Math. Res. Lett. **14** (2007), *no.* 6, 887–891

PÉRIODICITÉ DES POLYNÔMES DE DIVISION SUR UNE COURBE ELLIPTIQUE

Laurent Dewaghe

Résumé. Soit $\mathbb{F}_q$ un corps de caractéristique différente de 2 et 3 et E une courbe elliptique définie sur $\mathbb{F}_q$. Dans cet article, on considère la suite de valeurs $(\psi_n(P))_{n\in Z}$ des polynômes de division de la courbe elliptique E en un point P d'ordre fini de E. On montre, sans passage à la caractéristique zéro, que cette suite est périodique.

1. Introduction

Soit E une courbe elliptique définie sur un corps fini $\mathbb{F}_q$ de caratéristique p différente de 2 et 3. L'ensemble des $\mathbb{F}_q$-points de E, noté $E(\mathbb{F}_q)$, est un groupe abélien fini. Pour $n \in \mathbb{N}$, les sous-groupes de n-torsion sont notés $E[n]$. Les polynômes de division ψ_n de la courbe elliptique E explicitent l'endomorphisme de $E(\mathbb{F}_q)$ de multiplication par n et caractérisent le groupe $E[n]$. Les polynômes de division sont essentiels non seulement dans la théorie des courbes elliptiques mais aussi dans des domaines connexes comme l'étude des suites elliptiques. En 1948, Ward associe les valeurs d'une suite elliptique aux valeurs de polynômes de division, d'une courbe elliptique, en un point de torsion [5, 6]. Il montre, notamment, en utilisant la caractéristique zéro, qu'une suite elliptique modulo p est périodique. La périodicité des suites elliptiques pour un module arbitraire est étudié par Ayads [1]. Il obtient un résultat analogue pour de "pseudo polynômes de division" $\hat{\psi}_n(P) \in \mathbb{Z}$, pour $P \in \mathbb{Q}$, proportionnels à $\psi_n(P)$. Bien qu'utilisant l'argument simple de la récurrence, sa démonstration reste néanmoins laborieuse et nécessite l'expression de nP en fonction des polynômes de division et donc l'utilisation de la fonction de Weierstrass. Plus récemment, Silverman [3], étudie les propriétés p-adic des suites elliptiques. En particulier, il montre, en utilisant aussi un plongement dans $\mathbb{C}$, que la suite des polynômes de division modulo p est périodique et précise "It would be interesting to find a purely finite field proof".

Dans cet article, on apporte, non seulement, une démonstration élémentaire et sans utiliser l'analyse complexe, de la périodicité modulo p de la suite des polynômes de division $(\psi_n(P))_{n\in Z}$ en un point $P \in E[r]$ mais on précise aussi le résultat connu à ce jour [1], [3].

La courbe elliptique E est donnée par une équation projective définie par $\mathcal{F}(x, y, z) = y^2z - (x^3 + axz^2 + bz^3) = 0$ avec a et b dans $\mathbb{F}_q$. Le discriminant $\Delta = 4a^3 + 27b^2$ est non nul dans $\mathbb{F}_q$.On a

$$E(\mathbb{F}_q) = \{[x : y : z] \in \mathbb{P}^2(\mathbb{F}_q) \mid \mathcal{F}(x, y, z) = 0\} = \{(x, y) \in \mathbb{F}_q^2 \mid \mathcal{F}(x, y, 1) = 0\} \cup \{O_E\}$$

Received by the editors January 25, 2005. Revision Received September 9, 2005.
2000 *Mathematics Subject Classification.* 11G07, 4H52.
Key words and phrases. Courbes elliptiques ; polynômes de division ; suites elliptiques.

avec O_E l'unique point à l'infini de la courbe et qui est l'élément neutre de la loi de groupe sur E.

La loi de groupe sur $E(\mathbb{F}_q)$ est précisée par la proposition suivante [4] :

Proposition 1. *Soit E une courbe elliptique sur $\mathbb{F}_q$, un corps fini de caractéristique différente de 2 et 3, d'équation affine $\mathcal{F}(x,y,1)=0$.*

(1) *Soit $P_0=(x_0,y_0)\in E$. Alors $-P_0=(x_0,-y_0)$.*

(2) *Soit $P_1+P_2=P_3$ avec $P_i=(x_i,y_i)\in E$.*
Si $x_1=x_2$ et $y_1=-y_2$, alors $P_1+P_2=O_E$.
Sinon, soit
$$\begin{cases} \lambda=\frac{y_1-y_2}{x_1-x_2} & \text{si } x_1\neq x_2 \\ \lambda=\frac{3x_1^2+a}{2y_1} & \text{si } x_1=x_2 \end{cases}$$
alors $x_3=-x_1-x_2+\lambda^2$ et $y_3=\lambda(x_3-x_1)-y_1$.

Les polynômes de division $\psi_n(x,y)$ de la courbe elliptique E sont définis par les relations de récurrence suivantes [4] :
$$\psi_0(x,y)=0\ ;\ \psi_1(x,y)=1\ ;\ \psi_2(x,y)=2y;$$
$$\psi_3(x,y)=3x^4+6ax^2+12bx-a^2;$$
$$\psi_4(x,y)=2y(x^6+5ax^4+20bx^3-5a^2x^2-4abx-8b^2-a^3)$$
et pour n entier, $\psi_{-n}=-\psi_n$ puis pour tout (m,n) dans $\mathbb{Z}^2$
$$\psi_{m+n}\psi_{m-n}=\psi_{m+1}\psi_{m-1}\psi_n^2-\psi_{n+1}\psi_{n-1}\psi_m^2.$$
Ainsi, $\psi_{2n+1}=\psi_{n+2}\psi_n^3-\psi_{n+1}^3\psi_{n-1}$ et $\psi_{2n}\psi_2=\psi_n(\psi_{n+2}\psi_{n-1}^2-\psi_{n-2}\psi_{n+1}^2)$.

2. Propriétés

Pour $P=(x,y)\in E(\bar{F}_q)$, on pose $nP=(x(nP),y(nP))=(x_n,y_n)$. Les deux résultats qui suivent sont connus mais il n'existe pas dans la littérature de démonstration sans utiliser l'analyse complexe.

Proposition 2. *Soit $P=(x,y)\in E(\bar{F}_q)$. On a*

$$x_n=x-\frac{\psi_{n-1}\psi_{n+1}}{\psi_n^2} \tag{1}$$

$$y_n=\frac{\psi_{n+2}\psi_{n-1}^2-\psi_{n-2}\psi_{n+1}^2}{4y\psi_n^3}. \tag{2}$$

Démonstration On a $x_{n+m}=x_{n-m}-\frac{4y_ny_m}{(x_n-x_m)^2}$. Si (1) est vraie au rang n et m, alors $x_n-x_m=\frac{\psi_{m+n}\psi_{m-n}}{\psi_n^2\psi_m^2}$. D'autre part, $4y_ny_m=\frac{\psi_{2n}\psi_{2m}}{\psi_n^4\psi_m^4}$ et $\psi_{2n}\psi_{2m}=-\psi_{(n-m)+(n+m)}\psi_{(n-m)-(n+m)}=\psi_{n+m-1}\psi_{n+m+1}\psi_{n-m}^2-\psi_{n-m+1}\psi_{n-m-1}\psi_{n+m}^2$.
Ainsi, si, en plus, (1) est vraie au rang $n-m$, alors elle est vraie au rang $n+m$.

Pour les ordonnées, on utilise l'égalité $x_{n+2}=x_n-\frac{4y_{n+1}y}{(x_{n+1}-x)^2}$.

Une simple récurrence complète la démonstration.

Proposition 3. *Soit $P=(x,y)\in E(\bar{F}_q)$. On a*

$$P\in E[r]\Leftrightarrow \psi_r(x,y)\equiv 0 \bmod p. \tag{3}$$

Démonstration • Pour $r = 2$, si $p \mid 2y$, alors $y \equiv -y \bmod p$ ainsi $2P = (x, y) + (x, -y) = 0_E$. Réciproquement, si $2P = O_E$, alors $P = -P$ et donc $2y \equiv 0 \bmod p$.

• Pour $r = 2n$, on utilise l'égalité $\psi_{2n} = 2y_n\psi_n^4$. Si $p \mid \psi_{2n}$, alors, par hypothèse de récurrence, le cas $p \mid \psi_n$ entraîne $nP = 0_E$ et si $p \mid y_n$, alors $2nP = nP + nP = nP - nP = 0_E$. Réciproquement, si $2nP = O_E$, alors $2y_n \equiv 0 \bmod p$.

• Pour $r = 2n + 1$, on utilise l'égalité $\psi_n^2\psi_{n+1}^2(x_n - x_{n+1}) = \psi_{2n+1}$. De $\psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n+1}^3\psi_{n-1}$, si $p \mid \psi_n$, alors $p \mid \psi_{n+1}$ ou $p \mid \psi_{n-1}$ donc $P = 0_E$. De même si $p \mid \psi_{n+1}$, ainsi $p \mid x_n - x_{n+1}$ et on a donc, de l'équation de (E), $p \mid y_{n+1}^2 - y_n^2$. Par suite $p \mid y_{n+1} + y_n$ d'où $(n+1)P = -nP$. Réciproquement, on a donc $x_{n+1} - x_n \equiv 0 \bmod p$ d'où $p \mid \psi_{2n+1}$.

3. Périodicité des polynômes de division

Théorème 1. *Soient $\mathbb{F}_q$ un corps fini, $E/\mathbb{F}_q$ une courbe elliptique et $P \in E(\bar{\mathbb{F}}_q)$ un point d'ordre exact $r \geq 2$. Alors, il existe $w \in \bar{\mathbb{F}}_q$, dépendant de P, tel que*

(1) *si $r \geq 3$, alors pour tout k et n de $\mathbb{Z}$,*

• *si $r = 2m$, on a*

$$\psi_{rk+n}(P) = (-1)^{k^2} w^{k(n+km)} \psi_n(P). \tag{4}$$

• *si $r = 2m + 1$, on a*

$$\psi_{rk+n}(P) = (-1)^{k^2} w^{k(2n+k(2m+1))} \psi_n(P). \tag{5}$$

(2) *si $r = 2$, alors pour tout k de $\mathbb{Z}$*

$$\psi_{4k+1}(P) = (-1)^k \psi_3^{k(2k+1)}, \tag{6}$$

$$\psi_{4k+3}(P) = (-1)^k \psi_3^{(k+1)(2k+1)}. \tag{7}$$

Remarque Dans sa thèse [2], Shipsey étudie ces suites modulo p^2. Il serait intéressant d'obtenir une généralisation modulo p^k pour $k \in \mathbb{N}$.

Démonstration Les relations sont vraies pour $k = 0$.

(1) • Si $r = 2m \geq 3$, alors on pose $w = \frac{\psi_{m+1}}{\psi_{m-1}}$. On suppose d'abord que $k = 1$. La relation est donc vraie pour $n = -m + 1$. On la démontre par récurrence sur n, pour $-m + 1 \leq n \leq -1$. Au rang $n + 1$, l'égalité $x((2m + n)P) = x(-nP)$ conduit à l'expression correspondante pour ψ_{2m+n+1}. La relation est évidemment vraie pour $n = -m$ et $n = 0$ et donc pour n tel que $-m \leq n \leq 0$. Pour n tel que $-2m + 1 \leq n \leq -m - 1$, on pose $-d = r + n$ ainsi $-m + 1 \leq d \leq -1$ par suite $\psi_{r+d}(P) = -w^{d+m}\psi_d(P)$ et donc $\psi_{-d} = u^{-d-m}\psi_{r+d}(P)$ c'est à dire $\psi_{r+n}(P) = -w^{n+m}\psi_n(P)$. De là, on a, pour tous entiers n tels que $-r \leq n \leq 0$, $\psi_{r+n}(P) = -w^{n+m}\psi_n(P)$. Le passage de n à $n+1$ se démontre en exhibant l'expression de ψ_{r+n+1} dans l'égalité $x((2m + n)P) = x(nP)$ tandis que de n à $n - 1$, on exhibe l'expression de ψ_{r+n-1} dans la même égalité. Par suite pour tout $n \in \mathbb{Z}$, on a $\psi_{r+n} = -w^{n+m}\psi_n(P)$.

On suppose maintenant la relation de la proposition vraie au rang $k - 1$. L'égalité $\psi_{2km+1}\psi_{2km-3} = -\psi_1\psi_3\psi_{2km-1}^2$ conduit à l'expression de ψ_{2km+1} ($\psi_{2km-1} = \psi_{2(k-1)m+2m-1}$ et similairement pour ψ_{2km-3}) et $\psi_{2km+2}\psi_{2km-2}$ $= \psi_{2km+1}\psi_{2km-1}\psi_2^2$ conduit à celle de ψ_{2km+2}. On établit une récurrence sur

n à partir de l'égalité $x((2km+n-1)P) = x((n-1)P)$ qui donne l'expression de $\chi_n = \frac{\psi_{kr+n}(P)}{\psi_n(P)}$ en fonction de χ_{n-1} et χ_{n-2}. La récurrence descendante, pour obtenir la relation pour les entiers k négatifs, s'obtient à partir de $\psi_{2(k-1)m+n}(P) = \psi_{2km+n-2m}(P)$.

- Si $r = 2m+1 \geq 3$, alors on procède de la même manière avec $w = \frac{\psi_{m+1}}{\psi_m}$.

(2) Une récurrence, pour le cas $r = 2$, en utilisant $\psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n+1}\psi_{n-1}$ conduit facilement au résultat.

Exemple

a	b	p	P	r	m	w	k	n	$kr+n$	ψ_{kr+n}	$(-1)^{k^2}w^-\psi_n$
1	1	53	$(32,43)$	29	14	1	2	3	61	27	27
							7	9	212	39	39
							27	21	804	46	46
3	2	101	$(2,4)$	20	10	90	2	21	59	37	37
							21	12	432	28	28
							57	73	1213	63	63

Corollaire 1. *Si $P \in E(\bar{\mathbb{F}}_q)$ un point d'ordre exact égal à r, alors la suite $(\psi_n(P))_{n\in\mathbb{N}}$ est une suite périodique de période $ord(P)t$ avec $t \mid q-1$ si $ord(P) \geq 3$ et $t \mid 2q-2$ si $ord(P) = 2$.*

Démonstration C'est une simple conséquence de l'expression de l'exposant de w lorsque $r \geq 3$ et de ψ_3 lorsque $r = 2$ dans la proposition précédente. D'ailleurs, la période s'exprime en fonction de $ord(P)ord(w)$ suivant les parités respectives.

Exemple Soit la courbe elliptique d'équation $y^2 = x^3 + x + 1$ sur $\mathbb{F}_p$.

p	P	$r = ord(P)$	m	w	$ord(w)$	période	$ord(w)ord(P)$
23	$(18,20)$	28	14	10	22	616	616
23	$(12,19)$	14	7	16	11	308	154
23	$(5,4)$	7	3	9	11	154	77
53	$(8,16)$	29	14	22	52	754	1508
61	$(46,37)$	25	12	27	10	125	250
61	$(42,57)$	25	12	9	5	250	125

Remerciements

L'auteur tient à remercier le rédacteur de MRL pour ces remarques constructives.

Références

[1] M. Ayads, *Périodicité (mod q) des suites elliptiques et points S-entiers sur les courbes elliptiques*, *Annales de l'institut de Fourier*, **43**(3) (1993), 585–618.

[2] R. Shipsey, *Elliptic divisibility sequences*, Ph. D Thesis, Goldsmith's College (University of London), 2000.

[3] J. H. Silverman, *p-adic properties of division polynomials and elliptic divisibility sequences*, *Mathematische Annalen*, **332**(2)(2005), 443–471.

[4] ———, *The arithmetic of elliptic curves*, vol 106 of Graduate Texts in Mathematics. Spinger, 1986.

[5] M. Ward, *Memoir on elliptic divisibility sequences*, *Amer. J. Math* **70** (1948), 31–74.

[6] ———, *The law of repetition of primes in an elliptic divisibility sequence*, *Duke Math. J.* **15** (1948), 941–946.

ESIEE-Amiens, Ecole Supérieure d'Ingénieurs en Electronique et Electrotechnique, 14 quai de la somme-BP100, F-80082 Amiens cedex2

E-mail address: dewaghe@esiee-amiens.fr