Local-global principle

Ahmed Moussaoui

Université de Versailles Saint-Quentin
Fondation Jacques Hadamard

September 9^{th} 2016

The problem

Let $f \in \mathbb{Z}[x_1, \ldots, x_m]$ be a polynomial. We want to solve the following problem :
What are the solutions of $f(x) = 0$ with $x \in \mathbb{Z}^m$? Does a solution exist ?

- It is very hard to solve $f(x) = 0$ with $x \in \mathbb{Z}^m$.
- Using reduction modulo p, one can show that $f(x) = 0$ does not have a solution.

Example

$x^2 + 7y^3 = 3$ does not have a solution (modulo 7)

- Assume that for all prime p and all integers $n \in \mathbb{N}^*$, we have a solution $x_n \in \mathbb{Z}/p^n\mathbb{Z}$, can we deduce a solution in $\mathbb{Z}$?

p-adic integers

Let $p \in \mathbb{N}$ be a prime number.

$$\mathbb{Z}_p = \{(x_n)_n \in \prod_{n \in \mathbb{N}^*} (\mathbb{Z}/p^n\mathbb{Z}) \mid x_{n+1} \equiv x_n \pmod{p^n}\}.$$

$$\ldots \xrightarrow{(\text{mod } p^{n+1})} x_{n+1} \xrightarrow{(\text{mod } p^n)} x_n \xrightarrow{(\text{mod } p^{n-1})} \ldots \xrightarrow{(\text{mod } p^3)} x_3 \xrightarrow{(\text{mod } p^2)} x_2 \xrightarrow{(\text{mod } p)} x_1$$

The map $\mathbb{Z} \to \mathbb{Z}_p$ which associates to all $x \in \mathbb{Z}$, $(x \pmod{p^n})_n$ is an embedding $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$.

Idea

A p-adic integer gives information on reduction modulo all power of p.

p-adic integers

Let $p \in \mathbb{N}$ be a prime number.

$$\mathbb{Z}_p = \{(x_n)_n \in \prod_{n \in \mathbb{N}^*} (\mathbb{Z}/p^n\mathbb{Z}) \mid x_{n+1} \equiv x_n \pmod{p^n}\}.$$

$$\ldots \xrightarrow{(\mathrm{mod}\ p^{n+1})} x_{n+1} \xrightarrow{(\mathrm{mod}\ p^n)} x_n \xrightarrow{(\mathrm{mod}\ p^{n-1})} \ldots \xrightarrow{(\mathrm{mod}\ p^3)} x_3 \xrightarrow{(\mathrm{mod}\ p^2)} x_2 \xrightarrow{(\mathrm{mod}\ p)} x_1$$

Properties of $\mathbb{Z}_p$

- $\mathbb{Z}_p$ is an integral domain ;
- $\mathbb{Z}_p$ is a local ring (it has a unique maximal ideal) $p\mathbb{Z}_p$;
- $\mathbb{Z}_p \to \mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{Z}/p\mathbb{Z}$;
- $\forall x \in \mathbb{Z}_p$, $\exists! n \in \mathbb{N}, x = p^n u$ with $u \in \mathbb{Z}_p^\times$.

p-adic numbers

Definition

The field of p-adic numbers $\mathbb{Q}_p$ is the field of fraction of $\mathbb{Z}_p$.

For all $\forall x \in \mathbb{Q}_p,\ \exists! n \in \mathbb{Z}, x = p^n u$ with $u \in \mathbb{Z}_p^\times$. We denote by $v_p(x) = n$.

- $\forall x, y \in \mathbb{Q}_p,\ v_p(xy) = v_p(x) + v_p(y)$;
- $\forall x, y \in \mathbb{Q}_p,\ v_p(x+y) \geqslant \min(v_p(x), v_p(y))$.

$\forall x \in \mathbb{Q}_p,\ |x|_p = p^{-v_p(x)}$. $\forall x, y \in \mathbb{Q}_p,\ |x+y|_p \leqslant \max(|x|_p, |y|_p)$.

Proposition

The ultrametric norm $|\cdot|_p$ on $\mathbb{Q}_p$ defines a topology making it a topological space locally compact, totally disconnected and complete in which $\mathbb{Q}$ is dense.

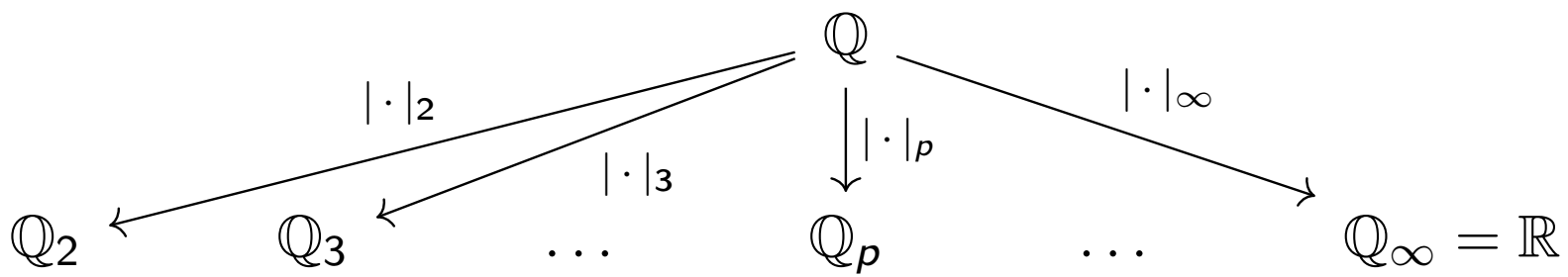
p-adic numbers

A norm on a field k is a map $|\cdot| : k \to \mathbb{R}_+$ which satisfies :

- $|x| = 0 \Leftrightarrow x = 0$;
- $|xy| = |x||y|$;
- $|x + y| \leqslant |x| + |y|$
- $|x + y| \leqslant \max(|x|, |y|)$.

Theorem (Ostrowski)

A norm on $\mathbb{Q}$ is equivalent to $|\cdot|_\infty$ (usual absolute value) or to $|\cdot|_p$ for some prime p.



Local-global principle

Local-global principle or Hasse principle

A polynomial equation with rationnal coefficient has a rational solution, if and only if, it has a solution in every p-adic field and in the field of real numbers. More generally, a property holds for $\mathbb{Q}$, if and only if, it holds for every $\mathbb{Q}_p$ and $\mathbb{R}$.

Easier to find a solution in $\mathbb{R}$ or in $\mathbb{Q}_p$.

Lifting solution from $\mathbb{Z}/p^n\mathbb{Z}$ to $\mathbb{Z}_p$

Hensel's lemma

Let $f \in \mathbb{Z}_p[X]$ and $x \in \mathbb{Z}_p$. Assume that there exists $n \in \mathbb{N}^*$ and $k \in \mathbb{N}$ such that $0 \leqslant 2k < n$ and

$$f(x) \equiv 0 \pmod{p^n} \text{ and } v_p(f'(x)) = k.$$

Then, there exists $y \in \mathbb{Z}_p$ such that $f(y) \equiv 0 \pmod{p^{n+1}}$, $v_p(f'(y)) = k$ and $y \equiv x \pmod{p^{n-k}}$.

- Newton method : $y = x - f(x)/f'(x)$;
- Taylor's formula : $f(x+t) = f(x) + tf'(x) + t^2 f''(x)/2 + \ldots$;
- $f(y) = 0 + (\text{valuations} \geqslant n+1)$;
- $f(y) \equiv 0 \pmod{p^{n+1}}$

Lifting solution from $\mathbb{Z}/p^n\mathbb{Z}$ to $\mathbb{Z}_p$

Theorem

Let $f \in \mathbb{Z}_p[X_1, \ldots, X_m]$ and $x = (x_i) \in \mathbb{Z}_p^m$. Assume that there exists $n \in \mathbb{N}^*, j \in [\![1, m]\!]$ and $k \in \mathbb{N}$ such that $0 \leqslant 2k < n$ and

$$f(x) \equiv 0 \pmod{p^n} \text{ and } v_p\left(\frac{\partial f}{\partial X_j}(x)\right) = k.$$

Then, there exists $y \in \mathbb{Z}_p$ such that $f(y) = 0$ and $y \equiv x \pmod{p^{n-k}}$.

- Hensel's lemma : $(x_q)_q \in \mathbb{Z}_p^{\mathbb{N}}$ such that $f(x_q) \equiv 0 \pmod{p^{n+k}}$ and $x_{q+1} \equiv x_q \pmod{p^{n+q-k}}$;
- $(x_q)_q$ is Cauchy and $\mathbb{Q}_p$ is complete ;
- the limit $y \in \mathbb{Z}_p$ of $(x_q)_q$ gives a solution.

Hilbert symbol

Problem : Let q be a quadratic form with rationnal coefficients.
Example : $q(x, y, z, t) = x^2 + 3y^2 + zt$.
Does a non-trivial rationnal solution of $q(v) = 0$ exists ?
For $k = \mathbb{R}$ or $\mathbb{Q}_p$, let $a, b \in k^*$.

$$(a, b) = \begin{cases} 1 & \text{if } z^2 - ax^2 - by^2 \text{ admits a non trivial zero in } k^3 \\ -1 & \text{either.} \end{cases}$$

Theorem

$$(a, b)_\infty = \begin{cases} 1 & \text{if } a > 0 \text{ or } b > 0 \\ -1 & \text{either.} \end{cases}$$

$$(a, b)_p = \begin{cases} (-1)^{\alpha\beta\varepsilon(p)} \left(\frac{u}{p}\right)^{\beta} \left(\frac{v}{p}\right)^{\alpha} & \text{si } p \geqslant 3 \\ \\ (-1)^{\varepsilon(u)\varepsilon(v)+\alpha\omega(v)+\beta\omega(u)} & \text{si } p = 2, \end{cases}$$

with $a = p^\alpha u, b = p^\beta v,\ \alpha, \beta \in \mathbb{Z},\ u, v \in {\mathbb{Z}_p}^*$ and if x is odd $\varepsilon(x) \equiv \frac{x-1}{2} \pmod 2, \omega(x) \equiv \frac{x^2-1}{8} \pmod 2$.

Invariant of a quadratic form

Let q be a quadratic form with coefficient in $\mathbb{Q}_p$. Assume that q is non-degenerate and that $q(x) = a_1 x_1^2 + \ldots + a_n x_n^2$.

- discriminant : $d(q) = \det(q) = a_1 \ldots a_n \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$;
- Hasse invariant : $\varepsilon(q) = \prod_{i<j}(a_i, a_j)$.

Theorem

Let n be the rank of q. Then q admits a non-trivial zero, if and only if :

- $n = 2$ and $d = -1$;
- $n = 3$ and $(-1, -d) = \varepsilon$;
- $n = 4$ and either $d \neq 1$ or $d = 1$ and $\varepsilon = (-1, -1)$;
- $n \geqslant 5$.

When $n \geqslant 5$

- $q = a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 + a_5x_5^2$;
- there are 3 coefficients for which their p-adic valuations have the same parity ;
- $a_1 = u_1b_1^2,\ a_2 = u_2b_2^2,\ a_13 = u_3b_3^2,$;
- $q_2 = u_1y_1^2 + u_2y_2^2 + u_3y_3^2,\ q_2(b_1x_1, b_2x_2, b_3x_3) = a_1x_1^2 + a_2x_2^2 + a_3x_3^2$;
- Chevalley-Warning theorem gives a non-trivial (z_1, z_2, z_3) solution mod p ;
- primitive solution + discriminant of q_2 invertible : one of partial derivative is not divisible by p ;
- Hensel's lemma : a solution in $\mathbb{Z}_p$;

Hasse-Minkowski theorem

Let q be a quadratic form with coefficient in $\mathbb{Q}$.

Theorem

q admits a non-trivial zero in $\mathbb{Q}$, if and only if, q admits a non-trivial zero in $\mathbb{Q}_p$ for every prime p and in $\mathbb{R}$.

Example

Let $q = 2x^2 + 5y^2 - 17z^2$.

ε_2	$=$	$(2,5)_2(2,-17)_2(5,-17)_2$	ε_5	$=$	$(2,5)_5(2,-17)_5(5,-17)_5$
	$=$	$(-1)\times 1\times 1$		$=$	$\left(\frac{2}{5}\right)\times 1\times\left(\frac{-17}{5}\right)$
	$=$	-1		$=$	$(-1)\times 1\times(-1)$
				$=$	1
$(-1,-d)_2$	$=$	$(-1,2)_2(-1,5)_2(-1,17)_2$	$(-1,-d)_5$	$=$	$(-1,2)_5(-1,5)_5(-1,17)_5$
	$=$	$1\times 1\times 1$		$=$	$1\times\left(\frac{-1}{5}\right)\times 1$
	$=$	1		$=$	1

ε_{17}	$=$	$(2,5)_{17}(2,-17)_{17}(5,-17)_{17}$
	$=$	$1\times\left(\frac{2}{17}\right)\times\left(\frac{5}{17}\right)$
	$=$	$1\times 1\times(-1)$
	$=$	-1
$(-1,-d)_{17}$	$=$	$(-1,2)_{17}(-1,5)_{17}(-1,17)_{17}$
	$=$	$1\times\left(\frac{-1}{17}\right)\times 1$
	$=$	1

q does not have a non-trivial zero in $\mathbb{Q}_2$ and $\mathbb{Q}_{17}$, so q does not have a non-trivial zero in $\mathbb{Q}$.

Let $q = 2x^2 + 12y^2 - 7z^2 - 5t^2$.

- the signature of q shows that q admits a zero in $\mathbb{R}$;
- if p is a prime number which is not in $\{2, 3, 5, 7\}$, reducing modulo p, we have a non-degenerate quadratic form with 3 variables in $\mathbb{Z}/p\mathbb{Z}$. The Chevalley-Warning theorem shows that there is a non-trivial zero and the Hensel lemma gives a solution in $\mathbb{Q}_p$;
- the discriminant of q is $d = 2^3.3.5.7$. So q has a non-trivial zero in $\mathbb{Q}_p$, if and only if, $d_p \neq 1$ or $d_p = 1$ and $\varepsilon_p = (-1, -1)_p$. Since the p-adic valuation of d is odd for these primes, d is not a square in $\mathbb{Q}_p$ for these p. This implies that q admits a non-trivial zero in $\mathbb{Q}_p$ for $p \in \{2, 3, 5, 7\}$.

Conclusion : q admits a non-trivial zero in $\mathbb{Q}$ (one can check that $(\frac{54}{7}, \frac{5}{7}, \frac{1}{7}, 5)$ is a solution).

Thank your for your attention.