Obstruction de Brauer-Manin et points entiers

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

Colloquium de l'Université de Bordeaux
21 janvier 2010

Congruences, corps locaux

Soit $f(x_1, \cdots, x_n)$ un polynôme à coefficients entiers.
On cherche des méthodes pour décider si une équation

$$f(x_1, \cdots, x_n) = 0$$

a des solutions entières.

Si f est homogène, on s'intéresse aux solutions primitives (entiers x_i premiers entre eux dans leur ensemble).

Il est parfois facile de décider qu'il n'y a pas de solutions.
Ainsi $x^2 + y^2 + 1 = 0$ n'a pas de solution dans $\mathbf{R}$, donc pas dans $\mathbf{Z}$.
On peut aussi utiliser des congruences pour voir qu'il n'y a pas de solutions.
Avec des congruences modulo 9 on voit que l'équation $x^2 + y^2 - 3z^2 = 0$ n'a pas de solution non triviale. On peut aussi le voir par des congruences modulo 4.
Soit p un nombre premier. Avec des congruences modulo p^3 on voit que l'équation

$$x^3 + py^3 + p^2z^3 = 0$$

n'a pas de solution non triviale.

Problème local-global : Si les conditions de congruence sont satisfaites modulo tout entier (et s'il y a des solutions réelles), y a-t-il des solutions entières ?

On doit à Kurt Hensel l'invention des corps locaux. A tout premier p on associe un anneau intègre $\mathbf{Z}_p$. Son corps des fractions $\mathbf{Q}_p$ est la complétion de $\mathbf{Q}$ par rapport à la métrique p-adique définie par

$$|p^n \cdot a/b|_p = 1/p^n$$

($a, b \in \mathbf{Z}$, a et b premiers à p.)
Une équation $f(x_1, \cdots, x_n) = 0$ à coefficients entiers a une solution (primitive) dans $\mathbf{Z}_p$ si et seulement si elle a une solution (primitive) modulo une puissance arbitraire de p.

Soit $X(R)$ l'ensemble des solutions de l'équation $f(x_1, \cdots, x_n) = 0$ à coordonnées dans l'anneau commutatif R. Les inclusions

$$X(\mathbf{Z}) \subset \prod_p X(\mathbf{Z}_p) \subset X(A_{\mathbf{Q}})$$

$$X(\mathbf{Q}) \subset X(A_{\mathbf{Q}}) \subset \prod_p X(\mathbf{Q}_p)$$

résument toutes les conditions de congruence (et de réalité).
Ici p est un premier ou $p = \infty$, dans ce dernier cas on pose $\mathbf{Z}_\infty = \mathbf{Q}_\infty = \mathbf{R}$. L'ensemble $X(\mathbf{Q}) \subset X(A_{\mathbf{Q}})$, l'espace des adèles, est formé des éléments entiers pour presque tout premier p.

Le théorème de Legendre

Théorème (Legendre, 1785) *Soit $q(x, y, z)$ une forme quadratique entière. Si l'équation $q(x, y, z) = 0$ a une solution non triviale dans chaque $\mathbf{Z}_p$, y compris $\mathbf{R}$, alors elle a une solution non triviale dans $\mathbf{Z}$.*

La démonstration relève de la géométrie des nombres. Elle donne une borne supérieure pour la taille de la plus petite solution.

Les diverses démonstrations n'utilisent pas toute l'hypothèse ; on peut par exemple omettre l'hypothèse $X(\mathbf{R}) \neq \emptyset$. Ainsi cette condition est imposée par l'hypothèse $X(\mathbf{Z}_p) \neq \emptyset$ pour p fini.

La loi de réciprocité quadratique (theorema fundamentale)

Soit $p \neq 2$ un premier impair, $a \in \mathbf{Z}$ premier à p,
Le symbole de Legendre $(a/p) = \pm 1$ est défini par :
$(a/p) = 1$ si et seulement si a est un carré mod. p.

Soient p, q des premiers impairs. Alors

$$(p/q)(q/p) = (-1)^{(p-1)/2.(q-1)/2}$$

Ceci fut conjecturé indépendamment par Euler et Legendre (1785).
La première d'une série de démonstrations fut trouvée par Gauß le 18 avril 1796.

Le principe de Hasse pour les formes quadratiques

Théorème (Minkowski; Hasse 1920) *Soit* $n \geq 2$. *Let* $q(x_1, \cdots, x_n)$ *une forme quadratique entière. Si l'équation*

$$q(x_1, \cdots, x_n) = 0$$

a des solutions non triviales dans tous les $\mathbf{Z}_p$ *y compris* $\mathbf{R}$, *alors elle a une solution non triviale dans* $\mathbf{Z}$.
L'argument principal dans la démonstration de Hasse se situe au passage de 3 variables (Legendre) à 4 variables. Hasse combine le théorème de Dirichlet sur les premiers dans une progression arithmétique avec la loi de réciprocité quadratique.

Voici quelques théorèmes célèbres que l'on peut considérer comme des principes locaux globaux pour les solutions en entiers des équations à coefficients entiers.
Tout premier p congru à 1 modulo 4 est une somme de deux carrés (Fermat).
L'équation $n = x^2 + y^2 + z^2$ pour n entier a une solution en entiers si elle a une solution sur $\mathbf{R}$ et sur $\mathbf{Z}_2$ (Legendre, Gauß)
L'équation $n = x^2 + y^2 + z^2 + t^2$ pour n entier a une solution en entiers si $n > 0$ (Lagrange)

Question de base : **Y a-t-il un tel théorème local-global, ou un substitut, pour d'autres familles d'équations ?**
On parle alors de "principe de Hasse".
Voici des résultats classiques dans ce sens.

Pour les points rationnels :

Les variétés projectives espaces homogènes de groupes algébriques linéaires connexes (mélange de théorie du corps de classes et de théorie des groupes algébriques linéaires, Eichler, Kneser, Harder).

Hypersurfaces projectives $F_d(x_0, \cdots, x_n) = 0$ avec n grand par rapport à d : méthode du cercle.

Pour les points entiers :

Représentation d'un entier par une forme quadratique entière *indéfinie* en au moins 4 variables (Eichler, Kneser)

Représentation d'un entier par certaines formes $F_d(x_0, \cdots, x_n)$ à coefficients entiers, avec n grand par rapport au degré d (problème de Waring, méthode du cercle).

Mais il y a beaucoup d'exemples qui montrent que le "principe de Hasse" ne vaut pas en général.

Points rationnels

Pour les points rationnels, de nombreux contre-exemples au principe de Hasse ont été construits dans la littérature.

Équations du type $\mathrm{Norm}_{K/\mathbf{Q}}(\xi) = c$ (Hasse, Witt), plus généralement espaces homogènes de groupes algébriques linéaires

Courbes de genre 1 (espaces homogènes d'une courbe elliptique) $2y^2 = x^4 - 17$ (Reichard, Lind)

Surfaces rationnelles :

Surfaces avec un pinceau de coniques $a(t)x^2 + b(t)y^2 + c(t)z^2 = 0$, par exemple (Iskovskikh) $x^2 + y^2 + (3 - t^2)(2 - t^2)z^2 = 0$.

Surfaces cubiques (Swinnerton-Dyer), surfaces cubiques diagonales (Cassels–Guy) $5x^3 + 9y^3 + 10z^3 + 12t^3 = 0$.

Points entiers

Question classique : étant donnée une forme quadratique binaire $q(x, y)$ à coefficients entiers et un entier n, y a-t-il une méthode systématique pour décider si l'équation $n = q(x, y)$ a une solution avec $x, y \in \mathbf{Z}$?

En général, les congruences ne suffisent pas.
L'équation $x(x+7y) = 23$ a des solutions dans tous les $\mathbf{Z}_p$ mais pas dans $\mathbf{Z}$.
L'équation $4x^2 + 25y^2 = 1$ a des solutions dans tous les $\mathbf{Z}_p$ mais pas dans $\mathbf{Z}$.
L'équation $13 = x^2 + 27y^2$ a des solutions dans tous les $\mathbf{Z}_p$ mais pas dans $\mathbf{Z}$.
L'équation $4x^2 - 475y^2 = 1$ a des solutions dans tous les $\mathbf{Z}_p$ mais pas dans $\mathbf{Z}$.

La non existence de points entiers se voit de façon élémentaire sur les trois premiers exemples, grâce à des arguments de divisibilité, de valeur absolue, et au fait que les seules unités dans $\mathbf{Z}$ sont ± 1.
Pour une équation $n = l(x, y).m(x, y)$, l et m linéaires, il y a un processus fini et simple, qui utilise $\mathbf{Z}^\times = \pm 1$. Que faire pour le problème analogue sur un corps de nombres ?
Et que faire pour $n = q(x, y)$ quand q est irréductible ?
Voici un théorème frappant (décrit dans le livre de Cox, Primes of the form $x^2 + ny^2$).
Pour q premier congru à 1 mod. 3, l'équation $q = x^2 + 27y^2$ a des solutions dans tous les $\mathbf{Z}_p$. Elle a a des solutions dans $\mathbf{Z}$ si et seulement si 2 est un cube dans le corps fini $\mathbf{F}_q$ (conjecturé par Euler, démontré par Gauß).]

Y a-t-il un moule commun pour tous ces contre-exemples.
Réponse (pour ceux cités) : oui !

C'est l'obstruction de Brauer–Manin au principe local-global.

Le groupe de Brauer d'un corps

Soit k un corps, $\mathrm{char}(k) = 0$, et soit $\overline{k}$ une clôture algébrique de k. Soient $a, b \in k^*$. Les relations

$$i^2 = a, j^2 = b, ij = -ji$$

définissent une k-algèbre $A = (a, b)_k$, de dimension 4 sur k. C'est une "forme tordue" de l'algèbre des matrices 2×2 :

$$A \otimes \overline{k} \simeq M_2(\overline{k}).$$

Pour $k = \mathbf{R}$, $a = b = -1$, ceci n'est autre que l'algèbre des quaternions de Hamilton.

De façon générale, une k-algèbre est appelée algèbre simple centrale s'il existe un entier $n \geq 1$ tel que

$$A \otimes_k \overline{k} \simeq M_n(\overline{k}).$$

Le produit tensoriel de deux k-algèbres centrales simples est une algèbre centrale simple.
On dit que deux telles k-algèbres sont équivalentes s'il existe des entiers $r, s \geq 1$ tels que $M_r(A) \simeq M_s(B)$. Le produit tensoriel définit alors une structure de groupe abélien sur l'ensemble des classes d'équivalence de telles algèbres. C'est le groupe de Brauer du corps k. On le note $\mathrm{Br}(k)$.

Théorie du corps de classes

Théorie du corps de classes local

$$\mathrm{Br}(\mathbf{Q}_p) \simeq \mathbf{Q}/\mathbf{Z}.$$

$$\mathrm{Br}(\mathbf{R}) = \mathbf{Z}/2$$

La suite exacte fondamentale de la théorie du corps de classes global

$$0 \to \mathrm{Br}(\mathbf{Q}) \to \bigoplus_{p \cup \infty} \mathrm{Br}(\mathbf{Q}_p) \to \mathbf{Q}/\mathbf{Z} \to 0.$$

Une conique $x^2 - ay^2 - bt^2 = 0$ sur un corps k (char.$(k) \neq 2$) a un point rationnel si et seulement si la classe de l'algèbre de quaternions $(a, b)_k \in \mathrm{Br}(k)$ est nulle.

La formule $\sum_p (a, b)_p = 0$ contient comme cas particulier la loi de réciprocité quadratique.

Le théorème de Legendre peut se reformuler ainsi : Si pour chaque premier p (fini ou infini) $(a, b)_p \in \mathbf{Z}/2 \subset \mathrm{Br}(\mathbf{Q}_p)$ s'annule, alors $(a, b) = 0 \in \mathrm{Br}(\mathbf{Q})$.

De l'égalité $\sum_p (a,b)_p = 0$ on voit que l'annulation de $(a,b)_p$ pour tous les p (fini ou infini) *sauf peut-être un* suffit à assurer l'annulation de tous et $(a,b) = 0 \in \mathrm{Br}(\mathbf{Q})$.

Outre le théorème de Dirichlet sur les premiers dans une progression arithmétique, ceci est l'autre ingrédient dans la démonstration de Hasse de son principe sur les formes quadratiques à 4 variables à partir du cas des formes à 3 variables.

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 $X(R) \times \mathrm{Br}(X) \to \mathrm{Br}(R)$.

La condition de Brauer-Manin

Théorème (Manin, 1970). *Soit X une variété projective sur $\mathbf{Q}$. L'image de $X(\mathbf{Q})$ dans $X(A_{\mathbf{Q}}) = \prod_p X(\mathbf{Q}_p)$ est dans le noyau à gauche de l'accouplement (bien défini)*

$$X(A_{\mathbf{Q}}) \times \mathrm{Br}(X) \to \mathbf{Q}/\mathbf{Z}$$

$$(\{M_p\}, \alpha) \mapsto \sum_p \mathrm{ev}_A(M_p).$$

On note $X(A_{\mathbf{Q}})^{\mathrm{Br}(X)}$ ce noyau.

Variante entière :

Théorème *Soit X un $\mathbf{Z}$-schéma de type fini. L'image de $X(\mathbf{Z})$ dans $\prod_p X(\mathbf{Z}_p)$ est dans le noyau à gauche de l'accouplement (bien défini)*

$$\prod_p X(\mathbf{Z}_p) \times \mathrm{Br}(X_{\mathbf{Q}}) \to \mathbf{Q}/\mathbf{Z}$$

$$(\{M_p\}, \alpha) \mapsto \sum_p \mathrm{ev}_A(M_p).$$

On note ce noyau $(\prod_p X(\mathbf{Z}_p))^{\mathrm{Br}(X_{\mathbf{Q}})}$.
On notera que l'accouplement est fait avec $\mathrm{Br}(X_{\mathbf{Q}})$.
L'accouplement plus naturel avec $\mathrm{Br}(X)$ donnerait moins d'information.

Un grand nombre de contre-exemples numériques au principe de Hasse *pour les points rationnels* relèvent du cadre proposé par Manin.

On cherche alors des classes de variétés algébriques projectives et lisses sur $\mathbf{Q}$ pour lesquelles l'obstruction de Brauer–Manin *pour les points rationnels* est la seule, i.e. pour X dans la classe, on a l'implication

$$X(A_{\mathbf{Q}})^{\mathrm{Br}(X)} \neq \emptyset \Longrightarrow X(\mathbf{Q}) \neq \emptyset$$

Question subsidiaire : comment décider si $X(A_{\mathbf{Q}})^{\mathrm{Br}(X)} \neq \emptyset$?

$X(A_{\mathbf{Q}})^{\mathrm{Br}(X)} \neq \emptyset \Longrightarrow X(\mathbf{Q}) \neq \emptyset$ pour :

les variétés dont un ouvert est un espace homogène d'un groupe algébrique linéaire connexe, avec isotropie géométrique connexe (Sansuc 1981; Borovoi 1996)

les surfaces fibrées en coniques avec au plus 4 mauvaises fibres, par exemple $y^2 - az^2 = P(x)$ avec $P(x)$ de degré 4 (CT, Sansuc, Swinnerton-Dyer 1987)

les intersections lisses de deux quadriques dans $\mathbf{P}^n$, $n \geq 8$ (CT, Sansuc, Swinnerton-Dyer 1987)

$X(A_{\mathbf{Q}})^{\mathrm{Br}(X)} \neq \emptyset \Longrightarrow X(\mathbf{Q}) \neq \emptyset$

modulo la finitude des groupes de Tate-Shafarevich pour :
Courbes de genre 1 (Manin 1970)
Courbes de genre plus grand que 1, dans certains cas (Scharashkin)
Beaucoup de surfaces cubiques diagonales sur $\mathbf{Q}$ (Swinnerton-Dyer 2000)

modulo l'hypothèse de Schinzel pour :
Surfaces fibrées en coniques sur $\mathbf{P}^1$ (CT, Sansuc, Serre, Swinnerton-Dyer)

modulo la finitude des groupes de Tate-Shafarevich et l'hypothèse de Schinzel pour :
Certains types de surfaces fibrées en courbes de genre 1, y compris des surfaces K3 (CT, Skorobogatov, Swinnerton-Dyer 1998)
Intersections lisses de deux quadriques dans $\mathbf{P}^n$, $n \geq 4$ (Wittenberg 2007)

On a aussi des expérimentations numériques pour

Surfaces cubiques diagonales (CT, Kanevsky, Sansuc 1987; ...)

Courbes de genre 2 (Bruin et Stoll 2008)
[Pour les courbes de genre au moins 2 sur un corps de fonctions d'une variable sur un corps fini, on a un théorème presque général (Poonen et Voloch 2008)]

Surfaces K3, en particulier les quartiques diagonales

Cependant : il existe des contre-exemples au principe de Hasse pour les points rationnels que l'on ne peut expliquer uniquement avec le groupe de Brauer.

Exemple de Skorobogatov (1999)
La méthode a été analysée (Harari, Skorobogatov, Demarche)
En un mot : on utilise des revêtements non ramifiés galoisiens, de groupe non commutatif

Exemple de Poonen (2009) (nouveau type)

Dans le reste de l'exposé, nous allons discuter ce que l'on peut faire du côté des points entiers

La version entière de l'obstruction de Brauer-Manin : une famille d'exemples

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

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

F. Xu et R. Schulze-Pillot ont étudié les solutions entières de cette équation. Soit $X/\mathbf{Z}$ le schéma que cette équation définit.
On vérifie $\prod_{p\cup\infty} X(\mathbf{Z}_p) \neq \emptyset$. Soit $U_{\mathbf{Q}} \subset X_{\mathbf{Q}}$ l'ouvert défini par $1 + n^k y \neq 0$. Fait : L'algèbre d'Azumaya $(1 + n^k y, n) \in \mathrm{Br}(U_{\mathbf{Q}})$ s'étend à $A \in \mathrm{Br}(X_{\mathbf{Q}})$.

Pour $p \neq 2$, l'image de $ev_A : X(\mathbf{Z}_p) \to \mathrm{Br}(\mathbf{Q}_p) \subset \mathbf{Q}/\mathbf{Z}$ est nulle.
Pour $p = 2$, l'image de cette application coïncide avec
$\{1/2\} \subset \mathbf{Q}/\mathbf{Z}$ si et seulement si
(i) 2 divise exactement m et $n \equiv 5\ (8)$
ou
(ii) 4 divise m et $n \equiv 3 \ \text{or} \ 5\ (8)$
Ainsi $X(\mathbf{Z}) = \emptyset$ dans les cas (i) et (ii).

En utilisant la théorie des genres, F. Xu et R. Schulze-Pillot (2004) ont montré :

Théorème *Dans tous les autres cas* $X(\mathbf{Z}) \neq \emptyset$.

Quelle est la généralité de ce théorème ?

Y a-t-il des classes de schémas de type fini sur $\mathbf{Z}$ pour lesquelles l'obstruction de Brauer–Manin pour les points entiers est la seule, i.e. pour X dans la classe, on a

$$(\prod_p X(\mathbf{Z}_p))^{\mathrm{Br}(X_{\mathbf{Q}})} \neq \emptyset \Longrightarrow X(\mathbf{Z}) \neq \emptyset$$

$\mathbf{P}^1$ moins un point

Un résultat presque trivial :

Soient $a, b, c \in \mathbf{Z}$ non tous nuls. Si la $\mathbf{Z}$-courbe X définie par l'équation $ax + by = c$ a des solutions dans tous les $\mathbf{Z}_p$, alors elle a des solutions dans $\mathbf{Z}$.

On a $X_{\mathbf{Q}} \simeq \mathbf{P}^1_{\mathbf{Q}} \setminus \{\infty\}$. Donc $\mathrm{Br}(X_{\mathbf{Q}})/\mathrm{Br}(\mathbf{Q}) = 0$ ne saurait créer d'obstruction !

On a mieux. Le théorème d'approximation forte (reste chinois) implique : $X(\mathbf{Z})$ *est dense dans* $\prod_{p<\infty} X(\mathbf{Z}_p)$
(Noter qu'on omet ici les réels.)

$\mathbf{P}^1$ moins deux points

La $\mathbf{Z}$-courbe X définie par

$$2x - 5y = 1, xt = 1$$

a des solutions dans tous les $\mathbf{Z}_p$ mais pas dans $\mathbf{Z}$.
On a $X_{\mathbf{Q}} \simeq \mathbf{P}^1_{\mathbf{Q}} \setminus \{0, \infty\}$. Donc $\mathrm{Br}(X_{\mathbf{Q}})/\mathrm{Br}(\mathbf{Q}) = H^1(\mathbf{Q}, \mathbf{Q}/\mathbf{Z})$.
Il y a une obstruction de Brauer-Manin attachée à l'algèbre de quaternions $(x, 5) \in \mathrm{Br}(X_{\mathbf{Q}})$.

La théorie du corps de classes donne (de façon pas tout à fait immédiate)

Théorème *Soit X un $\mathbf{Z}$-schéma de type fini. Si $X_{\mathbf{Q}} \simeq \mathbf{P}^1_{\mathbf{Q}} \setminus \{0, \infty\}$, alors*

$$(\prod_p X(\mathbf{Z}_p))^{\mathrm{Br}(X_{\mathbf{Q}})} \neq \emptyset \Longrightarrow X(\mathbf{Z}) \neq \emptyset.$$

Plus généralement, ceci vaut (D. Harari) si $X_{\mathbf{Q}}$ sur une clôture algébrique de $\mathbf{Q}$ est isomorphe à $\mathbf{P}^1$ moins deux points.
En particulier, ceci vaut pour les équations du type

$$a = q(x, y)$$

avec $a \in \mathbf{Z}$ et $q(x, y)$ une forme quadratique binaire à coefficients dans $\mathbf{Z}$.

Problème : le groupe de Brauer $\mathrm{Br}(X_{\mathbf{Q}})/\mathrm{Br}(\mathbf{Q}))$ est infini !

Pour un $X/\mathbf{Z}$ donné par une équation $a = q(x, y)$, il n'est donc pas clair comment décider si $(\prod_p X(\mathbf{Z}_p))^{\mathrm{Br}(X_{\mathbf{Q}})} \neq \emptyset$.

Il y a cependant des résultats partiels dans cette direction (Fei, Wei) généralisant des résultats comme celui de Gauß sur $p = x^2 + 27y^2$ (résultat que Cox explique du point de vue de la théorie du corps de classes et de la multiplication complexe).

La situation est nettement meilleure lorsque l'on considère la représentation d'un entier par une forme quadratique entière q, non dégénérée sur $\mathbf{Q}$, en $n \geq 3$ variables, si l'on suppose la forme q indéfinie sur $\mathbf{R}$.
Soit X le $\mathbf{Z}$-schéma défini par $a = q(x_1, \ldots, x_n)$.
Pour $n = 3$, on a $\mathrm{Br}(X_{\mathbf{Q}})/\mathrm{Br}(\mathbf{Q})) \subset \mathbf{Z}/2$, et pour $n \geq 4$, on a $\mathrm{Br}(X_{\mathbf{Q}})/\mathrm{Br}(\mathbf{Q})) = 0$.

Théorème *Soit $q(x_1, \cdots, x_n)$ une forme quadratique entière de rang n, indéfinie sur $\mathbf{R}$, et soit $a \in \mathbf{Z}$, $a \neq 0$. Soit $X/\mathbf{Z}$ le $\mathbf{Z}$-schéma défini par $q(x_1, \cdots, x_n) = a$. Supposons $\prod_p X(\mathbf{Z}_p) \neq \emptyset$.*
(a) Si $n \geq 4$, alors $X(\mathbf{Z}) \neq \emptyset$: on peut résoudre l'équation $q(x_1, \cdots, x_n) = a$ in $\mathbf{Z}$.
(b) Supposons $n = 3$ et $-a \cdot det(q)$ non carré. Alors $\mathrm{Br}(X_{\mathbf{Q}})/\mathrm{Br}(\mathbf{Q}) = \mathbf{Z}/2$. Soit $A \in \mathrm{Br}(X_{\mathbf{Q}})$ un élément engendrant ce quotient. On a $X(\mathbf{Z}) \neq \emptyset$ si et seulement si l'application

$$\prod_p X(\mathbf{Z}_p) \to \mathbf{Q}/\mathbf{Z}$$

$$\{M_p\} \mapsto \sum_p \mathrm{ev}_A(M_p)$$

contient zéro dans son image.

Le théorème (a) remonte aux années 1950 (Eichler, Kneser, Watson).
Le théorème (b) est une variante (CT/F. Xu, 2005) d'un résultat de Borovoi et Rudnick (1995).
Les points principaux de la démonstration de (b) sont :
– l'approximation forte pour le groupe des spineurs d'une forme quadratique indéfinie
– la représentation d'une surface quadrique affine $q = a$ sur $\mathbf{Q}$, avec un point $\mathbf{Q}$-rationnel, comme un quotient G/T, où G est le groupe des spineurs de q et T est un tore algébrique de dimension 1 sur $\mathbf{Q}$.

Dans le cas $n = 3$, on peut expliciter l'algèbre A. Soit M un point $\mathbf{Q}$-rationnel sur

$$q(x, y, z) = a.$$

(Denis Simon a un algorithme pour trouver un tel point). Soit $l(x, y, z) = 0$ l'équation du plan tangent à la quadrique affine $X_{\mathbf{Q}}$ au point M.
Pour A on peut prendre l'algèbre de quaternions

$$A = (l(x, y, z), -a \cdot det(q)).$$

On obtient ainsi une autre démonstration du théorème de F. Xu et Schulze-Pillot, par une méthode qui s'applique à toute équation $a = q(x, y, z)$ avec q indéfinie.

Les résultats ci-dessus sur la représentation d'un entier par une forme quadratique se généralisent. On considère un $\mathbf{Z}$-schéma X tel que $X_{\mathbf{Q}} \simeq G/H$ avec G et H groupes linéaires connexes sur $\mathbf{Q}$. Sous une hypothèse de non compacité pour le groupe dérivé de G, on a le théorème (2005/2009)

$$(\prod_p X(\mathbf{Z}_p))^{\mathrm{Br}(X_{\mathbf{Q}})} \neq \emptyset \Longrightarrow X(\mathbf{Z}) \neq \emptyset.$$

(CT/Xu, Harari, Demarche, Borovoi/Demarche)

Et quand il n'y pas de structure d'espace homogène ?

L'équation $a = x^3 + y^3 + z^3$, avec $a \in \mathbf{Z}$ non nul. Cette équation a des solutions avec $x, y, z \in \mathbf{Q}$.
Pour a de la forme $9n \pm 4$ avec $n \in \mathbf{Z}$, elle n'a pas de solutions avec $x, y, z \in \mathbf{Z}$.
Question classique : si a n'est pas de la forme $9n \pm 4$, cette équation a-t-elle une solution avec $x, y, z \in \mathbf{Z}$?

Théorème (CT/Wittenberg 2009) *Soit X_a le $\mathbf{Z}$-schéma défini par $x^3 + y^3 + z^3 = a$. Si $a \neq 9n \pm 4$, alors*

$$(\prod_p X_a(\mathbf{Z}_p))^{\mathrm{Br}(X_{a,\mathbf{Q}})} \neq \emptyset.$$

En d'autres termes, aucune loi de réciprocité ne saurait empêcher l'existence d'une solution en entiers.

Pour établir un tel résultat, il faut connaître le groupe $\mathrm{Br}(X_{a,\mathbf{Q}})$.
Notons $X^c_{a,\mathbf{Q}} \subset \mathbf{P}^3_{\mathbf{Q}}$ la surface cubique d'équation homogène $x^3 + y^3 + z^3 = at^3$ et E la courbe elliptique sur $\mathbf{Q}$ d'équation $x^3 + y^3 + z^3 = 0$, complémentaire de $X_{a,\mathbf{Q}}$ dans $X^c_{a,\mathbf{Q}}$.
On a une suite exacte

$$0 \to \mathrm{Br}(X^c_{a,\mathbf{Q}}) \to \mathrm{Br}(X_{a,\mathbf{Q}}) \to H^1(E, \mathbf{Q}/\mathbf{Z}).$$

Le dernier groupe classifie les revêtements cycliques non ramifiés de E.
On peut supposer a non cube. Un calcul algébrique donne $\mathrm{Br}(X^c_{a,\mathbf{Q}})/\mathrm{Br}(\mathbf{Q}) = \mathbf{Z}/3$, avec un générateur explicite $\beta \in \mathrm{Br}(X^c_{a,\mathbf{Q}})$, d'ordre 3.

Par un argument algébrique on montre que l'image de $\mathrm{Br}(X_{a,\mathbf{Q}}) \to H^1(E, \mathbf{Q}/\mathbf{Z})$ est constituée de classes qui s'annulent en chacun des points $(1,-1,0)$, $(0,1,-1)$, $(1,0,-1)$.

On fait ensuite intervenir l'arithmétique de la courbe elliptique E sur $\mathbf{Q}$ (connaissance de toutes les courbes isogènes) pour montrer qu'une telle classe est forcément nulle. Ainsi $\mathrm{Br}(X^c_{a,\mathbf{Q}}) = \mathrm{Br}(X_{a,\mathbf{Q}})$.

On montre enfin que pour tout $a \in \mathbf{Z}$ non cube et non de la forme $9n \pm 4$ il existe un premier p tel que β prenne trois valeurs distinctes sur $X_a(\mathbf{Z}_p)$.

C'est une question ouverte si tout entier peut s'écrire sous la forme $x^3 + y^3 + 2z^3$, avec $x, y, z \in \mathbf{Z}$.

Théorème (CT/Wittenberg)
Soit $a \in \mathbf{Z}$ non nul. Soit Y_a le $\mathbf{Z}$-schéma défini par $x^3 + y^3 + 2z^3 = a$, avec $a \neq 0$.
Alors

$$(\prod_p Y_a(\mathbf{Z}_p))^{\mathrm{Br}(X_{a,\mathbf{Q}})} \neq \emptyset.$$

En d'autre termes, aucune loi de réciprocité ne saurait empêcher l'existence d'une solution en entiers.

La démonstration est plus délicate, car la restriction $\mathrm{Br}(Y^c_{a,\mathbf{Q}}) \to \mathrm{Br}(Y_{a,\mathbf{Q}})$ n'est ici pas surjective. On a $\mathrm{Br}(Y_{a,\mathbf{Q}})/\mathrm{Br}(\mathbf{Q}) \simeq \mathbf{Z}/3 \oplus \mathbf{Z}/2$, et l'on explicite des générateurs.

Courbes hyperboliques

Conjecture (Harari et Voloch 2009)
Soit X un $\mathbf{Z}$-schéma tel que $X_{\mathbf{Q}}$ soit le complémentaire dans $\mathbf{P}^1$ d'au moins trois points.
Si l'ensemble $\prod_p X(\mathbf{Z}_p))^{\mathrm{Br}(X_{a,\mathbf{Q}})}$ est non vide, alors $X(\mathbf{Z}) \neq \emptyset$.

On peut formuler la question de façon un peu plus générale.
Elle est alors liée à une question de T. Skolem sur les équations exponentielles (1937).
Soit S un ensemble fini de nombres premiers $p_i, i = 1, \cdots, n$. Soit $R \subset \mathbf{Q}^*$ le sous-groupe engendré par les p_i.
Soient a_1, a_2, a_3 des éléments de R.
L'équation $\sum_{i=1}^{3} a_i x_i = 0$ a des solutions avec les $x_i \in R$ si et seulement si pour tout entier m premier à S, l'équation $\sum_{i=1}^{3} a_i x_i = 0 \ \ mod\ m$ a une solution avec les $x_i \in R$.

Un exemple (Harari et Voloch 2009)
Soit X le $\mathbf{Z}$-schéma défini par $y^2 = x^3 + 3$.
$X_{\mathbf{Q}}$ est la courbe hyperbolique complémentaire du zéro de la courbe elliptique d'équation homogène $Y^2T = X^3 + 3T^3$.
Les seuls point entiers de X sont les points M et N avec $(x, y) = (1, 2)$ et $(x, y) = (1, -2)$.
Soit p_n une suite de nombres premiers congrus à 3 modulo 8.
De la suite $\{p_n.M\} \in \prod_p E(\mathbf{Q}_p)$ on extrait une sous-suite convergente vers une famille $\{R_p\}$. On vérifie que chaque R_p est dans $X(\mathbf{Z}_p)$, et que R_2 est différent de M et de N.
Mais la famille $\{R_p\}$ est orthogonale à $\mathrm{Br}(X_{\mathbf{Q}})$.
Ainsi $X(\mathbf{Z})$ n'est pas dense dans $\prod_p X(\mathbf{Z}_p))^{\mathrm{Br}(X_{a,\mathbf{Q}})}$.

Bonus : Le langage classique pour les formes quadratiques (Eichler, Kneser)

Soient $f(x_1, \ldots, x_n)$ et $g(y_1, \ldots, y_m)$ des formes quadratiques sur $\mathbf{Z}$ comme plus haut, $1 \leq n < m$ avec $m \geq 3$.
On cherche à trouver des formes linéaires
$l_i(x_1, \ldots, x_n), i = 1, \ldots, m$ telles que

$$g(x_1, \ldots, x_n) = f(l_1(x_1, \ldots, x_n), \ldots, l_m(x_1, \ldots, x_n)).$$

Ceci définit un schéma $X = X(g, f)/\mathbf{Z}$, dont on suppose qu'il a des points sur chaque $\mathbf{Z}_l$ et dont on demande s'il a des points sur $\mathbf{Z}$.
On associe classiquement à f et g des réseaux quadratiques (Gitter) N et M dans un vectoriel fixe.
Soit $X = X(f, g)/\mathbf{Z}$.

Das Gitter N wird von der Klasse des Gitters M dargestellt.
(Le réseau quadratique N est représenté par la classe du réseau quadratique M)

Traduction :

$X(\mathbf{Z}) \neq \emptyset$

Das Gitter N wird von dem Geschlecht des Gitters M dargestellt.
(Le réseau quadratique N est représenté par le genre du réseau quadratique M)

Traduction :

$\prod_v X(\mathbf{Z}_v) \neq \emptyset$

Das Gitter N wird von dem Spinorgeschlecht des Gitters M dargestellt.
(Le réseau quadratique N est représenté par le genre spinoriel du réseau quadratique M)

Traduction :

$(\prod_v X(\mathbf{Z}_v))^{\mathrm{Br} X_{\mathbf{Q}}} \neq \emptyset$

Supposons $m - n = 2$ et $-\mathrm{disc}(f).\mathrm{disc}(g)$ non carré.

Ein Gitter N, das zwar von dem Geschlecht von M dargestellt ist, nicht aber von allen Spinorgschlechtern im Geschlecht von M dargestellt wird, nennt man eine Spinorausnahme.
(Un réseau N représenté par le genre de M est appelé une exception spinorielle pour le genre de M s'il existe un genre spinoriel dans le genre de M tel qu'aucun réseau dans ce genre spinoriel ne représente M.)

Traduction

Soit $A \in \mathrm{Br}X_{\mathbf{Q}}$ engendrant $\mathrm{Br}X_{\mathbf{Q}}/\mathrm{Br}\mathbf{Q} = \mathbf{Z}/2$. Alors pour chaque premier p, A ne prend qu'une seule valeur sur $X(\mathbf{Z}_p)$.