Nombres p-adiques et équations diophantiennes

Nicolas Billerey

Exposé C.I.E.S., 13 janvier 2006

Kurt Hensel (1861-1941)

Plan de l'exposé

Plan de l'exposé

Plan de l'exposé

Plan de l'exposé

Notations

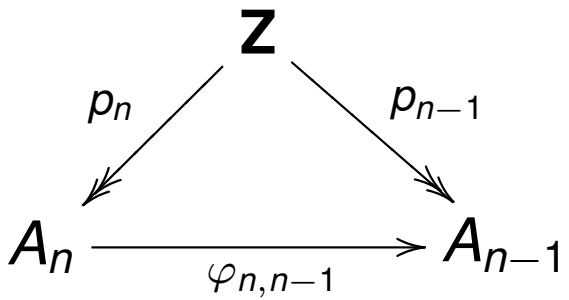
Soient p un nombre premier et n un entier naturel ≥ 1. On note :

- A_n l'anneau $\mathbf{Z}/p^n\mathbf{Z}$,
- p_n la projection canonique de $\mathbf{Z}$ sur A_n,
- $\varphi_{n,n-1}$ l'homorphisme naturel de A_n dans A_{n-1}.

Compatibilitité

Le diagramme ci-dessous est commutatif : pour tout $x \in \mathbf{Z}$,

$$\varphi_{n,n-1}(p_n(x)) = p_{n-1}(x).$$



On note π_n la projection canonique de $\mathcal{A} = \prod_{n\geq 1} A_n$ sur A_n.

Entiers p-adiques

L'application i de $\mathbf{Z}$ dans $\mathcal{A}$ définie par

$$i(z) = (p_n(z))_{n\geq 1}$$

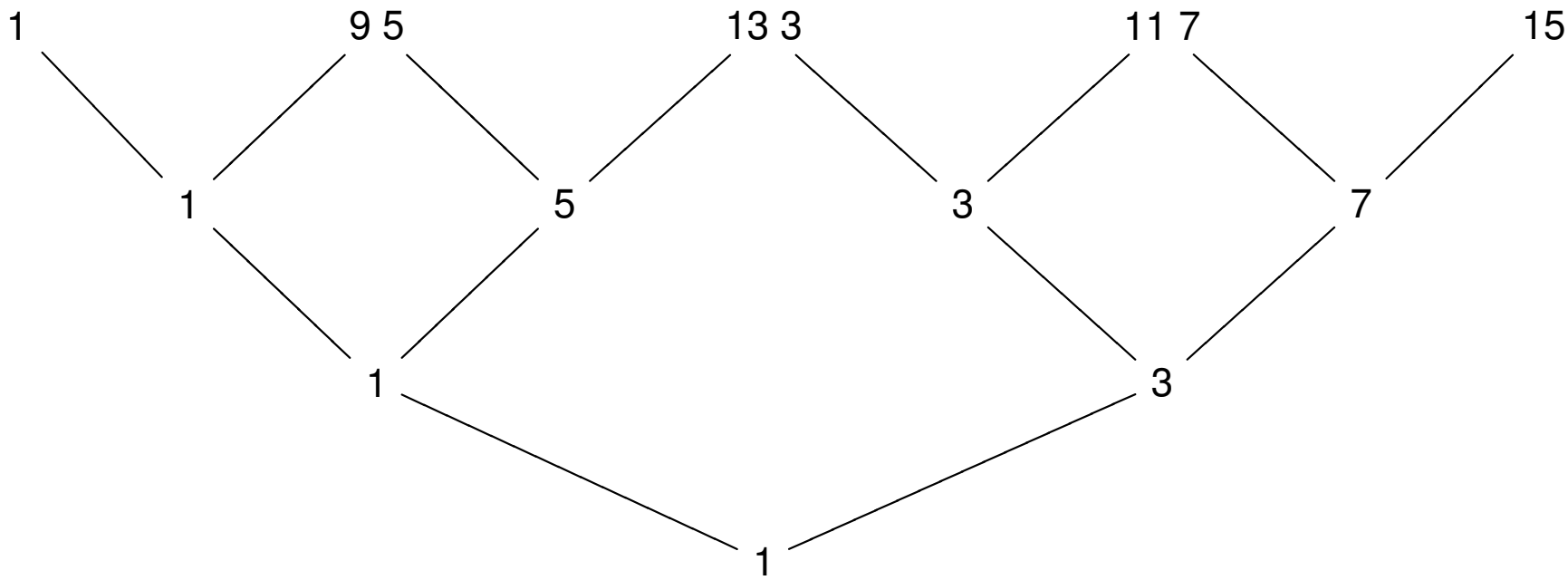
est un morphisme *injectif* d'anneaux. Pour $a \in i(\mathbf{Z})$, on a la relation

$$\forall n \geq 2, \quad \varphi_{n,n-1}(\pi_n(a)) \quad = \quad \pi_{n-1}(a). \qquad (1)$$

Définition

L'ensemble $\mathbf{Z}_p$ des éléments a de $\mathcal{A}$ qui satisfont à la relation (1) est sous-anneau de $\mathcal{A}$ contenant l'image $i(\mathbf{Z})$ de $\mathbf{Z}$. On l'appelle anneau des entiers p-adiques.

Un entier 2-adique



Un entier 5-adique

$$(3, 8, 33, 408, 1033, 7283, \dots)$$

$$\begin{aligned}
7283 &\pmod{5^6} &&\xmapsto{\varphi_{6,5}} && 1033 \pmod{5^5},\\
1033 &\pmod{5^5} &&\xmapsto{\varphi_{5,4}} && 408 \pmod{5^4},\\
408 &\pmod{5^4} &&\xmapsto{\varphi_{4,3}} && 33 \pmod{5^3},\\
33 &\pmod{5^3} &&\xmapsto{\varphi_{3,2}} && 8 \pmod{25},\\
8 &\pmod{25} &&\xmapsto{\varphi_{2,1}} && 3 \pmod{5}.
\end{aligned}$$

Nombres p-adiques

Proposition

L'anneau $\mathbf{Z}_p$ est intègre.

D'où la

Définition

Le corps des fractions de l'anneau $\mathbf{Z}_p$ s'appelle corps des nombres p-adiques et se note $\mathbf{Q}_p$.

Principe

Développement de Hensel

=

développement en série.

Topologie sur $\mathbf{Z}_p$

- L'ensemble $\mathcal{A}$ est muni de la topologie produit (chaque A_n est muni de la topologie discrète).
- L'anneau $\mathbf{Z}_p$ est un sous-anneau topologique de $\mathcal{A}$.
- Pour $a \in \mathbf{Z}_p$ la famille

$$V_k(a) = \{x \in \mathbf{Z}_p | \pi_k(x) = \pi_k(a)\},\ k \geq 1$$

est une base de voisinage de a dans $\mathbf{Z}_p$.

Développement de Hensel (1)

Proposition

Soit $x \in \mathbf{Z}_p$, il existe une unique suite $(a_n)_n$ d'entiers $0 \leq a_n < p$ telle que la série $\sum_{n\geq 0} a_n p^n$ converge vers x. Cette série est appelée développement de Hensel de x.

Exemples. Avec $p = 2$:

- $-1 = \sum_{n\geq 0} 2^n$,
- $\sum_{n\geq 0} 2^{2^n}$ est un élément de $\mathbf{Z}_p$ qui n'est pas dans $\mathbf{Z}$.

Avec $p = 5$:

- $2+5+2\times 5^2+5^3+3\times 5^4+4\times 5^5+2\times 5^6+3\times 5^7+3\times 5^9+2\times 5^{10}+2\times 5^{11}+4\times 5^{13}+5^{14}+3\times 5^{15}+2\times 5^{16}+4\times 5^{17}+4\times 5^{19}+\cdots = \ldots 141142140434042314022332431212_5$ est une racine carrée de -1 dans $\mathbf{Z}_5$.

Développement de Hensel (2)

- L'entier 5-adique $(3, 8, 33, 408, 1033, 7283, \dots)$ s'écrit $\dots 21313_5$.

Proposition

Tout nombre p-adique x admet un développement de Hensel de la forme $\sum_{n \geq n_0} a_n p^n$ où les $(a_n)_n$ vérifient $0 \leq a_n < p$ et n_0 est dans $\mathbf{Z}$.

Exercice. Le développement de Hensel d'un nombre p-adique x est périodique si, et seulement si, x est rationnel.

Plan de l'exposé

Principe du lemme de Hensel

Solution approchée

solution exacte

Lemme de Hensel

Lemme (Hensel, 1908)

Soit f un polynôme à coefficients dans $\mathbf{Z}_p$. Si $a \in \mathbf{Z}$ est une racine simple de l'équation de congruence :

$$f(x) \equiv 0 \pmod{p},$$

alors il existe un entier p-adique α tel que $\alpha \equiv a \pmod{p}$ et $f(\alpha) = 0$.

Un exemple d'application

(-1) n'a pas de racine carrée dans $\mathbf{Q}$, mais en a, par exemple, dans $\mathbf{Q}_5$. On pose :

$$f(X) = X^2 + 1 \in \mathbf{Z}_5[X].$$

Alors $f(2) = 5 \equiv 0 \pmod 5$ et $f'(2) = 2 \times 2 = 4 \not\equiv 0 \pmod 5$.

Lemme de Hensel $\Longrightarrow$ (-1) a une racine carrée dans $\mathbf{Q}_5$.

De plus, son développement de Hensel commence par 2. Il s'écrit :

$$\ldots 141142140434042314022332431212_5$$

Solutions q-adiques à l'équation de Fermat

Proposition

Soit p un nombre premier quelconque. L'équation

$$X^p + Y^p + Z^p = 0 \tag{2}$$

admet des solutions non triviales dans $\mathbf{Z}_q$ pour tout nombre premier q.

Démonstration (dans le cas où $p \neq q$)

On pose $f(X) = X^p + q^p - 1$.

- *Le polynôme f est à coefficients dans $\mathbf{Z}_q$.*
- *On a $f(1) \equiv 0 \pmod{q}$ et $f'(1) \not\equiv 0 \pmod{q}$.*

Démonstration (suite)

- *D'après le lemme de Hensel, il vient qu'il existe une solution* $(x, q, -1)$ *où* $x \in \mathbf{Z}_p^*$ *à l'équation (2).*

Plan de l'exposé

Définitions et objectifs

On dit qu'une courbe C définie sur $\mathbf{Q}$ présente une obstruction locale en p nombre premier si l'équation définissant C n'admet pas de solution dans $\mathbf{Q}_p$.

Objectif = chercher localement un renseignement global.

Si une courbe donnée présente une obstruction locale, elle n'a, en particulier, pas de point sur $\mathbf{Q}$ car

$$\mathbf{Q} \hookrightarrow \mathbf{Q}_p.$$

Soit $c \geq 1$ un entier sans puissance quatrième et $\mathcal{C}$ la courbe d'équation :

$$\mathcal{C} : \quad X^4 + Y^4 = cZ^4.$$

Problème

Déterminer les nombres premiers p pour lesquels $\mathcal{C}(\mathbf{Q}_p) \neq 0$?

Cela dépend de c!

On montre :

- $\mathcal{C}(\mathbf{Q}_2) \neq 0 \iff c \equiv 1 \text{ ou } 2 \pmod{16}$;
- pour p nombre premier impair divisant c,

$$\mathcal{C}(\mathbf{Q}_p) \neq 0 \iff p \equiv 1 \pmod{8};$$

- pour p un nombre premier ne divisant pas $2c$,

$$\mathcal{C}(\mathbf{Q}_p) \neq 0 \iff \widetilde{\mathcal{C}}(\mathbf{F}_p) \neq 0;$$

- pour $p \nmid 2c$ et $p \geq 37$, $\mathcal{C}(\mathbf{Q}_p) \neq 0$;
- Si $p \equiv 3 \pmod 4$, alors $\mathcal{C}(\mathbf{Q}_p) \neq 0$.

Restent les cas où suivants :

- $\mathcal{C}(\mathbf{Q}_5) \neq 0 \iff c \not\equiv 3 \text{ ou } 4 \pmod 5$;
- $\mathcal{C}(\mathbf{Q}_{13}) \neq 0 \iff c \not\equiv 7,\ 8 \text{ ou } 11 \pmod{13}$;
- $\mathcal{C}(\mathbf{Q}_{17}) \neq 0$;
- $\mathcal{C}(\mathbf{Q}_{29}) \neq 0 \iff c \not\equiv 4,\ 5,\ 6,\ 9,\ 13,\ 22 \text{ ou } 28 \pmod{29}$;

Le plus petit entier c sans puissance quatrième pour lequel $\mathcal{C}(\mathbf{Q}_p) \neq 0$ quel que soit p est $c = 146$.

Conclusion. Les obstructions locales sont fréquentes!

Une conjecture

On considère la courbe $\mathcal{C}(a,b,c)$ d'équation :

$$aX^p + bY^p + cZ^p = 0,$$

Conjecture

On suppose que a, b et c ne vérifient aucune relation linéaire non triviale à coefficients dans $\{-1,0,1\}$*. Alors il existe un réel* $g(a,b,c)$ *tel que pour tout nombre premier* $p > g(a,b,c)$*, la courbe* $\mathcal{C}(a,b,c)$ *présente au-moins une obstruction locale.*

Remarque. On a vu que ce n'est pas le cas de la courbe de Fermat classique qui a des solutions non triviales dans tous les $\mathbf{Q}_p$.

Principe de Hasse

Définition

Une courbe C définie sur $\mathbf{Q}$ contredit le principe de Hasse si $C(\mathbf{Q})$ est vide et C ne présente aucune obstruction locale.

Exemple. La courbe d'équation $3X^3 + 4Y^3 + 5Z^3 = 0$ contredit le principe de Hasse.

Exemples

La courbes dont les équations sont données ci-dessous contredisent le principe de Hasse :

$$X^7 + 3Y^7 + 19Z^7 = 0,$$

$$X^{19} + 5Y^{19} + 11Z^{19} = 0.$$

Problème ouvert

Peut-on construire des courbes de Fermat de degré quelconque contredisant le principe de Hasse?

Bibliographie I

Y. Amice.
Les nombres p-adiques.
P.U.F., coll. Sup (1975).

K. Hensel.
Théorie des nombres.
G. J. Göschen'sche Verlagshandlung, (1913).

J.-P. Serre.
Cours d'arithmétique.
P.U.F., 4ème éd., coll. "le mathématicien" (1995).

E. Halberstadt et A. Kraus.
Courbes de Fermat: résultats et problèmes.
J. reine angew. **548** , p. 167 – 234 (2002).