En guise de présentation ...

En 1982, l'I.R.E.M de Grenoble a mis sur pied un "Séminaire de l'IREM", destiné a priori aux animateurs-formateurs de l'IREM, aux professeurs de l'Enseignement secondaire, aux étudiants de Licence et de Maîtrise, mais également ouvert, naturellement, à tout autre auditeur intéressé. La liste des neuf exposés faits en 1982/83 est donnée à la page suivante. Sur ces neuf exposés, sept ont eu lieu à Grenoble, et deux autres à l'extérieur (exposé n° 6 au stage de Corps, exposé n° 7 au Lycée de Bourgoin).

Provisoirement (au 15 octobre 1983), seuls les exposés n° 1, 2 et 8 ont été rédigés : ce fascicule rassemble les trois textes correspondants. Les exposés n° 4 et 6 seront également rédigés et figureront dans le fascicule 1983/84. Signalons d'ailleurs qu'il est prévu, pour 1983/84 et la suite, de répéter certains de ces exposés (et, bien entendu, d'en faire de nouveaux !) de manière décentralisée, c'est-à-dire dans des villes de l'Académie (Valence, Annecy, Bourgoin, etc ...) autres que Grenoble même.

Séminaire IREM de Grenoble : CALENDRIER 1982/83

Mardi 02 novembre 1982 : *"Introduction à l'analyse non standard : Infiniment petits ; infiniment grands. Application aux notions de limite et continuité".*
par Bruno SOUBEYRAN

Mardi 14 décembre 1982 : *"Le petit théorème de Fermat, chez Fermat, Euler et Lagrange (1640-1770)".*
par Jean-René JOLY

Mardi 11 janvier 1983 : *"Ce merveilleux théorème des accroissements finis".*
par Marc LEGRAND

Mardi 08 février 1983 : *"A propos de la formule d'intégration par parties".*
par Jean-René JOLY

Mardi 08 mars 1983 : *"Maths et Musique".*
par Bernard CORNU

Samedi 12 mars 1983 : *"Aperçu historique sur les systèmes de numération et sur les conceptions des divers types de nombres".*
Stage de CORPS
par Jean-René JOLY

Mardi 29 mars 1983 : *"Développement de l'Algèbre depuis l'Antiquité jusqu'au milieu du XIXème Siècle".*
Stage de Bourgoin
par Jean-René JOLY

Mardi 26 avril 1983 : *"Nombres premiers".*
par Jean-René JOLY

Mardi 31 mai 1983 : *"Analyse des données".*
par R. FREDENUCCI (IMSS)

SEMINAIRE

irem de grenoble

compte rendu

de la réunion du 02 novembre 1982 :

exposé n° 1

INTRODUCTION A L'ANALYSE NON STANDARD : INFINIMENT PETITS ; INFINIMENT GRANDS. APPLICATION AUX NOTIONS DE LIMITE ET CONTINUITE.

par Bruno SOUBEYRAN.

NOMBRES HYPER-REELS.

I - Introduction.

Le but de cet exposé est de donner un sens précis à l'expression :

"x est infiniment près de x_0".

Ceci permettra de remplacer la définition de limite classique, dans laquelle on va à la "pêche aux η" par une définition plus algébrique. (le côté existentiel disparait).

Comme, dans $\mathbb{R}$, le seul élément susceptible de recevoir le label "infinement petit" est 0, on va être amené à construire un corps $\mathbb{R}^*$, contenant $\mathbb{R}$, et contenant aussi des infiniment petits et infiniment grands.

La construction de $\mathbb{R}^*$ va être tout à fait analogue à la construction de $\mathbb{R}$ par les suites de Cauchy de nombres rationnels.

Nous allons rappeler brièvement comment on peut construire les corps classiques : $\mathbb{Z}/p\mathbb{Z}$ (p 1er) ; $\mathbb{Q}$; $\mathbb{R}$ et $\mathbb{C}$.

II - Construction des corps classiques.

1) $\mathbb{Z}/p\mathbb{Z}$

$\mathbb{Z}/p\mathbb{Z}$ = ensemble des entiers modulo p. C'est un anneau (commutatif) pour les lois $\overline{x} + \overline{y} = \overline{x+y}$

$\overline{x} \cdot \overline{y} = \overline{x.y}$

$\overline{x}$ désignant la classe de $x \in \mathbb{Z}$, modulo p ; c'est-à-dire $\overline{x} = x + p\mathbb{Z}$. Si p est premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps (commutatif), c'est-à-dire l'équation $\overline{a}.\overline{x} = \overline{1}$ $(\overline{a} \neq 0)$ a une et une seule solution dans $\mathbb{Z}/p\mathbb{Z}$.

Commentons un peu ce résultat.

L'ensemble $\mathbb{Z}$ des entiers relatifs est un anneau (commutatif, unitaire). Dans $\mathbb{Z}$, l'équation $a \cdot x = 1$ n'a pas toujours de solution.

Puisque l'on ne peut trouver de solution exacte, on va se contenter de solutions approchées a $x = 1 + \varepsilon$, ε parcourant un ensemble $\mathcal{N}$ d'éléments considérés comme négligeables.

Il est clair que plus $\mathcal{N}$ est gros, plus on a de chances de pouvoir résoudre l'équation $a x = 1 + \varepsilon$, ε convenable dans $\mathcal{N}$

On veut bien travailler à ε près, mais comme on est raisonnable on demande :

d'abord que la somme de 2 négligeables soit un négligeable,

puis que le produit d'un négligeable par un entier quelconque soit encore négligeable.

Enfin qu'il y ait quand même des éléments que l'on ne va pas négliger ; c'est-à-dire que $\mathcal{N} \neq \mathbb{Z}$.

Les deux premières conditions traduisent le fait que $\mathcal{N}$ est ce que l'on appelle un idéal, la troisième condition dit que l'idéal est propre, c'est-à-dire $\neq \mathbb{Z}$.

Dans $\mathbb{Z}$, il se trouve que tout idéal $\mathcal{N}$ est de la forme $\mathcal{N} = n\mathbb{Z}$.

Le fait remarquable est que si $\mathcal{N}$ est le plus gros possible, c'est-à-dire est maximal, ce qui se produit si $\mathcal{N} = p\mathbb{Z}$, p 1er, alors, si a n'est pas négligeable, l'équation $a x + 1$ a une solution approchée à ε près, unique à ε près ($\varepsilon\varepsilon\mathcal{N}$). Ce qui se traduit algégriquement par : $\overline{a}\,\overline{x} = \overline{1}$ a une et une seule solution dans $\mathbb{Z}/_{p\mathbb{Z}}$. (c'est-à-dire $\mathbb{Z}/_{p\mathbb{Z}}$ corps).

Le corps $\mathbb{Z}/_{p\mathbb{Z}}$; c'est $\mathbb{Z}$ dans lequel on travaille à $\varepsilon \in p\mathbb{Z} = \mathcal{N}$ (ensemble négligeable maximal) près.

On remarque en passant que tout ensemble négligeable $\mathcal{N}$ ($= n\mathbb{Z}$) est contenu dans un ensemble négligeable maximal $\mathcal{N}' = p\mathbb{Z}$, p 1er divisant n.

2) Les constructions de $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont (peuvent être) tout à fait analogues.

En effet $Q = \mathbb{Z} \times \mathbb{Z}^*/_{\mathcal{N}}$; $\mathcal{N} = \{o\} \times \mathbb{Z}^*$

$\mathbb{Z} \times \mathbb{Z}^*$ étant muni d'une structure d'anneau par :

$(a,b) + (c,d) = (ad + bc, bd)$ ("addition croisée")

$(a,b) \cdot (c,d) = (ac,bd)$

On vérifie facilement que $\mathcal{M}$ est un idéal maximal.

$\mathbb{Q}$ est un corps pour les lois $\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$; $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$ (a/b désignant la classe de (a,b)).

$\mathbb{R} = \mathcal{E}/\mathcal{M}$ avec $\mathcal{E}$ = ensemble des suites de Cauchy de nombres rationnels
et $\mathcal{M}$ = ensemble des suites tendant vers 0

$\mathcal{E}$ est un anneau pour la somme et le produit composantes par composantes.

On vérifie aussi que $\mathcal{M}$ est un ensemble négligeable maximal.

Enfin on a $\mathbb{C} = \mathbb{R}[x]/\mathcal{M}$ avec $\mathcal{M}$: ensemble des multiples de $x^2 + 1$.
$\mathbb{R}[x]$ anneau des polynomes à une indéterminée sur $\mathbb{R}$.

Remarque : les constructions de $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ se font sur le principe suivant : on commence par agrandir par des produits cartésiens, puis on compresse par des quotients.

III - Construction du corps $\mathbb{R}^*$ des nombres hyper-réels.

On considère l'ensemble $\mathcal{S}$ de toutes les suites réelles.

C'est un anneau pour l'addition et le produit composante par composante ($\mathcal{S}$ est commutatif et unitaire).

On considère l'ensemble F des suites nulles à partir d'un certain rang. Alors F vérifie les propriétés des ensembles négligeables c'est-à-dire c'est un idéal, $\neq \mathcal{S}$. Mais F n'est pas le plus gros possible. On admet qu'il est contenu dans un ensemble négligeable (idéal) maximal $\mathcal{M}$.

On note $\mathbb{R}^*$ le corps quotient $\mathcal{S}/\mathcal{M}$: $\mathbb{R}^*$ c'est $\mathcal{S}$ où l'on travail à ε près, $\varepsilon \in \mathcal{M}$

Rappelons donc qu'un élément de $\mathbb{R}^*$ est la classe modulo $\mathcal{U}$ d'une suite réelle. C'est-à-dire : $a \in \mathbb{R}^*$ est de la forme $a = \overline{(x_n)} = (x_n) + \mathcal{U}$

Si $x = (x_n)$ et $y = (y_n) \in \mathcal{S}$, la somme et le produit dans $\mathbb{R}^*$ sont définis par :

$$\overline{x} + \overline{y} = \overline{x+y} = \overline{(x_n + y_n)}$$
$$\overline{x} \cdot \overline{y} = \overline{x.y} = \overline{(x_n \cdot y_n)}$$

Remarque : on montre que $\mathbb{R}^*$ est unique à un isomorphisme près

Propriété : $\mathbb{R}^*$ contient bien $\mathbb{R}$, quand on identifie le réel r avec la classe de la suite constante égale à r.

IV - Structure de $\mathbb{R}^*$.

Il va être commode d'introduire les définitions suivantes :

Définition : soit $X \subset \mathbb{N}$. On note φ_X la suite définie par $\varphi_X(n) = \begin{cases} 1 & n \in X \\ 0 & n \notin X \end{cases}$

Déf. soit $X \subset \mathbb{N}$:
- Si φ_X est négligeable, i.e. $\varphi_X \in \mathcal{U}$, x est dit négligeable
- Si $\varphi_X \notin \mathcal{U}$; x est dit gros

Proposition : soit X et $Y \subset \mathbb{N}$. Alors :

i) X et Y gros $\Rightarrow$ $X \cap Y$ gros
ii) X gros et $Y \supset X$ $\Rightarrow$ Y gros
iii) $X \cup Y$ gros $\Rightarrow$ X ou Y gros
iv) X gros $\Leftrightarrow$ $\mathbb{N} \setminus X$ négligeable
v) $\mathbb{N} \setminus X$ fini $\Rightarrow$ X gros (en particulier $\mathbb{N}$ est gros).

i) Supposons φ_X et $\varphi_Y \notin \mathcal{U}$. En prenant les classes modulo $\mathcal{U}$ on a :
$\overline{\varphi_X} \neq 0$ et $\overline{\varphi_Y} \neq 0$ donc $\overline{\varphi_{X \cap Y}} = \overline{\varphi_X}.\overline{\varphi_Y} \neq 0$ puisque $\mathcal{S}/\mathcal{U} = \mathbb{R}^*$ est un corps.

Donc $\varphi_{X \cap Y} \notin \mathcal{U}$ et $x \cap y$ est gros.

ii) Soit $\varphi_X \in \mathcal{U}$ c'est-à-dire $\overline{\varphi_X} \neq 0$. Si $Y \supset X$ alors $\varphi_X = \varphi_Y . \varphi_X$ d'où
$\overline{\varphi_X} . \overline{\varphi_Y} \neq 0$. Donc $\overline{\varphi_Y} \neq 0$ et $\varphi_Y \notin \mathcal{U}$ c'est-à-dire Y gros.

iii) On a $\varphi_{X\cup Y} = \varphi_X + \varphi_Y - \varphi_{XY}$. Si X et Y sont négligeables alors φ_X et φ_Y sont dans $\mathcal{N}$ c'est-à-dire $\overline{\varphi_X} = \overline{\varphi_Y} = o$ et $\overline{\varphi_{X\cup Y}} = o$ c'est-à-dire $X\cup Y$ négligeable

iv) Soit $\overline{\varphi}_X \neq o$ on a $\overline{\varphi}_X . \varphi_{\mathbb{N}\setminus X} = o$, donc $\overline{\varphi_X} . \overline{\varphi_{\mathbb{N}\setminus X}} = o$ et donc $\overline{\varphi_{\mathbb{N}-X}} = o$ car $\mathbb{R}^*$ est un corps. D'où $\mathbb{N}-X$ négligeable

Réciproquement si $\overline{\varphi_{\mathbb{N}-X}} = o$, comme $\varphi_X + \varphi(\mathbb{N}-X) = 1$ on a $\overline{\varphi_X} = \mathbb{1}$. et ainsi $\varphi_X \notin \mathcal{N}$ c'est-à-dire X gros.

v) Si X est fini alors par définition on a $\varphi_X \in \mathcal{N}$, donc X est négligeable et $\mathbb{N} - X$ est gros.

<u>Proposition</u> : soit $\overline{(x_n)}$ et $\overline{(y_n)} \in \mathbb{R}^*$ alors: $\overline{(x_n)} = \overline{(y_n)} \Longleftrightarrow \{n,\ x_n = y_n\} = X$ gros

on a $\varphi_X(n) = \begin{cases} 1 & n\in X \text{ c'est-à-dire } x_n - y_n = o \\ o & n\notin X \text{ c'est-à-dire } x_n - y_n \neq o \end{cases}$

donc $\varphi_X + (x_n - y_n)n \geq o \neq o\ \forall n \in \mathbb{N}$ donc inversible donc $\notin \mathcal{N}$

donc $\overline{\varphi_X} + \overline{(x_n - y_n)} \neq \overline{o}$ comme $\overline{(x_n - y_n)} = o$, on a $\overline{\varphi_X} \neq o$ c'est-à-dire $\varphi_X \notin \mathcal{N}$ c'est-à-dire : x gros.

<u>Définition d'une relation d'ordre sur $\mathbb{R}^*$</u>. Soit $a = \overline{(x_n)}$ et $b = \overline{(y_n)} \in \mathbb{R}^*$

On définit une relation $\leq$ sur $\mathbb{R}^*$ par : $a \leq b \Longleftrightarrow \{n,\ x_n \leq y_n\}$ est gros c'est bien une définition car si $\overline{(x_n)} = \overline{(x'_n)}$, alors $\{n,\ x_n = x'_n\}$ est gros

<u>Proposition</u> : <u>la relation "$\leq$" est une relation d'ordre total sur $\mathbb{R}^*$, compatible avec l'addition et la multiplication de $\mathbb{R}^*$, qui prolonge l'ordre sur $\mathbb{R}$.</u>

i) $a \leq a$ car $\{n\in\mathbb{N},\ x_n \leq x_n\} = \mathbb{N}$ gros

ii) Soit $a \leq b$ et $b \leq c$ alors : $\{n,\ x_n \leq y_n\}$ et $\{n,\ y_n \leq z_n\}$ sont gros
donc $\{n,\ x_n \leq y_n\} \cap \{n,\ y_n \leq z_n\} = \{n,\ x_n \leq y_n \leq z_n\}$ est gros
donc on a : $a \leq c$.

iii) Soit $a \leq b$ et $b \leq a$ alors $\{n,\ x_n \leq y_n\}$ et $\{n,\ y_n \leq x_n\}$ sont gros, donc $X = \{n,\ x_n = y_n\}$ est gros ; donc $\varphi_X \notin \mathcal{N}$
mais $(x_n - y_n) \times \varphi_X(n) = o$ quelque soit n ; donc la suite $n \mapsto x_n - y_n$ est dans $\mathcal{N}$; donc $\overline{(x_n - y_n)} = \overline{o}$ c'est-à-dire $\overline{(x_n)} = \overline{(y_n)}$ c'est-à-dire $a = b$

iv) Soit $a = \overline{(x_n)}$ et $b = \overline{(y_n)}$ soit $X = \{n,\ x_n \leq y_n\}$; alors X ou $\mathbb{N} \setminus X$ est gros. Si X est gros on a $a \leq b$; si $\mathbb{N} \setminus X$ est gros on a $a > b$.

La compatibilité de "≤" avec "+" et "×" se démontre d'une manière analogue.

Définition : soit $a \in \mathbb{R}^*$. On pose $|a| = a$ si $a \geq 0$; $|a| = -a$ si $a \leq 0$.

Définition : soit $a \in \mathbb{R}^*$. On dit que a est

i) fini, s'il existe $r \in \mathbb{R}$ tel que $|a| \leq r$

ii) infiniment petit si $|a| < r$ pour tout $r > 0$

iii) infiniment grand si $|a| > r$ pour tout $r > 0$

Exemple : soit $x_n = \frac{1}{n+1}$ et $y_n = n$; alors $a = \overline{(x_n)}$ est infiniment petit et $b = \overline{(y_n)}$ est infiniment grand.

Montrons que a est infiniment petit. Soit r réel > 0

$a < r \iff \{n,\ x_n < r\}$ est gros. Or il existe n_0 tel que $\{n,\ x_n < r\} \supset \{n,\ n \geq n_0\}$. Ce dernier ensemble est gros d'où le résultat. On procède d'une manière analogue pour montrer que b est infiniment grand.

Proposition : soit $(x_n)_{n\ 0}$ une suite réelle. Alors :

i) $x_n \underset{n \to +\infty}{\to} 0 \iff \forall\ k \geq 0,\ \{n,\ |x_n| \leq \frac{1}{k}\}$ est cofini (c'est-à-dire est le complémentaire d'un ensemble fini)

ii) $\overline{(x_n)}$ est infiniment petit $\iff \forall k \geq 0,\ \{n,\ |x_n| \leq \frac{1}{k}\}$ est gros.

i) est évident,

ii) est aussi évident car la condition $\{n,\ |x_n| \leq \frac{1}{k}\}$ gros est équivalente au fait que $\overline{(x_n)}$ est inférieur à 1/k

Corollaire : si x_n tend vers 0, alors $\overline{(x_n)}$ est infiniment petit.

En effet tout sous ensemble cofini de $\mathbb{N}$ est gros.

Remarque : 0 est le seul infiniment petit réel. Il n'y a pas d'infiniment grand dans $\mathbb{R}$.

Notation : $x \sim y \iff x - y$ infiniment petit.

Proposition : La somme de deux infiniment petits est un infiniment petit, le produit d'un infiniment petit par un hyper-réel fini est un infiniment petit.

Théorème de structure. Soit $a \in \mathbb{R}^*$, a fini, il existe un réel r unique tel que $a \sim r$ (c'est-à-dire tel que $a = r + \varepsilon$, avec ε infiniment petit).

Ce réel r s'appelle la partie réelle, ou la partie standard ou encore l'ombre de a et se note a^0.

Démonstration : soit donc $a \in \mathbb{R}^*$, a fini

soit $X = \{s \in \mathbb{R},\ s \leq a\}$ X est une partie majorée de $\mathbb{R}$ donc admet une borne supérieure que l'on va noter r. Montrons que a - r est infiniment petit. Supposons pour cela le contraire, c'est-à-dire : il existe $r' > 0$, réel, tel que $|a - r| > r'$

1er cas : $a < r$ alors $r - a > r'$

c'est-à-dire $a < r - r' < r$

mais r étant une borne supérieure, il existe $s \in X$ tel que $a < r - r' < s \leq r$ ce qui est impossible d'après la définition de X.

2ème cas : $a > r$ alors $a - r > r'$

c'est-à-dire $a > r + r' > r$

mais ceci est impossible car on aurait $r + r' \in X$ et $r + r' > \sup X$.

L'unicité provient du fait que 0 est le seul réel infiniment petit.

$(a \sim r \sim r' \Rightarrow r - r' \sim 0 \Rightarrow r = r')$

Exemple : soit $x_n = 0,\underbrace{9\ldots9}_{n \text{ fois}}$ et $a = \overline{(x_n)}$ alors $a^0 = 1$ et $a \neq 1$

En effet $x_n \to 1$ donc $a \sim 1$; $a \neq 1$ car $\{n,\ x_n = 1\} = \emptyset$.

Exercice : Soit a et $b \in \mathbb{R}^*$, finis. Alors

i) si $a \sim b$ on a $a^0 = b^0$

ii) si $a \leq b$ alors $a^0 \leq b^0$

iii) $(a+b)^0 = a^0 + b^0$

iv) $(ab)^0 = a^0 b^0$

i) $a = r + \varepsilon$; $b = r' + \varepsilon'$; si $a \sim b$ alors $a - b = r - r' + \varepsilon - \varepsilon'$ est infiniment petit donc $r - r'$ aussi donc $r = r'$.

ii) $a^0 = \sup. \{s \in \mathbb{R},\ s \leq a\} \leq \sup. \{s \in \mathbb{R},\ s \leq b\} = b^0$.

iii) $a = r + \varepsilon$, $b = r' + \varepsilon'$ $\Rightarrow$ $a + b = r + r' + \varepsilon + \varepsilon'$, $a.b = rr' + r\varepsilon' + \varepsilon\varepsilon'$

On conclu à l'aide de l'unicité de la partie standard.

Remarque : si $\mathbb{R}_f^*$ = ensemble des éléments finis de $\mathbb{R}^*$ alors $\mathbb{R}_f^*$ est un anneau et l'application "0" est un homomorphisme de $\mathbb{R}_f^*$ dans (et sur) $\mathbb{R}$ de noyau l'idéal I des infiniment petits.

On a donc $\mathbb{R}_f^* / I \simeq \mathbb{R}$.

Remarque : si a et b finis $a^0 \leq b^0 \not\Rightarrow a \leq b$.
prendre $b = 0$; $a = \varepsilon$ et $a' = -\varepsilon$

V - **Extensions et prolongements.**

Soit $f : \mathbb{R} \to \mathbb{R}$. On veut caractériser la continuité de f en $x_0 \in \mathbb{R}$ par les valeurs que f prend en des points infiniment près de x_0.

Pour cela il faut avant tout que f puisse être définie (prolongée) en de tels points. C'est ce dont nous allons nous occuper.

Définition : soit $A \subset \mathbb{R}$. On pose : $A^* = \{a = \overline{(x_n)} \in \mathbb{R}^*,\ \{n,\ x_n \in A\}\text{gros}\}$
C'est bien une définition.

Exercice : Montrer que
i) $[a,b]^* = [a,b]_{\mathbb{R}^*} = \{x \in \mathbb{R}^*,\ a \leq x \leq b\}$.
ii) $x \in [a,b]^* \Rightarrow x^0 \in [a,b]$ et x fini.

i) $x = \overline{(x_n)} \in [a,b]^* \Rightarrow \{n,\ a \leq x_n \leq b\}$ gros $\Leftrightarrow a \leq x \leq b$.
ii) si $x \in [a,b]^*$ alors $a \leq x \leq b$ d'où $a = a^0 \leq x^0 \leq b^0 = b$.

Proposition : Soit $A \subset \mathbb{R}$ et $B \subset \mathbb{R}$. On a alors :

i) $(A \cup B)^* = A^* \cup B^*$

ii) $(A \cap B)^* = A^* \cap B^*$,

iii) $(\mathbb{R} \setminus A)^* = \mathbb{R}^* \setminus A^*$

Exercice : soit $A \subset \mathbb{R}$. Si A est fini alors $A^* = A$.

Définition : Soit $f = A \subset \mathbb{R} \to \mathbb{R}$. On définit un prolongement de f, soit $f^* : A^* \to \mathbb{R}^*$, par :

si $a = \overline{(x_n)} \in A^*$ alors $f^*(a) = \overline{(y_n)}$ avec $y_n = \begin{cases} \text{élémt. qcq. si } x_n \notin A \\ f(x_n) \text{ , si } x_n \in A \end{cases}$

Ceci est bien une définition car l'ensemble des $n \in \mathbb{N}$ tels que $x_n \in A$ est gros et l'on sait que : $\overline{(\alpha_n)} = \overline{(\beta_n)}$ si et seulement si $\{n, \alpha_n = \beta_n\}$ est gros.

Remarque : f^* est bien un prolongement de f

Proposition :

i) $(gof)^* = g^* of^*$

ii) $(g+f)^* = g^*+f^*$; $(gf)^* = g^*.f^*$

iii) $f \leq g$ sur $A \Rightarrow f^* \leq g^*$ sur A^*.

Démonstration laissée en exercice.

VI - Limite et Continuité.

Proposition : soit $f : A \subset \mathbb{R} \to \mathbb{R}$, soit $x_0 \in \overline{A}$ et $l \in \mathbb{R}$. Alors :

$l = \lim_{x \to x_0} f(x) \iff$ pour tout $a \in A^*$: $a \sim x_0 \Rightarrow f(a) \sim l$.

sens $\Rightarrow$ $\varepsilon > 0$ donné, on prend $\eta > 0$ tel que $\begin{cases} x \in A \\ |x-x_0| < \eta \end{cases} \Rightarrow |f(x)-l| < \varepsilon$

soit $a = (\alpha_n) \in A^*$ avec $a \sim x_0$. Alors $|a-x_0| < \eta$. Donc on a :

$$\left.\begin{array}{l} \{n,\ |\alpha_n - x_0| < \eta\} \text{ gros} \\ \{n,\ \alpha_n \in A\} \quad \text{gros} \end{array}\right\} \Rightarrow \{n,\ \alpha_n \in A \text{ et } |\alpha_n - x_0| < n\} \text{ gros}$$

donc $\{n,\ |f(\alpha_n) - l| < \varepsilon$. Ceci étant vrai pour tout ε réel > 0, on a bien $f^*(a) \sim l$.

Réciproque : supposons $l \neq \lim_{x \to x_0} f(x)$. Alors il existe $\varepsilon > 0$ tel que pour

tout $\eta > {}_0$, il existe $x \in A$ et $|x-x_0| < \eta$ tel que $|f(x)-l| > \varepsilon$. En prenant $\eta = 1/n$ on met en évidence une suite $x_n \in A$; $x_n \to x_0$ et $|f(x)-l| > \varepsilon$. Posons alors $a = \overline{(x_n)}$; on a $a \in A^*$ et $a \sim x_0$ mais $|f^*(a)-l| > \varepsilon$ car $\{n, |f(x_n)-l| > \varepsilon\} = \mathbb{N}$ est gros ; donc $f^*(a) \not\sim l$.

Corollaire : soit $f = A \subset \mathbb{R} \to \mathbb{R}$. Alors f est continue sur A si et seulement si : pour tout $a \in A^*$ et tout $x \in A$: $a \sim x \Rightarrow f^*(a) \sim f(x)$.

Proposition : soit $f : A \subset \mathbb{R} \to \mathbb{R}$, alors f est uniformément continue sur A si et seulement si pour tout $a \in A^*$ et tout $b \in A^*$ on a :

$$a \sim b \Rightarrow f^*(a) \sim f^*(b)$$

sens $\Rightarrow$ soit ε donné et $\eta > {}_0$ tel que $|x-y| < \eta \Rightarrow |f(x)-f(y)| < \varepsilon$
soit $a = \overline{(\alpha_n)}$ et $b = \overline{(\beta_n)} \in A^*$, avec $a \sim b$; on a $|a-b| < \eta$ et donc :

$\{n, |\alpha_n-\beta_n| < \eta\}$ gros
$\{n, \alpha_n \in A\}$ gros $\Rightarrow \{n, \alpha_n$ et $\beta_n \in A$ et $|\alpha_n-\beta_n| < \eta\}$ gros
$\{n, \beta_n \in A\}$ gros

donc $\{n, |f(\alpha_n)-f(\beta_n)| < \varepsilon\}$ gros, c'est-à-dire $|f^*(a)-f^*(b)| < \varepsilon$

Ceci étant vrai pour tout réel $\varepsilon > o$; on a bien $f^*(a) \sim f^*(b)$.

Réciproque : si f n'est pas uniformément continue sur A alors on peut mettre en évidence deux suites α_n et $\beta_n \in A$ telles que :

$$\alpha_n - \beta_n \to o \quad \text{et} \quad |f(\alpha_n)-f(\beta_n)| \geq r > o.$$

si on pose : $a = \overline{(\alpha_n)}$ et $b = \overline{(\beta_n)}$; on a : $a \in A^*$, $b \in A^*$, $a \sim b$ et $|f^*(a)-f^*(b)| \geq r > o$; c'est-à-dire $f^*(a) \not\sim f^*(b)$.

Corollaire : soit $f : [a,b] \subset \mathbb{R} \to \mathbb{R}$ une application continue. Alors f est uniformément continue.

Soit x et $y \in [a,b]^*$, avec $x \sim y$. Alors x et y sont finis
donc x^0 et y^0 existent et on a : $x^0 = y^0 = r \in [a,b]$
donc puisque f est continue en r on a :
$f^*(x) \sim f(r) \sim f^*(y)$ et f est uniformément continue sur [a,b].

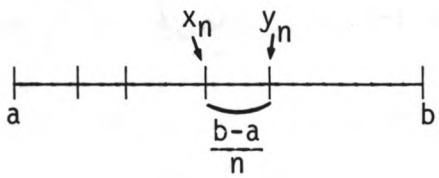
Corollaire : soit $f : [a,b] \to \mathbb{R}$ continue. Si $f(a) \leq o$ et $f(b) \geq o$, il existe $r \in [a,b]$ avec $f(r) = o$.

Soit n un entier quelconque (>o). On partage l'intervalle [a,b] en n parties égales. Il existe alors 2 points consécutifs du partage que l'on note x_n et y_n tels que $f(x_n) \leq o$; $f(y_n) \geq o$ (et $(x_n - y_n) = \frac{b-a}{n}$).

Cette construction étant valable pour tout $n \in \mathbb{N} - \{o\}$, par extension, ω étant un entier infiniment grand, on a deux points x^*_ω et y^*_ω de $[a,b]^*$ tels que $|x^*_\omega - y^*_\omega| = \frac{b-a}{\omega}$ et $f^*(x^*_\omega) \leq o$, $f^*(y^*_\omega) \geq o$.

Si r = partie réelle commune à x^*_ω et y^*_ω on a par continuité de f en r :

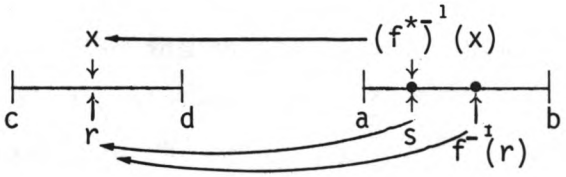
$$\left.\begin{array}{l} f(r) \sim f^*(x^*_\omega) \leq o \\ \sim f^*(y^*_\omega) \geq o \end{array}\right\} \Rightarrow \quad f(r) = o \quad \text{(car f(r) est réel)}$$



Corollaire : soit $f : [a,b] \to [c,d]$ continue et bijective alors f^{-1} est continue.

Supposons le contraire : il existe $x \in [c,d]^*$ et $r \sim x$, et $r \in [c,d]$ ($\Rightarrow r = x^0$), avec $(f^{-1})^*(x) \not\sim f^{-1}(r)$, c'est-à-dire :

$$s = \left((f^{-1})^*(x)\right)^0 \neq f^{-1}(r)$$



Comme f est continue on a $f^*(f^{*-1})(x) = x \sim f(s)$ donc $f(s) = r$ (car f(s) et r sont réels) et f n'est pas injective, contradiction. C.Q.F.D.

VII - Cas particulier des suites.

Proposition : soit $(x_n)_{n\geq 0}$ une suite réelle, et $l \in \mathbb{R}$. On a alors :

i) $l = \lim_{n \to +\infty} x_n \iff$ pour tout $\omega \in \mathbb{R}^*$, infiniment grand, on a $x^*_\omega \sim l$

ii) l est limite d'une sous suite de $(x_n)_{n\geq 0} \iff$ il existe $\omega \in \mathbb{N}^*$, infiniment grand tel que $x^*_\omega \sim l$.

i) Démonstration identique à celle de la limite d'une fonction. D'ailleurs on peut s'y ramener en considérant l'application :

$$\mathbb{N}^* \ni n \to \frac{1}{n} \in A = \{1/p,\ p \in \mathbb{N},\ p > 0\}$$

ii) sens $\Rightarrow$: supposons $x_{n_k} \to l$ qd $k \to +\infty$ alors d'après i) pour ω infiniment grand on a $x^*_{n^*_\omega} \sim l$; mais $n_k \geq k$ pour tout k donc $= n^*_\omega \geq \omega$ infiniment grand. Ainsi il existe $\omega' = n^*_\omega$ infiniment grand tel que $x^*_{\omega'} \sim l$.

Réciproque : supposons qu'aucune sous suite de $(x_n)_{n\geq 0}$ ne tende vers l. Alors il existe un réel $r > 0$ tel que pour tout $n \geq n_0$ on ait : $|x_n - l| \geq r$. Par extension pour tout ω infiniment grand de $\mathbb{N}^*$ on a : $|x^*_\omega - l| \geq r$, c'est-à-dire $x^*_\omega \not\sim l$.

Exercice : Montrer que toute suite réelle croissante majorée a une limite

soit $x_n \leq A$ et x_n croissante - soit ω infiniment grand on a :

$n \leq \omega \Rightarrow x_n = x^*_n \leq x^*_\omega \leq A$. Donc x^*_ω est fini ; on a :

$x^0_n = x_n \leq (x^*_\omega)^0$. Donc pour ω' infiniment grand on a :

$x^*_{\omega'} \leq (x^*_\omega)^0 \Rightarrow (x^*_{\omega'})^0 \leq (x^*_\omega)^0$. Par symétrie on a pour tout ω et ω' infiniment grand : $(x^*_\omega)^0 = (x^*_{\omega'})^0$. Cette valeur commune est la limite de la suite x_n.

Exercice : Toute suite réelle bornée admet une sous suite convergente.

Soit donc $|x_n| \leq A$ pour tout $n \in \mathbb{N}$. On a $|x^*_\omega| \leq A$ pour tout $\omega \in \mathbb{N}^*$ infiniment grand. D'où $x^*_\omega \sim (x^*_\omega)^0 = r$ et il y a une sous suite qui converge vers r.

SEMINAIRE irem de grenoble

compte rendu

de la réunion du 17 décembre 1982 :

exposé n° 2

LE PETIT THEOREME DE FERMAT CHEZ FERMAT EULER ET LAGRANGE (1640 - 1770).

par Jean-René JOLY.

AUTOUR DU PETIT THEOREME DE FERMAT

par Jean-René JOLY

Ce texte est une rédaction remaniée de l'exposé de Novembre 1982. Le § 1 montre, à travers la correspondance entre Fermat et l'"Académie Mersenne",

- d'une part, l'intérêt pris par Fermat, vers 1635-1640, aux nombres parfaits et aux nombres dits "de Mersenne" et "de Fermat" ;
- et d'autre part, la création progressive par Fermat de l'outil mathématique approprié à l'identification des nombres de Mersenne et de Fermat : le "petit" théorème de Fermat.

Le § 2 est consacré à l'histoire des démonstrations du petit théorème de Fermat (chez Fermat lui-même, Leibniz, Euler, Lagrange, Gauss, et enfin à l'époque contemporaine).

Le § 3, d'autre part, montre concrètement comment le petit théorème de Fermat permet de tester si un nombre 2^p-1 est premier (donc de Mersenne), ou si un nombre $2^{2^n}+1$ est premier (donc de Fermat) ; on traite explicitement les exemples classiques de $2^{37}-1$ (non premier, divisible par 223 : Fermat (1640)) ; et de $2^{32}+1$ (non premier, divisible par 641 : Euler (1732)).

Le texte est suivi de notes (références par numéros entre parenthèses) et d'une courte bibliographie (références par numéros entre crochets).

1. HISTOIRE DES NOMBRES PARFAITS ET GENESE DU PETIT THEOREME DE FERMAT.

Les Anciens, et notamment les Pythagoriciens, portaient un certain intérêt aux nombres parfaits ; rappelons qu'un nombre entier est dit parfait s'il est égal à la somme de tous ses diviseurs autres que lui-même ; ainsi,

$$6 = 1 + 2 + 3 \quad ; \quad 28 = 1 + 2 + 4 + 7 + 14 \ ,$$

sont des nombres parfaits. Les Anciens ne connaissaient d'ailleurs probablement que les quatre premiers nombres parfaits : 6 , 28 , 496 , 8 128 . (Voir note (1)).

On retrouve les nombres parfaits chez Euclide, vers 300 av. J.C. Au livre IX des Eléments, Euclide définit et étudie les nombres premiers, et prouve notamment le théorème suivant (de démonstration facile : exercice) :

THEOREME 1. - Si le nombre entier p est premier, et si le nombre $M_p = 2^p - 1$ est lui aussi premier, alors le nombre $P_p = 2^{p-1}(2^p-1) = 2^{p-1}M_p$ est parfait.

(Ainsi, les nombres parfaits 6, 28, 496, 8 128 correspondent respectivement à $p = 2, 3, 5, 7$).

Par ce théorème, Euclide caractérise une certaine famille de nombres parfaits pairs (disons : les nombres parfaits euclidiens), mais cette caractérisation soulève au moins trois problèmes :

a) Existe-t-il une infinité de nombres parfaits euclidiens ? Réponse : probablement non ; voir la suite.

b) Tout nombre parfait pair est-il euclidien ? Réponse : oui (Euler). Voir note (2).

c) Existe-t-il des nombres parfaits impairs ? Réponse : probablement non. Voir note (3).

*

Pendant les deux millénaires suivants (jusqu'au début du XVIIe siècle), l'intérêt porté aux nombres parfaits ne faiblit pas, mais on voit surtout fourmiller des assertions arbitraires ou approximatives, telles que : "le $k^{ième}$ nombre parfait possède k chiffres" - ce qui est complètement faux (voir la suite). De façon générale, l'étude des nombres parfaits est alors plus rhétorique que mathématique, et ne mérite pas d'être détaillée ici. (Le lecteur pourra consulter le livre de Dickson [1], pp. 3-12).

*

C'est vers 1635-1640 que l'étude mathématique des nombres parfaits va se trouver relancée (avec notamment Descartes, Mersenne, Frénicle et Fermat), et qu'on va voir apparaître une tehcnique arithmétique adaptée à cette étude : le "petit" théorème de Fermat.

Le scénario est à peu près le suivant :

• le 15 novembre 1638, Descartes écrit à Mersenne (voir note (4)) pour lui annoncer :

- qu'il sait prouver que tout nombre parfait pair est euclidien ;
- qu'il ne voit pas pourquoi il n'existerait pas de nombre parfait impair (voir cependant note (3)).

• Le 9 janvier 1639, Descartes "récidive" dans une lettre à Frénicle, où il décrit d'hypothétiques nombres parfaits impairs.

• En décembre 1638, Fermat annonce qu'il possède une méthode générale pour résoudre toutes les questions du type "somme des diviseurs", "nombres parfaits", etc.

• En mars 1639, Frénicle, par l'intermédiaire de Mersenne, défie Fermat de trouver un nombre parfait de 20 ou 21 chiffres. (Dans ce contexte, parfait signifie visiblement parfait euclidien ; ceci sera sous-entendu dans toute la suite).

• Dès mai 1639, Fermat répond qu'il n'existe aucun nombre parfait de 20 ou 21 chiffres (et réfute ainsi l'assertion : "le $k^{ième}$ nombre parfait possède k chiffres").

C'est entre juin et octobre 1640, dans la correspondance entre Fermat et Mersenne-Frénicle, que l'on voit apparaître le petit théorème de Fermat, son application à l'étude des nombres parfaits, et aussi son application à l'étude des nombres de Fermat, c'est-à-dire des nombres premiers du type $F_n = 2^{2^n}+1$. Suite du scénario :

• en juin 1640, Fermat affirme essentiellement ceci : si n est premier, alors 2^n-2 est divisible par $2n$, et tout diviseur premier de 2^n-1 est de la forme $2kn+1$.

La première assertion est un cas particulier du (futur) petit théorème de Fermat. En ce qui concerne la seconde, Fermat donne les deux exemples suivants :

$2^{23}-1$ est divisible par $47 = 2.23+1$;
$2^{37}-1$ est divisible par $223 = 6.37+1$;

il en résulte évidemment que P_{23} et P_{37} ne sont pas parfaits.

• En août 1640, dans une lettre à Frénicle, Fermat déclare ceci :

> "Mais voici ce que j'admire le plus : c'est que je suis quasi persuadé que tous les nombres progressifs augmentés de l'unité, desquels les exposants sont des nombres de la progression double, sont nombres premiers, comme
>
> 3 5 17 257 65 537 4 294 967 297
>
> et le suivant de 20 lettres
>
> 18 446 744 073 709 551 617 ; etc.
>
> Je n'en ai pas la démonstration exacte, mais j'ai exclu si grande quantité de diviseurs par démonstrations infaillibles, et j'ai de si grandes lumières, qui établissent ma pensée, que j'aurais peine à me dédire."

En langage moderne, ceci veut dire :

THEOREME 2. - Pour tout entier $n \geq 0$, posons

$F_n = 2^{2^n}+1$.

Alors, tous les F_n sont des nombres premiers.

Les nombres écrits explicitement sont les F_n avec $0 \leq n \leq 6$. En fait, ce théorème 2 est faux dès F_5 ; Euler a en effet prouvé en 1732 que F_5 est divisible par 641 . Voir § 3.2 et note (5).

• Enfin, une lettre à Frénicle datée du 18 octobre 1640, Fermat déclare :

> "Il me semble après cela qu'il m'importe de vous dire le fondement sur lequel j'appuie les démonstrations de tout ce qui concerne les progressions géométriques, qui est tel :
>
> Tout nombre premier mesure infailliblement une des puissances -1 de quelque progression que ce soit, et l'exposant de ladite puissance est sous-multiple du nombre premier donné -1 ; et, après qu'on a trouvé la première puissance qui satisfait à la question, toutes celles dont les exposants sont multiples de l'exposant de la première satisfont tout de même à la question".

En langage moderne, ceci devient, en notant p le nombre premier et a la base de la progression (géométrique) :

THEOREME 3. - Soient p un nombre premier, et a un entier positif non divisible par p . Alors :

1) il existe un plus petit entier $n \geq 1$ tel que p divise a^n-1 ;
2) cet entier n divise $p-1$;
3) tout entier m multiple de n est tel que p divise a^m-1 ;
4) en particulier, p divise $a^{p-1}-1$.

Il s'agit là exactement du petit théorème de Fermat ; Fermat le donne sans démonstration, mais non sans applications ; il traite notamment les exemples suivants, que nous reproduisons en notation moderne :

$\underline{p = 13}$, a = 3 ; p-1 = 12 ; n = 3 : $3^3 - 1 = 26$ est divisible par 13 , et 3 divise 12 .

$\underline{p = 23}$, a = 2 ; p-1 = 22 ; n = 11 : $2^{11} - 1$ est divisible par 23 , et 11 divise 22 .

$\underline{p = 47}$, a = 2 ; p-1 = 46 ; n = 23 : $2^{23} - 1$ est divisible par 47 , et 23 divise 46 .

$\underline{p = 223}$, a = 2 ; p-1 = 222 ; n = 37 : $2^{37} - 1$ est divisible par 223 , et 27 divise 222 .

(Les deux derniers exemples figurent dans la lettre de juin 1640, qui donne le petit théorème de Fermat pour a = 2).

*

La "grande période" de 1638-1640 s'achève pratiquement sur cette lettre de Fermat à Frénicle, qui, si l'on veut, permet de donner à la Théorie des Nombres "moderne" une date de naissance précise : le 18 octobre 1640. Par la suite, Fermat s'intéressera à d'autres questions, et se bornera (en ce qui concerne le sujet étudié dans ce § 1) à affirmer obstinément la primalité des nombres $F_n = 2^{2^n} + 1$, c'est-à-dire le théorème 2 (faux) ci-dessus : lettres à Carcavi, Huygens, Pascal,...

Voici par exemple un extrait d'une lettre à Pascal (29 août 1654) :

"... les puissances carrées de 2 , augmentées de l'unité, sont toujours des nombres premiers :
$2^2 + 1 = 5$, $2^{2^2} + 1 = 17$, $2^{2^3} + 1 = 257$, $2^{2^4} + 1 = 65\,537$,
sont premiers, et ainsi à l'infini. C'est une proposition de la vérité de laquelle je vous réponds. La démonstration en est très malaisée, et je vous avoue que je n'ai pu encore la trouver pleinement ; je ne vous la proposerais pas pour la chercher si j'en étais venu à bout...".

A propos des F_n , voir le § 3.2. Il faut signaler par ailleurs

qu'en 1644, Mersenne affirmera, sans démonstration, que $M_p = 2^p - 1$ est <u>premier</u> (et par conséquent que $P_p = 2^{p-1}(2^p-1)$ est <u>parfait</u>) pour les p (premiers) de la liste suivante :

$$2 \ , \ 3 \ , \ 5 \ , \ 7 \ , \ 13 \ , \ 17 \ , \ 19 \ , \ 31 \ , \ 67 \ , \ 127 \ , \ 257 \ ;$$

et que M_p est <u>composé</u> (et donc P_p <u>non parfait</u>) pour les 44 autres valeurs de p (premier) ≤ 257 . On sait maintenant que, pour les 55 valeurs de p envisagées, Mersenne avait commis 5 erreurs <u>seulement</u> (soit 9 %) : ceci est remarquable, vu la théorie et les moyens de calcul dont on disposait à l'époque. La notation M_p , et la qualification de <u>nombres de Mersenne</u> donnée aux M_p premiers, saluent cet exploit de Mersenne. Voir <u>note</u> (6).

2. DEMONSTRATIONS DU PETIT THEOREME DE FERMAT.

2.1. Fermat (vers 1640). -

Il est peu concevable que Fermat ait possédé une démonstration (au sens moderne) de son "petit" théorème. Il semble qu'au départ, il ait essayé expérimentalement de déterminer les diviseurs premiers p de nombres de la forme $2^m - 1$, puis $a^m - 1$, et qu'il se soit aperçu qu'il était beaucoup commode, pour a fixé, de fixer également p et de faire varier l'exposant m. La démarche devait être la suivante :

① se donner un a et un p fixés (p ne divisant pas a) ;

② calculer itérativement a^m pour $m = 0, 1, 2, \ldots$, en remplaçant chaque résultat plus grand que p par son reste de division par p (autrement dit, en travaillant modulo p avant la lettre : voir note (7)) ;

③ noter dans la "progression" ainsi obtenue les apparitions de 1 et les valeurs des exposants m correspondants ;

④ constater le caractère cyclique (de période $p-1$, ou diviseur de $p-1$) de ces apparitions de 1 .

Exemple (lettre à Frénicle d'Octobre 1640) :

$p = 13$, $a = 3$;

m : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12

a^m : 1, 3, 9, 1, 3, 9, 1, 3, 9, 1, 3, 9, 1

(il s'agit évidemment de a^m réduit modulo p).

On laisse au lecteur le soin de traiter, sur calculatrice de poche, les exemples $a = 2$, $p = 23, 47, 223$.

Dans cette démarche, deux choses sont claires :

• l'intérêt de fixer p , et de travailler "modulo p", ce qui accélère les calculs et surtout montre mieux la structure du phénomène mathématique étudié ;

• le caractère cyclique de la suite $(a^m \bmod p)_{m\geq 0}$, et plus généralement du "groupe" des restes non nuls modulo p .

Il fallut attendre Gauss (vers 1800) pour voir apparaître systématiquement, aux premières pages de ses Disquisitiones Arithmeticae, l'arithmétique modulo p ; et Euler, Lagrange, etc. (1740-1800) pour voir poindre lentement les notions de groupe, groupe cyclique, etc... Voir la suite.

La "démonstration" de Fermat (d'ailleurs parfaitement convaincante en soi, et très conforme aux "canons" mathématiques contemporains) devait donc reposer sur deux axiomes (basés sur l'expérience ; voir note (8)) ;

- l'arithmétique modulo p "existe", et "marche bien" ;
- pout tout a non divisible par p , la suite des a^m réduits modulo p est cyclique, et passe par la valeur 1 pour $m = 0$ et $m = p-1$.

Tout le reste s'en déduit facilement par utilisation de la division euclidienne. Voir d'ailleurs en 2.5 la démonstration "moderne".

*

2.2. Leibniz (vers 1680), Euler (1732-1765). -

Leibniz découvrit les travaux de Fermat (mort en 1665) lors de son séjour à Paris (1672-1676). On lui doit une démonstration du petit théorème de Fermat qui, en notation moderne, peut se décrire ainsi :

- si p est premier, tous les coefficients binomiaux sont divisibles par p , sauf C_p^0 et C_p^p , qui valent 1 ;
- si a et b sont deux entiers, on a donc : $(a+b)^p = a^p + b^p +$ mult. de p ;
- en particulier, avec $b = 1$, et en raisonnant par récurrence sur $a \geq 1$, on trouve successivement $2^p = 2 +$ mult. de p ; $3^p = 3 +$ mult. de p ; ...

et de façon générale, pour $1 \leq a \leq p-1$,
$a^p = a +$ mult. de p , donc $a^{p-1} = 1 +$ mult. de p .

(Ceci prouve en fait les points 1) et 4) du théorème 3, mais on sait que 2) et 3) s'en déduisent immédiatement).

Euler eut lui-même connaissance des travaux arithmétiques de Fermat à Saint-Pétersbourg, vers 1730, par l'intermédiaire de Goldbach. Le premier résultat arithmétique obtenu par Euler est la divisibilité par 641 du nombre de Fermat $F_5 = 2^{32} + 1$, donc la preuve de la fausseté du théorème 2, si cher à Fermat (voir note (5)). On doit à Euler trois démonstrations du petit théorème de Fermat ; les deux premières sont pratiquement équivalentes à celle de Leibniz ; la troisième est plus intéressante, c'est-à-dire plus proche des préoccupations du § 1. En la modernisant un peu, elle se réduit à ceci :

- si p est premier, et si $0 < a < p$, au plus $p-1$ des restes de division par p des termes 1 , a , a^2 , a^3 ,..., sont distincts ; d'où l'existence de ℓ et m , avec $0 \leq \ell < m$, tels que $a^m - a^\ell$ soit divisible par p ; puis l'existence, avec $n = m - \ell > 0$, d'un $n > 0$ tel que $a^n - 1$ soit divisible par p ;
- supposons de plus n minimum ; alors 1 , a , a^2 ,..., a^{n-1} ont des restes de division par p distincts, d'où $n \leq p-1$;
- si $n = p-1$, le petit théorème de Fermat est prouvé ; sinon, il existe b , $0 < b < p$, qui n'est reste de division par p d'aucune puissance de a ; alors les termes b , ba , ba^2 ,..., ba^{n-1} ont des restes de division par p distincts, et aucun de ces restes n'est reste d'une puissance de a . D'où $2n \leq p-1$, et $n \leq \frac{p-1}{2}$;
- si $n = \frac{p-1}{2}$, le petit théorème de Fermat est prouvé ; sinon, il existe c , $0 < c < p$, etc.

*

2.3. Lagrange (vers 1770). -

C'est lors de son séjour à Berlin (1766-1787) que Lagrange eut connaissance (notamment grâce aux travaux d'Euler) du petit théorème de Fermat, et également (grâce aux Meditationes Algebraicae de Waring, publiées en 1770) du théorème de Wilson. Il s'agit de l'énoncé suivant (non démontré avant Lagrange) :

THEOREME 4. - Soit p un nombre premier. Alors, le nombre $(p-1)! + 1$ est divisible par p .

A des détails près, la démonstration par Lagrange des théorèmes de Fermat et de Wilson est la suivante ([4] ; pour condenser l'exposition, nous employons ici la notation congruentielle) : posons

$$f(x) = x(x+1)\dots(x+p-1) \quad ;$$

on a évidemment

$$f(x+1) = (x+1)(x+2)\dots(x+p) = f(x) + pg(x) \quad ,$$

avec $g(x) = (x+1)(x+2)\dots(x+p-1)$. Si $a_0, a_1, \dots, a_p$ sont les coefficients de $f(x)$, on a donc :

$$a_0(x+1)^p + a_1(x+1)^{p-1} + \dots + a_{p-1}(x+1) + a_p$$
$$\equiv a_0x^p + a_1x^{p-1} + \dots + a_{p-1}x + a_p \pmod p \quad ,$$

ce qui signifie que les coefficients des puissances correspondantes de x dans les deux membres sont congrus modulo p . (Noter que $a_0 = 1$, $a_p = 0$, et surtout $a_{p-1} = (p-1)!$, ce qui justifie l'introduction de $f(x)$). On a donc successivement, pour les degrés p , $p-1$, $p-2$,..., 0 :

$$C_p^0 a_0 \equiv a_0 \pmod p$$

$$C_p^1 a_0 + C_{p-1}^0 a_1 \equiv a_1 \pmod p$$

$$C_p^2 a_0 + C_{p-1}^1 a_1 + C_{p-2}^0 a_2 \equiv a_2 \pmod p$$

$$\vdots$$

$$C_p^p a_0 + C_{p-1}^{p-1} a_1 + \dots + C_i^1 a_{p-i} + C_0^0 a_p \equiv a_p \pmod p \quad .$$

Mais on sait que $C_m^0 = 1$ pour $m \geq 0$, que $C_1^1 = 1$, et surtout que les C_p^i sont congrus à $0 \pmod p$, à l'exception de C_p^0 et de C_p^p , qui valent 1 . Ce système de congruences, pris à partir de la deuxième ligne, donne donc successivement

$$a_1 \equiv 0 , \quad a_2 \equiv 0 , \ldots , a_{p-2} \equiv 0 \pmod p$$

et surtout (puisque $a_0 = 1$)

$$1 + a_{p-1} \equiv 0 \pmod p ,$$

c'est-à-dire $(p-1)! + 1 \equiv 0 \pmod p$, ce qui établit le théorème 4 (Wilson). Ce calcul montre également (puisque $a_0 = 1$ et $a_p = 0$) que

$$f(x) \equiv x^p - x \pmod p ,$$

d'où, en simplifiant par x ,

$$(x+1)(x+2)\ldots(x+p-1) \equiv x^{p-1} - 1 \pmod p ,$$

ou encore, en changeant x en $-x$, et en notant que (sauf pour le cas trivial $p = 2$, qui se règle directement) $p-1$ est pair,

$$(x-1)(x-2)\ldots(x-(p-1)) \equiv x^{p-1} - 1 \pmod p .$$

Le premier membre est nul $(\text{mod } p)$ pour $a = 1, 2, \ldots, p-1$: d'où $a^{p-1} \equiv 1 \pmod p$, ce qui établit en définitive le théorème 3 (Fermat). ■

L'intérêt de cette démonstration est évidemment qu'elle donne la factorisation de $x^{p-1} - 1 \pmod p$, c'est-à-dire dans $\mathbb{F}_p[x]$ (avec $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$) : les théorèmes de Fermat et de Wilson ne sont que des corollaires de ce "théorème de Lagrange". Cette démonstration montre également que Lagrange était parfaitement à l'aise (en 1771) avec le calcul algébrique dans l'anneau $\mathbb{F}_p[x]$: on a le sentiment, en lisant le "mémoire" de Lagrange [4], de voir naître ce qu'on appelait naguère l'"Algèbre moderne".

*

2.4. Gauss (vers 1800). -

On doit à Gauss [5] l'introduction de la notation congruentielle (voir note (7)). Comme on l'a vu, cette notation permet d'écrire le petit théorème de Fermat sous la forme suivante : si $a \not\equiv 0 \pmod p$, alors $a^{p-1} \equiv 1 \pmod p$. Voici la démonstration annoncée :

• tout d'abord, l'application $x \mapsto xa$ (où $x, a, xa, \ldots$ sont conçus comme restes modulo p) est bijective : car $xa \equiv ya \pmod p$ implique que p divise $xa - ya = (x-y)a$, mais p est premier avec a , donc (lemme de Gauss !) p divise $x-y$, et donc $x \equiv y \pmod p$: d'où l'injectivité. La bijectivité résulte alors du fait que l'ensemble des restes modulo p est fini (à p éléments).

• Il résulte de cette bijectivité que les deux suites :

$1, 2, \ldots, p-1$, et $a, 2a, \ldots, (p-1)a$,

(dont les termes sont conçus comme restes modulo p), sont identiques, à l'ordre des termes près ; on a donc par multiplication

$$1.2.\cdots.(p-1) \equiv (a)(2a)\ldots((p-1)a) \pmod p$$

d'où $(p-1)! \equiv a^{p-1}(p-1)! \pmod p$, et finalement, après simplification

$$a^{p-1} \equiv 1 \pmod p \ . \blacksquare$$

(Assez malicieusement, cette démonstration fait apparaître $(p-1)! \pmod p$, mais ne permet pas d'obtenir le théorème de Wilson ; voir d'autre part note (7a)).

*

2.5. Démonstration des théorèmes 3 et 4 dans le style "moderne". -

Cette démonstration utilise essentiellement le langage "groupes, anneaux, corps" (mais n'ajoute en fait rien à la démonstration de Lagrange).

• Comme p est premier, l'anneau $F = \mathbb{Z}/p\mathbb{Z}$ des classes d'entiers modulo p est un corps (ceci résulte du lemme de Gauss) et l'ensemble G (représenté par $1, 2, \ldots, p-1$) des classes d'entiers non nulles modulo p est un groupe commutatif d'ordre $p-1$;

• si $\bar{a}$ est la classe de $a \pmod p$, $\bar{a}$ est dans G ; et si n est l'ordre de $\bar{a}$, on a :

$$\bar{a}^n = 1 \ , \quad \text{donc} \quad a^n \equiv 1 \pmod p \ ;$$

ceci prouve 1) (la minimalité de n résulte de la définition de l'ordre d'un élément dans un groupe) ;

• de plus, l'ordre n de $\bar{a} \in G$ divise l'ordre $p-1$ du groupe G tout entier ("théorème de Lagrange"!) : donc n divise $p-1$, ce qui prouve 2) ;

• les assertions 3) et 4) du théorème 3 sont alors évidentes ;

• le théorème 3 étant démontré, passons au théorème 4 ; le théorème 3 prouve que dans l'anneau de polynômes $F(X)$, le polynôme $X^{p-1} - 1$ a pour racines $\bar{1}, \bar{2}, \ldots, \overline{p-1}$; d'où immédiatement

$$X^{p-1} - \bar{1} = (X-\bar{1})(X-\bar{2})\ldots(X-\overline{p-1}) \ ;$$

en égalant les termes constants, on arrive en particulier à :

$$-1 \equiv (-1)^{p-1}(p-1)! \pmod p \ ;$$

mais (en écartant encore le cas trivial $p=2$), on voit que $p-1$ est pair, que $(-1)^{p-1} \equiv 1 \pmod p$, et donc finalement que :

$$(p-1)! \equiv -1 \pmod p \ ;$$

le théorème 4 est également démontré. ■

3. APPLICATIONS DU PETIT THEOREME DE FERMAT AUX NOMBRES PARFAITS, AUX NOMBRES DE MERSENNE ET AUX NOMBRES DE FERMAT.

3.1. Nombres parfaits et nombres de Mersenne. -

Compte tenu du théorème d'Euclide (th. 1), la recherche des nombres parfaits euclidiens P_p se ramène à celle des nombres de Mersenne M_p, c'est-à-dire à celle des p premiers tels que $M_p = 2^p - 1$ soit lui-même premier. L'application à cette recherche du petit théorème de Fermat tient dans les deux lemmes suivants, implicites chez Fermat (voir § 1) :

LEMME 1. - Soit q le plus petit diviseur premier de M_p. Alors, pour que M_p soit un nombre de Mersenne, et que P_p soit donc un nombre parfait, il faut et il suffit que $q = M_p = 2^p - 1$.

(Evident !)■

LEMME 2. - Tout diviseur premier q de $M_p = 2^p - 1$ est de la forme $1 + 2kp$, k entier $\equiv 1$. (On suppose $p \neq 2$).

Démonstration. - (Attention ! Dans cette démonstration, comme dans celle du lemme 3, on va travailler modulo p : le nombre premier fixé n'est pas p, mais q ; et p joue le rôle d'un exposant). Le petit théorème de Fermat (th. 3), démontré "rigoureusement" en fin de § 2, montre qu'il existe un plus petit n positif tel que $2^n \equiv 1 \pmod q$; et que n est un diviseur de $q-1$; il montre également, puisque $2^p \equiv 1 \pmod q$, que n est un diviseur de p, et donc (comme évidemment $n > 1$ et que p est premier) que $n = p$. Finalement, p divise $q-1$. Par ailleurs, $2^p - 1$ est impair, donc $q-1$ est impair, donc 2 divise $q-1$. Comme, pour $p \neq 2$, 2 est premier avec p, on voit au total que $q-1$ est divisible par $2p$; finalement, $q - 1 = 2kp$, et $q = 1 + 2kp$. ■

(Pour $p = 2$, on a $M_p = 2^2 - 1 = 3$ et $1 + 2p = 5$; le lemme 2 ne s'applique pas, mais c'est évidemment sans importance !).

Application à P_{37} et M_{37} . - (On laisse au lecteur le plaisir d'allumer sa calculatrice de poche et d'examiner par exemple les valeurs $p = 11, 13, 17, \ldots$). D'après le lemme 2, les diviseurs premiers de M_{37} sont tous de la forme $1 + 74k$, et appartiennent donc à la liste

$$149 \ , \ 223 \ , \ 593 \ , \ldots$$

Pour chaque terme (disons ℓ) de cette liste, il faut alors examiner $2^{37} \pmod{\ell}$. Si ce reste est différent de 1 , ℓ ne divise pas M_{37} ; si ce reste égale 1 , ℓ divise M_{37} ; etc. Pratiquement :

$\ell = 149$: les congruences étant mod 149 , on a

$2^7 \equiv 128$, et $2^{10} \equiv 130$, donc

$2^{37} \equiv 2^7 . 2^{30} \equiv 128 . (130)^3 \equiv 105 \not\equiv 1$;

$\ell = 149$ ne divise donc pas M_{37} .

$\ell = 223$: les congruences étant maintenant modulo 223 , on a

$2^7 \equiv 128$, et $2^{10} \equiv 132$, donc

$2^{37} \equiv 128 . (132)^3 \equiv 1$;

$\ell = 223$ divise donc M_{37} , et comme 223 est visiblement plus petit que M_{37} , on voit (lemme 1) que M_{37} n'est pas premier. Ainsi, M_{37} n'est pas un nombre de Mersenne, et P_{37} n'est pas un nombre parfait.

(Il est bien entendu inutile désormais de tester $\ell = 593, \ldots$, même si l'on cherche à décomposer M_{37} en facteurs premiers ; en effet, dans ce genre de situation, l'expérience, et de vagues considérations statistiques, montrent que le deuxième facteur premier de M_p est très grand).

*

3.2. Nombres de Fermat. -

On s'intéresse ici à la recherche des nombres de Fermat, c'est-à-dire à la recherche des entiers $n \geq 0$ tel que $F_n = 2^{2^n}+1$ soit un nombre premier. L'application à cette recherche du petit théorème de Fermat tient dans le lemme 1 (3.1) et dans le lemme 3 ci-dessous, réplique du lemme 2 (3.1).

LEMME 3. - Tout diviseur premier q de F_n est de la forme $1 + 2^{2^{n+1}} k$, k entier ≥ 1 .

Démonstration. - Tout d'abord, $q \neq 2$, puisque F_n est impair. De plus, le petit théorème de Fermat prouve qu'il existe un plus petit entier positif (notons-le ici N) tel que $2^N \equiv 1 \pmod q$; et que N divise $q-1$. Il montre également (puisque $2^{2^n} \equiv -1 \pmod q$ et que par suite $2^{2^{n+1}} \equiv 1 \pmod q$) que N divise $2^{2^{n+1}}$; N est donc de la forme 2^{2^i} , $0 \leq i \leq n+1$; mais la possibilité que $i \leq n$ est exclue, car on aurait alors $2^{2^n} \equiv 1 \pmod q$, donc $F_n - 1 \equiv 1 \pmod q$, ou $F_n \equiv 2 \pmod q$: absurde, puisque q est impair et divise F_n . On a donc en fait $N = 2^{2^{n+1}}$; $2^{2^{n+1}}$ divise $q-1$, $q-1$ est donc de la forme $2^{2^{n+1}} k$, $k \geq 1$, et finalement

$$q = 1 + 2^{2^{n+1}} k \ . \blacksquare$$

Application à $F_5 = 2^{2^5}+1 = 2^{32}+1$. - D'après le lemme 3, les diviseurs premiers de F_5 sont tous de la forme $1 + 64k$, et appartiennent donc à la liste

193 , 257 , 449 , 577 , 641 ,...

Notons tout de suite que $257 = F_3$ ne divise pas F_5 : en fait (exercice facile), quels que soient m et n , $0 \leq m < n$, F_m et F_n sont premiers entre eux. Pour chaque terme (disons ℓ) de la nouvelle liste (privée de 257)

193 , 449 , 577 , 641 ,...

il faut alors examiner $2^{32} \pmod{\ell}$; si ce reste est différent de -1 , ℓ ne divise pas F_5 ; sinon, ℓ divise F_5 , etc. En fait :

$\ell = 193, \ldots$: on laisse au lecteur le soin de faire le calcul comme au § 3.1. On constate que les $\ell < 641$ ne divisent pas F_5 .

$\ell = 641$: les congruences étant prises modulo 641 , on a (par exemple)

$$2^2 \equiv 4 \text{ , et } 2^{10} \equiv 1024 \equiv 383 \text{ , donc}$$
$$2^{32} \equiv 4.(383)^3 \equiv 640 \equiv -1 \text{ ;}$$

$\ell = 641$ divise donc F_5 , et comme 641 est visiblement plus petit que F_5 , on voit (lemme 1) que F_5 n'est pas premier (et n'est pas un nombre de Fermat).

*

3.3. En guise de conclusion. -

On a vu au § 1 que Fermat avait découvert le facteur premier 223 de $M_{37} = 2^{37} - 1$; le § 3.1 montre quelle était sa méthode. Le § 3.2 montre par ailleurs que les calculs nécessaires pour trouver le facteur premier 641 de $F_5 = 2^{32} + 1$ ne sont pas beaucoup plus longs. Il est donc surprenant que Fermat n'ait jamais découvert ce facteur premier, et ait persisté toute sa vie durant (voir § 1) à croire à la primalité de tous les F_n .

En revanche, il n'est pas surprenant qu'il ait fallu près d'un siècle (disons : de 1645 à 1732) pour que ce facteur premier soit découvert : les travaux arithmétiques de Fermat étaient tombés (avant même sa mort en 1665) dans le manque d'intérêt puis l'oubli les plus profonds, et Euler est en fait le premier grand mathématicien à s'y être passionnément et efficacement intéressé.

NOTES

(1) L'intérêt porté par les Anciens aux nombres parfaits était purement purement mystique. Voir à ce sujet le livre de Dickson [1], pp. 2-5.

(2) La démonstration figure dans les papiers posthumes d'Euler ; elle est courte et élémentaire ; on en trouvera un résumé dans [1], p. 19.

(3) En fait, on sait essentiellement à l'heure actuelle qu'il n'existe pas de nombre parfait impair $\leq 10^{50}$: d'où la vague conjecture qu'il n'en existe pas du tout !

(4) La place nous manque totalement ici pour décrire l'importance du Père Marin Mersenne (1588-1648) dans le développement scientifique en France au XVIIe siècle. Mersenne réunissait autour de lui une sorte d' "Académie", et correspondait de façon permanente avec de nombreux savants français (Descartes, Fermat (à partir de 1636),...) et européens ; ainsi se trouvait réalisée une communication rapide des idées, des découvertes, et aussi des défis (du genre : trouver un nombre parfait de 20 ou 21 chiffres : défi de Frénicle à Fermat...). A propos de Fermat lui-même (1601-1665), voir par exemple [7].

(5) Euler (1707-1783) est le premier mathématicien a avoir tiré de l'oubli les travaux de Fermat, et à avoir (en donnant des démonstrations de la plupart des résultats de Théorie des Nombres simplement énoncés par Fermat) créé effectivement cette branche des Mathématiques, aussitôt suivi par Lagrange (1736-1813), Gauss (1777-1855), etc. La divisibilité de $F_5 = 2^{32}+1$ par 641 date de 1732, et est le premier "résultat" arithmétique d'Euler. Voir [3].

(6) Les nombres premiers $p \leq 5\,000$ tels que M_p soit premier (donc de Mersenne) sont en fait :

2 , 3 , 5 , 7 , 13 , 17 , 19 , 31 , 61 , 89 ,
107 , 127 , 521 , 607 , 1279 , 2203 , 2281 ,
3217 , 4253 , 4423 ;

on sait en outre qu'entre 5 000 et 50 000 , les nombres premiers p suivants ont la même propriété :

9689 , 9941 , 11213 , 19937 , 21701 , 23209 , 44497 ;

mais cette deuxième liste n'est probablement pas complète. On conjecture que l'ensemble des nombres de Mersenne est fini.

(7) La notation congruentielle est due à Gauss ([5], 1799) ; rappelons que $a \equiv b \pmod{m}$ signifie que $a-b$ est divisible par le "module" m (≥ 1) .

(7a) Cette démonstration se lit entre les lignes dans [5], mais j'en ignore la référence exacte. Disons donc prudemment qu'elle est "à la manière de Gauss". A propos de Gauss et de Fermat-Wilson, voir [1], p. 75.

(8) A vrai dire, Fermat savait certainement en un certain sens "démontrer" le premier "axiome" ; en fait, la question n'est pas là ; il faut simplement se rappeler que le symbolisme algébrique utilisé par Fermat (l'algèbre de Viète) était insuffisant pour <u>écrire</u> telle ou telle démonstration (et à vrai dire Fermat a toujours montré une certaine maladresse à "rédiger") ; mais ceci n'empêchait nullement Fermat d'avoir une conception parfaitement claire de ce que serait cette démonstration. Feuilleter [2].

BIBLIOGRAPHIE

[1] DICKSON, Theory of Numbers, Vol. I (Chelsea).

[2] FERMAT, Oeuvres complètes, Vol. II (Gauthier-Villars), spécialement pp. 205-213.

[3] EULER, Oeuvres complètes, spécialement les premiers volumes.

[4] LAGRANGE, "Démonstration d'un théorème nouveau concernant les nombres premiers", Oeuvres complètes, Vol. III.

[5] GAUSS, Recherches Arithmétiques, traduction française par A.C.M. Poullet-Delisle (Blanchard).

[6] HARDY and WRIGHT, The Theory of Numbers (Oxford).

[7] ITARD, Pierre Fermat (Birkhaüser).

(novembre 83)

SEMINAIRE

irem de grenoble

compte rendu

de la réunion du 26 avril 1983 :

exposé n° 8

NOMBRES PREMIERS

par Jean-René JOLY

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.