# Nombres p-adiques

Université de Limoges

IREM Institut de Recherche sur l'Enseignement des Mathématiques

- Les brenoms : une activité pédagogique sur les nombres

- Dans le désordre
  - A quoi ça sert ?
  - Histoire : les débuts
  - Construction des nombres p-adiques
  - Quelques curiosités, quelques « beaux » résultats
  - Conclusion

Stage « arithmétique », Limoges le 12 février 2009

Université de Limoges

IREM Institut de Recherche sur l'Enseignement des Mathématiques

# Brenoms* ou nombres décadiques

Lorsque l'on passe des nombres entiers aux nombres réels on s'autorise à utiliser des nombres ayant une infinité de chiffres après la virgule.

Que se passerait-il si on essayait de calculer avec une infinité de chiffres avant la virgule ?

---

* Nombres en verlan

# Brenoms

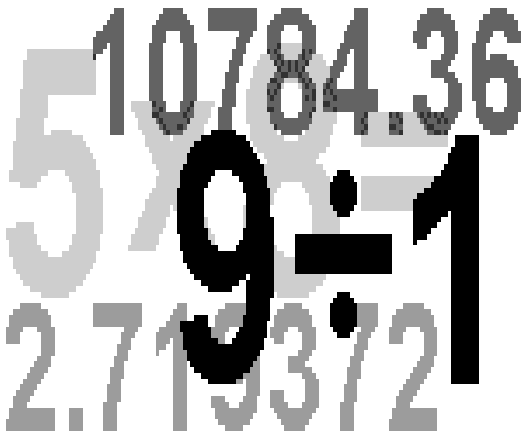
- Un nombre décadique ou brenom est un « nombre » ayant une infinité de chiffres (0,1,…,9) à gauche.

- Exemples

...010101

...12121212

...999917531459



# Opérations sur les décadiques

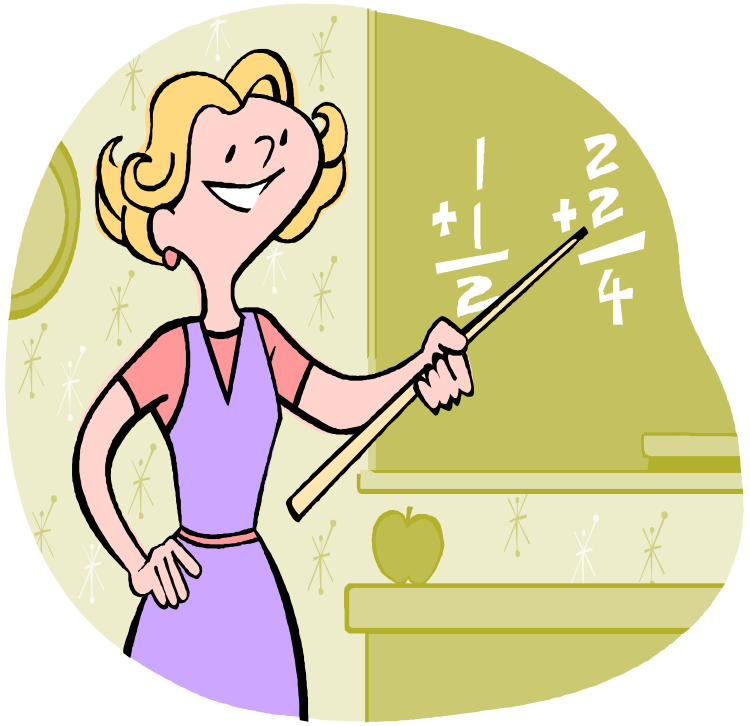
- Addition

…3456781

…9564210

---

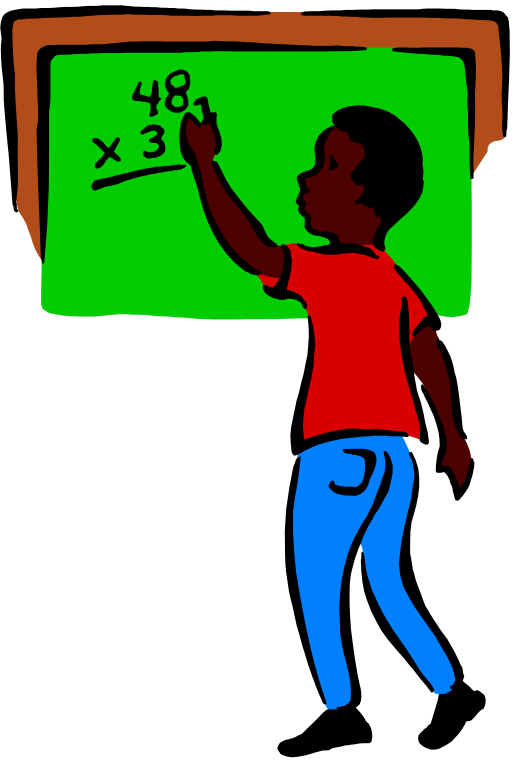
…3020991




Université de Limoges

IREM Institut de Recherche sur l'Enseignement des Mathématiques

# Multiplication (avec retenue)




...123

...456

...738

...615.

...492..

.....088

Université de Limoges

IREM Institut de Recherche sur l'Enseignement des Mathématiques

Université de Limoges

IREM Institut de Recherche sur l'Enseignement des Mathématiques

# Soustraction

$$\begin{array}{r} \ldots 00001 \\ +\ \ldots 99999 \\ \hline \ldots 00000 \end{array}$$

**Autrement dit : -1=…999**

**Autre exemple : -3=…9997**

**On n'a plus besoin du signe « - » devant les nombres !**
**Remarque : … 0000123 =123**

Université de Limoges

IREM Institut de Recherche sur l'Enseignement des Mathématiques

# Exercice

Soit $x=\ldots a_n a_{n-1} \ldots a_k \ldots 000$. Les $a_i$ sont des chiffres et k est le plus petit entier tel que $a_k$ non nul.

Vérifier que : $-x = \ldots(9-a_n)(9-a_{n-1})\ldots(10-a_k)$

Exemple 1
x= …45673000
-x= …54327000

Exemple 2
x= … 15603
-x= …84397

# La division

Université de Limoges

IREM Institut de Recherche sur l'Enseignement des Mathématiques

On a :

$$\begin{array}{r} \ldots6666667 \\ \times \qquad 3 \\ \hline 000000001 \end{array}$$

Ou encore :

$1/3 = \ldots6666667$

Peut-on inverser 2 ?

$$\begin{array}{r} \ldots00000002 \\ \times \quad ???????? \\ \hline 0000001 \end{array}$$

# Structure

Soit **B** l'ensemble des brenoms*.

Alors **B** est muni d'une structure d'anneau commutatif unitaire non intègre contenant une copie de **Z** (les relatifs). Le groupe des éléments inversibles de **B** est formé de tous les brenoms dont le premier chiffre est premier à 10 (*i.e.*, 1,3,7,9).

* On suppose que cela a un sens !

# Exercices

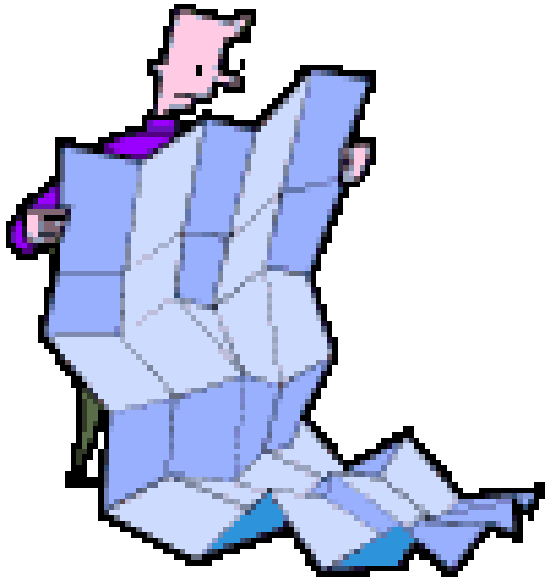
- Montrer que l'equation
$$X^2-X=0$$
possède 4 solutions dans **B.**

- Résoudre dans **B** : $X^2-1=0$.

- Et si on changeait de base ?

Pour en savoir plus et pour des activités scolaires voir les comptes rendus de MATh en Jeans :
http://www.mjc-andre.org/pages/amej/accueil.htm

# Le reste de l'exposé



- Donner une sens à ces nombres

  et construction des p-adiques.

- Les débuts de l'histoire des nombres p-adiques.

- A quoi ça sert ?

# A quoi ça sert ?

Élève de l'ENS, Charles PISOT (1910-1984)

1er au concours de l'agrégation de mathématiques (1932). Maître de conférences puis professeur à Bordeaux, il obtient un poste à la faculté des sciences de Paris (1955) et à l'école polytechnique. On lui doit des travaux remarquables en théorie des nombres principalement sur les nombres dits de Pisot-Vijayaraghavan.

# Entretien de J. Nimier avec C. Pisot *

« Quand vous prenez les nombres p-adiques, alors là, pour l'instant on ne voit encore aucune motivation due à la réalité ; mais d'ici quelque temps on trouvera dans la réalité des choses pour lesquelles les nombres p-adiques formeront un bon modèle. On ne l'a pas encore jusqu'à présent, cela reste encore entièrement dans l'esprit ; or, il y a des tas de théories constituées sur les nombres p-adiques, il y a des fonctions de variables p-adiques, il y a des bouquins, … »

« Il faut s'abstraire de la réalité si on veut faire des progrès »

*En 1974. Voir les publications de l'IREM de Lyon

# Environ trente ans après ...

- Topological Geometrodynamics (TGD) : une théorie physique en essor depuis les années 80

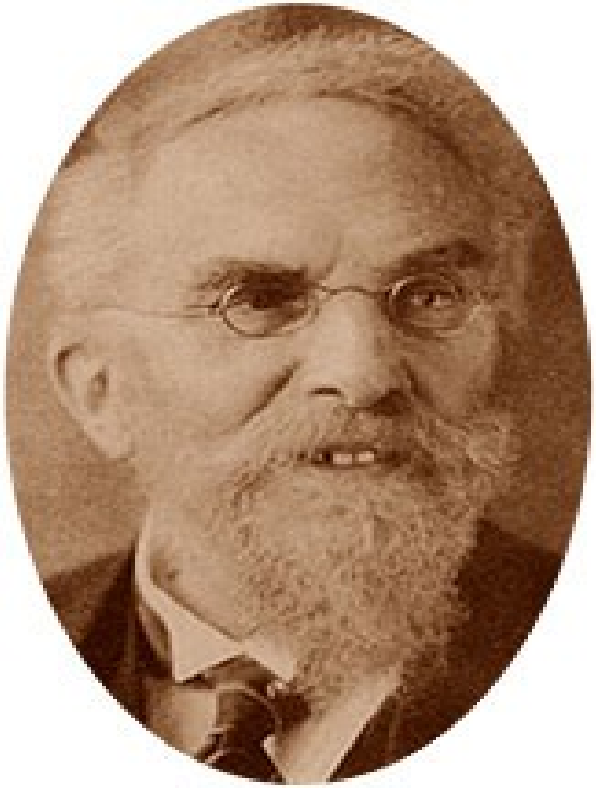
  http://www.physics.helsinki.fi

- Cryptographie
- Codes correcteurs d'erreurs

A. R. Calderbank , N. J. A. Sloane, Modular and p-adic cyclic codes, Designs, Codes and Cryptography, v.6 n.1, p.21-35, July 1995

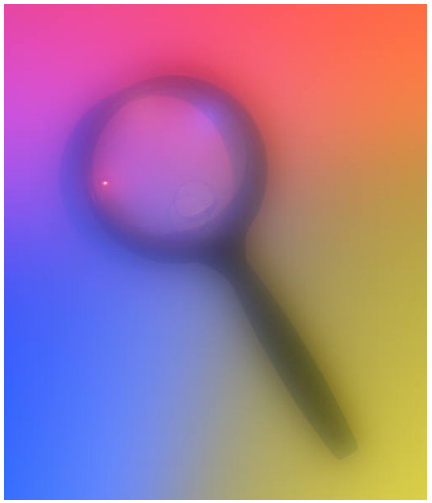
# Nombres p-adiques : le PAPA

Kurt Hensel ou le mathématicien par qui les p-adiques arrivent (en 1897) !



Université de Limoges
IREM Institut de Recherche sur l'Enseignement des Mathématiques

# Zoom sur le papa



- Kurt HENSEL est né le 29 Décembre 1861 à Königsberg en Prusse orientale (aujourd'hui : Kaliningrad, Russie) un des hauts lieux, avec Göttingen, des mathématiques allemandes, élève de KRONECKER, HENSEL enseignera à Berlin et à Marburg. Il prit la direction du célèbre journal de CRELLE de mathématiques pures et appliquées en 1901.
- Kurt HENSEL est décédé le 01 juin 1941 à Marburg (Allemagne).

**Kurt Hensel 1884 Berlin**

Kronecker 1845 Berlin

G.L. Dirichlet 1827 Berlin

J. FourierENS Paris (1822 ?)

J. Lagrange, ENS (1787 ?)

L. Euler Basel 1726

J. Bernouilli Basel 1690, 1694

S.D. Poisson Polytechnique 1800

P-S. Laplace Paris 1799 ?

J. d'Alembert

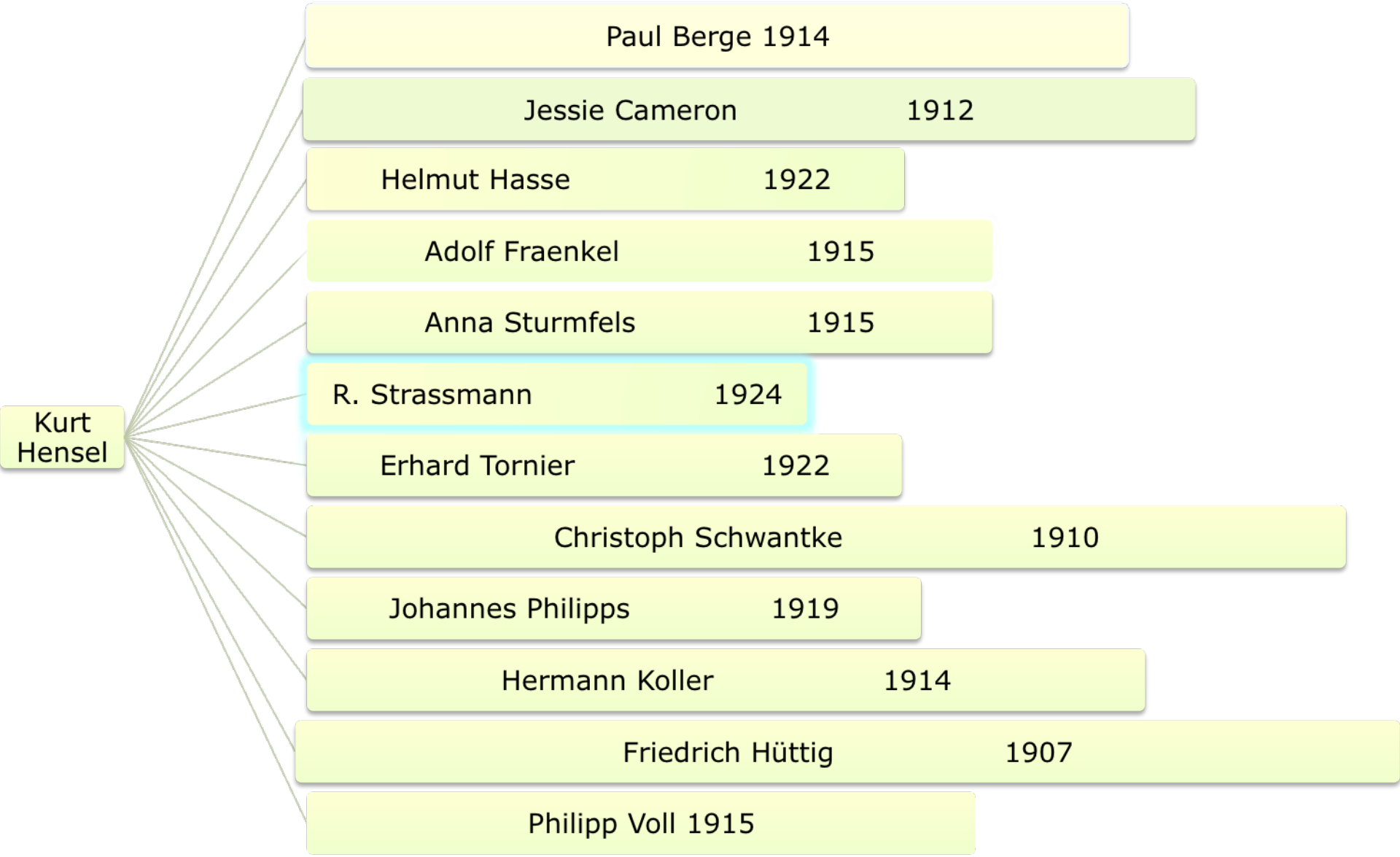
J.F.F. Enke 1844 Berlin

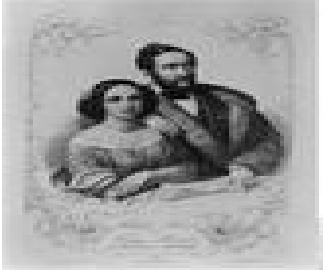
C.F. Gaus Helmstedt 1799

J. Pfaff Göttingen 1786

A. Kastner Leipzig 1739

J. Bode Hamburg


Kurt Hensel
Paul Berge 1914
Jessie Cameron 1912
Helmut Hasse 1922
Adolf Fraenkel 1915
Anna Sturmfels 1915
R. Strassmann 1924
Erhard Tornier 1922
Christoph Schwantke 1910
Johannes Philipps 1919
Hermann Koller 1914
Friedrich Hüttig 1907
Philipp Voll 1915



Jacob Ludwig von Adelson

Fanny Mendelssohn

Wilhelm Hensel

Julie von Adelson

Sebastian Hensel

Kurt Hensel

• Aussi douée p
Felix Mendelsso

• Fanny la gran
elle-même une
compositeur. El
compositions m
environ 120 piè

• Ce n’est qu’ur
décida de passe
et de publier se
commençait à é
commandes se
subitement au r
ses concerts

# Jeunesse de K. Hensel

- Les étudiants allemands de cette époque ne choisissaient pas une seule université pour étudier, mais suivaient des cours dans plusieurs institutions différentes.

- Hensel a étudié à Berlin et à Bonn. Parmi ses professeurs : Lipschitz, Weierstrass, Borchardt, Kirchhoff, Helmholtz et Kronecker. C'est Kronecker qui a eu le plus d'influence sur lui et a supervisé ses études de doctorat à l'Université de Berlin.

- Hensel a présenté sa thèse « Arithmetische Untersuchungen über Diskriminaten und ihre ausserwesentlichen Teiler » à Berlin en 1884 et il a continué à y travailler, présenter sa thèse d'habilitation et de devenir un « Privatdozent » en 1886.

# Hensel Biography (encore !)

- Hensel s'est à marié à Gertrud Hahn à Berlin en 1887
- Gertrud et Kurt Hensel ont  un fils et trois filles.
- Hensel a été nommé à un poste de professeur à l'Université de Marburg en 1901. Il a passé le reste de sa carrière, il a pris sa retraite en 1930 mais reste à Marburg.
- Il a consacré de nombreuses années à l'édition des œuvres de Kronecker. En fait, il a publié cinq volumes des œuvres de Kronecker entre les années 1895 et 1930.
- L'appelation « peiti théorème de Fermat » et « entier p-adique » sont de Hensel

- Helmut Hasse (1898 à Kassel-1979 à Ahrensburg) :

*« J'ai décidé de continuer mes études sous la direction de Kurt Hensel de Marburg. Qu'elle décision hâtive c'était ! En 1913, Hensel a publié un livre sur la théorie des nombres. J'ai trouvé un exemplaire de ce livre chez un antiquaire de Göttingen et l'ai acheté. J'ai trouvé ses nouvelles méthodes complètement fascinantes et digne d'une étude approfondie. »*

# Les inspirateurs

- **KUMMER Ernst Eduard, 1810-1893(Cantor fut un de nombreux élèves).**

  **Décomposition d'un nombre premier dans les extensions cyclotomiques. Arithmétique dans ces extensions.**

- **DEDEKIND Richard 1831-1916 Elève de Gauss et de Dirichlet.**

  **Généralisation des travaux de Kummer à des extensions algébriques et avec WEBER ils montrent que cette approche s'applique aux corps de fonctions**


**DEDEKIND**

# Idée de HENSEL*

- Pour étudier une fonction « au voisinagee d'un point », on utilise le développement de Taylor ou de Laurent en séries de puissances de (X- ).

- Pour étudier un nombre algébrique, on utilise un développement en termes de puissances d'un nombre premier.

*Première publication en 1897 suivie de plusieurs articles. Livres en 1908 et 1913.

# Applications mathématiques immédiates

- Décomposition du discriminant d'un corps de nombres (1897)

- Décomposition (factorisation) d'un nombre premier p dans **Q**( ) en termes de factorisation du polynôme minimal de modulo p

# Rappel : construction de **R**

## Valeur absolue usuelle

- L'application de **Q** dans **Q** : x $\longrightarrow$ |x|=Max(x,-x) définit une valeur absolue sur **Q** pour laquelle il existe des suites de Cauchy non convergente dans **Q. Exemple,** la suite de terme général

$$\mathcal{U}_n = \sum_{k=<n} (-1)^k / k!$$

est une suite de Cauchy* qui ne converge pas dans **Q.**

- On complète **Q** pour obtenir **R** : on comble les trous !

---

Une suite est dite de Cauchy si la différence en valeur absolue entre deux termes quelconques de la suite peut être rendue aussi petite qu'on veut.

# Valeur absolue p-adique

## $p$ est un nombre premier

Soit $x$ **dans** $\mathbb{Z}$. Il existe un unique $n$ dans $\mathbb{N}$ et $u$ dans $\mathbb{Z}$ tels que p ne divise pas $u$ et

$$x=p^n u.$$

On pose, pour $x$ **dans** $\mathbb{Z}$,

$$|x|_p=(1/p)^n.$$

On obtient une nouvelle valeur absolue sur $\mathbb{Z}$ dite valeur absolue p-adique.

---

L'entier positif $n$ est dit valuation p-adique de $x$

# Exemples

- Soit x=4. On a :

$$|x|_2=(1/2)^2$$
$$|x|_5=1$$
$$|x|_7= 1$$

- Comme, pour n dans N, $|p^n|=p^{-n}$, la suite $p^n$ tend vers zéro (pour la valeur absolue $p$-adique) !

# Prolongement à $\mathbb{Q}$

- Pour $x=(a/b)$ dans $\mathbb{Q}$ on pose
- $|x|_p=|a|_p/|b|_p$

On obtient ainsi une valeur absolue sur $\mathbb{Q}$ vérifiant, pour $x$ et $y$ dans $\mathbb{Q}$ :

4. $|x|_p=0$ si et seulement si $x=0$,
5. $|xy|_p= |x|_p|y|_p$,
6. $|x+y|_p \leq Max( |x|_p, |y|_p )$ (inégalité ultramétrique).

# Remarque

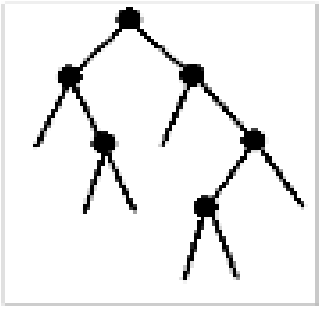
Pour x et y dans **Q**, la relation $|x-y|_p$ définit une distance dans **Q**.

Pour cette distance (topologie) deux nombres rationnels sont proches si de numérateur de leur différence est divisible par une grande puissance de **p**

# $\mathbb{Q}_p$

- Muni de cette valeur absolue $\mathbb{Q}$ est un **CORPS VALUÉ** (ultramétrique ou non archimédien) **NON COMPLET** (dans lequel il y des suites de Cauchy non convergentes).

- La complétion de $\mathbb{Q}$ donne $\mathbb{Q}_p$ (la valeur absolue de $\mathbb{Q}$ est étendue à $\mathbb{Q}_p$).



# En résumé

- Le corps $\mathbf{Q_p}$ est obtenu « grosso modo » à partir de $\mathbf{Q}$ en adjoignant à ce dernier toutes les limites des suites de Cauchy de Q.
- **EXEMPLES DE CALCUL**

⇨ La suite : $1, 1+p, 1+p+p^2, \ldots, 1+p+p^2+\ldots+p^n, \ldots$ est une suite dans $\mathbf{Z}$ qui converge (dans $\mathbf{Q\_P}$) vers $1/(1-p)$.

⇨ On a : $-1=(p-1)+(p-1)p+(p-1)p^2+\ldots+(p-1)p^n+\ldots$

# Développement de Hensel

- Tout élément x de $\mathbf{Q_p}$ s'écrit de manière unique

$$x = \sum_{i>=s} a_i p^i \quad (f)$$

où les $a_i$ sont des « chiffres » (de 0 à p-1) et s dans $\mathbf{Z}$.

- Inversement, toute série de la forme (f) ci-dessus est convergente dans $Q_p$

Dans (f) : $|x|_p = (1/p)^s$

# Comment marche le dévt. de Hensel (dans Q)* ?

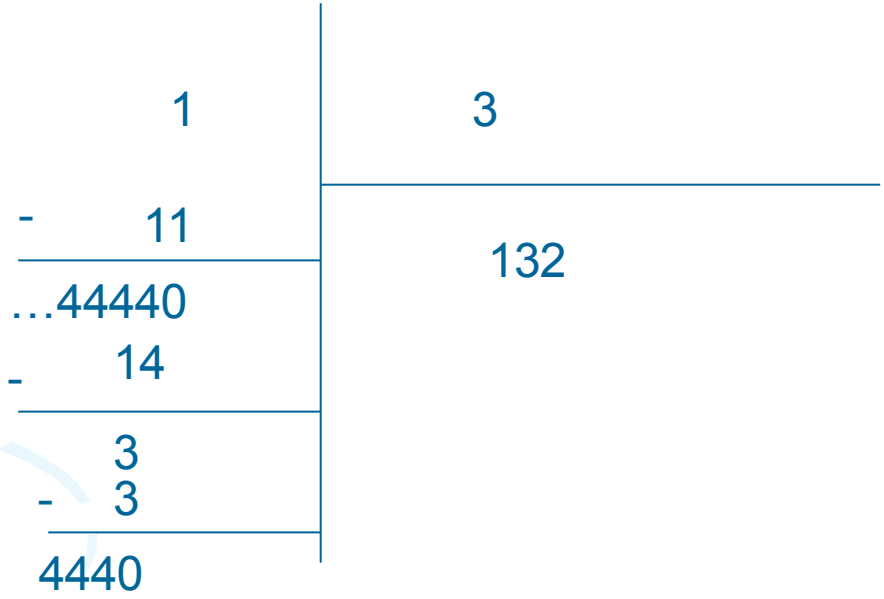
- Pour $x=(a/b)$ dans $Q$ avec $p$ ne divisant pas $b$
  - Comme $b$ est inversible modulo $p$, il existe $a_0$ dans $\{0,\dots,p-1\}$ tel que $x = a_0$ modulo $p$.
  - On écrit $x=a_0+px_1$ et on recommence avec $x_1$.
- Si $p$ divise $b$ on travaille avec $p^r x$ et on divise par $p^r$

On peut également utiliser la division selon les puissances croissantes de $a$ par $b$ écrits en base $p$.

* Pour les nombres algébriques, c'est un peu plus délicat !

# Exemple

- 1/3 dans $\mathbf{Q_5}$

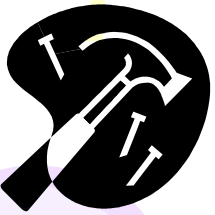


# Nombres dyadiques (2-adiques)

Ce sont toutes les sommes (finies ou infinies)

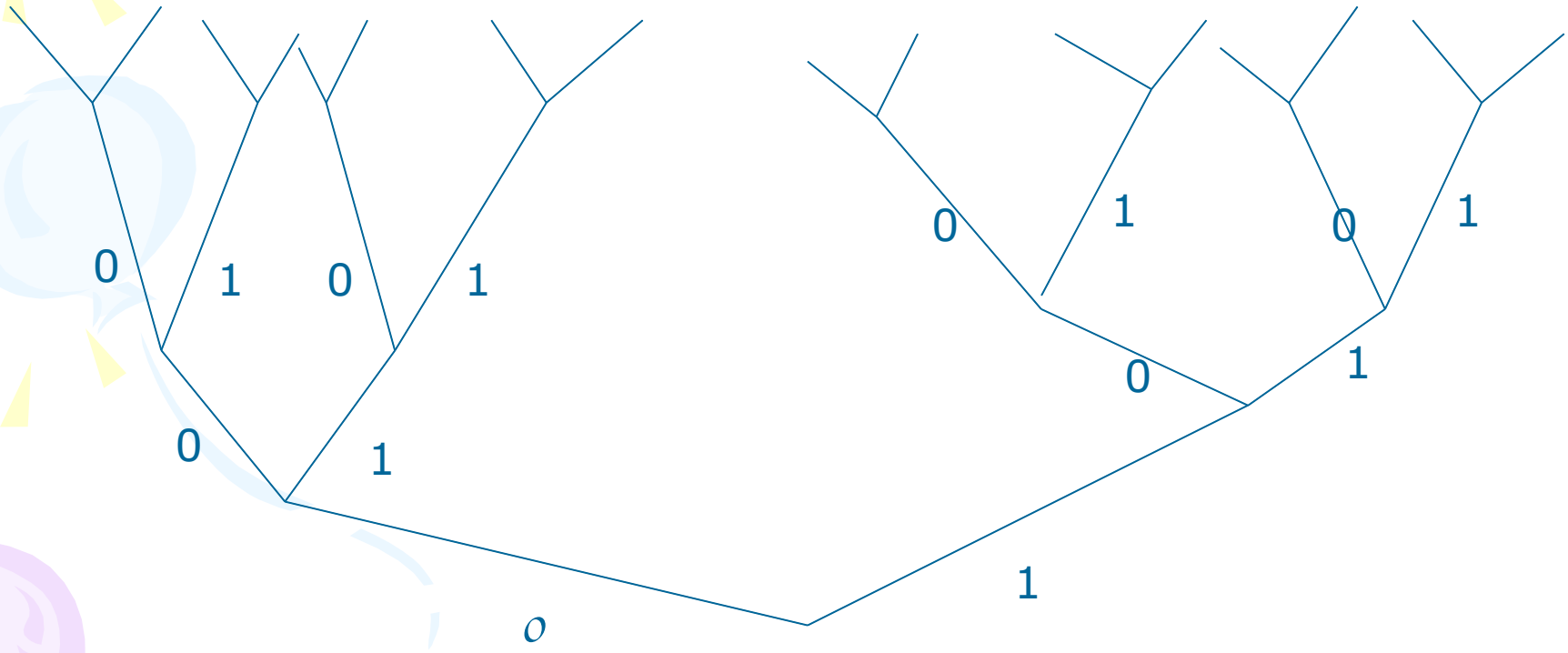
$$x = \sum_{i} a_i 2^i$$

avec $a_i$ dans $\{0,1\}$.



Remarque : on peut écrire $x = \ldots a_2 a_1 a_0$ (avec une infinité chiffres à gauche) et les opérations (additions, multiplications, ...) se font en reportant la retenue de gauche à droite.

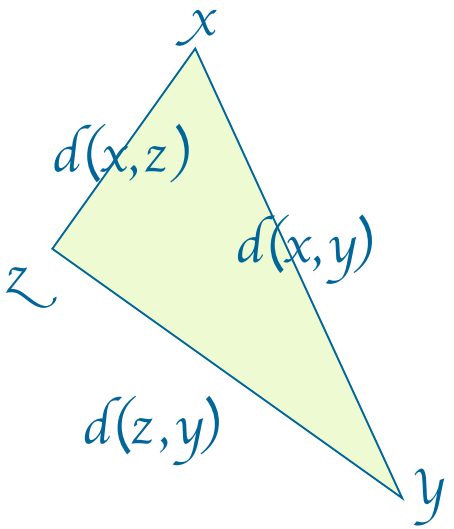
# Représentation, $p=2$ (pour simplifier)



# Conséquences de l'ultraméticité

- **TOUS LES TRIANGLES SONT ISOCÈLES !**

- **TOUT ÉLÉMENT D'UNE BOULE OUVERTE EST CENTRE DE LA BOULE !**




$$d(x,y) \leq Max(d(x,z),\ d(z,y))$$

B(x,r[ = {y € Qp / d(x,y)<r}, boule ouverte

# À quoi ça sert ? Un « beau » théorème (Hasse, 1920)

## Principe local-global

*Soit F une forme quadratique. L'équation F=0 a une solution non triviale dans* $\mathbf{Q}$ *(globalement) si, et seulement si, elle possède une solution non triviale dans* $\mathbf{R}$ *et une solution non triviale dans* $\mathbf{Q}_p$ *pour tout nombre premier p (localement).*

# Exemple

L'équation $x^2y+xy^2+x^3+y^3 = 0$ admet une solution non triviale dans $\mathbb{Q}$ si et seulement si elle en possède une (non triviale) dans chaque $\mathbf{Q_p}$ ($p=2, 3, 5, \ldots$) et dans $\mathbf{R}$.

# Aquoi ça sert ? Un autre beau résultat : le lemme de Hensel

Soit $f(x)$ dans $\mathbf{Z}[x]$. On suppose qu'il existe $a_0$ dans $\mathbf{Z}$ tel que :

$f(a_0) \equiv 0 \mod p$ et $f'(a_0) \not\equiv 0 \mod p$.

Alors il existe $a$ dans $\mathbf{Z}_p$ tel que $f(a)=0$ avec

$a = a_0 + a_1 p + \ldots$

**Autrement dit,**

Si on sait factoriser modulo **p** on saura faire dans $\mathbf{Q}_p$.

# Encore un peu d'histoire

- Le livre de Steinitz en **1910** (ou l'importance théorique du travail de Hensel) :

« C'est la découverte de ces derniers qui conduisit Steinitz, comme il le dit explicitement, à dégager les notions abstraites communes à toutes ces théories dans un travail fondamental qui peut être considéré comme ayant donné naissance à la conception actuelle de l'algèbre. »

**Steinitz 1871-1928**

*Eléments d'histoire des mathématiques,* N. Boubaki , Hermann 1960, p 109

# D’autres dates

- A partir de **1907** Hensel  construit les fonctions élémentaires : exp, log, sin,…
- En **1912** Kurschak introduit les valuations
- En **1917** Ostrowski établit son théorème

  « Les seules valeurs absolues sur **Q** sont (à équivalence près) les valeurs absolues p-adiques et la valeur absolue usuelle »

- Entre **1220** et **1935** : Théorie complète des valuations (Deuring, Schmidt, Krull, …)

# Et les décadiques dans tout ça ?

$B = Q_2 \times Q_5$

# En guise de conclusion

- Les p-adiques sont un pont entre deux champs différents des mathématiques (algèbre, analyse)
- Les questions  de convergence sont apparues plus tard : les p-adiques étaient considérés comme des objets formels
- La théorie des corps, des valuations est postérieure à celle des p-adiques

# Diviseurs de zéro

…112
…625
---
…560
…224.
672..
---
…000

# Tous les triangles sont isocèles

- On a : $d(x,y) \leq Max(d(x,z),d(z,y))$.
- Si $d(x,z) \neq d(z,y)$ alors on peut supposer $d(x,z) < d(z,y)$.
- Mé alors $d(x,y) < d(z,y)$ implique $d(z,y) < Max(d(z,x),d(x,y)) < d(z,y)$.

Ce qui est manifestement absurde.

Par conséquent si $d(x,z) \neq d(z,y)$ alors $d(x,y) = d(z,y)$. Cqfd

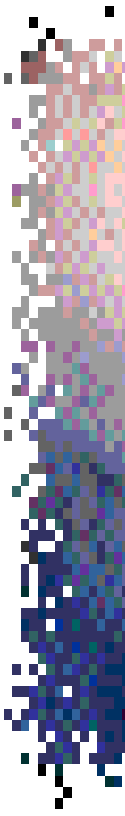
# Tout point de la boule est centre de la boule

- Boule ouverte de centre $x$ et de rayon $r$ :
  $B(x,r)=\{y \in Q_p \ / \ d(x,y)<r\}$.
- Soit $z \in B(x,r)$ (i.e., $d(z,x)<r$). On a :

$$d(z,y) \leq Max(d(z,x), d(x,y))$$

- Par conséquent,

$$d(z,y)<r.$$ Cqfd



# Références


- G. Christol & D. Barsky, *Les nombres p-adiques*, La Recherche, Juillet-Août 1995 vol. 26
- M. G. Dumas, *Sur quelques cas d'iréductibilité des polynômes à cofficients rationnels*, Journ. De Math. (6e série) tome II. –Fasc. III, 1906
- Fernando Gouvêa, *p-adic numbers*, an introduction Springer, collection Universitext, 1997 (2e édition)
- N. Bourbaki, *Eléments d'histoire des mathématiques,* Hermann 1974
- Y. Amice, *Les nombres p-adiques*, PUF, 1975
- N. Koblitz, *P-adic Numbers, p-adic Analysis, and Zeta-Functions* Springer, 1996 (2e édition)
- A. M. Robert, *A Course in p-adic Analysis. Springer 2000*

# Sitographie


- http://pagesperso-orange.fr/alain.pichereau/brenom.html
- http://www.vinc17.org/math/index.fr.html
- http://mathenjeans.free.fr/amej/edition/9301bren/brenoms
- http://www.animath.fr/old/UE/autres/brenoms.html
- http://en.wikipedia.org/wiki/P-adic_number
- http://mathenjeans.free.fr/amej/accueil.htm
- http://www-history.mcs.st-andrews.ac.uk/Biographies/Hensel.html