Solutions entières des équations diophantiennes

Jean-Louis Colliot-Thélène (CNRS et Université Paris-Sud)

Conférence Bernoulli
Centre interfacultaire Bernoulli
8 novembre 2012

Résumé : Si une équation linéaire affine $ax + by = c$, à coefficients a, b, c entiers, a des solutions (x, y) modulo tout entier, alors elle a des solutions (x, y) en entiers, et l'on peut préciser les congruences possibles pour ces solutions. On discutera ce qu'il en est pour des équations polynomiales, à coefficients entiers, de degré supérieur : existence de solutions entières, congruences imposables à ces solutions.

Applications linéaires affines

De façon plus générale, soient $L_i(x_1, \ldots, x_n)$, $i = 1, \ldots, r$ des formes linéaires à coefficients entiers, et soient c_i, $i = 1, \ldots, r$ des entiers.

Si le système

$$L_i(x_1, \ldots, x_n) = c_i$$

admet des solutions modulo tous les entiers $m > 0$, alors il admet une solution $\mathbf{b} \in \mathbb{Z}^n$.

De plus, soit $\mathbf{b}_m \in \mathbb{Z}^n$ une solution du sytème modulo un entier $m > 0$. Si cette solution $\mathbf{b}_m$ peut se relever en une solution $\mathbf{b}_{mM}$ modulo mM pour tout $M > 0$, alors il existe une solution $\mathbf{b} \in \mathbb{Z}^n$ du système initial à coefficients dans $\mathbb{Z}$ satisfaisant $\mathbf{b} \equiv \mathbf{b}_m \bmod m$.

De façon générale, on considère un système d'équations

$$P_i(x_1, \ldots, x_n) = 0, \quad i = 1, \ldots, r$$

où les P_i sont des polynômes à coefficients entiers, et on se demande s'il y a une solution en nombres entiers $(x_1, \ldots, x_n) \in \mathbb{Z}^n$.
Une condition nécessaire est qu'il y ait des solutions avec $(x_1, \ldots, x_n) \in \mathbb{R}^n$.
Une série de conditions nécessaires est :
Pour tout entier $m > 0$ on peut résoudre le système modulo m.
Il suffit pour cela (théorème du reste chinois) qu'il y ait des solutions modulo tout p^s avec p premier.

Supposons les conditions nécessaires d'existence de points entiers ci-dessus satisfaites. On dit que le système

$$P_i(x_1, \ldots, x_n) = 0, \quad i = 1, \ldots, r$$

satisfait l'*approximation forte* si pout tout entier $m > 0$ et toute famille $(b_1, \ldots, b_n) \in \mathbb{Z}^n$ satisfaisant les équations ci-dessus modulo m, et se relevant modulo mM pour tout $M > 0$, alors il existe une famille $(c_1, \ldots, c_n) \in \mathbb{Z}^n$ satisfaisant le système sur $\mathbb{Z}$ et congrue à $(b_1, \ldots, b_n)$ modulo m.

Un peu de langage : schémas

Un système

$$P_i(x_1, \ldots, x_n) = 0, \quad i = 1, \ldots, r$$

définit un schéma affine de type fini $\mathcal{X}$ sur l'anneau $\mathbb{Z}$.
Pour tout anneau commutatif unitaire A, on note $\mathcal{X}(A)$ l'ensemble des solutions du système à coordonnées dans A.
Pour tout homomorphisme $A \to B$ de tels anneaux, on a une application induite $\mathcal{X}(A) \to \mathcal{X}(B)$.
Exemple : $\mathbb{Z} \to \mathbb{Z}/m$, la réduction modulo $m > 1$.

Un peu de langage : les p-adiques (Hensel)

Soit p un nombre premier. Tout rationnel $x \in \mathbb{Q}^\times$ s'écrit $x = p^{n_p}.(u/v)$ avec $n \in \mathbb{Z}$ et u, v entiers premiers à p. On définit $abs_p(x) = 1/p^{n_p} \in \mathbb{Q}$ et $abs_p(0) = 0$.

On vérifie $abs_p(xy) = abs_p(x).abs_p(y)$ et $abs_p(x+y) \leq max(abs_p(x), abs(y)) \leq abs_p(x) + abs_p(y)$.

On a donc défini une "valeur absolue" (non archimédienne) sur $\mathbb{Q}$.

De même que l'on complète le corps $\mathbb{Q}$ par rapport à la valeur absolue usuelle pour obtenir le corps $\mathbb{R}$, on peut compléter le corps $\mathbb{Q}$ par rapport à cette autre valeur absolue, on obtient le corps $\mathbb{Q}_p$ des p-adiques, sur lequel la valeur absolue ci-dessus – à valeurs dans $\mathbb{Q}$ – s'étend. Ce corps est le corps des fractions de l'anneau $\mathbb{Z}_p$ des entiers p-adiques : ce sont les éléments de $\mathbb{Q}_p$ de valeur absolue au plus 1. C'est un anneau topologique complet.

On note $\mathbb{Z}_\infty = \mathbb{Q}_\infty = \mathbb{R}$.

Traductions

"Le système $P_i(x_1, \ldots, x_n) = 0, \quad i = 1, \ldots, r$ a des solutions modulo p^r pour p premier fixé et r variable" s'écrit :

$$\mathcal{X}(\mathbb{Z}_p) \neq \emptyset.$$

"Le système $P_i(x_1, \ldots, x_n) = 0, \quad i = 1, \ldots, r$ a des solutions modulo tout entier $m > 0$ et dans $\mathbb{R}$" s'écrit :

$$\mathcal{X}(\mathbb{R}) \times \prod_p \mathcal{X}(\mathbb{Z}_p) \neq \emptyset.$$

Sous l'hypothèse que ce produit d'ensembles topologiques est non vide, on a l'approximation forte si :
L'image diagonale de $\mathcal{X}(\mathbb{Z})$ est dense dans $\prod_{p \text{ premier}} \mathcal{X}(\mathbb{Z}_p)$.

On peut définir ces notions pour tout $\mathbb{Z}$-schéma $\mathcal{X}$.
On notera $X = \mathcal{X} \times_{\mathbb{Z}} \mathbb{Q}$ le schéma défini par les mêmes équations, mais "considéré" sur les rationnels.
En particulier, on peut considérer l'approximation pour un $\mathbb{Z}$-schéma $\mathcal{X}$ projectif, c'est-à-dire un fermé de l'espace projectif $\mathbb{P}^n_{\mathbb{Z}}$, fermé défini par un système d'équations homogènes à coefficients dans $\mathbb{Z}$. Dans ce cas $\mathcal{X}(\mathbb{Z}) = X(\mathbb{Q})$ et $\mathcal{X}(\mathbb{Z}_p) = X(\mathbb{Q}_p)$.
Dans ce cas, les problèmes considérés sont des problèmes de points rationnels, et la bonne notion d'approximation est celle d'approximation faible.

L'expérience montre que la nature des réponses aux problèmes arithmétiques dépend de la géométrie des espaces associés.

On va donc étudier et discuter l'existence et la densité des points de $\mathcal{X}(\mathbb{Z})$ suivant la géométrie de $X \times_{\mathbb{Q}} \mathbb{C}$, qui est une variété algébrique sur le corps des complexes.

Le cas initialement considéré,

$$L_i(x_1, \ldots, x_n) = c_i$$

correspond à $X \times_{\mathbb{Q}} \mathbb{C}$ vide ou isomorphe à un espace affine $\mathbb{A}^s_{\mathbb{C}}$. Ainsi $ax + by = c$ avec a, b non tous deux nuls correspond à $\mathbb{A}^1_{\mathbb{C}}$, c'est-à-dire $\mathbb{P}^1_{\mathbb{C}}$ moins 1 point.

Équations en une variable

Si $x^2 + bx + c = 0$ avec $b, c \in \mathbb{Z}$ admet une solution dans chaque $\mathbb{Z}_p$, alors elle a une solution dans $\mathbb{Z}$. C'est évident par un argument de factorisation (et de signe) du discriminant.

Mais $(2x - 1)(3x - 1) = 0$ a des solutions dans tous les $\mathbb{Z}_p$ mais pas dans $\mathbb{Z}$.

On a l'énoncé plus subtil : si une équation $x^2 + bx + c = 0$ a une solution dans presque tous les $\mathbb{Z}_p$, alors elle a une solution dans $\mathbb{Z}$. Plus généralement :

Théorème (Tchebotarev). Si un polynôme $P(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n \in \mathbb{Z}[x]$ avec $n \geq 2$ est irréductible, alors il existe une infinité de premiers p tel que $P(x)$ n'a pas de solution dans $\mathbb{Q}_p$.

Mais : le polynôme $(x^2 - 13)(x^2 - 17)(x^2 - 221)$ a des solutions dans tous les $\mathbb{Z}_p$ et $\mathbb{R}$, et n'a pas de solution dans $\mathbb{Z}$.

On va maintenant se limiter à considérer des schémas (séparés !) $\mathcal{X}$ sur $\mathbb{Z}$ tels que $X \times_{\mathbb{Q}} \mathbb{C}$ soit *irréductible* – et non singulier.

Une remarque immédiate : on ne saurait avoir l'approximation forte pour un tel $\mathcal{X}$ affine si $X(\mathbb{R})$ est compact, car alors $\mathcal{X}(\mathbb{Z}) \subset X(\mathbb{R})$ est fini : $\mathbb{Z}$ est discret dans $\mathbb{R}$.
[Nous ne discuterons donc pas des points entiers de l'équation

$$(x^2 + y^2)^2 - 2n^2(x^2 - y^2) = 0.]$$

Pour p fini, $\mathcal{X}(\mathbb{Z}_p)$ est en général infini, c'est un ouvert dans $X(\mathbb{Q}_p)$ pour la topologie p-adique.

Degré 2, deux variables

Équations $ax^2 + bxy + cy^2 = d$

Géométriquement :

$\mathbb{P}^1_{\mathbb{C}}$ **moins deux points**

ou encore

$\mathbb{G}_{m,\mathbb{C}}$

n entier

Équivalence (Fermat) :

(a) Pour tout p premier, $n = x^2 + y^2$ a une solution dans $\mathbb{Z}_p$

(b) $n = x^2 + y^2$ a une solution avec $x, y \in \mathbb{Z}$

MAIS

Il y a des solutions dans tous les $\mathbb{Z}_p$ et $\mathbb{R}$ mais pas dans $\mathbb{Z}$ pour :

L'équation $23 = x(x + 7y)$ (facile, via $\mathbb{Z}^\times = \{\pm 1\}$)
Le système $\{2x - 5y = 1, xt = 1\}$ (facile, via $\mathbb{Z}^\times = \{\pm 1\}$)
($\mathbb{P}^1_{\mathbb{Q}}$ moins deux points rationnels.)

L'équation $1 = 4x^2 + 25y^2$ (facile, via compacité de $X(\mathbb{R})$)
L'équation $1 = 4x^2 - 475y^2$ (plus dur)
($\mathbb{P}^1_{\mathbb{Q}}$ moins deux points conjugués.)

q premier

Équivalents :

(a) $q \equiv 1 \bmod 3$

(b) pour tout p premier, $q = x^2 + 27y^2$ a une solution dans $\mathbb{Z}_p$

(c) l'une des deux équations

$$q = x^2 + 27y^2$$
$$q = 4x^2 + 2xy + 7y^2$$

a une solution avec $x, y \in \mathbb{Z}$

(Euler, Lagrange)

Pour q premier, l'équation $q = x^2 + 27y^2$ a une solution dans $\mathbb{Z}$ si et seulement si

(a) elle a des solutions dans tous les $\mathbb{Z}_p$

ET

(b) 2 est un cube dans $\mathbb{F}_q$.

(conjecturé par Euler, démontré par Gauß, voir le livre de D. Cox)

Degré 2, trois variables

Équations $q(x, y, z) = a$ avec $q \in \mathbb{Z}[x, y, z]$ forme quadratique non dégénérée

Géométriquement, sur $\mathbb{C}$:

Quadrique dans $\mathbb{P}^3$ moins une section hyperplane lisse

ou encore

$\mathbb{P}^1 \times \mathbb{P}^1$ moins un $\mathbb{P}^1$ diagonal

ou encore

$Spin(3)/\mathbb{G}_m$

$n \in \mathbb{Z}$
$n = x^2 + y^2 + z^2$ si et seulement si il en est ainsi sur chaque $\mathbb{Z}_p$, ce qui se ramène à $n > 0$ et $n \neq 4^r(8m + 7)$.

Mais ...

Un exemple de Borovoi et Rudnick

$-9x^2 + 2xy + 7y^2 + 2z^2 = 1$
soit encore
$(y - x)(9x + 7y) = 1 - 2z^2$

a une solution dans chaque $\mathbb{Z}_p$ mais n'a pas de solution dans $\mathbb{Z}$.
Solutions (x, y, z) sur $\mathbb{Q}$: $(-1/2, 1/2, 1)$ et $(1/3, 0, 1)$ donc solution sur chaque $\mathbb{Z}_p$.
Pour toute solution sur $\mathbb{Z}_2$, on a $y - x \equiv \pm 3 \bmod 8$.
Si solution sur $\mathbb{Z}$, si p premier divise $y - x$ alors $1 - 2z^2 \equiv 0 \bmod p$ donc p est impair et 2 carré mod p. Donc
(Zweiter Ergänzungssatz der quadratischen Reciprocität)
$p \equiv \pm 1 \bmod 8$. Donc $y - x \equiv \pm 1 \bmod 8$. Contradiction.

Soient n, m, k des entiers positifs, $(n, m) = 1$. L'équation

$$m^2x^2 + n^{2k}y^2 - nz^2 = 1$$

peut se réécrire

$$(1 + n^k y)(1 - n^k y) = m^2x^2 - nz^2.$$

Cette équation a une solution dans tout $\mathbb{Z}_p$.
En utilisant la théorie des genres (Gauß), R. Schulze-Pillot et F. Xu ont montré : Cette équation n'a pas de solution dans $\mathbb{Z}$ exactement dans les deux cas suivants :

(i) $n \equiv 5\ (8)$ et 2 divise m
ou
(ii) $n \equiv 3\ (8)$ et 4 divise m.

Degré 2, au moins 4 variables

Théorème (Eichler, Kneser)
Soit $q(x_1, \ldots, x_n)$ une forme quadratique entière *indéfinie* non dégénérée en $n \geq 4$ variables. L'équation

$$m = q(x_1, \ldots, x_n)$$

a une solution dans $\mathbb{Z}$ si et seulement si elle a une solution dans tous les $\mathbb{Z}_p$.

Ce théorème est étroitement lié au cas $G = Spin(q)$ du théorème suivant.

Théorème (Kneser, Platonov). Soit $\mathcal{X}/\mathbb{Z}$ un $\mathbb{Z}$-schéma affine irréductible tel que $\prod_{p\cup\infty} \mathcal{X}(\mathbb{Z}_p) \neq \emptyset$ et que X est $\mathbb{Q}$-isomorphe à un $\mathbb{Q}$-groupe algébrique linéaire semisimple simplement connexe presque $\mathbb{Q}$-simple et que $X(\mathbb{R}) = G(\mathbb{R})$ soit non compact. Alors l'approximation forte vaut pour $\mathcal{X}$:

$\mathcal{X}(\mathbb{Z})$ est dense dans $\prod_{p \text{ fini}} \mathcal{X}(\mathbb{Z}_p)$.

Un format général pour beaucoup des contre-exemples au principe local-global pour les points entiers :

L'obstruction de Brauer–Manin entière

Le groupe de Brauer d'un schéma

Sur une variété algébrique et plus généralement sur un schéma X, les fibrés vectoriels sont les analogues des espaces vectoriels sur un corps.
Les algèbres d'Azumaya sur un schéma sont les analogues naturels des algèbres simples centrales sur un corps.
On peut introduire une relation d'équivalence sur les algèbres d'Azumaya qui étend celle donnée pour les algèbres simples centrales sur un corps. L'ensemble des classes d'équivalence forme un groupe abélien, le groupe de Brauer $\mathrm{Br}\,(X)$ de X.
Soit X un schéma. Pour tout anneau commutatif R il y a un accouplement naturel $X(R) \times \mathrm{Br}\,(X) \to \mathrm{Br}\,(R)$.

Corps de classes local

$$\mathrm{inv}_\infty : \mathrm{Br}\,\mathbb{R} = \mathbb{Z}/2$$
$$\mathrm{inv}_p : \mathrm{Br}\,\mathbb{Q}_p \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$$

Loi de réciprocité pour le groupe de Brauer : on a une suite exacte

$$0 \to \mathrm{Br}\,\mathbb{Q} \to \oplus_{p \cup \infty} \mathrm{Br}\,\mathbb{Q}_p \to \mathbb{Q}/\mathbb{Z} \to 0.$$

Ceci généralise les lois de réciprocité quadratique de Gauß, qui donnent $0 = \sum_{p \cup \infty} (a, b)_p$ pour (a, b) une classe de quaternions.

Soit $\mathcal{X}$ un $\mathbb{Z}$-schéma.
La loi de réciprocité pour le groupe de Brauer donne :
L'image de $\mathcal{X}(\mathbb{Z})$ dans $\prod_{p\cup\infty}\mathcal{X}(\mathbb{Z}_p)$ est dans le noyau à gauche de l'accouplement (bien défini)

$$\prod_{p\cup\infty}\mathcal{X}(\mathbb{Z}_p)\times \mathrm{Br}\,(X)\to \mathbb{Q}/\mathbb{Z}$$

$$(\{M_p\},\alpha)\mapsto \sum_p \mathrm{inv}_p(\alpha(M_p)).$$

L'accouplement à droite ne dépend que de la classe dans $\mathrm{Br}\,(X)/\mathrm{Br}\,(\mathbb{Q})$.
Le noyau à gauche est noté $[\prod_{p\cup\infty}\mathcal{X}(\mathbb{Z}_p]^{\mathrm{Br}\,(X)}$.

De $\mathcal{X}(\mathbb{Z}) \subset [\prod_{p \cup \infty} \mathcal{X}(\mathbb{Z}_p)]^{\mathrm{Br}\,(\mathcal{X})}$ on conclut :

Si $[\prod_{p \cup \infty} \mathcal{X}(\mathbb{Z}_p)]^{\mathrm{Br}\,(X)} = \emptyset$, alors $\mathcal{X}(\mathbb{Z}) = \emptyset$: il n'y a pas de point entier.
Ceci est une version "entière" de l'obstruction de Brauer-Manin (1970).

Cette obstruction a été principalement étudiée lorsque $\mathcal{X}/\mathbb{Z}$ est projectif, auquel cas $\mathcal{X}(\mathbb{Z}) = X(\mathbb{Q})$ et $\mathcal{X}(\mathbb{Z}_p) = X(\mathbb{Q}_p)$: on étudie alors les points *rationnels* des variétés.

Le cas "entier" – que l'on retrouve a posteriori dans de nombreux exemples anciens – fait l'objet d'études un peu systématiques depuis 2005.

Fait 1 : Tous les contre-exemples au principe local-global pour les points entiers décrits plus haut s'expliquent en termes de l'obstruction de Brauer-Manin entière, c'est-à-dire que l'on a $[\prod_{p\cup\infty} \mathcal{X}(\mathbb{Z}_p)]^{\mathrm{Br}\,(X)} = \emptyset$.

Fait 2 : Dans un certain nombre des situations décrites ci-dessus, si pour ce "type" d'équation on a $[\prod_{p\cup\infty} \mathcal{X}(\mathbb{Z}_p)]^{\mathrm{Br}\,(X)} \neq \emptyset$, alors $\mathcal{X}(\mathbb{Z}) \neq \emptyset$, et $\mathcal{X}(\mathbb{Z})$ est dense dans le plus grand sous-ensemble de $\prod_{p\ \mathrm{fini}} \mathcal{X}(\mathbb{Z}_p)$ autorisé par la condition de Brauer-Manin.

Même les plus blasé-e-s seront peut-être amusé-e-s par le cas du $\mathbb{Z}$-schéma de dimension relative nulle $\mathcal{X}/\mathbb{Z}$ défini par :

$(x^2 - 13)(x^2 - 17)(x^2 - 221) = 0.$

L'algèbre de quaternions $A = (x, 13)$ sur X satisfait :
pour tout $M_p \in \mathcal{X}(\mathbb{Z}_p)$, on a $A(M_p) = 0 \in \mathbb{Q}/\mathbb{Z}$ si $p \neq 13$ et $A(M_{13}) = 1/2 \in \mathbb{Q}/\mathbb{Z}$.

On a donc $[\prod_p \mathcal{X}(\mathbb{Z}_p)]^{\mathrm{Br}\,(X)} = \emptyset$.

Observons que la classe $(x, 13)$ vient de $\mathrm{Br}\,\mathbb{G}_{m,\mathbb{Q}}$ où $\mathbb{G}_{m,\mathbb{Q}} = \mathrm{Spec}\,\mathbb{Q}[x, x^{-1}]$, via le plongement $\mathcal{X} \times_{\mathbb{Z}} \mathbb{Q} \hookrightarrow \mathbb{G}_{m,\mathbb{Q}}$ donné par la coordonnée x.
Ceci est une illustration d'une version torique (CT et Xu, 2010, non rédigée) d'un énoncé de M. Stoll (2006) pour les sous-schémas finis d'une variété abélienne.

Borovoi–Rudnick

$(y-x)(9x+7y) = 1-2z^2$

On utilise la classe de $A = (y-x, 2) = (9x+7y, 2)$
On vérifie $A = 0$ sur $\mathcal{X}(\mathbb{Z}_p)$ pour $p \neq 2$ et $A = 1/2$ sur $\mathcal{X}(\mathbb{Z}_2)$.

Schulze-Pillot et Xu

$$(1 + n^k y)(1 - n^k y) = m^2 x^2 - n z^2.$$

On utilise la classe de $A = (1 + n^k y, m) = (1 - n^k y, m)$.
On vérifie que A s'annule sur $\mathcal{X}(\mathbb{Z}_p)$ pour $p \neq 2$ (aussi pour $p = \infty$) , et que sur $\mathcal{X}(\mathbb{Z}_2)$ c'est constant égal à 0 ou $1/2$, et que c'est égal $1/2$ si et seulement si
(i) $n \equiv 5\ (8)$ et 2 divise m
ou
(ii) $n \equiv 3\ (8)$ et 4 divise m.
Cela explique une direction du résultat de Schulze-Pillot et Xu.

Théorème (CT-Xu 2006/2009). *Pour toute équation* $q(x,y,z) = n$ *avec* $n \in \mathbb{Z}, n \neq 0$ *et* $q(x,y,z)$ *forme quadratique entière non dégénérée sur* $\mathbb{Q}$ *et indéfinie sur* $\mathbb{R}$, $\mathcal{X}(\mathbb{Z})$ *est dense dans la projection sur* $\prod_{p \text{ fini}} \mathcal{X}(\mathbb{Z}_p)$ *de* $[\prod_{p \cup \infty} \mathcal{X}(\mathbb{Z}_p)]^{\mathrm{Br}\, X}$.

De plus $\mathrm{Br}\, X/\mathrm{Br}\,(\mathbb{Q}) = \mathbb{Z}/2$, avec un générateur calculable, ce qui donne un algorithme explicite permettant de décider si $\mathcal{X}(\mathbb{Z})$ est non vide.

On retrouve ainsi l'énoncé d'existence de solutions entières dans le théorème de Schulze-Pillot et Xu.

Les contre-exemples au principe local-global pour les points entiers des équations $q(x, y) = n$, avec q forme binaire entière non dégénérée sur $\mathbb{Q}$ mentionnés au début peuvent s'interpréter en terme de groupe de Brauer. De fait :

Théorème (cas particulier d'un résultat de D. Harari 2008, élaboration de la théorie du corps de classes).
Pour une telle équation $q(x, y) = n$, l'adhérence de $\mathcal{X}(\mathbb{Z})$ dans $\prod_\bullet \mathcal{X}(\mathbb{Z}_p)$ coïncide avec l'ensemble de Brauer-Manin $[\prod_\bullet \mathcal{X}(\mathbb{Z}_p)]^{\mathrm{Br}\,(X)}$.
($\bullet$ indique que l'on remplace les $X(\mathbb{R})$ et $X(\mathbb{C})$ par leurs composantes connexes.)

Il y a ici a priori un problème d'effectivité : le quotient $\mathrm{Br}\,(X)/\mathrm{Br}\,(\mathbb{Q})$ est infini, on aurait donc a priori une infinité de conditions à vérifier pour décider si $\mathcal{X}(\mathbb{Z}) \neq \emptyset$!

La théorie du corps de classes permet dans certains cas de se ramener à un nombre fini, explicite, de conditions. C'est ce qu'on a vu sur l'exemple $p = x^2 + 27y^2$ (Gauß).

Ces théorèmes sont englobés dans des énoncés de plus en plus généraux (CT-Xu, Harari, Demarche, Demarche-Borovoi) dont la démonstration repose sur un certain nombre de résultats classiques (principe de Hasse et approximation forte pour les groupes semi-simples simplement connexes, théorie du corps de classes) :

Théorème (Borovoi-Demarche 2011) *L'analogue des théorèmes ci-dessus vaut pour tout $\mathbb{Z}$-schéma $\mathcal{X}$ tel que X soit un espace homogène d'un $\mathbb{Q}$-groupe linéaire connexe G, à stabilisateurs géométriques connexes, sous une hypothèse de non compacité sur les points réels de G.*
(On peut même dans une certaine mesure prendre G non linéaire.)

Au-delà des espaces homogènes

Familles à un paramètre d'espaces homogènes

Quelques équations $f(x, y, z) = 0$.

Quelques équations $F(X, Y, Z) \neq 0$.

Équations $F(X, Y) \neq 0$ et courbes hyperboliques.

Et sur $\mathbb{F}_p[t]$?

Familles à un paramètre d'espaces homogènes
Avec F. Xu, en 2010/11, nous avons étudié les équations

$$q(x, y, z) = P(t)$$

avec q forme quadratique ternaire à coefficients entiers, indéfinie sur $\mathbb{R}$, et $P(t) \in \mathbb{Z}[t]$ polynôme non constant. Nous avons montré que l'obstruction de Brauer-Manin à l'approximation forte est la seule obstruction. Pour $P(t)$ irréducible, on a approximation forte.

En repenant les méthodes d'Harari (1994, 1997) pour l'étude des points *rationnels* des fibrations, on peut généraliser ceci aux fibrations en espaces homogènes sur la droite affine, sous l'hypothèse que la fibre générique a ses stabilisateurs connexes et que toutes les fibres sont géométriquement intègres. Voici un cas particulier :

Théorème (CT-Harari 2011/12) *Soient $a_i(t), i = 1, 2, 3,$ et $p(t)$ dans $\mathbb{Z}[t]$ des polynômes. Supposons le produit $p(t).\prod_i a_i(t)$ non constant et sans facteur carré dans $\mathbb{Q}[t]$. Soit $\mathcal{X}/\mathbb{Z}$ le schéma affine défini dans $\mathbb{A}^4_{\mathbb{Z}}$ par*

$$\sum_{i=0}^{2} a_i(t)x_i^2 = p(t).$$

Supposons que pour presque tout $t \in \mathbb{R}$ la conique $\sum_{i=0}^{2} a_i(t)x_i^2 = 0$ a un point dans $\mathbb{R}$. Alors le principe local-global et l'approximation forte valent pour les points entiers de $\mathcal{X}$: L'image diagonale de $\mathcal{X}(\mathbb{Z})$ est dense dans le produit $\prod_{p \text{ fini}} \mathcal{X}(\mathbb{Z}_p)$ des solutions locales entières sur tous les premiers p.
[Le cas des a_i constants est celui traité par CT-Xu (2011).]

Un problème classique

Pour n entier $n \neq \pm 4 \bmod 9$, et $\mathcal{X}_n/\mathbb{Z}$ défini par

$$x^3 + y^3 + z^3 = n$$

puis $X_n = \mathcal{X}_n \times_{\mathbb{Z}} \mathbb{Q}$, on a

$$[\prod_{p \cup \infty} \mathcal{X}_n(\mathbb{Z}_p)]^{\mathrm{Br}\,(X_n)} \neq \emptyset.$$

(CT-Wittenberg 2009/12)

Une des difficultés ici est de calculer $\mathrm{Br}\,(X)/\mathrm{Br}\,(\mathbb{Q})$. Ce n'est pas un problème purement algébrique, l'arithmétique de la courbe "à l'infini" $x^3 + y^3 + z^3 = 0$ joue un rôle.

Plusieurs auteurs ont donné des contre-exemples au principe local-global pour les points entiers d'une équation

$$x^2 + y^2 = P_1(z)P_2(z)$$

avec les polynômes $P_i(z)$ à coefficients entiers et premiers entre eux. Ces contre-exemples s'expliquent aisément au moyen de l'algèbre de quaternions $A = (P_1(z), -1) = (P_2(z), -1)$.

Voici une remarque récente de F. Gundlach (2012), étendant un argument de CT/Sansuc 1979 sur les points rationnels.
Si une équation

$$x^2 + y^2 = P(z)$$

avec $P(z) = \mathbb{Z}[z]$ polynôme irréductible de degré impair a des solutions dans tous les $\mathbb{Z}_p$, alors si on accepte l'hypothèse de Bouniakowsky, Dickson, Schinzel, eh bien l'équation a une solution avec $(x, y, z) \in \mathbb{Z}$.
Le fait que l'on ait $x^2 + y^2$ (qui n'a qu'une seule forme dans son genre) plutôt que $q(x, y)$ quadratique binaire quelconque dans le membre de gauche joue malheureusement un rôle important.

Quelques équations $F(X, Y, Z) \neq 0$.

Soit $F(x, y, z)$ un polynôme homogène à coefficients dans $\mathbb{Z}$.
Soit $\mathcal{U}$ le $\mathbb{Z}$-schéma $\mathcal{X} \subset \mathbb{P}^2_{\mathbb{Z}}$ "défini" par $F \neq 0$.
Les points entiers qui nous intéressent sont donc les triplets $(x, y, z) \in \mathbb{Z}^3$, à multiplication par une unité (c'est-à-dire ± 1) près, satisfaisant

$$F(x, y, z) = \pm 1.$$

Pour F de degré au plus 2, $U = \mathcal{U} \times_{\mathbb{Z}} \mathbb{Q}$ est "log-del Pezzo". Pour F de degré 3, on trouve un objet en quelque sorte analogue d'une surface $K3$ sur $\mathbb{Q}$. Pour F de degré au moins 4, on trouve un objet analogue d'une surface de type général sur $\mathbb{Q}$. On a ici pour les points entiers l'analogue des questions pour les points rationnels des objets analogues, avec dans certains cas des réponses, grâce au théorème du sous-espace de Schmidt.

Le contre-exemple (évident) au principe local-global $2x^2 + 2y^2 + 3z^2 = \pm 1$ s'explique à la Brauer-Manin, via l'algèbre $A = ((2x^2 + 2y^2 + 3z^2)/z^2, -1)$.

Le contre-exemple (évident) au principe local-global $2x^2 + 3y^2 + 4z^2 = \pm 1$ ne s'explique pas à la Brauer-Manin. Mais $U(\mathbb{R})$ est compact.

Le contre-exemple (non évident) au principe local-global $16x^2 + 9y^2 - 3z^2 = \pm 1$ (CT-Wittenberg) ne s'explique pas à la Brauer-Manin, mais s'explique à la Brauer-Manin étale : c'est un analogue (facile) dans le cadre des points entiers de l'exemple de Skorobogatov (1999) pour les points rationnels.
Pour $F = F_d$ de degré d, on dispose en général du revêtement fini étale de groupe μ_d donné par la surface affine d'équation $F_d(x, y, z) = 1$.

Une courbe non singulière est dite hyperbolique si sur $\mathbb{C}$ elle est de l'un des types suivants

$\mathbb{P}^1_{\mathbb{C}}$ moins au moins 3 points
Une courbe elliptique moins au moins 1 point
Un ouvert d'une courbe de genre au moins 2.
Soit $\mathcal{U}/\mathbb{Z}$ une courbe affine relative avec $U = \mathcal{U}_{\mathbb{Q}}$ courbe hyperbolique.
C'est un théorème de Siegel que l'on a $\mathcal{U}(\mathbb{Z})$ fini.

Par analogie avec des questions posées par Scharaschkin et Skorobogatov sur les courbes projectives de genre au moins 2 sur $\mathbb{Q}$, déjà objet de certains tests (crible de Mordell-Weil), pour un tel $\mathcal{U}$ (avec $U(\mathbb{R})$ non compact ?) on peut demander :

(i) Si $[\prod_p \mathcal{U}(\mathbb{Z}_p)]^{\mathrm{Br}\,(U)} \neq \emptyset$, a -t-on $\mathcal{U}(\mathbb{Z}) \neq \emptyset$?

(ii) L'image diagonale de $\mathcal{U}(\mathbb{Z})$ dans le produit $\prod_\bullet \mathcal{U}(\mathbb{Z}_p)$ coïncide-t-elle avec $[\prod_\bullet \mathcal{U}(\mathbb{Z}_p)]^{\mathrm{Br}\,(U)}$?

Il y a à ce sujet un article de Harari et Voloch (2010).

Pour U de la forme $\mathbb{P}^1$ moins trois points, c'est lié à une conjecture de Skolem.

On a un énoncé de stabilité : si l'on a un morphisme $\mathcal{U}_1 \to \mathcal{U}_2$ de telles courbes sur $\mathbb{Z}$, si l'énoncé (ii) vaut pour $\mathcal{U}_2$, alors on l'a pour $\mathcal{U}_1$ (utiliser un résultat de Stoll, convenablement généralisé pour les ouverts de $\mathbb{P}^1$).
En particulier, $\mathcal{U}_1(\mathbb{Z}) = \emptyset$ implique $[\prod_p \mathcal{U}_1(\mathbb{Z}_p)]^{\mathrm{Br}\,(U_1)} = \emptyset$.

Variante. Soit f une fonction inversible sur $\mathcal{U}$, c'est-à-dire un morphisme $\mathcal{U} \to \mathbb{G}_{m,\mathbb{Z}}$. Alors $\mathcal{U}(\mathbb{Z})$ est clairement fini, puisque $\mathbb{G}_m(\mathbb{Z}) = \pm 1$. Si $U(\mathbb{Z}) = \emptyset$, alors $[\prod_p \mathcal{U}(\mathbb{Z}_p)]^{\mathrm{Br}\,(U)} = \emptyset$.

Mais cet article de Harari-Voloch contient un contre-exemple à l'énoncé (ii) pour U la courbe affine $\mathcal{U}$ d'équation $y^2 = x^3 + 3$ (qui contient le point $x = 1, y = 2$).
La preuve utilise le fait que la courbe U est le complémentaire d'un seul point rationnel dans une courbe projective E, ce qui implique $\mathrm{Br}\,(E) = \mathrm{Br}\,(U)$.

Soit $K = \mathbb{F}_p(t)$. Soit Ω l'ensemble des valuations de K, c'est-à-dire les polynômes unitaires irréductibles et la valuation à l'infini, de complété $K_\infty = \mathbb{F}_p((1/t))$.
Pour $P \in \Omega$, soient A_P le complété de A en P, et K_P le corps des fractions.
Un cas particulier d'un théorème de Harari-Voloch (2012) dit :
Soit $\mathcal{X}$ un $\mathbb{F}_p[t]$-schéma **affine** quelconque.
Si un point

$$\{P_v\} \in X(K_\infty) \times \prod_{P \text{ fini}} \mathcal{X}(A_P)$$

est orthogonal au groupe de Brauer de X pour l'accouplement de Brauer-Manin, alors cet élément est en fait exactement l'image d'un point de $\mathcal{X}(A)$.

La démonstration utilise uniquement la p-torsion du groupe de Brauer de X.

Une question

Soient $a, b, c \in \mathbb{Z}$ avec $c.(a-b) \neq 0$. Considérons dans $\mathbb{A}^4_{\mathbb{Z}}$ avec coordonnées (x, y, z, t) le fermé $\mathcal{V}$ défini par

$$y^2 = c(z - at)(z - bt), \quad zt = x^2$$

et l'ouvert $\mathcal{U} \subset \mathcal{V}$ complémentaire de $(0, 0, 0, 0)_{\mathbb{Z}}$. La $\mathbb{Q}$-variété $U = \mathcal{U}_{\mathbb{Q}}$ est le cône sur la courbe C de genre 1 dans $\mathbb{P}^3_{\mathbb{Q}}$ définie par les mêmes équations. Peut-on avoir $\prod_{p \cup \infty} \mathcal{U}(\mathbb{Z}_p)^{\mathrm{Br}\,(U)} = \emptyset$ mais $\prod_{p \cup \infty} C(\mathbb{Q}_p)^{\mathrm{Br}\,(C)} \neq \emptyset$?

L'algèbre A définie par recollement des algèbres de quaternions
$(z - at, t) = (z - at, z) = (c(z - bt), t) = (c(z - bt), z)$
est dans $\mathrm{Br}\,(U)$ mais ne provient pas de $\mathrm{Br}\,(C)$.