JOURNAL DE THÉORIE DES NOMBRES DE BORDEAUX

YVES HELLEGOUARCH

# Théorème de Terjanian généralisé

*Journal de Théorie des Nombres de Bordeaux 2^e série*, tome 2, n° 2 (1990), p. 245-254

<http://www.numdam.org/item?id=JTNB_1990__2_2_245_0>

*Séminaire de Théorie des Nombres,*
*Bordeaux* **2***(1990), 245–254*

# Théorème de Terjanian généralisé.

par YVES HELLEGOUARCH

**Résumé** — En 1977 G. Terjanian étonna tous les spécialistes du théorème de Fermat en prouvant le premier cas... pour les exposants pairs. Nous généralisons ici cette propriété dans le cas des corps de nombres de degré impair et ayant un nombre impair de classes d'idéaux.

**Abstract** — *In 1977 G. Terjanian startled everybody in proving the first case of Fermat's last theorem... for even exponents. Here we generalise this property to number fields of odd degree and with an odd class number.*

## 1 - A la recherche d'une généralisation

Rappelons l'énoncé du théorème de Terjanian [5].

THÉORÈME. *Soit donné un nombre premier $p$ et soient trois entiers $a, b, c \in \mathbb{Z}$, premiers entre eux dans leur ensemble, tels que :*

$$a^{2p} = b^{2p} + c^{2p}$$

*alors si $c$ est pair, $c$ est divisible par $p$.*

On peut encore dire que si $a$ et $b$ sont impairs et si :

$$a^{2p} - b^{2p} = 4^p c^{2p}$$

alors $c$ est divisible par $p$, lorsque $p$ est un nombre premier impair.

Dans quelle direction peut-on maintenant chercher à généraliser ce résultat ?

Soit une courbe $\mathcal{C}$ de genre $g \geq 2$ contenue dans $\mathbb{P}_r$ et définie sur un corps de nombres $K$, j'ai remarqué dans ma thèse [2] que si l'on accepte la conjecture de Mordell (devenue maintenant le non moins célèbre théorème de Faltings) il existe une constante $C(K, \mathcal{C})$ telle que si $n > C(K, \mathcal{C})$ et si $(x_0^n, x_1^n, ..., x_r^n) \in \mathcal{C}(K)$, alors les $x_i$ peuvent être choisis dans $\mu(K) \cup \{0\}$ où $\mu(K)$ désigne le groupe des racines de l'unité de $K^*$.

Manuscrit reçu le 19 juin 1990

Cette remarque implique donc que si $\ell \geq 4$ et si $(\alpha_0, \alpha_1, \alpha_2) \in K^3$ est tel que $\alpha_0\alpha_1\alpha_2 \neq 0$, la relation

$$\alpha_0 x_0^{\ell n} + \alpha_1 x_1^{\ell n} + \alpha_2 x_2^{\ell n} = 0$$

entraîne que les $x_i$ peuvent être pris dans $\mu(K) \cup \{0\}$, lorsque $n$ est assez grand.

Mais lorsque $\ell \in \{1, 2, 3\}$ on ne sait rien dire.

Notre but sera de montrer que si $p$ est premier impair et assez grand, si $\gamma \geq 1$ et si $\epsilon$ est une unité de $K$, la relation :

$$a^{2p} - b^{2p} = \epsilon 4^\gamma c^{2p}$$

avec $(a, b, c) \in \mathcal{O}_K^3$ (où $\mathcal{O}_K$ désigne l'ordre maximal de $K$) entraîne que $p$ divise la norme absolue de $c$.

En réalité on démontrera un résultat plus général relatif aux points entiers d'une surface affine...

## 2 - Enoncés

Nous allons donner trois énoncés, assez proches les uns des autres, qui se suivent par ordre de spécialisation croissante.

THÉORÈME 1. *Soient $K$ un corps de nombres de* **degré impair** *et $\mathcal{O}_K$ son ordre maximal. Soient $a$ et $b$ dans $\mathcal{O}_K$. Si*

1) *$a$ et $b$ sont étrangers entre eux*
2) *$a$ et $b$ sont étrangers à 2 (nombres "impairs")*
3) *$a^2 \equiv b^2$ mod 4 $\mathcal{O}_K$*
4) *$n$ est un entier impair $\geq 1$ non carré,*

*alors l'idéal de $K$ engendré par $\frac{a^{2n}-b^{2n}}{a^2-b^2}$ n'est pas un carré.*

Ce théorème permet d'obtenir les résultats suivants.

THÉORÈME 2. *Soit $K$ un corps de nombres de* **degré impair** *et ayant un* **nombre impair** *de classes d'idéaux ; on désigne par $\mathcal{O}_K$ son ordre maximal. Alors l'équation :*

$$a^{2p} - b^{2p} = \epsilon 4^\gamma c^2$$

*avec $(a,b,c) \in \mathcal{O}_K^3$, $a$ ou $b$ impair, $\epsilon$ unité de $\mathcal{O}_K$, $\gamma$ entier $\geq 1$, entraîne que $p$ et $c$ ne sont pas étrangers dès que l'entier premier impair $p$ est supérieur à une certaine constante $C(K)$.*

THÉORÈME 3. *Dans les mêmes conditions, l'équation :*

$$a^{2p} - b^{2p} = \epsilon 4^{\gamma} c^{2p}$$

*entraîne que $p$ et $c$ ne sont pas étrangers dès que l'entier premier impair $p$ est supérieur à une certaine constante $C(K,\gamma)$.*

### 3 - Le passage de 1 à 2 et 3

Pour effectuer ce passage nous utiliserons l'existence d'un corps $H$ (le corps de classes de Hilbert de $K$ [4]) dans lequel tout idéal de $K$ devient principal et dont le degré relatif à $K$ est égal au nombre de classes d'idéaux de $K$ : en vertu de nos hypothèses il est impair, et on en déduit que $[H : \mathbb{Q}]$ est impair.

Nous partons donc de la relation :

$$a^{2p} - b^{2p} = \epsilon 4^{\gamma} c^2 \tag{1}$$

avec $(a,b,c) \in \mathcal{O}_K^3$.

Le couple $(a,b)$ engendre un idéal de $\mathcal{O}_K$ qui devient principal dans $H$, on a donc :

$$a\mathcal{O}_H + b\mathcal{O}_H = d\mathcal{O}_H, \text{ avec } d \in H.$$

En divisant notre relation par $d^{2p}$, nous obtenons :

$$a'^{2p} - b'^{2p} = \epsilon 4^{\gamma} c'^2 \tag{2}$$

avec $(a',b') \in \mathcal{O}_H^2$, premiers entre eux, et $c' \in H$. Il est clair que $2^{\gamma} c' \in \mathcal{O}_H$ et que ce qui empêche $c'$ d'être entier est la présence éventuelle, en dénominateur, d'idéaux premiers $\mathfrak{q}$ au-dessus de 2 dans $H$.

Dans le cas du théorème 2, cela ne peut pas se produire car $a$ ou $b$ est étranger à 2. Dans le cas du théorème 3 on voit facilement que si $p > \gamma v_{\mathfrak{q}}(2)$, pour tous les idéaux premiers $\mathfrak{q}$ de $H$ au-dessus de 2, cela ne peut pas non plus se produire.

En résumé nous avons (pour $p$ assez grand) :

$$\begin{cases} (a',b') \in \mathcal{O}_H^2 \\ a' \text{ et } b' \text{ étrangers entre eux} \\ a' \text{ et } b' \text{ étrangers à 2 (puisque } \gamma \geq 1) \\ p \text{ entier impair, non carré} \end{cases}$$

Pour pouvoir appliquer le théorème 1, il reste à voir que $a'^2 \equiv b'^2 \ mod\ 4\mathcal{O}_H$ pour $p$ assez grand. Puisque $b'$ est étranger à 2, on sait que $b'$ est inversible dans l'anneau $\mathcal{O}_H/4\mathcal{O}_H$ et on déduit de (2) que :

$$\left(\frac{a'^2}{b'^2}\right)^p \equiv 1 \qquad mod\ 4\mathcal{O}_H.$$

Il en résulte que $\frac{a'^2}{b'^2}$ est une racine de l'unité dans l'anneau $\mathcal{O}_H/4\mathcal{O}_H$, donc que $p$ doit diviser l'ordre du groupe fini $(\mathcal{O}_H/4\mathcal{O}_H)^*$.

Donc, si $p$ est assez grand, on a :

$$\frac{a'^2}{b'^2} \equiv 1 \qquad mod\ 4\mathcal{O}_H$$

d'où

$$a'^2 \equiv b'^2 \qquad mod\ 4\mathcal{O}_H.$$

Le théorème 1 peut alors être appliqué à $H$ et à $\frac{a'^{2p}-b'^{2p}}{a'^2-b'^2}$ et il affirme que ce dernier nombre ne peut pas engendrer le carré d'un idéal dans $H$. Mais la relation (2) entraîne que le produit des idéaux engendrés par $a'^2 - b'^2$ et $\frac{a'^{2p}-b'^{2p}}{a'^2-b'^2}$ est un carré. Il en résulte que ces deux nombres ne peuvent pas être étrangers. Soit $\mathfrak{q}$ un diviseur premier commun à ces deux nombres, dans $H$ on a :

$$\frac{a'^{2p} - b'^{2p}}{a'^2 - b'^2} \equiv p\ a'^{2(p-1)} \equiv pb'^{2(p-1)}\ mod\ \mathfrak{q}$$

et, comme $a'$ et $b'$ sont étrangers, on voit que $\mathfrak{q}$ divise $p$.

Il existe donc, dans $H$, un idéal premier $\mathfrak{q}$ au-dessus de $p$, qui divise $c'$, ce qui prouve que $p$ et $c$ ne peuvent pas être étrangers.

## 4 - Retour au pays

Nous nous proposons ici de rappeler l'énoncé de la loi de réciprocité quadratique de Hecke, mais nous utiliserons les notations de [4].

### 4.1- Enoncé

Soit $K$ un corps de nombres quelconque et soit $\mathcal{O}_K$ son ordre maximal.

Pour $\alpha$ et $\beta \in \mathcal{O}_K$, étrangers à 2 et étrangers entre eux, on pose ([4] p. 111) :

$$\left(\frac{\alpha}{\beta}\right)_K = \prod_{\mathfrak{q}|\beta} \left(\frac{\alpha}{\mathfrak{q}}\right)_K^{v_{\mathfrak{q}}(\beta)}$$

où le *symbole de Legendre* $\left(\frac{\alpha}{\mathfrak{q}}\right)_K$ est défini par

$$\begin{cases} \left(\frac{\alpha}{\mathfrak{q}}\right)_K \in \{1,-1\} \\ \left(\frac{\alpha}{\mathfrak{q}}\right)_K \equiv \alpha^{\frac{N\mathfrak{q}-1}{2}} \qquad mod\ \mathfrak{q} \end{cases}$$

Nous dirons que $\left(\frac{\alpha}{\beta}\right)_K$ est le *symbole de Jacobi* de $\alpha$ et $\beta$.

Le symbole de Jacobi possède une propriété de symétrie qui est la loi de réciprocité de Hecke ([4] p. 111) :

$$\left(\frac{\alpha}{\beta}\right)_K \left(\frac{\beta}{\alpha}\right)_K = \prod_{\mathfrak{p}|2.\infty} \left(\frac{\alpha,\beta}{\mathfrak{p}}\right)_K \tag{3}$$

où $\left(\frac{\alpha,\beta}{\mathfrak{p}}\right)_K$ est le *symbole de Hilbert* de $\alpha$ et $\beta$ en $\mathfrak{p}$, c'est-à-dire

$$\left(\frac{\alpha,\beta}{\mathfrak{p}}\right)_K = \begin{cases} 1 & \text{si } \alpha X^2 + \beta Y^2 \text{ represente 1 sur } K_{\mathfrak{p}} \\ -1 & \text{sinon.} \end{cases}$$

*Remarques :*

1) Il est clair que si $\mathfrak{p}|\infty$ et si $\mathfrak{p}$ est complexe, le symbole de Hilbert vaut automatiquement 1 : seules les places réelles interviennent dans le second membre de (3).

2) D'une manière analogue si $\alpha$ ou $\beta$ est *primaire*, c'est-à-dire congru à un carré modulo 4, les places qui divisent 2 n'interviennent pas dans le second nombre de (3).

3) Il est dangereux de supprimer l'indice $K$ !

### 4.2 - Cas particulier

Nous allons appliquer la relation (3) à un ensemble plus restreint de nombres $\alpha$ ou $\beta$.

DÉFINITIONS.

*1) Nous dirons que $\alpha \in \overline{\mathbb{Q}}$ possède un signe, si $\alpha$ est totalement positif ou totalement négatif.*

*Si $\alpha >> 0$, nous écrivons que $s(\alpha) = 1$.*

*Si $\alpha << 0$, nous écrirons que $s(\alpha) = -1$.*

*2) Nous dirons que $\alpha \in \mathcal{O}_K$ est* **primaire dans** *$K$ si*

*i) $\alpha$ est étranger à 2 ($\alpha$ est impair)*

*ii) $\alpha$ est congru modulo $4\mathcal{O}_K$ au carré d'un nombre de $K$.*

Nous allons maintenant supposer que $\alpha$ et $\beta$ vérifient les

**Hypothèses :**

i) $\alpha$ **et** $\beta$ sont étrangers à 2.

ii) $\alpha$ **et** $\beta$ ont un signe.

iii) $\alpha$ **et** $\beta$ sont premiers entre eux.

iv) $\alpha$ **ou** $\beta$ est primaire dans $K$.

Alors la loi de réciprocité (3) s'écrit :

$$\left(\frac{\alpha}{\beta}\right)_K \left(\frac{\beta}{\alpha}\right)_K = (-1)^{r\frac{s(\alpha)-1}{2}\frac{s(\beta)-1}{2}} \tag{4}$$

où $r$ désigne le nombre de places réelles de $K$.

*Exemple :* Si $K = \mathbb{Q}$, on a $r = 1$ et on retrouve la loi de réciprocité quadratique (de Jacobi) pour les nombres impairs congrus à 1 modulo 4.

### 4.3 - Caractérisation du symbole de Jacobi

Soit $\mathcal{P}$ le monoïde multiplicatif des entiers primaires de $\mathbb{Z}$ et soit $\Delta$ la partie de $\mathcal{P} \times \mathcal{P}$ formée des couples $(m, n)$ tels que $m$ et $n$ ne soient pas premiers entre eux.

Le symbole de Jacobi définit une application :

$$\begin{cases} \mathcal{P} \times \mathcal{P} \setminus \Delta \to \{1 - 1\} \\ (m, n) \qquad \mapsto \left(\frac{m}{n}\right)_{\mathbb{Q}} \end{cases}$$

que l'on se propose de caractériser par des propriétés simples.

LEMME 1. *Soit $f : \mathcal{P} \times \mathcal{P} \setminus \Delta \to \{1, -1\}$ une application vérifiant les quatre conditions :*

*1) $f(1, 1) = 1$*

*2) $f(n, m) = (-1)^{\frac{s(n)-1}{2}\frac{s(m)-1}{2}} f(m, n)$*

*3)* $f(m_1, n) = f(m_2, n)$ *si* $m_1 \equiv m_2 \mod n$

*4)* $f(m_1, n) = (-1)^{\frac{s(n)-1}{2}} f(m_2, n)$ *si* $m_1 + m_2 \equiv 0 \mod n$

*Alors* $f(m, n)$ *est le symbole de Jacobi.*

Nous ne donnons pas de démonstration formelle de ce lemme car elle peut se faire de manière entièrement élémentaire par récurrence sur $\inf(|m|, |n|)$.

## 5 - Et au berceau...

Nous arrivons ici à la motivation première de ce travail qui était de trouver des illustrations de la notion de $\sigma$-dérivation ([1] p. 11) et de celle de "différences divisées". Les lemmes que nous allons établir serviront à la démonstration du théorème 1.

### 5.1 - Situation générique

Rappelons qu'une *$\sigma$-dérivation* d'un anneau intègre $A$, de corps des fractions $F$, muni d'un endomorphisme $\sigma : F \to F$, est une application additive $x \mapsto x'$ de $F$ dans $F$ telle que

$$(xy)' = x'y^\sigma + xy'.$$

*Exemple :* Nous nous intéresserons plus particulièrement à la situation où $A = \mathbb{Z}[X, X_1, X_2, ...]$, les $X_i$ étant des indéterminées, où $\sigma|\mathbb{Z} = id$ et

$$\sigma(X) = X_1, \quad \sigma(X_i) = X_{i+1} \text{ pour } 1 \leq i.$$

Si $P \in F$ et si $Y \in F \setminus \mathbb{Q}$, on pose :

$$P'_Y = \frac{P^\sigma - P}{Y^\sigma - Y} \in F.$$

Alors il est clair que $P \mapsto P'_Y$ est une $\sigma$-dérivation de $F$ puisque l'on a :

$$(PQ)'_Y = P'_Y Q^\sigma + PQ'_Y$$

*Remarques :*

1) Il est essentiel de remarquer que, dans cet exemple, on a l'implication :

$$(P \in \mathbb{Z}[X]) \Rightarrow (P'_X \in A).$$

Dans ce cas on écrira $P'$ à la place de $P'_X$.

2) Lorsque $P$ et $Q$ sont dans $\mathbb{Z}[X]$ on a la règle suivante :

$$(P \circ Q)'_Y = (P'_X \circ Q).Q'_Y.$$

### 5.2 - Spécialisation

On désignera par $A \longrightarrow \overline{A} \subset \overline{\mathbb{Z}}$ une spécialisation de $A$ dans l'anneau des entiers algébriques et on posera :

$$\overline{X} = a,\ \overline{\sigma(X)} = b,\ \overline{\sigma^2(X)} = c \quad , \quad etc.$$

Les lemmes suivants étant très élémentaires, nous renvoyons à [3] pour les démonstrations.

LEMME 2. *Si $P$ et $Q$ sont dans $\mathbb{Z}[X]$, on a :*

$$\overline{(P \circ Q)'} \equiv 0 \qquad \mod \overline{Q'}$$

LEMME 3. *Soient $m$ et $n \in \mathbb{N}$ de p.g.c.d. égal à $d$. Alors si $a$ et $b$ sont premiers entre eux dans $\mathbb{Z}$, $\overline{(X^d)'}$ est un p.g.c.d. de $\overline{(X^m)'}$ et de $\overline{(X^n)'}$ dans $\overline{\mathbb{Z}}$.*

LEMME 4. *Si $P \in \mathbb{N}[X]$, on a $\overline{(P \circ X^2)'_{X^2}} >> 0$.*

LEMME 5. *Soit $n$ primaire dans $\mathbb{Z}$, on considère $P(X) := X^{2|n|}$. Alors si $a$ et $b$ sont impairs et si $a^2 \equiv b^2$ mod 4, le nombre $s(n)\overline{P'_{X^2}}$ est primaire dans $\mathbb{Q}(a,b)$.*

LEMME 6. *Soient $m_1$ et $m_2 \in \mathbb{N}$.*

*i) Si $m_1 = nq + m_2$ avec $n$ et $q \in \mathbb{N}$ et si :*

$$P(X) = X^{2m_1},\ \ Q(X) = X^{2n},\ \ R(X) = X^{2m_2}$$

*on a :*

$$\overline{P'_{X^2}} \equiv a^{2nq}\overline{R'_{X^2}} \ \ mod \quad \overline{Q'_{X^2}}$$

*ii) Si $m_1 + m_2 = nq$ avec $n$ et $q \in \mathbb{N}$, on a :*

$$\overline{P'_{X^2}}b^{2m_2} \equiv -a^{2m_1}\overline{R'_{X^2}} \quad mod\ \overline{Q'}_{X^2}$$

*Remarque :* On trouvera encore d'autres illustrations de ces notions dans mon exposé aux Journées Arithmétiques de 1989 [3].

## 6 - Epilogue

On se propose maintenant de démontrer le théorème 1.

Pour tout $m \in \mathcal{P}$, on posera :

$$[m] = s(m)\overline{P'}_{X^2}$$

avec $P(X) = X^{2|m|}$ et les notations du paragraphe 5. On a donc :

$$[m] = s(m)\frac{b^{2|m|} - a^{2|m|}}{b^2 - a^2}.$$

La méthode de démonstration consiste à appliquer le lemme 1 à la fonction :

$$f(m,n) := \left(\frac{[m]}{[n]}\right)_K.$$

**6.1** - Pour commencer il faut voir que si $(m,n) \in \mathcal{P} \times \mathcal{P} \setminus \Delta$ , $f(m,n)$ est bien défini.

D'après l'hypothèse 1 du théorème 1 et le lemme 3 on voit que [m] et [n] sont étrangers. D'après les hypothèses 2 et 3 du théorème 1 et le lemme 5, on voit que [m] et [n] sont primaires dans $K$.

**6.2** - La condition 1) du lemme 1 est évidente. Pour démontrer la condition 2) nous allons appliquer la loi de réciprocité (4). Il suffit alors de remarquer que [m] et [n] possèdent les signes (respectifs) $s(m)$ et $s(n)$, d'après le lemme 4, pour obtenir le résultat, puisque $r$ est *impair*.

**6.3** - Il reste à démontrer les conditions 3 et 4, ce que l'on va faire d'un seul coup. Si $m_1$ et $m_2$ sont de même signe, ces conditions proviennent du lemme 6 et du fait que, d'après (4) et l'imparité de $r$ :

$$\left(\frac{-1}{[n]}\right)_K = (-1)^{\frac{s(n)-1}{2}}.$$

**6.4** - Nous pouvons donc appliquer le lemme 1 et nous obtenons :

$$\left(\frac{[m]}{[n]}\right)_K = \left(\frac{m}{n}\right)_{\mathbb{Q}} \tag{5}$$

lorsque $(m,n) \in \mathcal{P} \times \mathcal{P} \setminus \Delta$.

On peut alors terminer comme Terjanian. Si $n \geq 1$ est impair et non carré, alors $n^* = (-1)^{\frac{n-1}{2}} n \in \mathcal{P}$ et n'est pas un carré.

D'après le théorème de Dirichlet il existe un entier premier primaire $\ell \in \mathbb{Z}$ tel que :

$$\left(\frac{n^*}{\ell}\right)_{\mathbb{Q}} = -1.$$

D'après (4) on a :

$$\left(\frac{\ell}{n^*}\right)_{\mathbb{Q}} = -1$$

et d'après (5) on a :

$$\left(\frac{[\ell]}{[n^*]}\right)_K = -1$$

donc l'idéal engendré par $[n^*] = \pm[n]$ ne peut pas être un carré (voir paragraphe 4,1). □

## References

[1] P.M. COHN, *Skew Field Constructions.* Cambridge U.P. (1977).

[2] Y. HELLEGOUARCH, *Courbes elliptiques et équation de Fermat.* Thèse, Besançon, (1972).

[3] Y. HELLEGOUARCH, *Calcul différentiel Galoisien.* Journées Arithmétiques, Luminy, (1989), et prépublication n°42, Université de Caen.

[4] J. NEUKIRCH, *Class Field Theory.* Springer, (1980).

[5] G. TERJANIAN, *"Sur l'équation $x^{2p} + y^{2p} = z^{2p}$".* C.R. Acad. Sci. Paris, **285**, (1977), p. 973-975.

*Mots clefs*: Fermat, courbes elliptiques, corps de classes.

4, rue du Dr Rayer
14000 CAEN, France