $(0\leq k\leq n)$. D'où B_n est un multiple de :

$$\operatorname{ppcm}\left\{\binom{n}{0}_{\boldsymbol{a}},\binom{n}{1}_{\boldsymbol{a}},\ldots,\binom{n}{n}_{\boldsymbol{a}}\right\} = A_n.$$

Ce qui montre que $A_n \mid B_n$. Inversement, il est immédiat que :

$$\operatorname{ppcm}(a_1,a_2,\ldots,a_{n+1}) \text{ divise } \operatorname{ppcm}\left\{a_1\binom{n+1}{1}_{\boldsymbol{a}},a_2\binom{n+1}{2}_{\boldsymbol{a}},\ldots,a_{n+1}\binom{n+1}{n+1}_{\boldsymbol{a}}\right\},$$

qui est égal (en vertu de (3.4.2)) à :

$$\begin{aligned}\operatorname{ppcm}\left\{a_{n+1}\binom{n}{0}_{\boldsymbol{a}},a_{n+1}\binom{n}{1}_{\boldsymbol{a}},\ldots,a_{n+1}\binom{n}{n}_{\boldsymbol{a}}\right\} &= a_{n+1}\operatorname{ppcm}\left\{\binom{n}{0}_{\boldsymbol{a}},\binom{n}{1}_{\boldsymbol{a}},\ldots,\binom{n}{n}_{\boldsymbol{a}}\right\}\\ &= a_{n+1}A_n.\end{aligned}$$

D'où l'on déduit que :

$$\frac{\operatorname{ppcm}(a_1,\ldots,a_n,a_{n+1})}{a_{n+1}} = B_n \text{ divise } A_n.$$

Ce qui complète cette démonstration. ∎

Du théorème 3.7, nous tirons les deux corollaires suivants :

Corollaire 3.9. *Soit $\boldsymbol{a}=(a_n)_{n\geq 1}$ une suite à forte divisibilité. Alors, pour tout entier strictement positif n, on a :*

$$\operatorname{ppcm}(a_1,a_2,\ldots,a_n) = \operatorname{ppcm}\left\{a_1\binom{n}{1}_{\boldsymbol{a}},\ldots,a_n\binom{n}{n}_{\boldsymbol{a}}\right\}.$$

Démonstration. Pour tout entier strictement positif n, on a d'après la formule (3.4.2) :

$$\begin{aligned}\operatorname{ppcm}\left\{a_1\binom{n}{1}_{\boldsymbol{a}},\ldots,a_n\binom{n}{n}_{\boldsymbol{a}}\right\} &= \operatorname{ppcm}\left\{a_n\binom{n-1}{0}_{\boldsymbol{a}},a_n\binom{n-1}{1}_{\boldsymbol{a}},\ldots,a_n\binom{n-1}{n-1}_{\boldsymbol{a}}\right\}\\ &= a_n\operatorname{ppcm}\left\{\binom{n-1}{0}_{\boldsymbol{a}},\binom{n-1}{1}_{\boldsymbol{a}},\ldots,\binom{n-1}{n-1}_{\boldsymbol{a}}\right\}\\ &= \operatorname{ppcm}(a_1,\ldots,a_n) \qquad \text{(d'après le théorème 3.7)},\end{aligned}$$

comme il fallait le prouver. ∎

Corollaire 3.10. *Soit $\boldsymbol{a} = (a_n)_{n\geq 1}$ une suite à forte divisibilité. Alors, pour tout entier strictement positif n, on a :*

$$\operatorname{ppcm}(a_1, a_2, \ldots, a_n) = \operatorname{pgcd}\left\{ \binom{n}{k}_{\boldsymbol{a}} \operatorname{ppcm}(a_1, \ldots, a_k)\,;\ n/2 \leq k \leq n \right\}.$$

Pour présenter une preuve plus propre de ce corollaire, nous faisons intervenir le lemme élémentaire suivant :

Lemme 3.11. *Soient $n, m \in \mathbb{N}^*$ et $a_1, \ldots, a_n$, $b_1, \ldots, b_m$ des entiers strictement positifs. Alors, la propriété affirmant que : a_i divise b_j pour tous i, j tels que $1 \leq i \leq n$ et $1 \leq j \leq m$ est équivalente à la propriété affirmant que $\operatorname{ppcm}(a_1, \ldots, a_n)$ divise $\operatorname{pgcd}(b_1, \ldots, b_m)$.*

Démonstration du corollaire 3.10. Soit $n \in \mathbb{N}^*$ fixé. Pour $k, \ell \in \mathbb{N}$ tels que $n/2 \leq k \leq n$ et $1 \leq \ell \leq k$, on a visiblement $a_\ell \binom{n}{\ell}_{\boldsymbol{a}}$ divise $a_\ell \binom{n}{\ell}_{\boldsymbol{a}} \binom{n-\ell}{k-\ell}_{\boldsymbol{a}}$, qui est égale (en vertu de (3.4.3)) à $a_\ell \binom{n}{k}_{\boldsymbol{a}} \binom{k}{\ell}_{\boldsymbol{a}}$. Mais ce dernier nombre divise clairement le nombre :

$$\binom{n}{k}_{\boldsymbol{a}} \operatorname{ppcm}\left\{ a_i \binom{k}{i}_{\boldsymbol{a}}\,;\ i = 1, \ldots, k \right\},$$

qui est égale (en vertu du corollaire 3.9) à $\binom{n}{k}_{\boldsymbol{a}} \operatorname{ppcm}(a_1, \ldots, a_k)$. Par conséquent, pour tous $k, \ell \in \mathbb{N}$, tels que $n/2 \leq k \leq n$ et $1 \leq \ell \leq k$, on a :

$$a_\ell \binom{n}{\ell}_{\boldsymbol{a}} \text{ divise } \binom{n}{k}_{\boldsymbol{a}} \operatorname{ppcm}(a_1, \ldots, a_k)\,. \tag{3.4.5}$$

Nous affirmons que (3.4.5) reste vraie pour $n/2 \leq k \leq n$ et $k < \ell \leq n$. En effet, si k et ℓ sont des entiers tels que $n/2 \leq k \leq n$ et $k < \ell \leq n$, alors on a $1 \leq n-\ell+1 \leq n-k \leq k$ et $a_{n-\ell+1} \binom{n}{n-\ell+1}_{\boldsymbol{a}} = a_\ell \binom{n}{\ell}_{\boldsymbol{a}}$. L'application de (3.4.5) pour $\ell' = n-\ell+1$, au lieu de ℓ, confirme donc notre affirmation. Ainsi, (3.4.5) est vraie pour tous $k, \ell \in \mathbb{N}$ tels que $n/2 \leq k \leq n$ et $1 \leq \ell \leq n$. Par suite, en appliquant le lemme 3.11 pour toutes les relations de divisibilité (3.4.5), où $1 \leq \ell \leq n$ et $n/2 \leq k \leq n$, on en déduit que :

$$\operatorname{ppcm}\left\{ a_\ell \binom{n}{\ell}_{\boldsymbol{a}}\,;\ \ell = 1, \ldots, n \right\} \text{ divise } \operatorname{pgcd}\left\{ \binom{n}{k}_{\boldsymbol{a}} \operatorname{ppcm}(a_1, \ldots, a_k)\,;\ n/2 \leq k \leq n \right\};$$

ce qui est équivalent (en vertu du corollaire 3.9) à :

$$\operatorname{ppcm}(a_1, a_2, \ldots, a_n) \text{ divise } \operatorname{pgcd}\left\{ \binom{n}{k}_{\boldsymbol{a}} \operatorname{ppcm}(a_1, \ldots, a_k)\,;\ n/2 \leq k \leq n \right\}.$$

L'identité du corollaire 3.10 se déduit en observant que :

$$\operatorname{ppcm}(a_1,\ldots,a_n)=\binom{n}{n}_{\boldsymbol{a}}\operatorname{ppcm}(a_1,\ldots,a_n)\in\left\{\binom{n}{k}_{\boldsymbol{a}}\operatorname{ppcm}(a_1,\ldots,a_k)\,;\ n/2\leq k\leq n\right\}.$$

Ce qui complète la démonstration du corollaire 3.10. ∎

Remarque 3.12. *En prenant dans le théorème 3.7 $a_n=n$ $(\forall n\geq 1)$, on obtient l'identité de Farhi [18] (déjà démontrée dans le théorème 3.1). Par ailleurs, on démontre aisément que le théorème 3.7, le corollaire 3.9 et le corollaire 3.10 restent valables dans tout anneau factoriel $\mathcal{A}$, pris à la place de $\mathbb{Z}$ (nous renvoyons le lecteur à l'article de Bliss et al. [6] pour la définition et les propriétés des suites à forte divisibilité dans un anneau factoriel). Si l'on prend par exemple $\mathcal{A}=\mathbb{Z}[q]$ et $\boldsymbol{a}=(a_n)_{n\geq 1}$ la suite polynomiale de $\mathbb{Z}[q]$ définie par $a_n=[n]_q:=\frac{q^n-1}{q-1}$, on obtient l'identité de Guo [22] selon laquelle on a pour tout $n\in\mathbb{N}$:*

$$\operatorname{ppcm}\left\{\binom{n}{0}_q,\binom{n}{1}_q,\ldots,\binom{n}{n}_q\right\}=\frac{\operatorname{ppcm}([1]_q,[2]_q,\ldots,[n]_q,[n+1]_q)}{[n+1]_q},$$

où $[k]_q$ et $\binom{n}{k}_q$ $(0\leq k\leq n)$ sont les notations standards du q-calcul ; c'est-à-dire $[k]_q:=\frac{q^k-1}{q-1}$ et $\binom{n}{k}_q:=\frac{[n]_q[n-1]_q\cdots[n-k+1]_q}{[1]_q[2]_q\cdots[k]_q}$.

3.5 Estimations du ppcm de suites de Lucas

Un important exemple de suites à forte divisibilité nous est fourni par une classe spéciale de suites de Lucas. Plus précisément, en prenant P et Q des entiers non nuls et premiers entre eux et en désignant par $U(P,Q)$ leur suite de Lucas associée, c'est-à-dire la suite d'entiers définie récursivement par : $U_0=0$, $U_1=1$ et $U_{n+2}=PU_{n+1}-QU_n$ $(\forall n\in\mathbb{N})$, on montre que la suite $|U(P,Q)|$ est à forte divisibilité (voir par exemple [42, p. 9]). Particulièrement, la suite de tous les entiers positifs (qu'on obtient en prenant $(P,Q)=(2,1)$) et la suite de Fibonacci usuelle (qu'on obtient en prenant $(P,Q)=(1,-1)$) sont des suites à forte divisibilité. Par ailleurs, si $P^2-4Q>0$, alors en désignant par α et β les deux racines (distinctes) de l'équation quadratique : $X^2-PX+Q=0$, on montre que pour tout entier strictement positif n, on a :

$$U_n=\frac{\alpha^n-\beta^n}{\alpha-\beta}. \tag{3.5.1}$$

Pour en savoir plus sur le sujet des suites de Lucas, le lecteur est invité à consulter le livre de Honsberger [29]. Dans cette section, nous appliquons les corollaires 3.9 et 3.10 pour établir des estimations effectives et non triviales du plus petit commun multiple des termes consécutifs de certaines suites de Lucas. On a le théorème suivant :

Théorème 3.13. *Soient P et Q deux entiers non nuls et premiers entre eux, tels que $\Delta := P^2 - 4Q > 0$, et soit $U(P,Q)$ la suite de Lucas qui leur est associée. Alors, pour tout $n \in \mathbb{N}^*$, on a :*

$$|\alpha|^{\frac{n^2}{4}-\frac{n}{2}-1} \leq \operatorname{ppcm}(U_1, U_2, \ldots, U_n) \leq |\alpha|^{\frac{n^2}{3}+\frac{7n}{3}-\frac{8}{3}}, \tag{3.5.2}$$

où α est la racine la plus grande en valeur absolue de l'équation $X^2 - PX + Q = 0$.

Pour prouver le théorème 3.13, nous aurons besoin du lemme élémentaire suivant :

Lemme 3.14. *Dans la situation du théorème 3.13, on a pour tout entier strictement positif n :*

$$|\alpha|^{n-2} \leq |U_n| \leq |\alpha|^n.$$

Démonstration. Désignons par β la seconde racine de l'équation $X^2 - PX + Q = 0$; donc $|\beta| < |\alpha|$. On a $|\alpha| - |\beta| \in \{\alpha - \beta, \beta - \alpha, \alpha + \beta, -\alpha - \beta\}$. Puisque $\alpha - \beta = \pm\sqrt{\Delta}$, $\alpha + \beta = P$ et $|\alpha| - |\beta| > 0$, cela entraîne que $|\alpha| - |\beta| \in \left\{|P|, \sqrt{\Delta}\right\}$. Comme $P \in \mathbb{Z}^*$ et $\Delta \in \mathbb{Z}_+^*$, on en déduit que :

$$|\alpha| - |\beta| \geq 1. \tag{3.5.3}$$

En utilisant les formules (3.5.1) et (3.5.3), on obtient que pour tout $n \in \mathbb{N}^*$:

$$\begin{aligned} |U_n| = \left|\frac{\alpha^n - \beta^n}{\alpha - \beta}\right| &= \left|\beta^{n-1} \sum_{k=0}^{n-1} \left(\frac{\alpha}{\beta}\right)^k\right| \\ &\leq |\beta|^{n-1} \sum_{k=0}^{n-1} \left|\frac{\alpha}{\beta}\right|^k \\ &= \frac{|\alpha|^n - |\beta|^n}{|\alpha| - |\beta|} \\ &\leq |\alpha|^n - |\beta|^n \leq |\alpha|^n. \end{aligned}$$

D'autre part, on a pour tout entier $n \geq 2$:

$$\begin{aligned}
|U_n| = \left|\frac{\alpha^n - \beta^n}{\alpha - \beta}\right| &= \frac{|\alpha^n - \beta^n|}{|\alpha - \beta|} \geq \frac{||\alpha^n| - |\beta^n||}{|\alpha - \beta|} = \frac{|\alpha|^n - |\beta|^n}{|\alpha - \beta|} \\
&= \frac{(|\alpha| - |\beta|)\left(|\alpha|^{n-1} + |\alpha|^{n-2} \cdot |\beta| + \cdots + |\alpha| \cdot |\beta|^{n-2} + |\beta|^{n-1}\right)}{|\alpha - \beta|} \\
&\geq \frac{(|\alpha| - |\beta|)\left(|\alpha|^{n-1} + |\alpha|^{n-2} \cdot |\beta|\right)}{|\alpha - \beta|} \\
&= |\alpha + \beta| \cdot |\alpha|^{n-2} \\
&= |P| \cdot |\alpha|^{n-2} \geq |\alpha|^{n-2}.
\end{aligned}$$

En remarquant que $|U_n| \geq |\alpha|^{n-2}$ est aussi vraie pour $n = 1$ (puisque $U_1 = 1$ et $|\alpha| \geq |\alpha| - |\beta| \geq 1$), on en déduit que pour tout entier strictement positif n, on a :

$$|\alpha|^{n-2} \leq |U_n| \leq |\alpha|^n,$$

comme il fallait le prouver. Le lemme est ainsi démontré. ∎

Démonstration du théorème 3.13. Désignons par β la seconde racine de l'équation $X^2 - PX + Q = 0$; donc $|\beta| < |\alpha|$. En appliquant l'estimation du lemme 3.14 pour $n \geq 2$ et en replaçant U_1 par 1, nous en déduisons immédiatement que pour tous $n, k \in \mathbb{N}^*$ tels que $n \geq k$, on a :

$$|\alpha|^{k(n-k-2)+1} \leq \left|\binom{n}{k}_{\boldsymbol{U}}\right| \leq |\alpha|^{k(n-k+2)-1}. \tag{3.5.4}$$

Montrons d'abord l'inégalité de gauche de (3.5.2). Pour $n = 1$, cette inégalité est triviale. Ensuite, en utilisant successivement le corollaire 3.9, le lemme 3.14 puis (3.5.4), on obtient pour tout entier $n \geq 2$:

$$\begin{aligned}
\operatorname{ppcm}(U_1, U_2, \ldots, U_n) &= \operatorname{ppcm}\left\{U_1\binom{n}{1}_{\boldsymbol{U}}, U_2\binom{n}{2}_{\boldsymbol{U}}, \ldots, U_n\binom{n}{n}_{\boldsymbol{U}}\right\} \\
&\geq \max_{1 \leq k \leq n}\left\{|U_k| \cdot \binom{n}{k}_{\boldsymbol{U}}\right\} \\
&\geq \max_{1 \leq k \leq n} |\alpha|^{k(n-k-1)-1} \\
&\geq |\alpha|^{\left\lfloor \frac{n}{2} \right\rfloor\left(n - \left\lfloor \frac{n}{2} \right\rfloor - 1\right) - 1} \\
&\geq |\alpha|^{n^2/4 - n/2 - 1},
\end{aligned}$$

comme il fallait le prouver. L'inégalité de gauche de (3.5.2) est prouvée. Montrons maintenant l'inégalité de droite de (3.5.2) ; c'est-à-dire que $\operatorname{ppcm}(U_1, U_2, \ldots, U_n) \leq |\alpha|^{\frac{n^2}{3}+\frac{7n}{3}-\frac{8}{3}}$ $(\forall n \geq 1)$. Pour ce faire, on procède par récurrence sur n. Pour $n = 1$, cette inégalité est triviale. Pour $m \geq 1$, supposons que l'inégalité précédente est vraie pour tout entier strictement positif $n < 2m$ et montrons qu'elle reste vraie pour $n = 2m$ et pour $n = 2m+1$. En utilisant successivement le corollaire 3.10, l'hypothèse de récurrence et (3.5.4), on obtient :

$$\begin{aligned}
\operatorname{ppcm}(U_1, U_2, \ldots, U_{2m}) &\leq \operatorname{ppcm}(U_1, U_2, \ldots, U_m) \cdot \left| \binom{2m}{m}_{\boldsymbol{U}} \right| \\
&\leq |\alpha|^{\frac{m^2}{3}+\frac{7m}{3}-\frac{8}{3}} \cdot |\alpha|^{m^2+2m-1} \\
&= |\alpha|^{\frac{4m^2}{3}+\frac{13m}{3}-\frac{11}{3}} \\
&\leq |\alpha|^{\frac{(2m)^2}{3}+\frac{7(2m)}{3}-\frac{8}{3}},
\end{aligned}$$

comme il fallait le prouver. De même, on a :

$$\begin{aligned}
\operatorname{ppcm}(U_1, U_2, \ldots, U_{2m+1}) &\leq \operatorname{ppcm}(U_1, U_2, \ldots, U_{m+1}) \cdot \left| \binom{2m+1}{m+1}_{\boldsymbol{U}} \right| \\
&= \operatorname{ppcm}(U_1, U_2, \ldots, U_{m+1}) \cdot \left| \binom{2m+1}{m}_{\boldsymbol{U}} \right| \\
&\leq |\alpha|^{\frac{(m+1)^2}{3}+\frac{7(m+1)}{3}-\frac{8}{3}} \cdot |\alpha|^{m^2+3m-1} \\
&= |\alpha|^{\frac{4m^2}{3}+6m-1} \\
&\leq |\alpha|^{\frac{4m^2}{3}+6m} = |\alpha|^{\frac{(2m+1)^2}{3}+\frac{7(2m+1)}{3}-\frac{8}{3}},
\end{aligned}$$

comme il fallait le prouver. Ce qui achève cette récurrence et confirme que l'inégalité de droite de (3.5.2) est vraie pour tout entier $n \geq 1$. La preuve du théorème est complète. ■

Remarques 3.15.

1. *Dans le contexte du théorème 3.13, si P et Q sont de signes particuliers (par exemple $P > 0$, $Q < 0$) alors l'estimation (3.5.2) peut être légèrement améliorée. Par exemple, pour le cas de la suite de Fibonacci usuelle $(F_n)_{n\in\mathbb{N}}$ (définie récursivement par : $F_0 = 0$, $F_1 = 1$ et $F_{n+2} = F_n + F_{n+1}$, $\forall n \in \mathbb{N}$), on montre que l'on a pour tout entier $n \geq 1$:*

$$\Phi^{\frac{n^2}{4}-\frac{9}{4}} \leq \operatorname{ppcm}(F_1, F_2, \ldots, F_n) \leq \Phi^{\frac{n^2}{3}+\frac{4n}{3}}, \tag{3.5.5}$$

où Φ *désigne le nombre d'or* ($\Phi := \frac{1+\sqrt{5}}{2}$). *La qualité de l'estimation* (3.5.5) *peut être appréciée à partir du célèbre résultat de Matiyasevich et Guy [36] qui énonce que :*

$$\lim_{n\longrightarrow+\infty} \frac{\log \operatorname{ppcm}(F_1, F_2, \ldots, F_n)}{n^2 \log \Phi} = \frac{3}{\pi^2}.$$

En effet, ce résultat implique que si $\lambda_1, \mu_1, \eta_1, \lambda_2, \mu_2, \eta_2 \in \mathbb{R}$ *vérifient :*

$$\Phi^{\lambda_1 n^2+\mu_1 n+\eta_1} \leq \operatorname{ppcm}(F_1, F_2, \ldots, F_n) \leq \Phi^{\lambda_2 n^2+\mu_2 n+\eta_2} \qquad (\forall n \geq 1),$$

alors, on a nécessairement $\lambda_1 \leq \frac{3}{\pi^2}$ *et* $\lambda_2 \geq \frac{3}{\pi^2}$. *Puisque* (3.5.5) *correspond à* $\lambda_1 = \frac{1}{4} = 0,25$ *et* $\lambda_2 = \frac{1}{3} = 0,33\ldots$ *et que* $\frac{3}{\pi^2} = 0,303\ldots$, *nous voyons bien que notre estimation* (3.5.5) *est assez précise.*

Plus généralement, l'estimation du théorème 3.13 peut être appréciée à partir du résultat de Kiss et Matyas [33], généralisant celui de Matiyasevich et Guy [36].

2. *Notons aussi que la méthode suivie ici peut être adaptée pour estimer le* ppcm *de toute suite à forte divisibilité d'ordre connu, comme celles d'ordre exponentiel.*

CHAPITRE 4

Majorations non triviales du ppcm d'une suite arithmétique

4.1 Introduction

Dans ce chapitre, nous établissons des majorations non triviales du plus petit commun multiple de termes consécutifs d'une progression arithmétique finie. Comme conséquence, nous obtenons d'une part un encadrement effectif et un équivalent à l'infini de :

$$M(n) := \frac{1}{\varphi(n)} \sum_{\substack{1\leq \ell \leq n \\ \operatorname{pgcd}(\ell,n)=1}} \frac{1}{\ell} \quad (\forall n \in \mathbb{N}^*),$$

où φ désigne la fonction indicatrice d'Euler ; et d'autre part une majoration non triviale de la fonction de Chebyshev $\theta(x; k, \ell)$ sous certaines conditions sur x, k et ℓ. Bien que des majorations de $\theta(x; k, \ell)$ existent dans la littérature mathématique, il convient de noter que celles-ci sont toutes obtenues de façon non élémentaire (c'est-à-dire en utilisant de l'analyse complexe). L'intérêt ici est justement d'en donner des estimations par le biais de l'analyse réelle.

Étant donné $n \in \mathbb{N}^*$, on désigne par $\omega(n)$ le nombre de facteurs premiers distincts de n. Étant donnés $n, a, b \in \mathbb{N}^*$, on définit $L_{a,b,n} := \operatorname{ppcm}(a, a+b, \ldots, a+nb)$. Afin d'alléger

certains énoncés, on pose : $c_1 := 41,30142$, $c_2 := 12,30641$, $c_3 := 1,25507$, $c_4 := 3,35609$, $c_5 := 1,38402$, $c_6 := 1,57681$ et $c_7 := 2,1284$.

4.2 Énoncés des résultats

Théorème 4.1. *Soient a et b deux entiers strictement positifs tels que $b \geq 2$ et $\mathrm{pgcd}(a,b) = 1$. Alors, pour tout entier $n \geq b+1$, on a :*

$$\mathrm{ppcm}\,(a, a+b, \ldots, a+nb) \leq (c_1 \cdot b \log b)^{n+\left\lfloor \frac{a}{b} \right\rfloor}. \tag{4.2.1}$$

Théorème 4.2. *Soient a un entier strictement positif et b un nombre premier tels que $a < b$. Alors, pour tout entier $n \geq b+1$, On a :*

$$\mathrm{ppcm}\,(a, a+b, \ldots, a+nb) \leq \left(c_2 \cdot b^{\frac{b}{b-1}}\right)^n. \tag{4.2.2}$$

Corollaire 4.3. *Pour tout entier $r \geq 2$, on a :*

$$\log(r+1) \leq rM(r) \leq \log r + \log\log r + \log c_1. \tag{4.2.3}$$

Le corollaire suivant est immédiat.

Corollaire 4.4. *On a :*

$$M(r) \sim_{+\infty} \frac{\log r}{r}. \tag{4.2.4}$$

Corollaire 4.5. *Soient k un nombre premier et $\ell < k$ un entier strictement positif. Alors, pour tout nombre réel $x \geq k(k+1)$, on a :*

$$\theta(x; k, \ell) \leq x\left(\frac{2c_3}{k} + \frac{\log k}{k-1}\right). \tag{4.2.5}$$

4.3 Préparation

Les preuves de nos résultats nécessitent les résultats intermédiaires suivants :

4.3.1 Résultats connus antérieurement

Théorème 4.6 (Rosser et al. [44])**.**

1. *Pour tout entier $n \geq 2$, on a :* $\sum_{p \leq n} \frac{\log p}{p} \leq \log n$.
2. *Pour tout entier $n \geq 6$, on a :* $p_n \leq n(\log n + \log\log n)$.
3. *La série* $\sum_p \frac{\log p}{p(p-1)}$ *converge vers le nombre* $0,7553666111\cdots < \log c_7$.

Théorème 4.7 (Robin [43])**.** *Pour tout entier $n \geq 3$, on a :*

$$\omega(n) \leq c_5 \frac{\log n}{\log\log n}.$$

Pour mettre à l'aise le lecteur, nous lui rappelons aussi le théorème de Hanson [23] suivant qui est déjà vu au §1.4.

Théorème 4.8 (Hanson [23])**.** *Pour tout réel $x > 1$, on a :*

$$\pi(x) \leq c_3 \frac{x}{\log x}.$$

4.3.2 Lemmes préparatifs

Lemme 4.9. *Soient a et b deux entiers strictement positifs et premiers entre eux tels que $a < b$. Alors, pour tout entier $n \geq b+1$, on a :*

$$\prod_{p \leq n} p^{\vartheta_p(L_{a,b,n})} \leq \frac{{c_2}^n}{(a+nb)^{\omega(b)}}.$$

Démonstration. Soit $n \geq b+1$ un entier. On constate que pour tout nombre premier p divisant b, on a $\vartheta_p(L_{a,b,n}) = 0$. En effet, $p \nmid b$ entraîne $p \nmid a$ (puisque $\operatorname{pgcd}(a,b) = 1$), ce qui entraîne que p ne divise aucun terme de la suite arithmétique $(a+kb)_{k\in\mathbb{N}}$; d'où $p \nmid L_{a,b,n}$. D'autre part, pour tout nombre premier p, le nombre $p^{\vartheta_p(L_{a,b,n})}$ est la plus grande puissance de p qui divise l'un au moins des nombres $a, a+b, \ldots, a+nb$; ce qui entraîne que $p^{\vartheta_p(L_{a,b,n})} \leq a+nb$. On a par conséquent :

$$\prod_{p \leq n} p^{\vartheta_p(L_{a,b,n})} = \prod_{\substack{p \leq n \\ p \nmid b}} p^{\vartheta_p(L_{a,b,n})} \leq \prod_{\substack{p \leq n \\ p \nmid b}} (a+nb) = (a+nb)^{\pi(n)-\omega(b)}.$$

Comme par ailleurs, on a : $a+nb \leq n^2$ (car $n \geq b+1 > a$), il s'ensuit que :

$$\prod_{p\leq n} p^{\vartheta_p\left(L_{a,b,n}\right)} \leq \frac{n^{2\pi(n)}}{(a+nb)^{\omega(b)}} = \frac{e^{2\pi(n)\log n}}{(a+nb)^{\omega(b)}}.$$

L'estimation requise en découle via le théorème 4.8. ∎

Lemme 4.10. *Soient a et b deux entiers strictement positifs et premiers entre eux. Alors, pour tout entier naturel n, on a :*

$$\prod_{p>n} p^{\vartheta_p\left(L_{a,b,n}\right)} \quad \textit{divise} \quad \frac{a\,(a+b)\cdots(a+nb)\cdot \prod_{\substack{p\leq n\\ p\mid b}} p^{\vartheta_p(n!)}}{n!\cdot \prod_{\substack{p\leq n\\ p\mid b}} p^{\vartheta_p(n+1)}}. \tag{4.3.1}$$

Démonstration. La relation (4.3.1) est triviale pour $n \in \{0,1\}$. Supposons pour la suite que $n \geq 2$ et désignons respectivement par A_n et B_n les membres de gauche et de droite de (4.3.1). Nous allons monter que $\vartheta_q(A_n) \leq \vartheta_q(B_n)$ pour tout nombre premier q, ce qui conclura que A_n divise B_n. Soit q un nombre premier arbitraire. Dans le cas où q divise b, on a $q \nmid a$ (puisque $\operatorname{pgcd}(a,b)=1$) et donc q ne divise aucun terme de la suite arithmétique $(a+kb)_{k\in\mathbb{N}}$; ce qui entraîne que q ne divise pas $L_{a,b,n}$ et on a par conséquent :

$$\vartheta_q(B_n) = \vartheta_q\left(\frac{\prod_{\substack{p\leq n\\ p\mid b}} p^{\vartheta_p(n!)}}{n!}\right) = \vartheta_q(n!) - \vartheta_q(n!) = 0 = \vartheta_q(A_n).$$

Il nous reste donc à montrer l'inégalité $\vartheta_q(A_n) \leq \vartheta_q(B_n)$ dans le cas où q ne divise pas b. Supposons pour toute la suite que $q \nmid b$ et définissons $S_{a,b,n} := \{a, a+b, \ldots, a+nb\}$. On distingue les deux cas suivants :

• **<u>1er cas :</u>** (si $q \leq n$). Dans ce cas, on a visiblement $\vartheta_q(A_n) = 0$. On doit donc montrer que $\vartheta_q(B_n) \geq 0$. Pour tout entier strictement positif ℓ, désignons par x_ℓ l'unique solution de la congruence $a+bx \equiv 0 \pmod{q^\ell}$ dans l'ensemble $\{0,1,\ldots,q^\ell-1\}$. Le nombre d'éléments de l'ensemble $S_{a,b,n}$ qui sont multiples de q^ℓ est alors égale au nombre d'entiers x tels que $0 \leq x \leq n$ et $x \equiv x_\ell \pmod{q^\ell}$; ce qui est clairement égale à $\left\lfloor \frac{n-x_\ell}{q^\ell} \right\rfloor + 1$. On a par conséquent :

$$\begin{aligned}\vartheta_q(a\,(a+b)\cdots(a+nb)) &= \sum_{\ell\geq 1}\left(\left\lfloor \frac{n-x_\ell}{q^\ell}\right\rfloor + 1\right) = \sum_{\ell\geq 1}\left(\left\lfloor \frac{n-x_\ell+q^\ell}{q^\ell}\right\rfloor\right)\\ &\geq \sum_{\ell\geq 1}\left\lfloor \frac{n+1}{q^\ell}\right\rfloor = \vartheta_q((n+1)!).\end{aligned}$$

D'où : $\vartheta_q(B_n) = \vartheta_q(a(a+b)\cdots(a+nb)) - \vartheta_q((n+1)!) \geq 0$, comme il fallait le prouver.

• **2nd cas :** (si $q > n$). Dans ce cas, comme la congruence $a + bx \equiv 0 \pmod{q}$ possède une et une unique solution dans l'ensemble $\{0, 1, \ldots, q-1\}$ (car $\text{pgcd}(b, q) = 1$) alors elle possède au plus une solution dans l'ensemble $\{0, 1, \ldots, n\}$. Autrement dit, q divise au plus un élément de l'ensemble $S_{a,b,n}$. On a par conséquent : $\vartheta_q(A_n) = \vartheta_q(L_{a,b,n}) = \vartheta_q(a(a+b)\cdots(a+nb)) = \vartheta_q(B_n)$. Ce qui confirme le résultat requis pour ce cas et complète cette démonstration. ■

Lemme 4.11. *Pour tout entier $b \geq 3$, on a : $\prod_{p|b} p^{1/p} \leq c_6 \log b$.*

Démonstration. Si $\omega(b) = 1$ alors il existe un nombre premier q_1 et un entier strictement positif m tels que $b = {q_1}^m$. On a par conséquent : $\prod_{p|b} p^{1/p} = {q_1}^{1/q_1} \leq 3^{1/3} \leq c_6 \log 3 \leq c_6 \log b$ (car la fonction $n \mapsto n^{1/n}$ atteint son maximum sur $\mathbb{N}^*$ en $n = 3$). Supposons pour la suite que $\omega(b) \geq 2$ et montrons préalablement que l'on a :

$$\sum_{p|b} \frac{\log p}{p} \leq \sum_{p \leq p_{\omega(b)}} \frac{\log p}{p}. \tag{4.3.2}$$

Dans le cas où b est pair, l'inégalité (4.3.2) découle directement de la décroissance de la fonction $x \mapsto \frac{\log x}{x}$ sur l'intervalle $[3, +\infty[$. Si maintenant b est impair alors en désignant par q le plus grand facteur premier de b, on a (puisque $\omega(b) \geq 2$ par hypothèse) : $q \geq 5$. Il s'ensuit alors de la décroissance de la fonction $x \mapsto \frac{\log x}{x}$ sur l'intervalle $[3, +\infty[$ que :

$$\sum_{p|b} \frac{\log p}{p} = \sum_{\substack{p|b \\ p \neq q}} \frac{\log p}{p} + \frac{\log q}{q} \leq \sum_{3 \leq p \leq p_{\omega(b)}} \frac{\log p}{p} + \frac{\log 5}{5} \leq \sum_{p \leq p_{\omega(b)}} \frac{\log p}{p};$$

confirmant ainsi (4.3.2) également dans le cas où b est impair.

En prenant maintenant les exponentielles des deux membres de (4.3.2), on a :

$$\prod_{p|b} p^{\frac{1}{p}} \leq \prod_{p \leq p_{\omega(b)}} p^{\frac{1}{p}}. \tag{4.3.3}$$

Pour $\omega(b) \in \{2, 3, 4, 5\}$, on vérifie à la main que $\prod_{p \leq p_{\omega(b)}} p^{1/p} \leq c_6 \log\left(\prod_{p \leq p_{\omega(b)}} p\right) \leq c_6 \log b$, ce qui conclut (via (4.3.3)) à l'estimation requise par le lemme. Si par contre $\omega(b) \geq 6$, on a (d'après le théorème 4.6) :

$$\prod_{p \leq p_{\omega(b)}} p^{\frac{1}{p}} \leq p_{\omega(b)} \leq \omega(b)\left(\log \omega(b) + \log\log \omega(b)\right).$$

En combinant ceci avec le théorème 4.7 et l'inégalité $\omega(b) \leq \log b$ (qui elle-même découle du théorème 4.7 et du fait que $\log\log b \geq c_5$, vu que $b \geq 2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13 \geq e^{e^{c_5}}$), on aboutit à :

$$\begin{aligned}\prod_{p\leq p_{\omega(b)}} p^{\frac{1}{p}} &\leq c_5\frac{\log b}{\log\log b}\left(\log c_5 + \log\log b - \log\log\log b + \log\log\log b\right)\\ &= \left(c_5 + \frac{c_5\log c_5}{\log\log b}\right)\log b\\ &\leq \left(c_5 + \frac{c_5\log c_5}{\log\log\left(2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13\right)}\right)\log b \leq c_6\log b.\end{aligned}$$

Ce qui conclut encore (via (4.3.3)) à l'estimation requise par le lemme. Notre démonstration est complète. ∎

Lemme 4.12. *Soient b et n deux entiers ≥ 2. Alors, on a : $\prod_{p|b} p^{\vartheta_p(n!)} \leq (c_4\log b)^n$.*

Démonstration. Pour $b = 2$, l'estimation du lemme découle immédiatement de la formule de Legendre. En effet, on a :

$$\prod_{p|2} p^{\vartheta_p(n!)} = 2^{\vartheta_2(n!)} = 2^{\lfloor\frac{n}{2}\rfloor+\lfloor\frac{n}{4}\rfloor+\lfloor\frac{n}{8}\rfloor+\cdots} \leq 2^{\frac{n}{2}+\frac{n}{4}+\frac{n}{8}+\cdots} = 2^n \leq (c_4\log 2)^n\,.$$

Supposons maintenant que $b \geq 3$. En utilisant successivement la formule de Legendre, le lemme 4.11 et le point 3 du théorème 4.6, on obtient que :

$$\begin{aligned}\prod_{p|b} p^{\vartheta_p(n!)} = \prod_{p|b} p^{\lfloor\frac{n}{p}\rfloor+\lfloor\frac{n}{p^2}\rfloor+\cdots} \leq \prod_{p|b} p^{\frac{n}{p}+\frac{n}{p^2}+\cdots} &= \left(\prod_{p|b} p^{\frac{1}{p}}\right)^n\left(\prod_{p|b} p^{\frac{1}{p(p-1)}}\right)^n\\ &\leq (c_6c_7\log b)^n \leq (c_4\log b)^n\,,\end{aligned}$$

comme il fallait le prouver. Ce qui complète notre démonstration. ∎

4.4 Preuves de nos résultats principaux

Démonstration du théorème 4.1. Soit $n \geq b+1$ un entier. Supposons d'abord que $a < b$. En utilisant successivement les lemmes 4.9, 4.10 et 4.12, on obtient que :

$$\begin{aligned} L_{a,b,n} &= \left(\prod_{p\leq n} p^{\vartheta_p\left(L_{a,b,n}\right)}\right)\left(\prod_{p>n} p^{\vartheta_p\left(L_{a,b,n}\right)}\right) \\ &\leq \frac{{c_2}^n}{(a+bn)^{\omega(b)}} \cdot \frac{a\,(a+b)\cdots(a+nb)}{n!} \cdot \prod_{\substack{p\leq n\\ p\mid b}} p^{\vartheta_p(n!)} \\ &\leq {c_2}^n \frac{(a+nb)}{(a+nb)^{\omega(b)}} \cdot \frac{b(2b)(3b)\cdots(nb)}{n!} \cdot \prod_{p\mid b} p^{\vartheta_p(n!)} \\ &\leq {c_2}^n b^n \left(c_4 \log b\right)^n \leq \left(c_1 \cdot b \log b\right)^n, \end{aligned}$$

comme il fallait le prouver. Si maintenant on a au contraire $a > b$, alors en posant $q := \lfloor a/b \rfloor$ et $a' := a - qb < b$, on a visiblement : $L_{a,b,n}$ divise $L_{a',b,q+n}$; ce qui permet de conclure au résultat requis en appliquant le premier cas au triplet $(a', b, q+n)$ au lieu de (a, b, n). Notre démonstration est complète. ∎

Démonstration du théorème 4.2. Il suffit de reprendre la preuve précédente du théorème 4.1 (le premier cas précisément) et d'utiliser la majoration :

$$\prod_{\substack{p\leq n\\ p\mid b}} p^{\vartheta_p(n!)} = b^{\vartheta_b(n!)} = b^{\left\lfloor \frac{n}{b} \right\rfloor + \left\lfloor \frac{n}{b^2} \right\rfloor + \cdots} \leq b^{\frac{n}{b-1}}$$

au lieu de celle du lemme 4.12. ∎

Démonstration du corollaire 4.3. Étant donné r un entier ≥ 2 et n un entier $\geq r+1$, on a en utilisant l'inégalité (1.6.1) puis le théorème 4.1 :

$$\frac{n-1}{n}\log(r+1) \leq \frac{\log L_{1,r,n}}{n} \leq \log r + \log\log r + \log c_1.$$

Le résultat requis en découle par passage à la limite lorsque n tend vers l'infini, tout en se servant de l'estimation (1.9.1). ∎

Preuve du corollaire 4.5. Soient $x \geq k(k+1)$ et $m := \left\lfloor \frac{x}{k} \right\rfloor$. On a clairement :

$$\theta(x; k, \ell) \leq \log \operatorname{ppcm}(\ell, \ell+k, \ldots, \ell+mk) = \log L_{\ell,k,m}.$$

Par ailleurs, puisque $m \geq k+1$ (car $x \geq k(k+1)$), on a en vertu du théorème 4.2 :

$$\log L_{\ell,k,m} \leq m\left(\log c_2 + \frac{k\log k}{k-1}\right) \leq x\left(\frac{2c_3}{k} + \frac{\log k}{k-1}\right).$$

Ce qui conclut au résultat requis. ■

CHAPITRE 5

Un encadrement effectif du ppcm de la suite $(n^2+1)_n$

5.1 Introduction

Dans ce chapitre, il est question d'estimer les nombres entiers :

$$L_n := \text{ppcm}\left(1^2+1, 2^2+1, \ldots, n^2+1\right) \qquad (n \in \mathbb{N}^*).$$

On se propose d'une part d'améliorer la minoration de Oon [41] (pour le cas $c = 1$), qui énonce que $L_n \geq 2^n$ $(\forall n \in \mathbb{N}^*)$ et d'autre part d'établir une première majoration effective et non triviale de L_n. Pour ce faire, nous adaptons la méthode du chapitre 4 pour la suite $(n^2+1)_n$ à la place des suites arithmétiques. Étant donné un entier strictement positif n, on désigne par Q_n l'entier strictement positif défini par :

$$Q_n := \left(1^2+1\right)\left(2^2+1\right)\cdots\left(n^2+1\right).$$

Pour $i \in \{1,3\}$, on définit :

$$\mathcal{P}_{4,i} := \{p \text{ premier};\ p \equiv i \pmod 4\}.$$

Afin d'alléger certains énoncés, nous posons : $\alpha_1 := 0,7993$, $\alpha_2 := 10,3624$, $\alpha_3 := 3,9497$, $\beta_1 := 0,6722$, $\beta_2 := 0,5981$, $\beta_3 := 0,281$,

$c_1 := \frac{1}{2} - \frac{0,4}{3\log 10} + \int_1^{10^3} \frac{\theta(t;4,3)}{t^2}\mathrm{d}t - \frac{3}{2}\log 10 + 0,4\log\log(10^3) = 0,1608548666\ldots$, $c_2 := \left(\frac{1}{2} + \frac{0,4}{3\log 10}\right) = 0,5579\ldots$, $c_3 := 2,1284$, $c_4 := \left(1 + \frac{5}{6\log 10}\right) = 1,3619\ldots$ et $c_5 := e^{\frac{c_4}{6\cdot 10^3 \log 10}} = 1,0001\ldots$. Le théorème principal de ce chapitre est le suivant :

Théorème 5.1. *Pour tout entier $n \geq 2$, on a :*

$$\left(\alpha_1\sqrt{n}\,(\log n)^{-0,4}\right)^n \leq \operatorname{ppcm}\left(1^2+1, 2^2+1, \ldots, n^2+1\right) \leq \alpha_2\left(\alpha_3 n\,(\log n)^{0,8}\right)^n. \quad (5.1.1)$$

5.2 Préparation

La preuve du théorème 5.1 nécessite les résultats intermédiaires suivants :

5.2.1 Résultats antérieurs

Théorème 5.2 (Bennett et al. [3])**.** *Pour tout nombre réel $x \geq 10^3$, on a :*

$$\left|\theta(x;4,3) - \frac{x}{2}\right| \leq 0,4\frac{x}{\log x} \quad \textit{et} \quad \pi(x;4,1) \leq \frac{x}{2\log x}\left(1 + \frac{5}{2\log x}\right).$$

Théorème 5.3 (classique)**.** *Soient $\ell \in \mathbb{N}^*$, $n \in \mathbb{Z}$ et p un nombre premier impair ne divisant pas n. Alors, la congruence $x^2 \equiv n \pmod{p^\ell}$ possède exactement $1 + \left(\frac{n}{p}\right)$ solutions, où $\left(\frac{\cdot}{\cdot}\right)$ représente le symbole de Legendre.*

La preuve du théorème 5.3 peut être trouvée dans le livre de Hua [30, Theorem 5.1].

5.2.2 Lemmes préparatifs

Lemme 5.4. *Soit n un entier strictement positif. Alors, le nombre entier ${L_n}^2$ est multiple du nombre rationnel*

$$D_n := \frac{2^{\lfloor n/2\rfloor+1}Q_n}{{n!}^2}\prod_{p\in\mathcal{P}_{4,3}\cap[1,n]} p^{2\vartheta_p(n!)}.$$

Démonstration. Nous allons montrer que $\vartheta_p(D_n) \leq \vartheta_p(L_n^2)$ pour tout nombre premier p, ce qui conclura au résultat requis. Pour $p = 2$, on constate que l'on a pour tout entier naturel k :

$$\vartheta_2\left(k^2+1\right) = \begin{cases} 1 & \text{si } k \textit{ est impair} \\ 0 & \text{sinon} \end{cases};$$

ce qui entraîne que :

$$\vartheta_2(Q_n) = \#\{i \in \mathbb{N}^*;\ i \leq n\ ,\ i \text{ impair}\} = \left\lfloor \frac{n-1}{2} \right\rfloor + 1.$$

On a par conséquent :

$$\begin{aligned}
\vartheta_2(D_n) &= \left\lfloor \frac{n}{2} \right\rfloor + 1 + \vartheta_2(Q_n) - 2\vartheta_2(n!) \\
&= \left\lfloor \frac{n-1}{2} \right\rfloor + \left\lfloor \frac{n}{2} \right\rfloor + 2 - 2\vartheta_2(n!) \\
&\leq \left\lfloor \frac{n-1}{2} \right\rfloor - \left\lfloor \frac{n}{2} \right\rfloor + 2 \leq 2 = \vartheta_2\left(L_n^2\right),
\end{aligned}$$

comme il fallait le prouver. Prenons pour la suite p un nombre premier > 2 et montrons que l'on a $\vartheta_p(D_n) \leq \vartheta_p(L_n^2)$. Si $p \in \mathcal{P}_{4,3}$ alors, d'après le théorème 5.3, l'équation $x^2 \equiv -1 \pmod{p}$ n'a pas de solution (car : $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = -1$). Ce qui entraîne que $\vartheta_p(D_n) = 2\vartheta_p(n!) - \vartheta_p\left(n!^2\right) = 0 = \vartheta_p(L_n) = \vartheta_p(L_n^2)$ et confirme l'inégalité requise. Si au contraire $p \in \mathcal{P}_{4,1}$, on conclura par distinction de cas. Posons préalablement $S_n := \{1^2+1, 2^2+1, \ldots, n^2+1\}$.

• **1er cas :** (si $p > 2n$).

Nous affirmons d'abord que p divise au plus un seul élément de l'ensemble S_n. Procédons par l'absurde en supposant que p divise à la fois (i^2+1) et (j^2+1) pour certains $i, j \in \mathbb{N}^*$, tels que $i < j \leq n$. Cela entraîne que p divise $(j^2+1) - (i^2+1) = (j-i)(j+i)$, donc p divise l'un des nombres $(j-i)$ ou $(j+i)$, d'où $p \leq (i+j) < 2n$. Ce qui contredit le fait que $p > 2n$ et confirme notre affirmation. D'après cette affirmation, on a : $\vartheta_p(D_n) = \vartheta_p(Q_n) = \vartheta_p(L_n) \leq \vartheta_p(L_n^2)$, comme il fallait le prouver.

• **2ème cas :** (si $n < p < 2n$).

Dans ce cas, on a clairement $p^2 > n^2 + 1$, donc p^2 ne divise aucun élément de l'ensemble S_n. Puisque le nombre de solutions de l'équation $x^2 \equiv -1 \pmod{p}$ est égal à 2 (en vertu du théorème 5.3), alors p divise au plus deux éléments de l'ensemble S_n. D'où, $\vartheta_p(D_n) = \vartheta_p(Q_n) \leq 2\vartheta_p(L_n) = \vartheta_p(L_n^2)$, comme il fallait le prouver.

• **3ème cas :** (si $p \leq n$).

En posant $\nu_k := \left\lfloor \frac{n}{p^k} \right\rfloor$ $(\forall k \in \mathbb{N}^*)$, il s'ensuit (en vertu du théorème 5.3) que :

$$\begin{aligned}\vartheta_p(Q_n) &= \sum_{k=1}^{\vartheta_p(L_n)} \#\left\{i\in\mathbb{N}^*;\ i\le n,\ p^k \mid i^2+1\right\}\\ &\le \sum_{k=1}^{\vartheta_p(L_n)}\left[\left(\sum_{\ell=0}^{\nu_k-1}\#\left\{i\in\mathbb{N}^*;\ \ell p^k+1\le i\le(\ell+1)p^k,\ p^k\mid i^2+1\right\}\right)+2\right]\\ &\le 2\sum_{k=1}^{\vartheta_p(L_n)}\left(\left\lfloor\frac{n}{p^k}\right\rfloor+1\right)\le 2\vartheta_p(n!)+2\vartheta_p(L_n).\end{aligned}$$

D'où l'on a : $\vartheta_p(D_n)=\vartheta_p(Q_n)-2\vartheta_p(n!)\le 2\vartheta_p(L_n)=\vartheta_p(L_n^2)$, comme il fallait le prouver. Ce qui complète cette démonstration. ■

Lemme 5.5. *Pour tout entier $n\ge 2$, on a :*

$$G_n:=\prod_{p>n}p^{\vartheta_p(L_n)}\ \textit{divise}\ M_n:=\frac{2^{2\vartheta_2(n!)-\lfloor(n-1)/2\rfloor-1}Q_n}{n!^2}\prod_{p\in\mathcal{P}_{4,3}\cap[1,n]}p^{2\vartheta_p(n!)}.$$

Démonstration. Soit p un nombre premier. On vérifie facilement que : $\vartheta_p(G_n)=\vartheta_p(M_n)=0$ pour $p\in\mathcal{P}_{4,3}\cup\{2\}$. Supposons maintenant que $p\in\mathcal{P}_{4,1}\cap[1,n]$ et posons $\nu_k:=\left\lfloor\frac{n}{p^k}\right\rfloor$ $(\forall k\in\mathbb{N}^*)$. D'après le théorème 5.3, on a :

$$\begin{aligned}\vartheta_p(Q_n) &= \sum_{k\ge1}\#\left\{i\in\mathbb{N}^*;\ i\le n\text{ et }p^k\mid i^2+1\right\}\\ &\ge \sum_{k=1}^{\vartheta_p(L_n)}\sum_{\ell=0}^{\nu_k-1}\#\left\{i\in\mathbb{N}^*;\ \ell p^k+1\le i\le(\ell+1)p^k,\ p^k\mid i^2+1\right\}\\ &= 2\sum_{k\ge1}\left\lfloor\frac{n}{p^k}\right\rfloor=2\vartheta_p(n!).\end{aligned}$$

Ce qui montre que $\vartheta_p(M_n)=\vartheta_p(Q_n)-2\vartheta_p(n!)\ge\vartheta_p(G_n)=0$. Supposons enfin que $p>n$. En raisonnant comme dans la démonstration du lemme 5.4 (en distinguant les cas $n<p<2n$ et $p>2n$), on montre que $\vartheta_p(G_n)=\vartheta_p(L_n)\le\vartheta_p(M_n)$. Dans tous les cas, on a bien $\vartheta_p(G_n)\le\vartheta_p(M_n)$; ce qui conclut au résultat requis et complète cette démonstration. ■

Lemme 5.6. *Pour tout entier $n\ge 10^3$, on a :*

$$\left(\beta_1\sqrt{n}\,(\log n)^{-0,4}\right)^n\le\prod_{p\in\mathcal{P}_{4,3}\cap[1,n]}p^{\vartheta_p(n!)}\le\left(\beta_2\sqrt{n}\,(\log n)^{0,4}\right)^n. \tag{5.2.1}$$

Démonstration. Montrons d'abord l'inégalité de gauche de (5.2.1). En vertu de la formule sommatoire d'Abel et du théorème 5.2, on a :

$$\begin{aligned}\sum_{p\in\mathcal{P}_{4,3}\cap[1,n]}\frac{\log p}{p} &= \frac{\theta\left(n;4,3\right)}{n}+\int_1^n\frac{\theta\left(t;4,3\right)}{t^2}\mathrm{d}t\\ &\geq \frac{1}{2}-\frac{0,4}{3\log 10}+\int_1^{10^3}\frac{\theta\left(t;4,3\right)}{t^2}\mathrm{d}t+\frac{1}{2}\int_{10^3}^n\frac{1}{t}\mathrm{d}t-0,4\int_{10^3}^n\frac{1}{t\log t}\mathrm{d}t\\ &\geq \frac{1}{2}\log n-0,4\log\log n+c_1.\end{aligned}$$

D'autre part, d'après le lemme 5.2, on a pour tout entier $n\geq 10^3$:

$$\sum_{p\in\mathcal{P}_{4,3}\cap[1,n]}\log p=\theta\left(n;4,3\right)\leq\frac{n}{2}+0,4\frac{n}{\log n}\leq c_2 n.$$

Nous déduisons alors de ce qui précède que :

$$\prod_{p\in\mathcal{P}_{4,3}\cap[1,n]}p^{\vartheta_p(n!)}\geq\prod_{p\in\mathcal{P}_{4,3}\cap[1,n]}p^{\frac{n}{p}-1}\geq\left(\frac{e^{(c_1-c_2)}\sqrt{n}}{(\log n)^{0,4}}\right)^n\geq\left(\frac{\beta_1\sqrt{n}}{(\log n)^{0,4}}\right)^n,$$

comme il fallait le prouver. Pour l'inégalité de droite de (5.2.1), on montre de la même façon que pour tout entier $n\geq 10^3$, on a :

$$\prod_{p\in\mathcal{P}_{4,3}\cap[1,n]}p^{\frac{1}{p}}\leq\beta_3\sqrt{n}\left(\log n\right)^{0,4}.$$

Par suite, en utilisant l'estimation $\prod_p p^{1/p(p-1)}\leq c_3$ (qui découle du troisième point du théorème 4.6), on obtient :

$$\begin{aligned}\prod_{p\in\mathcal{P}_{4,3}\cap[1,n]}p^{\vartheta_p(n!)} &\leq \prod_{p\in\mathcal{P}_{4,3}\cap[1,n]}p^{\frac{n}{p}+\frac{n}{p(p-1)}}\\ &\leq\left(\prod_{p\in\mathcal{P}_{4,3}\cap[1,n]}p^{\frac{n}{p}}\right)\left(\prod_p p^{\frac{n}{p(p-1)}}\right)\\ &\leq\left(c_3\beta_3\sqrt{n}\left(\log n\right)^{0,4}\right)^n\\ &\leq\left(\beta_2\sqrt{n}\left(\log n\right)^{0,4}\right)^n,\end{aligned}$$

comme il fallait le prouver. Notre démonstration est complète. ∎

5.3 Preuve de notre résultat principal

Démonstration du théorème 5.1. En se servant d'un logiciel de calcul (Maple ou Mathematica par exemple), on vérifie que (5.1.1) est valable pour tout entier $2 \leq n < 10^3$. Supposons pour la suite que $n \geq 10^3$. En utilisant successivement le lemme 5.4 et le lemme 5.6, on obtient :

$$L_n \geq \sqrt{2}^{\lfloor n/2 \rfloor + 1} \sqrt{\frac{Q_n}{n!^2}} \left(\frac{\beta_1 \sqrt{n}}{(\log n)^{0,4}} \right)^n \geq \left(\frac{\sqrt[4]{2}\beta_1 \sqrt{n}}{(\log n)^{0,4}} \right)^n \geq \left(\frac{\alpha_1 \sqrt{n}}{(\log n)^{0,4}} \right)^n .$$

Ce qui conclut à la minoration de (5.1.1). Pour montrer la majoration de (5.1.1), nous écrivons d'abord :

$$L_n = \prod_p p^{\vartheta_p(L_n)} = \left(\prod_{p \leq n} p^{\vartheta_p(L_n)} \right) \left(\prod_{p > n} p^{\vartheta_p(L_n)} \right). \tag{5.3.1}$$

D'une part, on a (en vertu du théorème 5.2) :

$$\prod_{p \leq n} p^{\vartheta_p(L_n)} = 2 \prod_{p \in \mathcal{P}_{4,3} \cap [1,n]} p^{\vartheta_p(L_n)} \leq 2 \left(n^2+1\right)^{\pi(n;4,1)} \leq 2 \left(n^2+1\right)^{\frac{n}{2 \log n}\left(1+\frac{5}{6 \log 10}\right)} \leq 2c_5 e^{c_4 n}.$$

D'autre part, d'après les lemmes 5.5 et 5.6, on a :

$$\prod_{p > n} p^{\vartheta_p(L_n)} \leq M_n \leq e^{\pi^2/6} \left({\beta_2}^2 2^{3/2} n (\log n)^{0,8} \right)^n .$$

En reportant ces estimations dans (5.3.1), on aboutit à :

$$L_n \leq 2c_5 e^{\pi^2/6} \left({\beta_2}^2 2^{3/2} e^{c_4} n (\log n)^{0,8} \right)^n \leq \alpha_2 \left(\alpha_3 n (\log n)^{0,8} \right)^n ,$$

comme il fallait le prouver. Le théorème est ainsi démontré. ∎

Conclusion générale

Le sujet initialement fixé de cette thèse consistait à établir des encadrements effectifs du plus petit commun multiple de termes consécutifs de certaines suites d'entiers.

En utilisant des arguments d'algèbre commutative et d'analyse complexe, nous avons obtenu un diviseur rationnel non trivial du nombre entier :

$$L_{c,m,n} := \operatorname{ppcm}\left(m^2+c, (m+1)^2+c, \ldots, n^2+c\right),$$

avec $n, m, c \in \mathbb{N}^*$ et $m \leq n$. Comme corollaire, nous en avons déduit des minorations effectives et non triviales pour $L_{c,m,n}$, et cela sans la contrainte "$1 \leq m \leq \left\lceil \frac{n}{2} \right\rceil$" (qui figure dans le résultat de Oon [41]). Dans une autre direction, nous avons généralisé quelques identités dues à Farhi [17], Nair [39] et Guo [22] aux suites à forte divisibilité. Nous avons appliqué ces identités ensuite pour estimer le ppcm de certaines suites de Lucas. En fait, la méthode utilisée est même applicable pour estimer le ppcm de toute suite à forte divisibilité d'ordre connu, comme celles d'ordre exponentiel. Par ailleurs, nous avons développé une toute première méthode permettant d'obtenir une majoration effective du ppcm d'une progression arithmétique finie. Comme conséquence, nous en avons déduit une estimation d'une certaine moyenne harmonique forte intéressante ainsi qu'une estimation de l'expression $\theta(x; k, \ell)$ de Chebyshev. Enfin, nous avons réussi à adapter notre méthode pour la suite quadratique particulière $\left(n^2+1\right)_n$ et obtenir ainsi un encadrement pour son ppcm, qui est presque optimal. En particulier, les minorations antérieures de Farhi [17] et de Oon [41] pour le ppcm de la même suite sont de beaucoup améliorées.

Perspectives

Bien évidemment, il reste plusieurs problèmes que nous n'avons pas traités dans cette thèse, mais qui font partie (plus au moins) de sa thématique. En voici quelques-uns qui pourront faire l'objet de nos recherches postérieures :

1. Prouver la conjecture de Cilleruelo (voir la conjecture 1) qui énonce que pour tout polynôme irréductible $f \in \mathbb{Z}[X]$, de degré ≥ 3, le logarithme du plus petit commun multiple des termes consécutifs de la suite $\left(f(n)\right)_n$ est de même ordre que le logarithme du produit de ces termes (lorsque n voisine l'infini).
2. Améliorer notre majoration du ppcm d'une suite arithmétique et étendre notre méthode à d'autres suites.
3. Améliorer la minoration "uniforme" de Hong et al. [27] du ppcm de certaines suites polynomiales (ce qui semble réalisable par des techniques d'algèbre polynomiale).
4. Établir des majorations non triviales du ppcm d'une suite polynomiale.
5. **Difficile !** Tenter d'établir un analogue du théorème des nombres premiers (sous sa version $\log \mathrm{ppcm}(1, 2, \ldots, n) \sim_{+\infty} n$) pour d'autres suites d'entiers strictement positifs.

Bibliographie

[1] E. Artin, The Gamma Function, *Holt, Rinehart and Winston*, New York, 1964.

[2] P. Bateman, J. Kalb & A. Stenger, A limit involving least common multiples : 10797, *Amer. Math. Monthly* **109** (2002), p. 393–394.

[3] M.A. Bennett, G. Martin, K. O'Bryant & A. Rechnitzer, Explicit bounds for primes in arithmetic progressions, *Illinois J. Math.* **62** (2018), p. 427–532.

[4] J.-P. Bézivin, A. Pethö & A. van der Porten, A full characterisation of divisibility sequences, *Amer. J. Math.* **112** (1990), 985–1001.

[5] A. Blanchard, Initiation à la Théorie Analytique des Nombres Premiers, *Dunod*, Paris, 1969.

[6] N. Bliss, B. Fulan, S. Lovett & J. Sommars, Strong divisibility, cyclotomic polynomials, and iterated polynomials, *Amer. Math. Monthly* **120** (2013), p. 519–536.

[7] S.A. Bousla & B. Farhi, Identities and estimations involving the least common multiple of strong divisibility sequences, *arXiv :1907.06700v2 [math.NT]*, 10 Apr 2020.

[8] S.A. Bousla & B. Farhi, Identités et estimations concernant le plus petit commun multiple de suites à forte divisibilité, *C. R. Acad. Sci. Paris, Sér. I*, **358** (2020), p. 481-487.

[9] S.A. Bousla & B. Farhi, Nontrivial effective lower bounds for the least common multiple of some quadratic sequences, *J. Integer Seq.* **23** (2020), Article 20.6.6.

[10] S.A. Bousla, Nontrivial upper bounds for the least common multiple of an arithmetic progression, *Asian-Eur. J. Math.* (2020), https://doi.org/10.1142/S1793557121501382. (à paraître)

[11] S.A. Bousla, On the least common multiple of binary linear recurrence sequences, *arXiv :2011.03858v1 [math.NT]*, 7 Nov 2020. (soumis)

[12] P.L. Chebyshev, Mémoire sur les nombres premiers, *J. Math. Pures Appl.* **17** (1852), p. 366–390.

[13] J. Cilleruelo, The least common multiple of a quadratic sequence, *Compos. Math.* **147** (2011), p. 1129–1150.

[14] H. Davenport, Multiplicative Number Theory, *Springer-Verlag*, New York, 1980.

[15] D. Duverney, Théorie des Nombres, *Dunod*, Paris, 1998.

[16] B. Farhi, Minorations non triviales du plus petit commun multiple de certaines suites finies d'entiers, *C. R. Acad. Sci. Paris, Sér. I*, **341** (2005), p. 469–474.

[17] B. Farhi, Nontrivial lower bounds for the least common multiple of some fnite sequences of integers, *J. Number Theory* **125** (2007), p. 393–411.

[18] B. Farhi, An identity involving the least common multiple of binomial coefficients and its application, *Amer. Math. Monthly* **116** (2009), p. 836–839.

[19] B. Farhi, An analog of the arithmetic triangle obtained by replacing the products by the least common multiples, *arXiv :1002.1383v2 [math.NT]*, 9 Feb 2010.

[20] B. Farhi, On the derivatives of the integer-valued polynomials, *Funct. Approx. Comment. Math.* **61** (2019), p. 227–241.

[21] B. Farhi & D. Kane, New results on the least common multiple of consecutive integers, *Proc. Amer. Math. Soc.* **137** (2009), p. 1933–1939.

[22] Victor J.W. Guo, On the least common multiple of q-binomial coefficients, *Integers* **10** (2010), p. 351–356.

[23] D. Hanson, On the product of the primes, *Canad. Math. Bull.* **15** (1972), p. 33–37.

[24] G.H. Hardy & E.M. Wright, The Theory of Numbers, *Oxford university press*, London, 5^{th} ed, 1979.

[25] S. Hong & W. Feng, Lower bounds for the least common multiple of finite arithmetic progressions, *C. R. Acad. Sci. Paris, Sér. I*, **343** (2006), p. 695–698.

[26] S. Hong & S. D. Kominers, Further improvements of lower bounds for the least common multiples of arithmetic progressions, *Proc. Amer. Math. Soc.* **138** (2010), 809–813.

[27] S. Hong, Y. Luo, G. Qian & C. Wang, Uniform lower bound for the least common multiple of a polynomial sequence, *C. R. Acad. Sci. Paris, Sér. I*, **351** (2013), p. 781–785.

[28] S. Hong & G. Qian, New lower bounds for the least common multiple of polynomial sequences, *J. Number Theory* **175** (2017), p. 191–199.

[29] R. Honsberger, Mathematical Gems III, *The Mathematical Association of America*, Washington, DC, 1985.

[30] L.K. Hua, Introduction to Number Theory, *Springer-Verlag*, Berlin, 1982.

[31] D.M. Kane & S.D. Kominers, Asymptotic improvements of lower bounds for the least common multiples of arithmetic progressions, *Canad. Math. Bull.* **57** (2014), 551–561.

[32] C. Kimberling, Strong divisibility sequences and some conjectures, *Fibonacci Quart.* **17** (1979), p. 13–17.

[33] P. Kiss & F. Matyas, An asymptotic formula for π, *J. Number Theory* **31** (1989) 255–259.

[34] D.E. Knuth & H. Wilf, The power of a prime that devides a generalized binomial coefficient, *J. Reine Angew. Math.* **396** (1989), p. 212–219.

[35] J.-M. De Koninck & F. Luca, Analytic Number Theory Exploring the Anatomy of Integers, *Graduate Studies in Mathematics*, Vol. 134, American Mathematical Society, 2012.

[36] Y.V. Matiyasevich & R. K. Guy, A new formula for π, *Amer. Math. Monthly* **93** (1986), p. 631–635.

[37] L. Moser, On the product of the primes not exceeding n, *Canad. Math. Bull.* **2** (1959), p. 119–121.

[38] G. Myerson, What the least common multiple divides, *J. Number Theory* **48** (1994), p. 80–87.

[39] M. Nair, On Chebyshev-type inequalities for primes, *Amer. Math. Monthly* **89** (1982), p. 126–129.

[40] A. Nowicki, Strong divisibility and lcm-sequences, *Amer. Math. Monthly* **122** (2015), p. 958–966.

[41] S.-M. Oon, Note on the lower bound of least common multiple, *Abstr. Appl. Anal.* (2013), Article ID 218125.

[42] P. Ribenboim, My Numbers, My Friends : Popular Lectures on Number Theory, *Springer-Verlag*, 2000.

[43] G. Robin, Estimation de la fonction de Tchebychef θ sur le k-ième nombre premier et grandes valeurs de la fonction $\omega(n)$ nombre de diviseurs premiers de n, *Acta Arith.* **42** (1983), p. 367–389.

[44] J.B. Rosser & L. Schoenfeld, Approximate formulas for some functions of prime numbers, *Illinois J. Math.* **6** (1962), p. 64–94.

[45] J. Rué, P. Sarka & A. Zumalacarregui, On the error term of the logarithm of the lcm of a quadratic sequence, *J. Théor. Nombres Bordeaux* **25** (2013), p. 457–470.

[46] W. Rudin, Real and Complex Analysis, *McGraw-Hill, Inc*, 3rd ed, 1987.

[47] J.J. Sylvester, On arithmetical series, *Messenger Math.* **21** (1892) 1-19, 87–120.

[48] G. Tenenbaum, Introduction to Analytic and Probabilistic Number Theory, *Amer. Math. Society*, 3rd ed, 2010.

[49] G. Tenenbaum & M. Mendès France, Les Nombres Premiers, *Presses Universitaires de France*, 1re édition, 1997.

[50] N.N. Vorob'ev, Fibonacci Numbers, *Pergamon Press, Ltd*, 1961.

[51] M. Ward, Note on the divisibility sequences, *Bull. Amer. Math. Soc.* **42** (1936), p. 843–845.

Résumé

Cette thèse consiste à étudier des estimations effectives du plus petit commun multiple de certaines suites d'entiers. Nous nous focalisons notamment sur une certaine classe de suites quadratiques, ainsi que les progressions arithmétiques et les suites à forte divisibilité. Premièrement, nous avons utilisé des méthodes d'algèbre commutative et d'analyse complexe pour établir de nouvelles minorations non triviales du ppcm de certaines suites quadratiques. Ensuite, une étude plus profonde des propriétés arithmétiques de suites à forte divisibilité nous a permis d'obtenir trois identités intéressantes concernant le ppcm de ces suites, ce qui généralise certaines identités antérieures de B. Farhi (2009) et M. Nair (1982). Nous en avons déduit par suite des estimations assez précises du ppcm d'une suite de Fibonacci généralisée (ce que l'on appelle les suites de Lucas). Nous avons également développé une première méthode permettant d'effectiviser un résultat asymptotique de P. Bateman (2002) sur le ppcm d'une progression arithmétique. Vers la fin, nous avons constaté que cette dernière méthode peut être adaptée pour encadrer le ppcm de la suite $(n^2+1)_n$, ce qui nous a permis en particulier d'améliorer les minorations de B. Farhi (2005) et S. M. Oon (2013). La thèse comprend aussi une présentation générale de quelques résultats de littérature.

Mots clés : Plus petit commun multiple, plus grand diviseur commun, suite à divisibilité, suite à forte divisibilité, suite de Lucas, suite de Fibonacci, progression arithmétique, suite quadratique, suite polynomiale, théorèmes de Chebychev, théorème des nombres premiers, répartition des nombres premiers.

Abstract

This thesis is devoted to studying estimates of the least common multiple of some integer sequences. Our study focuses on effective bounding of the lcm of some class of quadratic sequences, as well as arithmetic progressions and strong divisibility sequences. First, we have used methods of commutative algebra and complex analysis to establish new nontrivial lower bounds for the lcm of some quadratic sequences. Next, a more profound study of the arithmetic properties of strong divisibility sequences allowed us to obtain three interesting identities involving the lcm of these sequences, which generalizes some previous identities of B. Farhi (2009) and M. Nair (1982) ; as consequences, we have deduced a precise estimates for the lcm of generalized Fibonacci sequence (the so-called Lucas sequences). We have also developed a method that provides an effective version to the asymptotic result of P. Bateman (2002) concerning the lcm of an arithmetic progression. Finally, we found that the latter method can be adapted to estimate the lcm of the sequence $(n^2+1)_n$, which allowed us in particular to improve the lower bounds of B. Farhi (2005) and S. M. Oon (2013). The thesis also includes a general presentation of some literature results.

Key words : Least common multiple, greatest common divisor, divisibility sequences, strong divisibility sequences, Lucas sequences, Fibonacci sequence, arithmetic progressions, quadratic sequences, polynomial sequences, Chebychev theorems, prime number theorem, distribution of prime numbers.

ملخّص

تندرج هذه الأطروحة في إطار دراسة تقديرات المضاعف المشترك الأصغر لبعض متتاليات الأعداد الطبيعية. ركزنا دراستنا خصوصًا على الحصر الفعّال للمضاعف المشترك الأصغر لفئة من المتتاليات التربيعية، بالإضافة إلى المتتاليات الحسابية و المتتاليات ذات قوة في قابلية القسمة. بدأنا باستخدام طرق مستمدة من الجبر التبديلي و التحليل المركب لإيجاد حدود من الأدنى جديدة و غير تافهة للمضاعف المشترك الأصغر لبعض المتتاليات التربيعية. إنتقلنا بعدها إلى دراسة عميقة للخواص الأرثماطقية للمتتاليات ذات قوة في قابلية القسمة، أمكنتنا من إيجاد ثلاث متطابقات جد هامة تتعلق بالمضاعف المشترك الأصغر للحدود المتعاقبة من هذه المتتاليات. و على وجه الدقة، فلقد تحصلنا على تعميمات لمتطابقات معروفة سابقا، أوردها كل من **نير** (1982) و **فرحي** (2005) . و ترتبت على هذه المتطابقات تقديرات جدّ دقيقة للمضاعف المشترك الأصغر لمتتاليات **فيبوناتشي** المعمّمة (أو ما يعرف بمتتاليات **لوكا**) . من جهة أخرى، طورنا طريقة جديدة أمكنتنا من إيراد صيغة فعّالة للنتيجة المقاربة لِـ **بيتمان** (2002) و الّتي تخصّ المضاعف المشترك الأصغر للمتتاليات الحسابية. و في الأخير، قمنا بتطبيق هذه الطريقة على المتتالية $(n^2+1)_n$ ، مما سمح لنا على وجه الخصوص بتحسين الحدود الدنيا المعروفة سابقا من طرف **فرحي** (2005) و **أون** (2013) لِـ $\operatorname{lcm}(1^2+1, 2^2+1, \ldots, n^2+1)$. هذا و لقد قدمنا في هذه الأطروحة أيضًا عرضًا شاملًا و مفصّلًا لمعظم النّتائج المعروفة سابقًا في مجال دراستنا.

الكلمات المفتاحية : المضاعف المشترك الأصغر، القاسم المشترك الأكبر، متتاليات ذات قابلية القسمة، متتاليات ذات قوة في قابلية القسمة، متتاليات **لوكا** ، متتالية **فيبوناتشي** ، المتتاليات الحسابية، المتتاليات التّربيعية، متتاليات كثيرات الحدود، نظريات **شبيشاف** ، نظرية الأعداد الأولية، توزيع الأعداد الأولية.