1. COMPTER LES NOMBRES PREMIERS

1.1. Euclide

(**1.1**) On trouve dans le livre VII des *Éléments* d'Euclide les résultats fondamentaux de l'arithmétique des nombres entiers.

THÉORÈME 1.1. (THÉORÈME FONDAMENTAL DE L'ARITHMÉTIQUE) — *Tout nombre entier* $n > 1$ *est un produit de nombres premiers, et cette écriture est* unique *à l'ordre des facteurs près.*

Cet énoncé est bien connu, mais il est important d'avoir conscience :

(i) que l'existence d'une factorisation est très facile à démontrer (par récurrence) [1] ;

(ii) que l'unicité, par contre, est plus délicate ; il faut en effet faire appel au *lemme d'Euclide* [2], lequel peut se déduire du théorème de Bachet-Bézout (et donc de l'algorithme de la division euclidienne) ;

(iii) que l'unicité est ce qui est le plus utile dans la pratique (par exemple la résolution dans $\mathbf{Z}^3$ de l'équation de Pythagore $x^2+y^2=z^2$, que l'on peut trouver dans [**2**] ou encore [**1**]).

(1.2) Considérons un nombre premier p. La *valuation p-adique* d'un nombre entier $n \in \mathbf{Z}$, notée $v_p(n)$, est la plus grand exposant de p divisant n :

$$v_p(n) = \max\{k \in \mathbf{N} \mid p^k | n\}.$$

C'est un élément de $\mathbf{N} \cup \{\infty\}$ tel que $v_p(n) = \infty$ ssi $n = 0$, $v_p(1) = 0$ et, pour tous $m, n \in \mathbf{N}$,

(i) $v_p(nm) = v_p(n) + v_p(m)$;

(ii) $v_p(m+n) \geqslant \min\{v_p(m), v_p(n)\}$.

EXERCICE 1. — *Démontrer les deux propriétés précédentes.*

La notion de valuation p-adique permet d'énoncer le théorème fondamental de l'arithmétique sous la forme équivalente suivante : *tout nombre entier* $n \geqslant 1$ *s'écrit sous la forme*

$$n = \prod_p p^{v_p(n)}.$$

Il est important de remarquer ici que, si le produit porte a priori sur l'ensemble des nombres premiers, le facteur $p^{v_p(n)}$ est égal à 1 dès que $p > n$; il s'agit donc en réalité du produit d'un nombre *fini* de termes.

EXERCICE 2. — *Démontrer que le dernier énoncé ci-dessus est équivalent au théorème 1.*

(**1.3**) Euclide démontre que l'ensemble des nombres premiers est bel et bien *infini.*

THÉORÈME 1.2. (EUCLIDE) — *L'ensemble des nombres premiers est infini.*

Démonstration. Pour tout entier $n \geqslant 1$, le nombre entier $n! + 1 > 1$ admet au moins un facteur premier p. Celui-ci ne peut être égal à aucun des entiers $2, 3, \ldots, n$ car il diviserait sinon $n!$, et donc également $1 = (n!+1) - n!$; on en déduit $p > n$. L'ensemble des nombres premiers est non borné, donc il est infini. □

1. Il s'agit par ailleurs d'un phénomène très général : dans tout anneau *noethérien,* chaque élément non nul peut toujours s'écrire sous la forme d'un produit d'éléments irréductibles

2. Si p est un nombre premier et a, b sont deux entiers tels que $p|ab$, alors $p|a$ ou $p|b$

REMARQUE 1.3. — Notons $(p_n)_{n\geqslant 1}$ la suite croissante des nombres premiers. On peut déduire de l'argument d'Euclide une majoration très grossière du n-ième nombre premier p_n :

$$p_n \leqslant 2^{2^{n-1}}$$

pour tout $n \geqslant 1$. On prouve aisément cette inégalité en raisonnant par récurrence (exercice). Pour tout nombre réel $x > 1$,

$$2^{2^{n-1}} \leqslant x \iff n \leqslant \log_2 \log_2 x + 1,$$

donc

$$p_{\lfloor \log_2 \log_2 x \rfloor + 1} \leqslant x$$

et

$$\log_2 \log_2(x) \leqslant \pi(x).$$

Cette minoration est loin d'être optimale, mais elle a le mérite de quantitifer à peu de frais le théorème d'Euclide.

1.2. Euler

Euler exposa en 1737 une nouvelle preuve de l'infinitude de l'ensemble des nombres premiers, reposant sur le théorème fondamental de l'arithmétique et des considérations analytiques simples.

(2.1) Toute l'analyse requise dans l'approche d'Euler est contenue dans l'énoncé suivant, qui est une version *quantitative* de la comparaison série-intégrale [3].

LEMME 1.4. — *Soit $y < x$ deux nombres réels. Pour toute fonction monotone $f : [y,x] \to \mathbf{R}$,*

$$\left| \sum_{n\in\mathbf{Z},\ y\leqslant n\leqslant x} f(n) - \int_y^x f(t)\,\mathrm{d}t \right| \leqslant 3(|f(y)| + |f(x)|).$$

De façon un peu moins précise :

$$\sum_{n\in\mathbf{Z},\ y\leqslant n\leqslant x} f(n) = \int_y^x f(t)\,\mathrm{d}t + \mathrm{O}(|f(y)| + |f(x)|),$$

où la constante implicite dans O *ne dépend ni de f, ni de x et y.*

Démonstration. Quitte à remplacer f par $-f$, nous pouvons supposer que f est *croissante.*

3. Il faut quand même ajouter l'estimation $\ln(1+x) = x + \mathrm{O}(x^2)$ sur $[-1/2, 1/2]$, sous la forme : il existe un nombre réel $A > 0$ tel que

$$|\ln(1+x) - x| \leqslant Ax^2$$

pour tout $x \in [-1/2, 1/2]$. On peut le justifier en observant que la fonction définie sur $]-1,0[\cup]0,+\infty[$ par $x \mapsto \frac{\ln(1+x)-x}{x^2}$ se prolonge en une fonction continue sur l'intervalle $]-1,+\infty[$, donc bornée sur tout segment qu'il contient.

Si x et y sont entiers, nous pouvons écrire

$$\begin{aligned}\sum_{n\in\mathbf{Z},\ y\leqslant n\leqslant x} f(n) &= \sum_{n=y}^{x-1}\int_n^{n+1} f(n)\,\mathrm{d}t + f(x)\\ &= \sum_{n=y}^{x-1}\int_n^{n+1} f(\lfloor t\rfloor)\,\mathrm{d}t + f(x)\\ &= \int_y^x f(\lfloor t\rfloor)\,\mathrm{d}t + f(x)\\ &\leqslant \int_y^x f(t)\,\mathrm{d}t + f(x)\end{aligned}$$

en utilisant la croissance de f. De la même manière,

$$\sum_{n\in\mathbf{Z},\ y\leqslant n\leqslant x} f(n) = f(y) + \sum_{n=y+1}^{x}\int_{n-1}^{n} f(n)\,\mathrm{d}t = f(y) + \int_y^x f(\lceil t\rceil)\,\mathrm{d}t \geqslant f(y) + \int_y^x f(t)\,\mathrm{d}t,$$

ce qui établit l'estimation voulue :

$$\left|\sum_{y\leqslant n\leqslant x} f(n) - \int_y^x f(t)\,\mathrm{d}t\right| \leqslant \max\{|f(x)|,|f(y)|\} \leqslant |f(x)| + |f(y)|.$$

Le cas général s'en déduit aisément en introduisant les parties entières des bornes de sommation. On a en effet

$$\sum_{n\in\mathbf{Z},\ y\leqslant n\leqslant x} f(n) = \sum_{\lceil y\rceil\leqslant n\leqslant\lfloor x\rfloor} f(n)$$

et

$$\int_y^x f(t)\,\mathrm{d}t - \int_{\lceil y\rceil}^{\lfloor x\rfloor} f(t)\,\mathrm{d}t = \int_y^{\lceil y\rceil} f(t)\,\mathrm{d}t + \int_{\lfloor x\rfloor}^x f(t)\,\mathrm{d}t,$$

avec

$$\left|\int_y^{\lceil y\rceil} f(t)\,\mathrm{d}t\right| \leqslant \max\{|f(y)|,|f(\lceil y\rceil)|\},\quad \left|\int_{\lfloor x\rfloor}^x f(t)\,\mathrm{d}t\right| \leqslant \max\{|f(x)|,|f(\lfloor x\rfloor)|\}$$

En vertu de la croissance de f,

$$f(y) \leqslant f(\lceil y\rceil) \leqslant f(\lfloor x\rfloor) \leqslant f(x)$$

et donc

$$\max\{|f(y)|,|f(\lceil y\rceil)|,|f(x)|,|f(\lfloor x\rfloor)|\} = \max\{|f(x)|,|f(y)|\}.$$

Au final, nous avons obtenu la majoration

$$\left|\sum_{y\leqslant n\leqslant x} f(n) - \int_y^x f(t)\,\mathrm{d}t\right| \leqslant 3\max\{|f(x)|,|f(y)|\} \leqslant 3\left(|f(x)| + |f(y)|\right).$$

□

REMARQUE 1.5. — Bien que très élémentaire, cette estimation est fort utile et nous l'utiliserons à de nombreuses reprises. Nous en verrons également deux raffinements : la formule d'Abel et la formule d'Euler-Maclaurin.

En guise d'illustration, rappelons le comportement des séries de Riemann. Pour tout nombre réel $s > 1$,

$$\sum_{n=M}^{N}\frac{1}{n^s} = \int_M^N t^{-s}\,\mathrm{d}t + \mathrm{O}(M^{-s}+N^{-s}) = \frac{M^{1-s}-N^{1-s}}{s-1} + \mathrm{O}(M^{-s}+N^{-s}),$$

donc la série $\zeta(s) = \sum_{n\geqslant 1} n^{-s}$ est convergente et

$$1 < \zeta(s) = \frac{1}{s-1} + \mathrm{O}(1).$$

Précisons que le terme $\mathrm{O}(1)$ désigne une fonction *bornée* sur $]1,+\infty[$, donc cette identité :

(i) établit que la fonction ζ est bornée sur tout intervalle de la forme $[a,+\infty[$, avec $a > 1$;

(ii) fournit le comportement asymptotique de ζ au voisinage de 1^+ :

$$\zeta(s) \sim \frac{1}{s-1}$$

quand s tend vers 1 dans $]1,+\infty[$.

(2.2) L'observation capitale d'Euler est que le théorème fondamental de l'arithmétique permet d'exprimer $\zeta(s)$ à l'aide des nombres premiers. Pour comprendre cela, introduisons pour tout nombre premier p et tout $s > 1$ la série

$$\zeta_p(s) = 1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \ldots = \sum_{k\geqslant 0} \frac{1}{p^{ks}}$$

restreinte aux entiers qui sont des puissances de p. Il s'agit bien entendu d'une série géométrique, de somme

$$\zeta_p(s) = \left(1 - \frac{1}{p^s}\right)^{-1}.$$

Le produit

$$\zeta_2(s)\zeta_3(s) = \left(\sum_{m_2\geqslant 0} \frac{1}{2^{m_2 s}}\right)\left(\sum_{m_3\geqslant 0} \frac{1}{3^{m_3 s}}\right) = \sum_{m_2,m_3\geqslant 0} \frac{1}{(2^{m_2}3^{m_3})^s}$$

n'est pas autre chose, en vertu de la règle usuelle de développement, que la série zêta restreinte aux entiers de la forme $2^{m_2}3^{m_3}$. Plus généralement, pour tout entier $N \geqslant 2$,

$$\prod_{p\leqslant N} \zeta_p(s) = \prod_{p\leqslant N} \left(1 - \frac{1}{p^s}\right)^{-1} = \sum_{n\in E_N} \frac{1}{n^s},$$

où E_N désigne l'ensemble des entiers obtenus en faisant tous les produits possibles des nombres premiers $p \leqslant N$. Le théorème fondamental de l'arithmétique garantit que l'ensemble E_N contient *tous les nombres* $n \leqslant N$ (existence d'une factorisation, les facteurs premiers étant nécessairement inférieurs à N), et que chacun d'eux ne s'obtient qu'une seule fois, c'est-à-dire pour un seul terme du développement du produit de gauche (unicité de la factorisation). Nous pouvons donc écrire

$$\left|\prod_{p\leqslant N} \zeta_p(s) - \sum_{n\leqslant N} \frac{1}{n^s}\right| = \sum_{n\in E_N \text{ et } n>N} \frac{1}{n^s} \leqslant \sum_{n>N} \frac{1}{n^s}.$$

Le membre de droite (reste d'une série convergente...) est majoré par $\frac{N^{1-s}}{s-1} + \mathrm{O}(N^{-s})$ (Lemme 1.4), donc il tend vers 0 lorsque N tend vers $+\infty$.

Nous venons ainsi de démontrer le résultat fondamental suivant.

THÉORÈME 1.6 (FORMULE DU PRODUIT — *Pour tout réel $s > 1$, la suite des produits finis $\prod_{p\leqslant N} \zeta_p(s)$ est convergente, de limite $\zeta(s)$. Autrement dit,*

$$\sum_{n\geqslant 1} \frac{1}{n^s} = \zeta(s) = \prod_{p\in\mathscr{P}} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

(2.3) On a manifestement $\zeta(s) > 1$ et $\frac{1}{p^s} < \frac{1}{2}$ pour tout $s > 1$ et tout p premier. Il est donc licite de passer aux logarithmes dans l'identié d'Euler, qui se réécrit alors

$$\begin{aligned}\ln\zeta(s) &= \sum_{p\in\mathscr{P}} -\ln\left(1-\frac{1}{p^s}\right)\\ &= \sum_{p\in\mathscr{P}}\left(\frac{1}{p^s}+\mathrm{O}\left(\frac{1}{p^{2s}}\right)\right)\\ &= \sum_{p\in\mathscr{P}}\frac{1}{p^s}+\mathrm{O}\left(\sum_{p\in\mathscr{P}}\frac{1}{p^{2s}}\right).\end{aligned}$$

pour tout $s\in]1,+\infty[$.

Il faut ici observer que l'interversion de la somme et du $\mathrm{O}(\cdot)$ est licite car on utilise l'estimation

$$\ln(1+x) = x+\mathrm{O}(x^2)$$

pour tout x dans $[-1/2,1/2]$ (la constante de O ne dépend *pas* de x), puis on substitue $p^{-s}\in[0,1/2]$ à x. Enfin, en observant que la série des p^{-2s} est bornée par la somme de la série (de Riemann) convergente des n^{-2} pour tout $s\in]1,+\infty[$, nous obtenons

$$\sum_{p\in\mathscr{P}}\frac{1}{p^s} = \ln\zeta(s)+\mathrm{O}(1)$$

pour tout $s\in]1,+\infty[$.

Il reste à exploiter notre connaissance du comportement asymptotique de $\zeta(s)$ au voisinage de 1^+, rappelé ci-dessus (à la suite de la remarque 1.5) :

$$\zeta(s) = \frac{1}{s-1}+\mathrm{O}(1),$$

donc

$$\sum_{p\in\mathscr{P}}\frac{1}{p^s} = \ln\left(\frac{1}{s-1}+\mathrm{O}(1)\right)+\mathrm{O}(1) = \ln\frac{1}{s-1}+\ln(1+\mathrm{O}(s-1))+\mathrm{O}(1)$$

et

$$\sum_{p\in\mathscr{P}}\frac{1}{p^s} = -\ln(s-1)+\mathrm{O}(1)$$

lorsque s tend vers 1^+.

THÉORÈME 1.7. (EULER) — *La série*

$$\sum_{p\in\mathscr{P}}\frac{1}{p}$$

est divergente.

Démonstration. Pour tout $s>1$,

$$\sum_{p\in\mathscr{P}}\frac{1}{p}\geqslant\sum_{p\in\mathscr{P}}\frac{1}{p^s}$$

dans $\mathbf{R}\cup\{+\infty\}$. L'estimation asymptotique du membre de droite quand s tend vers 1 que l'on vient d'obtenir fournit la conclusion voulue. □

REMARQUE 1.8. — 1. On peut déduire de ce théorème l'estimation $\pi(x) = o(x)$ quand x tend vers l'infini, c'est-à-dire que la proportion des nombres premiers parmi les nombres entiers $\leqslant x$ tend vers 0 lorsque x tend vers $+\infty$. De manière imagée, la probabilité qu'un nombre entier choisi au hasard soit premier est nulle.

2. La formule

$$\sum_{p\in\mathscr{P}} \frac{1}{p^s} = \ln\zeta(s) + \mathrm{O}(1)$$

quand s tend vers 1^+ relie le comportement asymptotique de la suite des nombres premiers, exprimé via celui de la série des $\frac{1}{p^s}$ quand $s \longrightarrow 1^+$, à celui d'une fonction spécifique, ici $\zeta(s)$, au voisinage de $s = 1$. Ce phénomène est au cœur de la théorie analytique des nombres.

3. Des arguments analogues à ceux utilisés précédemment permettent d'encadrer les sommes partielles de la séries des inverses des nombres premiers : il existe un réel $C > 0$ tel que

$$\ln\ln x - \ln 2 \leqslant \sum_{p\in\mathscr{P}, p\leqslant x} \frac{1}{p} \leqslant e\ln\ln x + C$$

pour tout réel $x > 1$. La démonstration fait l'objet de l'exercice 3 du TD1. Cet encadrement détermine l'ordre de grandeur de $\sum_{p\leqslant x} \frac{1}{p}$. Nous verrons plus loin un développement asymptotique de ces sommes partielles, de terme dominant $\ln\ln x$.

1.3. Tchébychev

(3.1) En 1850, le mathématicien russe Pafnouti Tchébychev démontra que la fonction de comptage des nombres premiers a bien l'ordre de grandeur attendu.

THÉORÈME 1.9. — *Il existe des nombres réels $0 < c < C$ tels que, pour tout x assez grand,*

$$c\,\frac{x}{\log x} \leqslant \pi(x) \leqslant C\,\frac{x}{\log(x)}.$$

On peut déduire de ce théorème l'existence de nombres premiers dans certains intervalles. En effet, si $a < b$ sont deux nombres réels (suffisamment grands) tels que

$$C\frac{a}{\log a} < c\frac{b}{\log b},$$

alors $\pi(a) < \pi(b)$ et l'intervalle $]a,b]$ contient donc un nombre premier. De fait, les bornes obtenues par Tchébychev, à savoir $c = 0,92$ et $C = 1,11$, étaient assez bonnes pour lui permettre de de démontrer le *postulat de Bertrand* :

pour tout nombre entier $n \geqslant 2$, l'intervalle $]n,2n[$ contient toujours un nombre premier.

Nous allons exposer une version simplifiée de la démonstration de Tchébychev, conduisant aux bornes plus grossières $c = \frac{1}{2}$ et $C = 2$. Si ces bornes ne suffisent pas à déduire le postulat de Bertrand, une preuve plus élémentaire de ce résultat, découverte par P. Erdös en 1936, fait l'objet du problème du TD1.

La démonstration de Tchébychev est *élémentaire*, au sens où elle n'utilise que le théorème fondamental de l'arithmétique et des estimations relevant de l'analyse réelle asymptotique, et non pas l'analyse complexe. Elle n'en demeure pas moins ingénieuse, son point de départ étant l'observation que le coefficient binomial $\binom{2n}{n}$ ne diffère « pas trop » du produit de tous les nombres premiers dans l'intervalle $]n,2n]$.

(3.2) Nous allons avoir besoin de quatre résultats auxiliaires, tous intéressants indépendamment de l'utilisation que nous allons en faire.

Le premier consiste en une formule explicitant la valuation p-adique des coefficients binomiaux.

LEMME 1.10. (FORMULE DE LEGENDRE) — *Pour tout nombre entier naturel n et tout nombre premier p,*

$$v_p(n!) = \sum_{\alpha \geqslant 1} \left\lfloor \frac{n}{p^\alpha} \right\rfloor.$$

Démonstration — Si l'on factorise chaque entier $m \leqslant n$ sous la forme $m = p^{v_p(m)} m'$, avec $p \nmid m'$, alors le facteur p^α apparaît dans

$$n! = \prod_{1 \leqslant m \leqslant n} m$$

pour chaque entier m tel que $p^\alpha | m$ et $p^{\alpha+1} \nmid m$, c'est-à-dire $\left\lfloor \frac{n}{p^\alpha} \right\rfloor - \left\lfloor \frac{n}{p^{\alpha+1}} \right\rfloor$ fois (le nombre des multiples de p^α moins celui des multiples de $p^{\alpha+1}$ dans $[1,n]$.). On a donc

$$v_p(n!) = \sum_{\alpha \geqslant 1} \left(\left\lfloor \frac{n}{p^\alpha} \right\rfloor - \left\lfloor \frac{n}{p^{\alpha+1}} \right\rfloor \right) \alpha = \sum_{\alpha \geqslant 1} \left\lfloor \frac{n}{p^\alpha} \right\rfloor.$$

□

Le second est un encadrement du coefficient binomial médian.

LEMME 1.11. — *Pour tout entier $n \geqslant 1$,*

$$\frac{2^n}{n+1} \leqslant \binom{n}{\lfloor n/2 \rfloor} \leqslant 2^{n-1}.$$

Démonstration — Les coefficients binomiaux $\binom{n}{k}$ sont croissants avec $k \in \{0, \dots, \lfloor n/2 \rfloor\}$, puis décroissants avec $k \in \{\lfloor n/2 \rfloor, n\}$; la plus grande valeur est donc atteinte en

$$\binom{n}{\lfloor n/2 \rfloor} = \binom{n}{n - \lfloor n/2 \rfloor}.$$

On en déduit facilement la minoration souhaitée :

$$2^n = \sum_{k=0}^{n} \binom{n}{k} \leqslant (n+1) \binom{n}{\lfloor n/2 \rfloor},$$

donc

$$\frac{2^n}{n+1} \leqslant \binom{n}{\lfloor n/2 \rfloor}.$$

Pour établir la majoration, distinguons deux cas suivant la parité de n.

(i) Si $n = 2m+1$ est impair, alors nous pouvons aparier les coefficients binomiaux $\binom{n}{k}$ et $\binom{n}{n-k}$ pour tout $k \in \{0, \dots, m\}$, d'où :

$$2^n = \sum_{k=0}^{n} \binom{n}{k} = 2 \sum_{k=0}^{m} \binom{n}{k} \geqslant 2 \binom{n}{m},$$

ce qui est la majoration souhaitée.

(ii) Si $n = 2m$, alors $\binom{n}{m}$ est l'unique coefficient binomial maximal, donc l'argument précédent ne fonctionne plus. On a cependant

$$\binom{2m}{m} = \frac{m+2}{m} \binom{2m}{m+1} \leqslant 2 \binom{2m}{m+1},$$

donc

$$2^n \geqslant \binom{2m}{m-1} + \binom{2m}{m} + \binom{2m}{m+1} = \binom{2m}{m} + 2\binom{2m}{m+1} \geqslant 2\binom{2m}{m},$$

ce qui est encore la majoration souhaitée.

□

Le troisième fournit une seconde majoration des coefficients binomiaux, faisant apparaître la fonction de comptage.

LEMME 1.12. — *Soit $n \geqslant 1$ et $k \geqslant 0$ deux nombres entiers.*

(i) Soit p un nombre premier. En posant $\alpha_p = v_p\left(\binom{n}{k}\right)$, on a

$$p^{\alpha_p} \leqslant n.$$

(ii) On en déduit la majoration :

$$\binom{n}{k} \leqslant n^{\pi(n)}.$$

Démonstration — (i) Nous pouvons expliciter la valuation p-adique du coefficient binomial $\binom{n}{k}$ à l'aide de la formule de Legendre (Lemme 1.10) :

$$\begin{aligned} \alpha_p &= v_p\left(\frac{n!}{k!(n-k)!}\right) \\ &= v_p(n!) - v_p(k!) - v_p((n-k)!) \\ &= \sum_{m \geqslant 1} \left(\left\lfloor \frac{n}{p^m} \right\rfloor - \left\lfloor \frac{k}{p^m} \right\rfloor - \left\lfloor \frac{n-k}{p^m} \right\rfloor \right) \end{aligned}$$

La fonction réelle f définie sur $\mathbf{R}^2$ par

$$f(x,y) = \lfloor x+y \rfloor - \lfloor x \rfloor - \lfloor y \rfloor$$

est *1-périodique* par rapport à chacune des variables : il suffit de le vérifier pour la première par symétrie de f, et

$$f(x+1,y) = \lfloor x+y+1 \rfloor - \lfloor x+1 \rfloor - \lfloor y \rfloor = \lfloor x+y \rfloor + 1 - (\lfloor x \rfloor + 1) - \lfloor y \rfloor = f(x,y)$$

pour tous $x, y \in \mathbf{R}^2$. On en déduit

$$\sup_{x,y \in \mathbf{R}^2} f(x,y) = \sup_{x,y \in [0,1[} f(x,y),$$

puis

$$\sup_{x,y \in \mathbf{R}^2} f(x,y) = 1$$

puisque

$$f(x,y) = \lfloor x+y \rfloor = \begin{cases} 0 & \text{si} \quad x+y < 1 \\ 1 & \text{si} \quad x+y \geqslant 1 \end{cases}$$

pour tous $x, y \in [0,1[$. En observant que, dans la somme ci-dessus pour α_p, les seuls entiers m ayant une contribution éventuellement non nulle sont ceux tels que $p^m \leqslant n$, c'est-à-dire $m \leqslant \log_p n$, nous obtenons finalement

$$\alpha_p \leqslant \log_p n \ \text{ et donc } \ p^{\alpha_p} \leqslant p^{\log_p n} = n.$$

(ii) Avec les notations en vigueur, nous pouvons écrire la factorisation du coefficient binomial sous la forme

$$\binom{n}{k} = \prod_{p \mid \binom{n}{k}} p^{\alpha_p}.$$

Chaque facteur p^{α_p} figurant dans le membre de droite est majoré par n en vertu premier point, et tout diviseur premier de $\binom{n}{\lfloor n/2 \rfloor}$ divise $n!$, donc est inférieur à n. Ces observations conduisent immédiatement à la majoration

$$\binom{n}{\lfloor n/2 \rfloor} \leqslant n^{\pi(n)}.$$

□

Le quatrième et dernier résultat préliminaire décrit les plus grands facteurs premiers du coefficient binomial médian.

LEMME 1.13. — *Soit $n \geqslant 2$ un nombre entier. Le coefficient binomial $\binom{2n}{n}$ est divisible une fois et une seule par chaque nombre premier p dans l'intervalle $]n, 2n]$; en particulier,*

$$\prod_{n < p \leqslant 2n} p \mid \binom{2n}{n}.$$

De même, le coefficient binomial $\binom{2n+1}{n}$ est divisible une fois et une seule par chaque nombre premier p dans l'intervalle $]n+1, 2n]$; en particulier,

$$\prod_{n+1 < p \leqslant 2n+1} p \mid \binom{2n+1}{n}.$$

Démonstration — En écrivant

$$(2n)! = \binom{2n}{n} (n!)^2,$$

il est manifeste que chaque nombre premier $p \in]n, 2n]$, divisant $(2n)!$ mais ne divisant pas $n!$, doit diviser le coefficient binomial. Le produit de ces nombres premiers divise donc le coefficient binomial en vertu du lemme d'Euclide. Enfin, la condition $p > n$ implique $p^2 > n^2 \geqslant 2n$, donc $v_p((2n)!) = 1$ en vertu de la formule de Legendre (Lemme 1.10) et p^2 ne peut donc pas diviser le coefficient binomial.

Le cas du coefficient binomial $\binom{2n+1}{n}$ se traite de manière analogue. □

(3.3) Venons-en maintenant à la démonstration du théorème 1.9, avec les constantes $c = \frac{1}{2}$ et $C = 2$.

La minoration —- Soit $x > 1$ un nombre réel et posons $n = \lfloor x \rfloor$, ce qui fournit l'encadrement $n \leqslant x < n+1$.

En combinant les lemmes 1.11 et 1.12, nous obtenons l'inégalité

$$\frac{2^n}{n+1} \leqslant n^{pi(n)},$$

soit la minoration

$$\pi(n) \geqslant \frac{n \ln 2 - \ln(n+1)}{\ln n} \geqslant \frac{(x-1)\ln 2 - \ln(x+1)}{\ln x}.$$

Le membre de droite est supérieur à $\frac{1}{2}\frac{x}{\ln x}$ pour tout réel $x \geqslant 20$ [4] donc la minoration annoncée est acquise pour tout $x \geqslant 20$. Par aileurs, on la vérifie explicitement pour $3 \leqslant x < 20$ en observant sur une table des valeurs de $\pi(n)$ l'inégalité

$$\pi(n) \geqslant \frac{1}{2}\frac{n+1}{\ln(n+1)}$$

pour tout entier $n \in [3,20]$.

La majoration — La fonction $x \mapsto \frac{x}{\ln x}$ est croissante, donc il suffit d'établir la majoration pour x entier puisqu'alors

$$\pi(x) = \pi(\lfloor x \rfloor) \leqslant 2\frac{\lfloor x \rfloor}{\ln \lfloor x \rfloor} \leqslant 2\frac{x}{\ln x}.$$

Nous allons donc établir l'inégalité

$$\pi(n) \leqslant 2\frac{n}{\ln n}$$

en raisonnant par récurrence forte sur le nombre entier $n \geqslant 2$. En fait, nous allons avoir besoin d'initialiser cette récurrence à $n = 106$, donc il faut commencer par vérifier explicitement que la majoration vaut pour tout entier $n \leqslant 106$; cela se fait aisément à l'aide d'une table des valeurs de $\pi(n)$.

Prouvons maintenant l'hérédité forte, en distinguant deux cas, selon la parité de n.

(i) Si n est pair, alors $\pi(n) = \pi(n-1)$ et l'inégalité pour n découle immédiatement de celle pour $n-1$.

(ii) Supposons maintenant que $n = 2m+1$ soit impair et $n \geqslant 106$. En combinant les lemmes 1.11 et 1.13, on obtient

$$\prod_{m+1<p\leqslant 2m+1} p \leqslant 2^{2m}.$$

Le membre de gauche est minoré par $(m+2)^{\pi(2m+1)-\pi(m+1)}$, donc

$$\pi(2m+1) - \pi(m+1) \leqslant \frac{2m\ln 2}{\ln(m+2)},$$

puis

$$\pi(n) = \pi(2m+1) \leqslant 2\frac{m+1}{\ln(m+1)} + \frac{2m\ln 2}{\ln(m+2)} \leqslant \frac{(1+\ln 2)n+1}{\ln(n/2)}$$

en utilisant l'hypothèse de récurrence. On vérifie finalement que le membre de droite est majoré par $2\frac{n}{\ln n}$ pour tout $n \geqslant 106$ [5].

□

4. La fonction $f : x \mapsto (x-1)\ln 2 - \ln(x+1) - \frac{1}{2}x$ est *convexe* sur $[0,+\infty[$, strictement négative en 0 et de limite $+\infty$ en $+\infty$, donc elle admet un minimum strictement négatif en un point x_0 et est strictement croissante sur $[x_0,+\infty[$; on en déduit qu'elle s'annule en un unique point $x_1 > x_0$, elle qu'elle est strictement positive sur $]x_1,+\infty[$. Comme $f(20) \simeq 0,17 > 0$, cette fonction est positive sur $[20,+\infty[$ et la minoration souhaitée est donc valable sur cet intervalle.

5. La fonction $f : x \mapsto ((1+\ln 2)x+1)\ln x - 2x\ln(x/2) = (\ln 2 - 1)x\ln x + \ln x + (2\ln 2)x$ est *concave* sur $[3,+\infty[$, strictement positive en 3 et de limite $-\infty$ en $+\infty$, donc elle possède un (unique) maximum en un point x_0, et est strictement décroissante sur $[x_0,+\infty[$; elle s'annule donc en un unique point $x_1 > x_0$ et est strictement négative sur $]x_1,+\infty[$. Comme $f(106) \simeq -0,07 < 0$, f est strictement négative sur $[106,+\infty[$ et la majoration souhaitée vaut donc pour $n \geqslant 106$.

Bibliographie

[1] G. H. HARDY and E. M. WRIGHT. *An introduction to the theory of numbers*. Clarendon Press, 1979.

[2] Marc HINDRY. *Arithmétique*. Calvage & Mounet.

[3] Gérald TENENBAUM. *Introduction à la théorie analytique et probabiliste des nombres*. Dunod, 2022

[4] Gérald TENENBAUM et Jie WU. *Théorie analytique et probabiliste des nombres : 307 exercices corrigés*. Belin, 2014

Table des matières