SUR LA DISTRIBUTION DES NOMBRES PREMIERS.

Ce texte est la rédaction d'un exposé fait le 26 avril 1983 et annoncé sous le titre "*Nombres premiers*". Le §1 décrit ce qu'est la théorie de la Distribution des nombres premiers. Les §§2, 3 et 4 sont consacrés respectivement :

- à diverses démonstrations de l'infinité des nombres premiers ;
- au théorème de Tchebychev ;
- au lien entre théorie des nombres premiers et fonction zêta de Riemann.

Le texte est suivi :

- d'un index (notations, vocabulaire) ;
- de notes, auxquelles le renvoi est fait par numéro entre parenthèses ;
- d'une bibliographie élémentaire, assez accessible (matériellement) à laquelle le renvoi est fait par numéro entre crochets.

On conseille vivement au lecteur :

- de travailler avec papier et stylo ;
- de commencer par parcourir l'index et de noter la signification des symboles $\pi(x)$, $\sim$ et des expressions "théorème des nombres premiers" et "équivalence".

1. Introduction.

La théorie de la distribution des nombres premiers s'occupe de questions du genre suivant :

a) soit $\mathbf{P}$ l'ensemble de tous les nombres premiers :

Question n°1 : l'ensemble $\mathbb{P}$ est-il infini ?

Réponse : oui (Euclide ; voir §2).

Plus généralement, soient k et a deux entiers premiers entre eux, tels que $1 < a < k$, et soit $\mathbb{P}(k, a)$ l'ensemble des nombres premiers de la forme $p = kn + a$, $n \geq 0$.

Question n° 2 : l'ensemble $\mathbb{P}(k,a)$ est-il infini ?

Réponse : oui (Dirichlet ; voir note (1)).

b) Soit maintenant x une variable réelle ≥ 1, et notons $\pi(x)$ le nombre des p premiers et $\leq x$ ($\pi(x)$ est dite fonction de comptage des nombres premiers). Puisque $\mathbb{P}$ est infini (voir a)), on a $\lim_{x \to \infty} \pi(x) = \infty$.

Question n° 3 : que peut-on dire de $\lim_{x \to \infty} \pi(x)/x$ quand $x \to \infty$?

Réponse : on a $\lim_{x \to \infty} \pi(x)/x = 0$ (Legendre : voir § 3).

Question n° 4 : quel est l'ordre de grandeur de $\pi(x)$ quand $x \to \infty$?

Réponse : $x/\log x$ (Gauss, Legendre ; Tchebychev : voir § 3).

Question n° 5 : quel est (s'il en existe) un équivalent de $\pi(x)$ quand $x \to \infty$?

Réponse : $x/\log x$ ("théorème des nombres premiers" : Riemann ; Von Mangoldt, Hadamard, De La Vallée-Poussin ; voir § 4).

c) Convenons maintenant de ne considérer que les p premiers impairs ($p \geq 3$) et de noter p^* le plus petit nombre premier $> p$ (le successeur de p). La différence $p^* - p$ est évidemment ≥ 2, et il arrive fréquemment que $p^* - p = 2$: par exemple, pour $p = 3, 5, 11, 17, \ldots$ puisque $3^* = 5$, $5^* = 7$, $11^* = 13$, $17^* = 19$, ...

Question n° 6 : l'égalité $p^* - p = 2$ est-elle réalisée une infinité de fois ?

Réponse : probablement (problème des nombres premiers jumeaux : voir note (2)).

Question n° 7 : la différence $p^* - p$ est-elle bornée ?

Réponse : non (facile ; voir note (3)).

On a donc pour le moment $2 \leq p^* - p < \infty$!

Question n° 8 : peut-on majorer $p^* - p$ par une fonction raisonnable de p ?

Réponse : oui ; par exemple, on sait prouver assez facilement que $p^* - p \leq p$ (c'est-à-dire que $p^* \leq 2p$: voir [3], pp. 343-344 ; mais ceci est très loin de l'ordre de grandeur véritable) ; ou, mieux, mais très difficilement, que $p^* - p \leq p^\alpha$, $\alpha < 1$; par exemple, $\alpha = 3/5$; mais ceci est encore apparemment très loin de l'or-

dre de grandeur exact). Remarquons que l'ordre de grandeur moyen de $p^* - p$ est de la forme $\ell og\ p$.

•

Ces quelques specimens de question-réponse doivent donner au lecteur une idée de ce qu'est la théorie de la Distribution des nombres premiers. Dans ce qui suit, nous allons examiner en détail les questions n°1 (§ 2), n°4 (§ 3) et n°5 (§ 4). Les §§ 2-3 sont élémentaires. Le § 4 fait appel à un peu d'analyse complexe (prolongement analytique, théorème des résidus), mais devrait malgré tout être à peu près lisible par quiconque souhaite avoir une idée de ce que sont la fonction zêta de Riemann, l'hypothèse de Riemann, et leurs rapports avec le théorème des nombres premiers (c'est-à-dire l'équivalence $\pi(x) \sim x / \ell og\ x$ $(x \to \infty)$).

2. Infinité des nombres premiers.

Notons toujours $\mathbb{P}$ l'ensemble des nombres premiers. Il s'agit de prouver le résultat suivant :

Théorème 1. - L'ensemble $\mathbb{P}$ est infini.

Nous allons en donner cinq démonstrations assez différentes, rangées par ordre de "modernité" croissante (mais l'ordre chronologique est en réalité 1-5-3-4-2 !).

Démonstration n° 1 (Euclide, vers 300 avant J. C.). -

a) Soit $\mathbb{P}_h = \{p_1, p_2, \ldots, p_h\}$ un ensemble fini (quelconque) de h nombres premiers distincts. Posons $q = (p_1\ p_2 \ldots p_h) + 1$.
On a $q \geq 2 + 1 = 3$, et q admet donc au moins un diviseur premier p (voir note (4)). Si p appartenait à $\mathbb{P}_h$, on aurait à la fois $p \mid (p_1\ p_2 \ldots\ p_h)$ et $p \mid q$, donc par différence

$$p \mid (q - (p_1\ p_2 \ldots p_h)), \text{ soit } p \mid 1 :$$

absurde ! (ici et dans la suite, une écriture telle que $p \mid q$ signifie "p divise q"). ainsi, p n'appartient pas à $\mathbb{P}_h$.

b) Supposons maintenant $\mathbb{P}$ fini ; soit h le nombre d'éléments de $\mathbb{P}$; dans le raisonnement a), on peut alors prendre $\mathbb{P} = \mathbb{P}_h$, et ce raisonnement nous donne un nombre premier $p \notin \mathbb{P}$: absurde ! $\mathbb{P}$ est donc nécessairement infini. ■

Démonstration n° 2 (Polya, vers 1920). - a) Soit

$$F_n = (2^{2^n}) + 1 \quad , \quad n \geq 0 \quad (F_n \text{ premier ou non})$$

la suite des nombres de Fermat (voir note (5)). Montrons d'abors que si $m \neq n$ disons : $m < n$, $n - m = h \geq 1$), alors F_m et F_n sont premiers entre eux : on a en effet $F_m - 1 = 2^{2^n}$; $F_n - 1 = 2^{2^n} = 2^{2^{m+h}} = (F_m - 1)^{2^h}$.
Posons pour simplifier $N = 2^h$ (pair : $h \geq 1$) et appliquons la formule du binôme :

$$F_n - 1 = (F_m - 1)^N = \sum_{j=1}^{N} C_N^j F_m^j (-1)^{N-j} + (-1)^N \ ;$$

d'où $F_n = AF_m + 1 + (-1)^N = AF_m + 2$, A désignant un facteur entier qui se calculerait facilement. Ceci montre que le p. g. c. d. de F_m et F_n divise 2 ; mais puisque F_m et F_n sont évidemment impairs, ce p. g. c. d. est lui-même impair, donc finalement égal à 1, comme annoncé.
b) Soit alors (pour tout $n \geq 0$) p_n un diviseur premier de F_n. Si $m \neq n$, on a certainement $p_m \neq p_n$ (F_m et F_n sont premiers entre eux). $\mathbb{P}$ contient donc un sous-ensemble infini :

$$\{p_0, p_1, p_2, \ldots, p_n, \ldots\} \ ,$$

et $\mathbb{P}$ est lui-même a fortiori infini. ■

Démonstration n° 3 (classique). - a) Soit (comme plus haut) $\mathbb{P}_h$ un ensemble fini de h nombres premiers distincts. Notons $\mathbb{N}_h$ l'ensemble des nombres entiers dont tous les facteurs premiers sont dans $\mathbb{P}_h$, et notons $\nu_h(x)$ le nombre des entiers n appartenant à $\mathbb{N}_h$ et $\leq x$. Un tel entier peut s'écrire

$$n = p_1^{c_1} p_2^{c_2} \ldots p_h^{c_h} \ m^2 \ ,$$

avec $c_i = 0$ ou 1 pour $1 \leq i \leq h$, et on a évidemment

$$m \leq \sqrt{n} \leq \sqrt{x}.$$

Cette écriture est en fait unique (exercice ; regarder des exemples). Du fait qu'il existe exactement 2^h systèmes $(c_1, c_2, \ldots, c_h)$ répondant à la condition ci-dessus, on voit qu'il existe au plus $2^h \sqrt{x}$ éléments $n \leq x$ dans $\mathbb{N}_h$, donc que $\nu_h(x) \leq 2^h \sqrt{x}$.

b) Supposons maintenant $\mathbb{P}$ fini, $\mathbb{P} = \mathbb{P}_h$. On a alors évidemment $\mathbb{N}_h = \mathbb{N}$ (ensemble de tous les entiers ≥ 1) et $\nu_h(x) = [x]$ (partie entière de x), donc (par a))

$$[x] \leq 2^h \sqrt{x}.$$

Mais ceci est absurde : car quant $x \to \infty$, $[x] \sim x$, et le nombre de droite de l'inégalité tend au contraire vers l'infini beaucoup plus lentement que x. $\mathbb{P}$ est donc infini. ■

Démonstration n° 4 (de style fin XIXème siècle). - a) Supposons $\mathbb{P}_h$, $\mathbb{N}_h$ et $\nu_h(x)$ définis comme dans la démonstration n° 3. On voit que $\nu_h(x)$ est égal au nombre de systèmes d'entiers ≥ 0 $(y_1, y_2, \ldots, y_h)$ tels que

$$p_1^{y_1}\, p_2^{y_2} \ldots p_h^{y_h} \leq x ,$$

ou mieux

(1) $$a_1 y_1 + a_2 y_2 + \ldots + a_h y_h \leq \log x$$

en prenant les logarithmes des deux membres et en posant pour simplifier $a_i = \log p_i$, $1 \leq i \leq h$. Dans l'espace $\mathbb{R}^h$ rapporté à des coordonnées $y_1, y_2, \ldots, y_h$, l'inégalité (1), jointe aux conditions $y_i \geq 0$, $1 \leq i \leq h$, définit une hyperpyramide H de sommet O et de base l'hyperplan

(2) $$a_1 y_1 + a_2 y_2 + \ldots + a_h y_h = \log x.$$

L'hypervolume V de H est donné par

$$V = \frac{1}{h!} (a_1\, a_2 \ldots a_h)^{-1} (\log x)^h$$

(le vérifier pour $h = 2, 3$), et les systèmes $(y_1, y_2, \ldots, y_h)$ cherchés en (1) correspondent aux points entiers dans H. Le nombre de ces points est très voisin de V (le vérifier pour $h = 2$) : en fait, on peut démontrer l'équivalence

(3) $$\nu_h(x) \sim \frac{1}{h!} (a_1\, a_2 \ldots a_h)^{-1} (\log x)^h \quad \text{quand } x \to \infty.$$

b) Supposons maintenant $\mathbb{P}$ fini, et (comme plus haut), $\mathbb{P} = \mathbb{P}_h$. Comme dans la démonstration n° 3, on a alors $\nu_h(x) = [x]$, donc $\nu_h(x) \sim x$ et (d'après (3))

(4) $$x \sim \frac{1}{h!} (a_1\, a_2 \ldots a_h)^{-1} (\log x)^h \text{ quand } x \to \infty :$$

absurde, puisque le nombre de droite de (4) tend vers l'infini beaucoup plus lentement que le nombre de gauche. $\mathbb{P}$ est donc infini. ■ (Voir note (6)).

Démonstration n° 5 (Euler, vers 1750). - Supposons toujours $\mathbb{P}_h$ et $\mathbb{N}_h$ définis comme dans les démonstrations n° 3 et 4, et considérons le produit

(5) $$E_h = \prod_{i=1}^{h} \frac{1}{1 - \frac{1}{p_i}} .$$

Chaque facteur peut se développer en série géométrique

$$S_i = 1 + \frac{1}{p_i} + \left(\frac{1}{p_i}\right)^2 + \ldots$$

et on a évidemment $E_h = S_1\, S_2 \ldots S_h$. Le théorème de factorisation unique pour

les entiers montre que $S_1\ S_2\ \ldots\ S_h$ peut à son tour être écrit sous forme de série

$$\sum_{n \in \mathbb{N}_h} \frac{1}{n} = \left\{ \begin{array}{l} \text{somme des inverses des entiers} \\ \text{appartenant à } \mathbb{N}_h \end{array} \right.$$

(Le vérifier par exemple pour $h = 2$, $\mathbb{P}_h = \{2, 3\}$; pour $h = 3$, $\mathbb{P}_h = \{2, 3, 5\}$; etc ...) : (5) donne donc

$$(6) \qquad E = \sum_{n \in \mathbb{N}_h} \frac{1}{n} .$$

b) Supposons maintenant (une dernière fois) $\mathbb{P}$ fini , $\mathbb{P} = \mathbb{P}_h$ et $\mathbb{N}_h = \mathbb{N}$. Dans (6), la série de droite est alors la série harmonique (somme des inverses de tous les entiers), de somme infinie. Absurde, puisque le membre de gauche E_h, produit fini de termes finis (d'après (5) et l'hypothèse $\mathbb{P}$ fini) est lui-même fini. $\mathbb{P}$ est donc infini. ■ (Voir note (7)).

3. Théorème de Tchebychev.

On doit à Legendre et Gauss (dans la période 1790-1830, plus de deux mille ans après Euclide) la première étude systématique de l'ordre de grandeur de $\pi(x)$. Dans un premier temps, en utilisant le crible d'Eratosthène, Legendre démontre que

$$\pi(x) < \frac{a\,x}{\log \log x} \quad , \quad a \ : \text{ constante } > 0 \ ,$$

ce qui implique notamment que $\pi(x)/x \to 0$ quand $x \to \infty$. D'une étude expérimentale, il déduit d'autre part que, pour x assez grand, $\pi(x)$ a probablement pour ordre de grandeur $x/(\log x - b)$, b : constante voisine de 1. Simultanément et indépendamment, Gauss compte le nombre N_t de nombres premiers dans des intervalles $[t, t + 1000]$ de 1000 entiers consécutifs, calcule le rapport $N_t/1000$, sorte de "densité locale en voisinage de t" des nombres premiers parmi les nombres entiers, constate que pour t assez grand, $N_t/1000$ est voisin de $1/\log t$, et en déduit que, pour x assez grand, $\pi(x)$ est probablement de l'ordre de grandeur de $\int_2^x \frac{dt}{\log t}$; une intégration par parties montre d'ailleurs que cette fonction de x est équivalente à $x/\log x$ quand $x \to \infty$. Legendre et Gauss arrivent donc essentiellement aux deux conjectures suivantes (la seconde impliquant la première) :

(C1) Pour x assez grand, $\pi(x)$ est de l'ordre de grandeur de $x/\log x$.

(C2) Quand $x \to \infty$, $\pi(x)$ est équivalent à $x/\log x$, ou (ce qui revient au même) à $\int_2^x \frac{dt}{\log t}$.

On doit à Tchebychev (vers 1850) la première démonstration de la conjecture (C1). Pour l'histoire de la conjecture (C2) (c'est-à-dire, puisqu'elle est maintenant démontrée, du thèorème des nombres premiers), voir le § 4.

•

Théorème 2 (Tchebychev). - Il existe deux constantes positives c_1 et c_2 ($0 < c_1 < 1 < c_2$) telles que pour tout x assez grand, on ait l'encadrement

$$(1) \qquad \frac{c_1 x}{\log x} < \pi(x) < \frac{c_2 x}{\log x} .$$

Démonstration. - Elle repose essentiellement sur deux idées :

. l'introduction de deux fonctions $\theta(x)$ et $\psi(x)$, du même style que $\pi(x)$, mais plus maniables (on retrouvera d'ailleurs $\psi(x)$ au § 4) ;

. l'analyse détaillée de l'ordre de grandeur et des propriétés arithmétiques du coefficient binomial $C_{2n}^{n} = (2n)\,!\,/(n!)^2$.

a) Les fonctions $\theta(x)$ et $\psi(x)$. - Ici, x est toujours une variable réelle ≥ 1, et les deux fonctions sont définies par

$$(2) \qquad \theta(x) = \sum_{p \leq x} \log p \; ; \qquad \psi(x) = \sum_{p^m \leq x} \log p \; .$$

$\psi(x)$ diffère de $\theta(x)$ par le fait que le terme $\log p$ apparaît dans la somme autant de fois qu'il existe de m vérifiant $m \geq 1$ et $p^m \leq x$. En utilisant le double crochet pour désigner la partie entière, on a donc aussi

$$(2') \qquad \psi(x) = \sum_{p \leq x} \left[\frac{\log x}{\log p} \right] \log p.$$

Exemple : $\theta(10) = \log 2 + \log 3 + \log 5 + \log 7$, mais
$\psi(10) = 3 \log 2 + 2 \log 3 + \log 5 + \log 7$ (puisque $2, 3, 2^2, 5, 7, 2^3, 3^2 < 10$).

b) Le coefficient binominal C_{2n}^{n}. - Rappelons tout d'abord que $\log(n!) = \sum_{m=1}^{n} \log m \sim \int_1^n \log t \, dt = n \log n - n \sim n \log n$. Comme $C_{2n}^{n} = (2n)\,!\,/\,(n!)^2$, on déduit de là l'équivalence

$$(3) \qquad \log C_{2n}^{n} \sim (2 \log 2)\, n \quad \text{quand } n \to \infty .$$

Mais $C_{2n}^{n} = \dfrac{(n+1)(n+2)\ldots(2n)}{1 \cdot 2 \cdot \ldots \cdot n}$ est un nombre entier, et tout p premier tel que

$n < p \leq 2n$ figure au numérateur, mais non au dénominateur de C_{2n}^n ; C_{2n}^n est donc divisible par (et a fortiori supérieur ou égal à) $\prod_{n<p\leq 2n} p$; en passant aux logarithmes, on a donc

$$(4) \qquad \sum_{n<p\leq 2n} \log p = \theta(2n) - \theta(n) \leq \log C_{2n}^n .$$

Rappelons d'autre part (voir note (8)) que dans la décomposition en facteurs premiers

$$(5a) \qquad n! = \prod_p p^{e(n,p)},$$

les exposants sont donnés comme sommes de parties entières :

$$(5b) \qquad e(n,p) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots = \sum_{p^m \leq n} \left[\frac{n}{p^m}\right]$$

(on suppose $m \geq 1$, comme d'ailleurs en (2)). En passant aux logarithmes, (5a) et (5b) donnent

$$(6) \qquad \log (n!) = \sum_p e(n,p) \log p$$

puis, comme $\log C_{2n}^n = \log \frac{(2n)!}{(n!)^2} = \log(2n!) - 2 \log n!$,

$$(7a) \qquad \log C_{2n}^n = \sum_p \{e(2n,p) - 2\, e(n,p)\} \log p,$$

soit

$$(7b) \qquad \log C_{2n}^n = \sum_p c(n,p) \log p$$

avec $$c(n,p) = \sum_{p^m \leq 2n} \left\{\left[\frac{2n}{p^m}\right] - 2\left[\frac{n}{p^m}\right]\right\}.$$

(On a utilisé (5b) et noté que pour $p^m > 2n$, tous les coefficients sont nuls.) Mais il est facile de voir (exercice) que pour tout nombre réel x, on a $[2x] - 2[x] = 0$ ou 1. En appliquant ceci à $c(n,p)$, on déduit de (7b) l'inégalité

$$(8) \qquad \log C_{2n}^n \leq \sum_{p^m \leq 2n} \log p = \psi(2n).$$

Fin de la démonstration du théorème 2. - Soit a_2 un réel > 1. L'utilisation de (3) et (4), et le remplacement de $2n$ (entier pair) par x (réel ≥ 1 quelconque : voir

note (9)) donnent, pour x assez grand,

$$\theta(x) - \theta(\tfrac{x}{2}) \leq a_2(\log 2)\, x \text{ , puis}$$
$$\theta(\tfrac{x}{2}) - \theta(\tfrac{x}{4}) \leq a_2(\log 2)\, \tfrac{x}{2} \text{ , puis}$$
$$\theta(\tfrac{x}{4}) - \theta(\tfrac{x}{8}) \leq a_2(\log 2)\, \tfrac{x}{4} \text{ , etc ...}$$

Comme $\theta(y) = 0$ pour $y < 2$, le premier nombre de la $n^{\text{ième}}$ inégalité est nul dès que $2^n > x$. Par addition des n premières inégalités, on a donc

$$\theta(x) \leq a_2(\log 2)(x + \frac{x}{2} + \frac{x}{4} + \ldots + \frac{x}{2^n})$$

soit

(9) $\underline{\theta(x) \leq b_2\, x}$, $b_2 = 2a_2\,(\log 2) > 2 \log 2$

(Noter que b_2 est peu différent de $2 \log 2 = 1{,}39\ldots$.)

Soit maintenant a_1 un réel < 1. L'utilisation de (3) et de (8), et le remplacement de $2n$ par x (voir note (9)) donnent, pour x assez grand ,

$$a_1(\log 2)x < \psi(x) ,$$

soit

(10) $\underline{b_1\, x < \psi(x)}$, $b_1 = a_1 \log 2 < \log 2$.

(Noter que b_1 est peu différent de $\log 2 = 0{,}69\ldots$.)

Il reste pour terminer à comparer $\theta(x)$ et $\psi(x)$ à $\pi(x)$. On a d'abord

$$\theta(x) = \sum_{p \leq x} \log p \leq (\log x) \sum_{p \leq x} 1 = (\log x)\, \pi(x) ,$$

du fait que le logarithme est croissant. Comme de plus le logarithme varie très lentement, il est facile, en "serrant" ce raisonnement, de voir qu'en fait

(11) $\underline{\pi(x) \sim \theta(x) / \log x}$ quand $x \to \infty$.

On a par ailleurs

$$\psi(x) = \sum_{p \leq x} \log p + S_2 + S_3 + \ldots$$

avec $S_2 = \sum_{p \leq x^{1/2}} \log p$, $S_3 = \sum_{p \leq x^{1/3}} \log p$, etc ...

soit évidemment

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

La somme de droite est finie et s'arrête au $k^{\text{ième}}$ terme avec $x^{\sqrt{k}} < 2$. En utilisant (9), on déduit facilement de là que

(12) $\psi(x) \sim \theta(x)$ quand $x \to \infty$,

et donc (en utilisant (11)) que

(13) $\pi(x) \sim \psi(x) / \log x$ quand $x \to \infty$.

En divisant alors les deux membres de (9) et (10) par $\log x$, et en remplaçant b_1 et b_2 par c_1 et c_2 telles que $0 < c_1 < b_1 < 1 < b_2 < c_2$, on déduit de (9), (10), (11) et (13) que, pour x assez grand, on a

$$\frac{c_1 x}{\log x} < \pi(x) < \frac{c_2 x}{\log x}.$$

Le théorème 2 est (à peu près) démontré. ■

Remarque. - Euler (voir § 2, note (7)), avait aussi prouvé que la série $\sum_p \frac{1}{p}$ est divergente (ce qui démontre évidemment l'infinité des nombres premiers !) Avec le théorème de Tchebychev, on peut prouver que

$$\sum_{p \le x} \frac{1}{p} \sim \log \log x \quad \text{quand } x \to \infty.$$

Ceci mesure la vitesse de divergence (très faible) de $\sum_p \frac{1}{p}$.

4. Fonction zêta de Riemann et théorème des nombres premiers.

Soient s une variable réelle > 1 et $\mathbb{P}_h$ l'ensemble fini des h premiers nombres premiers. Posons

$$E_h(s) = \prod_{p \in \mathbb{P}_h} \frac{1}{1 - \frac{1}{p^s}}.$$

Une variante du raisonnement fait au § 5, démonstration n° 5, montre que

$$E_h(s) = \sum_{n \in \mathbb{N}_h} \frac{1}{n^s}.$$

Si maintenant on fait tendre h vers l'infini (s restant fixe et > 1), il vient à la limite

(1) $$\prod_p \frac{1}{1 - \frac{1}{p^s}} = \sum_{n=1}^{\infty} \frac{1}{n^s};$$

La série de droite est convergente ($s > 1$) ; le terme de gauche est un produit infini, étendu à tous les nombres premiers : c'est l'analogue multiplicatif d'une somme infinie (c'est-à-dire d'une série), et l'identité (1) montre que ce produit infini est convergent. Cette identité est due à Euler (vers 1750), ainsi d'ailleurs que les formules célèbres

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6} \quad , \quad \sum_{n=1}^{\infty} \frac{1}{n^4} = \frac{\pi^4}{90} \quad , \text{ etc ...}$$

qui donnent la valeur commune des deux membres de (1) pour $s = 2$, 4, etc ... . Signalons en passant que c'est une généralisation de (1) qui a permis à Dirichlet (vers 1840) de démontrer le théorème de la progression arithmétique (voir § 1, question-réponse n° 2, et note (1)).

•

On doit à Riemann (vers 1860) l'idée de considérer s comme une variable complexe, $s = u + it$, et donc les deux membres de (1) comme une même fonction de la variable complexe s ; cette fonction est notée $\zeta(s)$: c'est la fonction zêta de Riemann. Les deux membres de (1) convergent (et $\zeta(s)$ est donc a priori définie) dans le demi-plan $u > 1$. (On conseille au lecteur de tracer sur une feuille de papier l'axe réel Ou, l'axe imagianire Ot, et de suivre sur cette feuille ce qui va être décrit dans la suite.)

Donnons maintenant, dans une présentation modernisée, les principaux résultats de Riemann (voir note (10)) :

a) Résultats démontrés par Riemann :

a0) Pour u (partie réelle de s) > 1, il existe entre $\zeta(s)$ et $\psi(x)$ (voir § 3) la relation

$$(2) \qquad -\frac{\zeta'(s)}{\zeta(s)} = s \int_1^{\infty} \frac{\psi(x)}{x^{s+1}}\, dx \quad ;$$

cette formule s'inverse en

$$(3) \qquad \psi(x) = \frac{1}{2\pi i} \int_{(a)} \left\{ -\frac{\zeta'(s)}{\zeta(s)} \right\} x^s \frac{ds}{s}$$

où a est un nombre réel quelconque > 1, et où (a) désigne la droite verticale

$u = a$, paramétrée par $s = a + it$ ($-\infty < t$ réel $< +\infty$) (voir note (11)). Naturellement, $\zeta'(s)$ désigne la dérivée de $\zeta(s)$.

a1) La fonction $h(s) = \zeta(1) - \frac{1}{s-1}$ (définie seulement a priori pour $u > 1$) se prolonge analytiquement en une fonction holomorphe sur le plan complexe tout entier. Comme $\zeta(1) = \frac{1}{s-1} + h(s)$, on voit que $\zeta(s)$ est en fait une fonction méromorphe sur le plan complexe tout entier, avec un seul pôle en $s = 1$.

a2) Il existe entre $\zeta(s)$ et $\zeta(1-s)$ une relation précise ("équation fonctionnelle" voir note (12)) qui permet de déduire facilement le comportement de $\zeta(s)$ pour $u < 0$ de son comportement pour $u > 1$ (le demi-plan de départ, où $\zeta(s)$ est donnée par les deux membres de (1)). En particulier, on vérifie que

$$\zeta(-2) = \zeta(-4) = \ldots = 0.$$

a3) En dehors de - 2, - 4, ..., la fonction $\zeta(s)$ admet une infinité de zéros dans la bande verticale délimitée par les deux droites $u = 0$ et $u = 1$ ("bande critique"). Les cinquante plus petits zéros "critiques" de $\zeta(s)$ ont tous pour partie réelle $\frac{1}{2}$, et sont donc sur la droite médiane $u = \frac{1}{2}$ de la bande critique ("droite critique").

b) Résultats conjecturés par Riemann :

b1) Posons $\mathrm{li}(x) = \int_0^x \frac{dt}{\log t} = 1{,}04\ldots + \int_2^x \frac{dt}{\log t}$

(voir note (13)). On a alors, entre $\pi(x)$ et $\mathrm{li}(x)$, la relation remarquable :

$$\pi(x) = \mathrm{li}(x) - \frac{1}{2}\,\mathrm{li}(x^{1/2}) - \frac{1}{3}\,\mathrm{li}(x^{1/3}) - \ldots$$

(Cette formule appartient au folklore ; elle "signifie" en tout cas

$$\pi(x) \sim \mathrm{li}(x) \sim \int_2^x \frac{dt}{\log t} \sim \frac{dt}{\log x} \quad \text{quand } x \to \infty,$$

et "démontrerait" donc le théorème des nombres premiers ...).

b2) Les zéros critiques ($0 < u < 1$) de $\zeta(s)$ sont tous sur la droite critique ("hypothèse de Riemann").

Ceci complète évidemment a3), et est d'ailleurs en harmonie avec a2) (la droite critique est invariante par $s \mapsto 1 - s$). Signalons qu'à coups de formules subtiles et d'ordinateurs, on a pu calculer plus de dix millions de zéros critiques de $\zeta(s)$, et que ces zéros sont effectivement tous sur la droite critique ; l'hypothèse de Riemann est donc assez bien confirmée expérimentalement ; en revanche

elle n'est toujours pas démontrée, et ne semble pas près de l'être ...

•

Indiquons maintenant quel est, en gros, le lien entre fonction zêta de Riemann, hypothèse de Riemann et théorème des nombres premiers. (Les puristes sont invités à ne pas lire ce qui va suivre). Soient b et a deux nombres réels tels que $\frac{1}{2} < b < 1 < a$, et soient (b) et (a) les droites verticales $u = b$ et $u = a$ (voir ce §, formule (3) et la suite). Si l'hypothèse de Riemann est vérifiée, ou plus simplement, si la bande verticale $b \leq u \leq a$ ne contient pas de zéros de $\zeta(s)$, la seule singularité (dans cette bande) de $(-\zeta'(s)/\zeta(s))\ (x^s/s)$, est un pôle simple en $s = 1$. (Rappelons en effet que $\zeta(s) = \frac{1}{s-1} + h(1)$ et donc $\zeta'(s) = -\frac{1}{(s-1)^2} + h'(s)$, $h(s)$ et $h'(s)$ holomorphes ; de plus, on montre assez facilement que $\zeta(s)$ n'a pas de zéros dans le demi-plan $u \geq 1$.) Le résidu en ce pôle est $(x^s/s)_{s=1} = x$. Une application formelle du théorème des résidus au bord de la bande $a \leq u \leq b$ (considérée comme un rectangle "infini") donne (l'élément intégré étant $(-\zeta'(s)/\zeta(s))(x^s/s)ds$)

$$\int_{(a)} - \int_{(b)} = 2\pi i . x ,$$

soit, puisque $\psi(x) = \frac{1}{2\pi i} \int_{(a)}$ (formule (3))

$$\psi(x) - x = \frac{1}{2\pi i} \int_{(b)} \underset{déf}{=} I_b \tag{4}$$

Dans l'intégrale I_b, on a $s = b + it$ $(-\infty < t < \infty)$ et donc $|x^s| = x^b$, ce qui suggère une majoration formelle du type

$$|I_b| \leq Ax^b , \quad A : \text{constante positive.} \tag{5}$$

les formules (4) et (5) donnent alors

$$|\psi(x) - x| \leq Ax^b , \qquad b < 1 , \tag{6}$$

donc $\psi(x) \sim x$, puis (voir §3) $\pi(x) \sim x/\log x$, quand $x \to \infty$: on arrive bien au théorème des nombres premiers. ■

•

En fait, cette démonstration est, sinon fausse, du moins très incomplète ;

signalons-en les lacunes :

- Il faut prouver que le demi-plan $u \geq 1$ ne contient pas de zéros de $\zeta(s)$: ce n'est pas trop difficile ;
- L'hypothèse de Riemann n'est en fait pas démontrée ; et on ne connaît même pas de b tels que la bande $b \leq u \leq 1$ ne contienne pas de zéros de $\zeta(s)$. Il faut donc remplacer la bande $b \leq u \leq a$ par un domaine de forme plus compliquée... C'est la partie la plus délicate.
- Il faut justifier l'application de la formule des résidus, et pour cela étudier en détail le comportement de $-\zeta'(s)/\zeta(s)$ à l'infini "verticalement". C'est long et délicat.
- Etc ... (voir par exemple [1] et [4]).

(De toute façon, le résultat final est moins bon que (6)).

L'ensemble de la démonstration représente entre 20 et 40 pages de calcul. La mise au point de cette démonstration (entre 1860 et 1895) a d'ailleurs fait progresser énormément la théorie des fonctions d'une variable complexe (voir note (14)).

Index. -

$\mathbb{N}$: l'ensemble des nombres entiers ;

$m|n$: m divise n ; (m,n) : p. g. c. d. de m et n ;

$\mathbb{P}$: l'ensemble des nombres premiers ;

p^* : le plus petit nombre premier $> p$, lui-même premier ;

$\mathbb{P}(k,a)$: l'ensemble des nombres premiers de la forme $kn + a$;

$\log x$: le logarithme naturel de x, $\int_1^x dt/t$;

$li\,(x)$: le logarithme intégral de x, défini par $\int_0^x dt/\log t$; (la discontinuité en $t = 1$ ne pose aucun problème ; on a

$li(x) = 1{,}04\ldots + \int_2^x dt/\log t \sim x/\log x$ (voir ci-dessous la définition de $\sim$).)

$\pi(x)$: le cardinal de l'ensemble (fini) des nombres premiers $\leq x$.

$\theta(x)$: la somme $\sum_{p\leq x} \log p$;

$\psi(x)$: la somme $\sum_{p\leq x} \sum_{\substack{n=p^m \\ p^m\leq x}} \log n$;

$\zeta(s)$: la fonction zêta de Riemann, définie au départ par

$\sum_{n=1}^{\infty} \frac{1}{n^s}$, $s > 1$;

Conjecture : propriété découverte empiriquement (expérimentalement, par un mélange d'intuition et de raisonnement, etc...), considérée comme "vraie", mais dont on ne possède pas de démonstration complète et rigoureuse. L'hypothèse de Riemann (§ 4) est une conjecture.

Equivalence : dans le contexte de cet exposé, deux fonctions $f(x)$ et $g(x)$, > 0 et définies pour $x \geq 1$, sont dites équivalentes quand $x \to \infty$ si

$$\lim_{x\to\infty} f(x)/g(x) = 1.$$

On écrit alors $f(x) \sim g(x)$ quand $x \to \infty$.

Théorème des nombres premiers : il s'agit de l'équivalence

$$\pi(x) \sim x/\log x \quad \text{quand } x \to \infty$$

(conjecture jusqu'en 1895 (voir § 3) ; théorème depuis cette date (voir § 4).)

•

Notes. -

(1) Ce résultat, obtenu par Dirichlet vers 1840, est connu sous le nom de théorème de la progression arithmétique.

(2) Deux nombres premiers p et q sont dits jumeaux si $q - p = 2$, donc si $q = p^*$ avec $p^* - p = 2$. Si $\pi_2(x)$ désigne la fonction de comptage correspondante, on vérifie expérimentalement que, pour une certaine constante $c > 0$, on a

$$\pi_2(x) \sim cx/(\log x)^2 \quad \text{quand} \quad x \to \infty$$

Ceci laisse supposer que l'ensemble des nombres premiers jumeaux est infini. Toutefois, le principal résultat démontré (compatible d'ailleurs avec l'équivalence ci-dessus) est que la série $\Sigma \frac{1}{p}$, étendue aux seuls p jumeaux, est convergente (V. Brun, 1917 ; naturellement, la théorie a progressé depuis cette date !). Rappelons que $\Sigma \frac{1}{p}$, étendue à tous les nombres premiers, est divergente (Euler).

(3) Soit n un entier arbitrairement grand. Chacun des entiers $n! + 2$, $n! + 3$, ..., $n! + n$ est composé (ils sont divisibles respectivement par 2, 3, ... n). Si alors p = le plus grand nombre premier $\leq n! + 1$, on a $p^* \geq n! + n + 1$, et donc $p^* - p \geq n$, ce qui prouve bien que la différence $p^* - p$ n'est pas bornée.

(4) Rappelons que le livre IX des Eléments d'Euclide contient notamment : la définition des nombres premiers ; le fait que tout $n \geq 2$ possède un facteur premier, et se factorise de façon unique en facteurs premiers ; le fait que l'ensemble des nombres premiers est infini. Il expose également le lien entre nombres premiers et nombres parfaits pairs (voir l'exposé "Autour du petit thèorème de Fermat").

(5) Voir à ce propos l'exposé "Autour du petit théorème de Fermat".

(6) On remarquera l'analogie de structure entre la démonstration n° 3 et la démonstration n° 4. Naturellement, cette démonstration n° 4 est incomplète (calcul de V, estimation $\nu_h(x) \sim$ V, ...), mais son principe est très naturel, et l'approximation

$$\nu_h(x) \sim \frac{1}{h!} (a_1 \; a_2 \; \ldots \; a_h)^{-1} \; (\log x)^h$$

est excellente.

(7) En modifiant légèrement ce calcul (passage aux logarithmes) on peut montrer

également que la série $\sum_{p \in \mathbf{P}} \frac{1}{p}$ est divergente (Euler).

(8) Démonstration de la formule (5b). - Pour p donné et pour tout $k \geq 1$, notons n_k le nombre d'entiers $\leq n$ qui sont divisibles par p^k mais non par p^{k+1}. On a d'une part $e(n, p) = n_1 + 2n_2 + 3n_3 + \ldots$ et d'autre part $n_k = \left[\frac{n}{p^k}\right] - \left[\frac{n}{p^{k+1}}\right]$ (d'où $n_k = 0$ dès que $p^k > n$). La combinaison de ces deux formules donne (5b)

(9) Il faudrait évidemment montrer ici que le remplacement de $2n$ par x n'entraine pas de "bouleversements" dans les calculs. Pour éviter d'alourdir l'exposé, nous nous bornerons à l'admettre.

(10) En fait, Riemann travaillait, non pas avec $-\zeta'(s)/\zeta(s)$ et $\psi(x)$, mais avec $\log \zeta(s)$ et $\pi(x)$. On trouvera dans [2] , pp. 299-305, une traduction anglaise intégrale du mémoire de Riemann.

(11) La formule (2) exprime que $-\zeta'(s)/\zeta(s)$ (fonction de s) est la transformée de Mellin de $\psi(x)$ (fonction de x). Le passage de la formule (2) à la formule (3) est une inversion de Mellin, analogue à l'inversion de Fourier.

(12) Posons par définition

$$Z(s) = \pi^{-s/2}\, \Gamma(s/2)\, \zeta(s)$$

(π = le nombre pi ; Γ = la fonction gamma). L'équation fonctionnelle en question s'écrit alors tout simplement

$$Z(1-s) = Z(s).$$

(13) Il y a une petit problème en $t = 1$, où la fonction $\log t$ s'annule. Malgré cela, $\int_0^2 dt/\log t$ a un sens et vaut 1,04... : d'où la formule.

(14) La démonstration du théorème des nombres premiers décrite ici est la démonsgration "classique". Il en existe deux autres démonstrations, dites "élémentaires" : une par Erdös et Selberg (1949) et une toute récente par Williams (1981).

•

Bibliographie. -

[1] Blanchard, Initiation à la Théorie analytique des nombres premiers, Dunod, 1969.

[2] Edwards, Riemann's Zeta Function, Academic Press, 1974.

[3] Hardy and Wright, The Theory of Numbers, Clarendon Press, 1965.

[4] Ingham, The Distribution of Prime Numbers, Cambridge, 1964.

[5] Lucas, Théorie des Nombres, Blanchard, 1958.

[6] Serre, Cours d'Arithmétique , P. U. F. , 1970.