Lois de réciprocité et solutions d'équations polynomiales

Jean-Louis Colliot-Thélène
CNRS, Université Paris-Sud
Barcelone, 26 Janvier 2007

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.

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.

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. On a les inclusions naturelles

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

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

Ici p est un premier ou $p = \infty$, dans ce dernier cas on pose $\mathbf{Z}_\infty = \mathbf{Q}_\infty = \mathbf{R}$.
Il y a un plongement plus précis

$$X(\mathbf{Q}) \subset X(A_\mathbf{Q}),$$

où $X(A_\mathbf{Q}) \subset \prod_p X(\mathbf{Q}_p)$ est l'ensemble des adèles of X.

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.

Soit p un premier impair.
Première loi complémentaire

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

Ainsi : -1 est un carré modulo p si et seulement si $p \equiv 1(4)$.

Deuxième loi complémentaire

$$(2/p) = (-1)^{(p^2-1)/8}$$

Ainsi : 2 est un carré modulo p si et seulement si $p \equiv \pm 1(8)$.

Le principe de Hasse pour les formes quadratique

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. En ce point Hasse a recours au théorème de Dirichlet sur les premiers dans une progression arithmétique.

Question de base : **Y a-t-il un tel théorème local-global, ou un substitut, pour d'autres familles d'équations ?**

Il y a une méthode, la méthode du cercle (Hardy, Littlewood) qui donne de tels résultats.
La plupart des résultats portent sur des formes homogènes dont le nombre de variables est grand par rapport au degré.
Un résultat excellent dans cette direction est le théorème suivant, obtenu par une amélioration d'un résultat de Heath-Brown (cas de 10 variables) :

Théorème (C. Hooley) *Le principe de Hasse vaut pour les formes cubiques non singulières en au moins 9 variables sur* $\mathbf{Q}$.

On comparera ce résultat avec le problème ouvert bien connu : le principe de Hasse vaut-il pour les formes cubiques non singulières en au moins 5 variables ?

Il y a beaucoup d'exemples qui montrent que le "principe de Hasse" ne vaut pas en général. Je vais en décrire quelques-uns.

L'exemple de Lind (1940)
Il y a une courbe de genre 1 sur $\mathbf{Q}$ qui a des points dans tous les $\mathbf{Q}_p$ et $\mathbf{R}$, et qui n'a pas de point dans $\mathbf{Q}$.

$$2y^2 = x^4 - 17, \quad x, y \in \mathbf{Q}$$

$$2u^2 = v^4 - 17w^4 \neq 0, \quad u, v, w \in \mathbf{Z}, \quad (v, w) = 1$$

Par réduction modulo 17^2, on voit que u n'est pas divisible par 17.
Comme 2 n'est pas une puissance quatrième modulo 17, ceci implique : *u n'est pas un carré modulo 17*.
Si p est un premier impair qui divise u (et donc $p \neq 17$), alors 17 est un carré modulo p, donc (loi de réciprocité quadratique) p est un carré modulo 17. Puisque 2 est aussi un carré modulo 17, on conclut : *u est un carré modulo 17*.
Contradiction, $X(\mathbf{Q}) = \emptyset$.

L'exemple d' Iskovskikh (1971)

C'est une surface "rationnelle" qui a des points dans tous les $\mathbf{Q}_p$ et dans $\mathbf{R}$ mais qui n'a pas de points dans $\mathbf{Q}$.

$$y^2 + z^2 = (3 - x^2)(x^2 - 2)$$

Solution avec $x, y, z \in \mathbf{Q}$?

$$u^2 + v^2 = (3y^2 - x^2)(x^2 - 2y^2) \neq 0,$$

avec $u, v, x, y \in \mathbf{Z}, (x, y) = 1$, donc $(3y^2 - x^2, x^2 - 2y^2) = 1$
Modulo 4, le couple $(3y^2 - x^2, x^2 - 2y^2)$ prend l'une des valeurs suivantes :

$$(2, -1), (-1, 1), (3, 2)$$

Dans $\mathbf{R}$ on a $3y^2 - x^2 > 0, \;\; x^2 - 2y^2 > 0.$

$$u^2 + v^2 = (3y^2 - x^2)(x^2 - 2y^2) \neq 0,$$

Soit p un premier impair. Si p^{2n+1} divise exactement soit $3y^2 - x^2$ soit $x^2 - 2y^2$, alors p^{2n+1} divise exactement $u^2 + v^2$, ainsi -1 is est un carré mod. p, donc (première loi complémentaire) $p \equiv 1$ mod. 4.
Ainsi le couple $(3y^2 - x^2, x^2 - 2y^2)$ prend l'une des valeurs suivantes modulo 4 :

$$(1, 1), (2, 1), (1, 2)$$

donc aucune des précédentes valeurs

$$(2, -1), (-1, 1), (3, 2)$$

Contradiction, $X(\mathbf{Q}) = \emptyset$.

Un exemple en entiers de Borovoi et Rudnick (1995)
Considérons l'équation sur $\mathbf{Z}$:

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

soit

$$(x - y)^2 + 8(x - y)(x + y) = 2z^2 - 1$$

Solution dans $\mathbf{Q}$

$$(x, y, z) = (-1/2, 1/2, 1)$$

donc solutions dans tous les $\mathbf{Z}_p$ pour $p \neq 2$.

Solution dans $\mathbf{Z}_2$, en utilisant $q(4, 1, 1) = -127 \equiv 1(8)$.

$$(x-y)^2 + 8(x-y)(x+y) = 2z^2 - 1$$

Solution avec $(x, y, z) \in \mathbf{Z}$?

Si on étudie l'équation modulo des puissances de 2, on trouve

$$x - y \equiv \pm 3 \, (8)$$

Soit p un premier.
Si p divise $x - y$, alors p divise $2z^2 - 1$.
Ainsi p est impair et 2 est un carré mod. p
(deuxième loi complémentaire) $\Longrightarrow p \equiv \pm 1(8)$.
Ainsi $x - y \equiv \pm 1 \, (8)$.
Contradiction, $X(\mathbf{Z}) = \emptyset$.

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 particuliers la loi de réciprocité quadratique et les deux lois complémentaires.

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 un suffit à assurer $(a, b) = 0 \in \mathrm{Br}(\mathbf{Q})$.

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.

L'exemple de Lind du point de vue de l'obstruction de Brauer-Manin

L'équation

$$2y^2 = x^4 - 17 \neq 0$$

définit un ouvert U d'une courbe projective lisse $X/\mathbf{Q}$.

On a $\prod_{p \cup \infty} X(\mathbf{Q}_p) \neq \emptyset$.

Fait : L'algèbre d'Azumaya $(y, 17) \in \mathrm{Br}(U)$ s'étend en une algèbre d'Azumaya $A \in \mathrm{Br}(X)$.

Pour $p \neq 17$ l'image de $ev_A : X(\mathbf{Q}_p) \to \mathrm{Br}(\mathbf{Q}_p) \subset \mathbf{Q}/\mathbf{Z}$ est nulle si $p \neq 17$.

Pour $p = 17$ l'image de $ev_A : X(\mathbf{Q}_{17}) \to \mathrm{Br}(\mathbf{Q}_{17}) \subset \mathbf{Q}/\mathbf{Z}$ est $\{1/2\} \subset \mathbf{Q}/\mathbf{Z}$.

Donc $X(\mathbf{Q}) = \emptyset$.

L'exemple d'Iskovskikh du point de vue de l'obstruction de Brauer-Manin

Soit $c \in \mathbf{Z}, c > 0, c$ impair. L'équation

$$y^2 + z^2 = (c - x^2)(x^2 - c + 1) \neq 0$$

définit un ouvert U_c dans une surface projective lisse $X_c/\mathbf{Q}$.
On a $\prod_{p \cup \infty} X_c(\mathbf{Q}_p) \neq \emptyset$.
L'algèbre d'Azumaya $(c - x^2, -1) \in \mathrm{Br}(U_c)$ s'étend en $A \in \mathrm{Br}(X_c)$.

$$y^2 + z^2 = (c - x^2)(x^2 - c + 1) \neq 0$$

Pour $p \neq 2$, l'image de

$$ev_A : X_c(\mathbf{Q}_p) \to \mathrm{Br}(\mathbf{Q}_p) \subset \mathbf{Q}/\mathbf{Z}$$

est nulle.
Pour $p = 2$, cette image est $\{1/2\} \subset \mathbf{Q}/\mathbf{Z}$ si et seulement si $c \equiv 3(4)$.
Ainsi : *Si* $c \equiv 3(4)$, *alors* $X_c(A_{\mathbf{Q}})^{\mathrm{Br}(X)} = \emptyset$, *et donc* $X_c(\mathbf{Q}) = \emptyset$.
Le même calcul montre : *Si* $c \equiv 1(4)$, *alors* $X_c(A_{\mathbf{Q}})^{\mathrm{Br}(X)} \neq \emptyset$.
Théorème *Si* $c \equiv 1(4)$ *alors* $X_c(\mathbf{Q}) \neq \emptyset$.
(cas particulier d'un théorème de CT, Coray et Sansuc, 1981)

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) and (ii).

Théorème (F. Xu et R. Schulze-Pillot, 2004). *Dans tous les autres cas* $X(\mathbf{Z}) \neq \emptyset$.

Le résultat général suivant fournit une démonstration de ce résultat qui évite la théorie des genres.

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 $\mathbf{Q}$.

On peut expliciter l'algèbre A. Soit M un point $\mathbf{Q}$-rationnel sur

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

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

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

Espaces homogènes de groupes algébriques linéaires

Une longue série de travaux a établi le principe de Hasse pour les espaces homogènes principaux des groupes linéaires semisimples et simplement connexes (Hasse, Landherr, Eichler, Kneser, Harder, Chernousov).
Une conséquence est la généralisation suivante du théorème de Minkowski-Hasse :
Théorème (Harder, 1970) *Soit $X/\mathbf{Q}$ une variété projective qui est un espace homogène d'un groupe linéaire connexe. Le principe de Hasse vaut pour X.*

Une autre conséquence est

Théorème *Soit $X/\mathbf{Q}$ une variété projective lisse connexe. Supposons qu'il existe un ouvert non vide $U \subset X$ qui est un espace homogène d'un groupe linéaire connexe, les groupes d'isotropie géométriques étant connexes.*

Alors $X(\mathbf{Q})$ est dense dans $X(A_{\mathbf{Q}})^{\mathrm{Br}(X)}$.

En particulier $X(A_{\mathbf{Q}})^{\mathrm{Br}(X)} \neq \emptyset$ implique $X(\mathbf{Q}) \neq \emptyset$.
(Sansuc 1981, Borovoi, 1996)

Courbes de genre 1

Exemples : cubiques non singulières dans $\mathbf{P}^2$, intersections non singulières de deux quadriques dans $\mathbf{P}^3$.
Une courbe elliptique sur $\mathbf{Q}$ est une courbe de genre 1 avec une structure de groupe, en particulier avec un point $\mathbf{Q}$-rationnel marqué.

A toute courbe projective non singulière $X/\mathbf{Q}$ de genre 1 on associe une courbe elliptique $J = J_X$ sur $\mathbf{Q}$, la jacobienne de X. La courbe X est un espace homogène principal de J.

L'ensemble des classes d'isomorphie de courbes $X/\mathbf{Q}$ de genre 1 avec la même jacobienne $J_X = J$ a une structure naturelle de groupe abélien. C'est le groupe de Weil-Châtelet $WC(J)$. La classe de X dans $WC(J)$ est nulle si et seulement si $X(\mathbf{Q}) \neq \emptyset$.
Le groupe de Tate-Shafarevich

$$Ш(J) \subset WC(J)$$

consiste en les classes de courbes qui ont des points dans tous les les $\mathbf{Q}_p$'s.

Espoir *Pour tout $J/\mathbf{Q}$, le groupe $Ш(J)$ est fini.*

Théorème (Manin 1970). *Soit $X/\mathbf{Q}$ une courbe de genre 1. Supposons $Ш(J_X)$ fini. Si $X(A_{\mathbf{Q}})^{\mathrm{Br}(X)} \neq \emptyset$, alors $X(\mathbf{Q}) \neq \emptyset$.*

C'est une conséquence de résultats de Cassels. Cassels a défini une forme alternée sur $Ш(J)$, à valeurs dans $\mathbf{Q}/\mathbf{Z}$. Il a montré : si $Ш(J)$ est fini, alors la forme est non dégénérée.

Sous l'hypothèse de finitude, ceci implique que pour tout $r \geq 1$ le sous-groupe ${}_rШ(J)$ des éléments de r-torsion dans $Ш(J)$ est une somme direct de groupes de la forme $(\mathbf{Z}/n)^2$. En particulier l'ordre de ${}_rШ(J)$ est un carré.

Ceci implique un modeste principe de Hasse :

Théorème

Soit $X/\mathbf{Q}$ une courbe de genre 1 et l un premier. Si l'on suppose

(i) le groupe $Ш(J_X)$ est fini
(ii) pour tout premier p, on a $X(\mathbf{Q}_p) \neq \emptyset$
(iii) le groupe ${}_lШ(J)$ a au plus l éléments
(iv) la classe de X dans $Ш(J)$ est annulée par l

alors $X(\mathbf{Q}) \neq \emptyset$.

Courbes de genre ≥ 2

Soit $X/\mathbf{Q}$ une courbe projective lisse de genre $g \geq 2$. A toute telle courbe on associe sa Jacobienne $J_X/\mathbf{Q}$. C'est une variété abélienne sur $\mathbf{Q}$, de dimension g.

L'ensemble $X(\mathbf{Q})$ est fini (Faltings).

Théorème

Supposons $X(A_{\mathbf{Q}})^{\mathrm{Br}(X)} \neq \emptyset$ *et* $Ш(J_X)$ *fini.*

(a) Il existe un plongement $X \hookrightarrow J_X$.

(b) L'image de $X(A_{\mathbf{Q}})^{\mathrm{Br}(X)}$ *dans* $\prod_{p \text{ fini}} J(\mathbf{Q}_p)$ *est dans l'adhérence topologique de* $J_X(\mathbf{Q})$.

(c) (Scharaschkin) Si $J(\mathbf{Q})$ *est fini, alors* $X(\mathbf{Q}) = X(A_{\mathbf{Q}})^{\mathrm{Br}(X)}$; *en particulier*

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

implique $X(\mathbf{Q}) \neq \emptyset$.

Question (Skorobogatov) *Soit $X/\mathbf{Q}$ une courbe projective lisse de genre $g \geq 2$. Si $X(\mathbf{Q}) = \emptyset$, a-t-on $X(A_{\mathbf{Q}})^{\mathrm{Br}(X)} = \emptyset$?*
Cette question a mené à des recherches récentes dans diverses directions.

Courbes de Shimura (Skorobogatov, Siksek, Rotger, Yafaev).

Mathématiques expérimentales avec des courbes hyperelliptiques de genre 2 et de petits coefficients (Flynn, 2004; Stoll).

Résultat inconditionnel sur un corps global de caractéristique positive (Poonen et Voloch, 2007).

Theorem (Stoll, 2005) *Soient $E/\mathbf{Q}$ une courbe elliptique, X une courbe projective lisse et $f : X \to E$ un morphisme fini. Supposons $E(\mathbf{Q})$ fini et l'ensemble $X(\mathbf{Q}) \cap f^{-1}(E(\mathbf{Q}))$ vide.*
(i) Alors $X(\mathbf{Q}) = \emptyset$ (trivial).
(ii) Si $Ш(E)$ est fini, alors $X(A_{\mathbf{Q}})^{\mathrm{Br}(X)} = \emptyset$.

Surfaces avec un pinceau de courbes de genre zéro

Théorème *Soient* $a(t), b(t), c(t) \in \mathbf{Q}[t]$, $abc \neq 0$. *Soit* $X/\mathbf{Q}$ *une surface projective non singulière birationnelle à la surface affine d'équation*

$$a(t)x^2 + b(t)y^2 + c(t) = 0.$$

Si l'on admet l'hypothèse de Schinzel, alors $X(\mathbf{Q})$ *est dense dans* $X(A_{\mathbf{Q}})^{\mathrm{Br}(X)}$.

(CT/Sansuc 1978, Serre 1992, CT/Swinnerton-Dyer 1994)

L'hypothèse de Schinzel (1958)
Soient $P_1(t), \cdots, P_m(t) \in \mathbf{Z}[t]$ *des polynômes irréductibles à coefficients entiers et à coefficient dominant positif. Supposons qu'aucun premier ne divise tous les* $\prod_i P_i(n)$, $n \in \mathbf{Z}$. *Il existe alors une infinité d'entiers* $n \in \mathbf{N}$ *tels que chaque* $P_i(n)$ *soit un nombre premier.*

Le seul cas connu est $m = 1$, $P_1(t) = at + b$ (Dirichlet).
Un cas particulier est la conjecture des nombres premiers jumeaux.
Des cas particuliers avaient été conjecturés par Bouniakowsky et par Dickson.

Si le nombre de $t \in \overline{\mathbf{Q}}$ avec $a(t)b(t)c(t) = 0$ est au plus 5, alors on peut donner une démonstration inconditionnelle du théorème d'existence de points rationnels dans le théorème précédent.

Voici une conséquence.
Théorème (CT/Sansuc/Swinnerton-Dyer 1987) *Soit $n \geq 8$. Si une intersection complète lisse de deux quadriques dans $\mathbf{P}^n_{\mathbf{Q}}$ a des points dans $\mathbf{R}$, alors elle a des points dans $\mathbf{Q}$.*

Résultats antérieurs : Mordell ($n \geq 12$); Swinnerton-Dyer ($n \geq 10$).

Surfaces avec un pinceau de courbes de genre 1

Nous avons vu un cas très spécial de principe de Hasse pour certaines courbes de genre 1.

Vers 1994 Swinnerton-Dyer a vu comment on peut utiliser ce résultat pour prédire l'existence de points rationnels sur certaines surfaces contenant un pinceau de courbes de genre 1.

La technique fut formalisée par CT, Skorobogatov et Swinnerton-Dyer (1998) puis améliorée par Wittenberg (2005).

Elle est fort élaborée.

Je citerai seulement quelques résultats frappants qu'elle permet d'obtenir.

Théorème (Swinnerton-Dyer, 2001) *Soient $a_i \in \mathbf{Z}, i = 0, \cdots, 3$ des entiers sans facteur cubique et sans facteur commun. Soit $X \subset \mathbf{P}^3_{\mathbf{Q}}$ la surface cubique*

$$\sum_{i=0}^{3} a_i x_i^3 = 0.$$

Supposons les groupes de Tate-Shafarevich finis. Si l'une des conditions suivantes est satisfaite :
(i) Il existe un premier $p \neq 3$ qui divise a_0 mais aucun des autres a_i, et il existe un premier $q \neq 3$ qui divise a_1 mais aucun des autres a_i.
(ii) Il existe un premier $p \neq 3$ qui divise a_0 mais aucun des autres a_i, et les classes de a_1, a_2, a_3 dans $\mathbf{F}_p^*/\mathbf{F}_p^{*3}$ ne sont pas toutes égales.
Alors le principe de Hasse vaut pour X.

Théorème (Swinnerton-Dyer 2001)
Supposons les groupes de Tate-Shafarevich finis. Alors le principe de Hasse vaut pour toute hypersurface cubique

$$\sum_{i=0}^{n} a_i x_i^3 = 0$$

sur $\mathbf{Q}$, *dès que* $n \geq 4$.

Théorème (Wittenberg, 2005)
Soient $q_1(x_0, \cdots, x_4)$ *et* $q_2(x_0, \cdots, x_4)$ *deux formes quadratiques à coefficients dans* $\mathbf{Q}$. *Supposons que la variété* $X \subset \mathbf{P}^4_{\mathbf{Q}}$ *définie par*

$$q_1(x_0, \cdots, x_4) = 0, q_2(x_0, \cdots, x_4) = 0$$

est non singulière.
Si le groupe de Galois de l'équation $\det(\lambda q_1 + \mu q_2)$ *est le groupe symétrique* S_5 *tout entier, et si l'on accepte l'hypothèse de Schinzel et la finitude des groupes de Tate-Shafarevich, alors le principe de Hasse vaut pour* X.

Théorème (Wittenberg, 2005)
Soit $X \subset \mathbf{P}^n_{\mathbf{Q}}$, $n \geq 5$ *une intersection complète non singulière de deux quadriques. Si l'on accepte l'hypothèse de Schinzel et la finitude des groupes de Tate-Shafarevich, alors le principe de Hasse vaut pour* X.

Des cas très particuliers de ces deux théorèmes avaient été obtenus dans des articles antérieurs (CT/Skorobogatov/Swinnerton-Dyer, Swinnerton-Dyer/Bender, CT).
La démonstration de Wittenberg passe par une réécriture systématique des travaux antérieurs et fait intervenir de la géométrie algébrique délicate. Elle utilise aussi un résultat récent de Harari (méthode des fibrations au-dessus d'une base de dimension quelconque).