

MÉMOIRES DE LA S. M. F.

YVES HELLEGOUARCH

Points d'ordre fini des variétés abéliennes de dimension un

Mémoires de la S. M. F., tome 25 (1971), p. 107-112

http://www.numdam.org/item?id=MSMF_1971__25__107_0

© Mémoires de la S. M. F., 1971, tous droits réservés.

L'accès aux archives de la revue « Mémoires de la S. M. F. » (<http://smf.emath.fr/Publications/Memoires/Presentation.html>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

POINTS D'ORDRE FINI DES VARIETES ABELIENNES DE DIMENSION UN

par

Yves HELLEGOUARCH

--:--:--

1. - Introduction

Une variété abélienne de dimension un définie sur le corps des nombres rationnels \mathbb{Q} peut être représentée par une cubique de genre un :

$$Y^2 = X^3 + AX + B \quad \begin{array}{l} A, B \in \mathbb{Q} \\ 4A^3 + 27B^2 \neq 0 \end{array}$$

munie d'une loi de groupe algébrique. On obtient cette loi en définissant la somme de deux points d'arguments elliptiques u_1 et u_2 comme étant le point d'argument elliptique $u_1 + u_2$.

Un point (x, y) de la cubique \mathcal{C} est dit rationnel sur \mathbb{Q} si x et y sont dans \mathbb{Q} .

Le groupe G des points de \mathcal{C} rationnels sur \mathbb{Q} est de type fini (théorème de Mordell). En particulier son sous-groupe de torsion T est fini.

L'étude du plongement de T dans le groupe des points réels de \mathcal{C} montre que T est ou bien cyclique ou bien du type $(2n, 2)$.

Une conjecture classique sur T est que son ordre possède une borne supérieure finie indépendante de A et de B .

Ces préliminaires étant rappelés nous nous posons la question suivante :

(I_n) n étant un entier impair donné, existe-t-il des groupes de torsion T admettant un sous-groupe du type $(2n, 2)$?

On sait que la réponse à (I_n) est négative pour $n = 5, 7$ et 11 . Nous allons relier la question (I_n) à deux autres questions :

(II_p) p étant un nombre premier, existe-t-il des solutions non triviales de l'équation diophantienne :

$$X^p + Y^p = Z^p + T^p \quad ?$$

(III_p) p étant un nombre premier, existe-t-il des solutions non triviales de l'équation diophantienne :

$$X^p = Y^{2p} + Z^{2p} \quad ?$$

Remarques : Le choix des équations (II) et (III) présente une certaine part d'arbitraire, ceci apparaîtra plus loin.

D'autre part les trois questions posées admettent des solutions dans tous les corps π -adiques, ainsi une réponse négative ne pourra pas être obtenue par localisation.

2. - Dans ce paragraphe nous allons voir que si $p \geq 5$:

$$\text{oui } (I_p) \Rightarrow \text{oui } (II_p) .$$

Soit donc une cubique \mathcal{C} admettant un sous-groupe de points rationnels du type $(2p^2, 2)$. Comme les points d'ordre deux de \mathcal{C} sont tous rationnels on peut mettre \mathcal{C} sous la forme :

$$(IV) \quad Y^2 = X(X-a)(X-b) ,$$

et on peut même supposer a et b entiers et a pair. Quitte à remplacer (X, Y) par $(\lambda^2 X, \lambda^3 Y)$ on peut aussi supposer que (a, b) n'est pas divisible par le carré d'un nombre premier.

Exprimons maintenant l'hypothèse que \mathcal{C} possède un point rationnel d'ordre p^2 . Mais plus généralement, soit un point (x, y) rationnel d'ordre n dans le groupe des points de \mathcal{C} .

D'après un théorème de Nagell x et y sont entiers et on voit encore que x , $x-a$ et $x-b$ sont des carrés parfaits (prendre la formule de duplication pour la loi de groupe sur \mathcal{C}).

On peut donc écrire :

$$\begin{cases} x = w^2 w'^2 \\ x-a = w^2 w''^2 \\ x-b = w'^2 w''^2 \end{cases} \quad \begin{array}{l} w, w', w'' \in \mathbb{N} \\ (w, w') = (w, w'') = (w', w'') = 1 . \end{array}$$

LEMME 1. - Si $n = p \geq 5$ et si la cubique (IV) admet un point rationnel d'ordre p^2 , on a toujours pour un point rationnel d'ordre p :

$$\begin{cases} w = 2v^p \\ w' = v'^p \\ w'' = v''^p \end{cases}$$

où v, v', v'' sont des entiers naturels premiers entre eux deux à deux, où v est pair et $v v' v''$ est divisible par p .

Remarques :

1) Si l'on désigne par w_v, w'_v, w''_v les entiers w associés au $v^{\text{ième}}$ multiple de (x,y) et si $r = \frac{p-1}{2}$ on a :

$$\begin{cases} v_v = a_1 \binom{v}{p} a_2 \binom{2v}{p} \dots a_r \binom{rv}{p} \\ v'_v = a'_1 \binom{v}{p} a'_2 \binom{2v}{p} \dots a'_r \binom{rv}{p} \\ v''_v = a''_1 \binom{v}{p} a''_2 \binom{2v}{p} \dots a''_r \binom{rv}{p} \end{cases}$$

où les a_i, a'_i, a''_i sont des entiers naturels premiers deux à deux et où le symbole $\binom{x}{p}$ désigne la valeur absolue du nombre de l'intervalle $[-r,r]$ qui est congru à x modulo p .

Cette remarque nous sera utile plus tard.

2) La démonstration du lemme 1 se fait par localisation en tous les nombres premiers qui divisent $w w' w''$ ainsi que dans \mathbb{Q}_2 et \mathbb{Q}_p .

3) Pour $p = 3$ les résultats sont un peu différents.

Signification algébrique des w

Le point (w,w',w'') est situé sur la courbe \mathcal{C} d'équations :

$$\begin{cases} a = w^2 (w'^2 - w''^2) \\ b = w'^2 (w^2 - w''^2) \end{cases}$$

et l'application rationnelle φ telle que

$$\varphi(w,w',w'') = (w^2 w'^2, w^2 w'^2 w''^2)$$

est un revêtement de degré 8 de la cubique \mathcal{Q} .

Si le point (x,y) est d'ordre impair dans le groupe G , les huit points de $\varphi^{-1}(x,y)$ sont

1°) $(\pm w, \pm w', \pm w'')$ si $y > 0$.

2°) $(\pm iw, \pm iw', \pm iw'')$ si $y < 0$, i désignant $\sqrt{-1}$.

Soit (w_1, w'_1, w''_1) un point de \mathcal{C} , alors les points (w_2, w'_2, w''_2) tels que :

$$(w_2, w'_2, w''_2) = 2 (w_1, w'_1, w''_1)$$

vérifient les équations :

$$(V) \quad \begin{cases} 2W_2 W'_2 = W_1^2 + W_1'^2 - W_1''^2 \\ 2W_2 W''_2 = W_1^2 - W_1'^2 + W_1''^2 \\ 2W'_2 W''_2 = -W_1^2 + W_1'^2 + W_1''^2 \end{cases}$$

Si l'on pose :

$$T = W + W' + W''$$

on déduit des équations (V) que :

$$(VI) \quad T_2 = \frac{W_2^2 + W_1^2}{W_2} = \frac{W_1'^2 + W_1^2}{W'_2} = \frac{W_1''^2 + W_1^2}{W''_2}$$

Maintenant la troisième égalité de la relation (VI) et le lemme 1 entraînent que :

$$v''_2{}^p (v'_2{}^{2p} \pm v_1^{2p}) = v'_2{}^p (v''_2{}^{2p} \pm v_1^{2p})$$

ce qui est une solution de l'équation (II_p). Cette solution est non triviale en vertu de la remarque qui suit le lemme 1 et qui nous renseigne sur les exposants des facteurs premiers qui interviennent dans les v_1 .

Remarques :

1) La seconde égalité de la relation (VI) et le lemme 1 entraînent que l'équation

$$2(X^p + Y^p) = Z^p + T^p$$

admet des solutions non triviales.

2) On peut affirmer en fait que ces équations admettent $r = \frac{p-1}{2}$ solutions distinctes non triviales.

3. - Nous allons voir finalement que si $p \geq 5$ et si p divise un nombre de la forme $(-2)^h + 1$ avec $h \geq 2$, on a l'implication :

$$\text{oui } (I_{p^2}) \Rightarrow \text{oui } (III_p)$$

LEMME 2. - Si $p \geq 5$ divise $(-2)^h + 1$ avec $h \geq 2$, tout facteur premier de T_2 (par exemple) est facteur des $W W' W''$.

Démonstration. Cette démonstration est basée sur la relation

$$(VII) \quad 2W_{2v} W'_{2v} W''_{2v} T_{2v} = (W_v W'_v - W_{2v} W'_{2v}) T_v (T_v - 2W''_v)$$

qui se déduit des relations (V) et sur le fait que les 8 points appliqués par φ sur $-(W, W', W'')$ sont $(\pm iW, \pm iW', \pm iW'')$ avec $i = \sqrt{-1}$

D'autre part (VI) montre que les T sont des entiers de Gauss associés à des entiers naturels. Nous raisonnons maintenant par l'absurde en supposant que q divise T_2 sans diviser les $W W' W''$. Alors la relation (VII) montre que q divise tous les T_{2^m} .

En vertu de la première relation (VI) on a :

$$W_{2^{m+1}}^2 \equiv W_{2^m}^2 \pmod{q}$$

et en multipliant ces congruences :

$$\prod_{m=0}^{h-1} W_{2^{m+1}}^2 \equiv (-1)^h \prod_{m=0}^{h-1} W_{2^m}^2 \pmod{q}$$

Distinguons deux cas suivant la parité de h .

Si h est pair $(-1)^h = 1$, mais $W_{2^h}^2 = -W_1^2$ donc

$$2 \prod_{m=0}^{h-1} W_{2^m}^2 \equiv 0 \pmod{q}$$

ce qui est contraire à la supposition que q ne divise pas les $W W' W''$.

Si h est impair $(-1)^h = -1$, mais $W_{2^h}^2 = W_1^2$ ce qui nous conduit au même résultat et démontre le lemme.

Appliquons maintenant les lemmes 1 et 2 aux relations (VI). On voit que T_2 est associé au double de la puissance p ième d'un entier rationnel et on obtient une relation de la forme :

$$X^p = Y^{2p} \pm Z^{2p}$$

entre entiers rationnels.

Si (x,y) est le point dont l'argument elliptique est la p ième partie de la plus petite période réelle, on constate que l'on a le signe $+$ c'est-à-dire que l'on obtient une solution de (III)_p. Cette solution est non triviale pour la même raison que dans le second paragraphe.

Remarques :

1) On obtient en fait des solutions non triviales des équations (non simultanées) :

$$X^p = Y^{2p} - Z^{2p}$$

$$2X^p = Y^{2p} + Z^{2p}$$

$$2X^p = Y^{2p} - Z^{2p} .$$

2) Ce résultat entraîne que la réponse à (I_2) est négative chaque fois que le dernier théorème de Fermat est démontré pour l'exposant p et que p divise un nombre du type $(-2)^h + 1$. Remarquons que cette dernière condition est vérifiée si $(\frac{-2}{p}) = -1$, soit $p \in 8\mathbb{Z} + 5$ ou $p \in 8\mathbb{Z} + 7$.

-:-:-:-

BIBLIOGRAPHIE

- J.W.S. CASSELS. - Diophantine equations with special reference to elliptic curves. Journ. London Math. Soc. 41 - 1966 - (193-291).
- Y. HELLEGOUARCH. - Etude des points d'ordre fini des variétés abéliennes de dimension un définies sur un anneau principal. à paraître dans J. Reine und angew. Math.

-:-:-:-

Faculté des Sciences de Caen
Département de Mathématiques
Esplanade de la Paix
14 - Caen (France)