Journal de Théorie des Nombres
de Bordeaux **10** (1998), 125–134

Nombres de racines d'un polynôme entier modulo q

par Monique BRANTON et Olivier RAMARÉ

Résumé. Nous montrons que l'ensemble des racines modulo une puissance d'un nombre premier d'un polynôme à coefficients entiers de degré d est une union d'au plus d progressions arithmétiques de modules assez grands. Nous en déduisons une majoration du nombre de ses racines dans un intervalle réel court.

Abstract. We prove that the set of the residues modulo a power of a prime number which are roots of an integral polynomial with degree d is a collection of at more d arithmetic progressions. An upper bound of the number of these roots lying in a given small interval is deduced.

1. Introduction

Soit F un polynôme à coefficients dans $\mathbb{Z}$ et q un entier ≥ 2. Nous nous intéressons à l'ensemble

$$\mathcal{N}(F,q) = \{z \in \mathbb{Z}, /\ F(z) \equiv 0\ [q]\}. \tag{1.1}$$

Notons $c(F)$ le pgcd des coefficients de F. Puisque $c(F)$ peut se mettre en facteur, il nous suffit d'étudier le cas $c(F) = 1$, hypothèse que nous prenons dans la suite. Nous dirons que F est primitif. Nous supposons en outre que F est de degré $d \geq 2$. Nous dirons F est un polynôme entier pour signifier que ses coefficients sont entiers (et non pas que ses valeurs sur les entiers sont encore des entiers). Notre premier théorème détermine la structure de $\mathcal{N}(F, p^M)$ lorsque p est un nombre premier. D'un point de vue qualitatif, nous établissons que cet ensemble est une union de moins de d progressions arithmétiques de module assez grand. Pour exprimer notre résultat, nous définissons les cônes affines convexes $\mathcal{C}(\Delta_1, \ldots, \Delta_r, M)$ dépendant des paramètres entiers strictement positifs r, $\Delta_1, \ldots, \Delta_r$ et M

Manuscrit reçu le 13 novembre 1995.

qui sont constitués des r-uplets de réels $(x_1, \ldots, x_r)$ vérifiant

$$(1.2)\qquad \begin{cases} 1 \leq x_1 \leq x_2 \leq \cdots \leq x_r, \\ \forall u \in \{1, \ldots, r\} \quad \sum_{v<u} \Delta_v x_v + \sum_{v \geq u} \Delta_v x_u \geq M + \sum_{v \neq u} \Delta_v. \end{cases}$$

Si l'on pose $d_0 = \sum_v \Delta_v$, alors les points de $\mathcal{C}(\Delta_1, \ldots, \Delta_r, M)$ satisfont à

$$(1.3)\qquad d_0 x_u \geq M + d_0 - \Delta_u \qquad (\forall u \in \{1, \ldots, r\}),$$

et en particulier à $d_0 x_u \geq M + r - 1$. Nous avons alors

Théorème 1. *Soit F un polynôme primitif entier de degré $d \geq 2$, p un nombre premier et $M \geq 1$ un entier. Supposons que F admette une racine modulo p^M. Alors il existe un entier $r \leq d$, des entiers $m_1, \ldots, m_r$, $\Delta_1, \ldots, \Delta_r$ tous ≥ 1 et $y_1, \ldots, y_r$ tels que*

$$\sum_{i=1}^{r} \Delta_i \leq d \quad , \quad (m_1, \ldots, m_r) \in \mathcal{C}(\Delta_1, \ldots, \Delta_r, M) \quad , \quad \mathcal{N}(F, p^M) = \bigcup_{u=1}^{r} y_u + p^{m_u}\mathbb{Z}.$$

De plus cette dernière union est disjointe.

Cette description de $\mathcal{N}(F, p^M)$ appelle quelques commentaires. Tout d'abord il est possible d'avoir $\bigcup_{u \in I} y_u + p^{m_u}\mathbb{Z} = z + p^n\mathbb{Z}$ pour certains sous-ensembles I (auquel cas nous dirons qu'il y a amalgame), mais nous ne pouvons plus garantir de minoration sur n, ni même garantir $n \geq 1$. De tels exemples sont donnés par $F = X^p - X$ modulo p et $F = X^p - p^{p-1}X$ modulo p^3. Une telle situation est bien sûr impossible si $d < p$. Ensuite les bornes données sont optimales comme l'on s'en convainc avec les exemples $F = X^d$ qui correspond à $d_0 = d$ et $r = 1$, et $F = (X - p^m)(X - 2p^m) \ldots (X - dp^m)$ pour $d \leq p$ et $M = dm + 1$ où l'on a $d_0 = d = r$ et $m_u = m + 1$.

Nous le démontrons en deux temps : le premier consiste à ramener le problème à un problème combinatoire que nous étudions dans un second temps. Notre approche diffère notoirement de l'approche classique qui consiste à relever de proche en proche les solutions modulo p à l'aide d'un lemme de Hensel en ce que nous nous donnons l'ensemble de solutions a priori et en étudions la structure.

Nous utiliserons le résultat précédent pour majorer la quantité

$$(1.4)\qquad \mathrm{N}(F, q, I) = \mathrm{Card}(\mathcal{N}(F, q) \cap I)$$

où I est un intervalle réel de longueur L. Nagell & Ore (cf [Na]), Sándor (cf [Sa]) et Huxley (cf [Hu]) ont donné des majorations de $\mathrm{N}(F, q, [1, q]) = q\rho(F, q)$ en fonction du discriminant de F, mais ces bornes (excellentes dans beaucoup de cas) demandent d'une part de connaître ce discriminant et d'autre part ne donnent aucun résultat si ce discriminant est nul. En 1923, Kamke [Ka] établissait la majoration $\rho(F, q)q^{1/d} \leq \tau(q)^{(d-1)}$ (où $\tau(q)$

est le nombre de diviseurs de q) qui fut améliorée en 1977 dans le cas où q admet beaucoup de facteurs premiers par Stečkin [St] en

$$\rho(F,q)q^{1/d} \leq \exp\left\{cd\left(\frac{(\operatorname{Log} q)^{1/d}}{\operatorname{Log}\operatorname{Log} q}+1\right)\right\}.$$

Finalement en 1980, Konjagin [Ko] donnait une majoration de $q^{1/d}\rho(F,q)$ indépendante de q et son résultat est optimal : il obtient $\rho(F,q) \leq C_0(d)q^{-1/d}$ où $C_0(d) = d/e + \mathcal{O}(\operatorname{Log}^2 d)$ et montre que le terme principal de $C_0(d)$ ne peut pas être réduit. Notons que les références que nous donnons de cet article (écrit en russe en 1979) sont les références de la traduction et que cette traduction tient compte du corrigendum. Le théorème 1 donne facilement $q^{1/d}\rho(F,q) \leq \exp(1.6d)$.

En combinant le résultat de Konjagin avec le théorème 1, nous obtenons ici des majorations de $N(F,q,I)$ dans le cas d'un interval I court.

Théorème 2. *$N(F,q,I) = \rho(F,q)L + \theta d^{\omega(q)}$ où $|\theta| \leq 1$ et où $\omega(q)$ est le nombre de facteurs premiers de q comptés sans multiplicité. En particulier, nous avons $N(F,q,I) \leq C_0(q)L\,q^{-1/d} + d^{\omega(q)}$.*

Cette borne est valable sans exception mais la preuve du théorème 2 donne une meilleure majoration dans beaucoup de cas. Par exemple, si q est sans facteurs carrés, alors $N(F,q,I) \leq d^{\omega(q)}(L\,q^{-1}+1)$. Dans le cas $L = q$, le théorème 2 contient le résultat de Konjagin (au terme d'erreur près).

Les méthodes employées sont élémentaires. Nous proposerons une approche plus algébrique dans un travail à venir. Notons que des majorations de ce type sont utiles pour étudier le nombre de points au voisinage de courbes régulières (cf [HS1], [HS2]).

2. Réduction à un problème combinatoire

Le lemme suivant détermine la structure de l'ensemble des solutions d'une équation polynomiale modulo une puissance d'un nombre premier en fonction de systèmes d'équations linéaires. Il est utile de garder l'exemple $F = (X-1)^2 + p$ en tête.

Lemme 3. *Soit $F \in \mathbb{Z}[X]$ un polynôme primitif, p un nombre premier et $M \geq 1$ un entier. Il existe un entier $d_0 \leq \deg(F)$ et $2d_0$ entiers $\rho_1,\dots,\rho_{d_0} \in \mathbb{Z}$ et $\ell_1,\dots,\ell_{d_0} \in [0,M]$ tels que pour tout $m \leq M$ on ait*

$$F(z) \equiv 0\ [p^m] \iff \begin{cases} \forall i \in [1,d_0],\ \exists h_i \in [0,M],\ z \equiv \rho_i\ [p^{h_i}], \\ \forall i \in [1,d_0],\ \displaystyle\sum_{j=i}^{d_0} h_j \leq \ell_i \quad ,\sum_{i=1}^{d_0} h_i = m. \end{cases}$$

Preuve. Nous raisonnons par récurrence sur le degré de F. Pour les besoins de la récurrence nous supposons uniquement que $(c(F),p)=1$ et nous dirons que F est p-primitif. Supposons tout d'abord que $F=aX+b$. Si $(a,p)=1$, la propriété est aisément établie. Sinon $(b,p)=1$ et l'équation $az+b\equiv 0\ [p^m]$ n'admet de solutions que si $m=0$. Nous prenons alors $d_0=1$, $\ell_1=0$ et $\rho_1=0$.

Soit maintenant F un polynôme p-primitif de degré ≥ 2. Soit ℓ_0 le plus grand des entiers $m\leq M$ pour lesquels $F(z)\equiv 0\ [p^m]$ admet une solution. Soit ρ_0 une racine de F modulo p^{ℓ_0}. Ecrivons $F(X)\equiv (X-\rho_0)G(X) \mod p^{\ell_0}$ où G est p-primitif défini modulo p^M et de degré $=\deg(F)-1$. Notre hypothèse de récurrence permet alors de conclure facilement. □

Remarquons que le lemme précédent n'est pas tout à fait complet puisque tous les systèmes $(M,d_0,\rho_1,\ldots,\rho_{d_0},\ell_1,\ldots,\ell_{d_0})$ ne sont pas possibles. Par exemple si $\deg(F)=1$, on a nécessairement $\ell_{d_0}=\ell_1=0$ ou M. Nous pouvons par ailleurs supposer $\ell_1\geq\ell_2\cdots\geq\ell_{d_0}$ quitte à remplacer ℓ_i par $\ell_i^*=\min(\ell_1,\ell_2,\ldots,\ell_i)$, ce que nous ferons dans la suite.

Il serait intéressant de construire un polynôme G dépendant uniquement des ℓ_i et ρ_i tel que $F(z)\equiv 0\ [p^M] \iff G(z)\equiv 0\ [p^M]$. Dans cette direction, nous avons le résultat suivant.

Corollaire 4. *Pour tout polynôme primitif entier F de degré $d\geq 1$, et pour tout entier $q\geq 1$, il existe des entiers $\rho_1,\ldots,\rho_d$ tels que pour tout diviseur q' de q on ait*

$$F(z)\equiv 0\ [q'] \ \Rightarrow\ \prod_{k=1}^{d}(z-\rho_k)\equiv 0\ [q'].$$

Preuve. Lorsque $q=p^M$, le lemme précédent nous donne un entier $d_0\leq\deg(F)$ et d_0 entiers $\rho_1,\ldots,\rho_{d_0}$ tels que pour tout $z\in\mathbb{Z}$ et tout $m\leq M$, on ait

$$F(z)\equiv 0\ [p^m] \ \Rightarrow\ \prod_{i=1}^{d_0}(z-\rho_i)\equiv 0\ [p^m]. \tag{2.1}$$

Il nous suffit pour cela de majorer les ℓ_i par M. Quite à rajouter des ρ_i, nous pouvons supposer que $d_0=\deg(F)$. En utilisant le théorème chinois, nous obtenons notre corollaire. □

Nous donnons maintenant une formulation du lemme 3 où les variables h_i n'interviennent plus. Pour cela nous posons

$$v_{p,m}(z)=\min(m,v_p(z)) \qquad (v_{p,0}(z)=0) \tag{2.2}$$

où $v_p(z)$ est le plus grand des entiers n tels que $p^n|z$. La valeur de $v_{p,m}(z)$ ne dépend que de la classe de z modulo p^m ce qui justifie l'écriture $v_{p,m}(z)$

si z est un entier modulo p^n avec $n \geq m$. Les entiers $\ell_1, \ldots, \ell_{d_0}$ étant fixés, nous posons

(2.3)
$$\begin{cases} D_{d_0}(z,m) = \min(\ell_{d_0}, v_{p,m}(z-\rho_{d_0})), \\ D_i(z,m) = \min(\ell_i, v_{p,m}(z-\rho_i) + D_{i+1}(z,m)) \quad (1 \leq i \leq d_0 - 1). \end{cases}$$

Lemme 5. *Sous les hypothèses et notations du lemme 3, nous avons pour tout $m \leq M$:*

$$F(z) \equiv 0\ [p^m] \iff D_1(z,m) \geq m.$$

Preuve. Le plus simple consiste à reprendre la démonstration du lemme 3 avec une hypothèse de récurrence adaptée au lemme 5. Les détails ne posant aucun problème, nous laissons cette preuve au soin du lecteur. □

3. Preuve du théorème 1

Soit donc p un nombre premier, $M \geq 1$ un entier et F un polynôme entier primitif admettant une racine modulo p^M.

Nous considérons le graphe orienté construit sur $\{(x,m), x \in \mathbb{Z}/m\mathbb{Z}, 0 \leq m \leq M\}$ où l'on met une arête de (x,m) à (x',m') si et seulement si $m' = m-1$ et $x \equiv x'\ [p^{m'}]$. Il s'agit donc d'un arbre de racine $(0,0)$. A chaque arête $(x,m) \to (x,m-1)$ de ce graphe nous associons le poids $\Delta_1(x,m)$ défini en (3.2) ci-dessous, de telle sorte que si l'on va de (x,m) à $(0,0)$, la somme des poids des arêtes que l'on parcourt est $D_1(x,m)$. Nous considérons ensuite l'ensemble $\mathcal{S}$ des points (x,m) tels que $D(x,m) \geq M$. Cet ensemble vérifie "si $(x,m) \to (x,m-1)$ et si $(x,m-1) \in S$, alors $(x,m) \in \mathcal{S}$". Il est important de remarquer que $\mathcal{S}$ n'est pas toujours égal à l'ensemble $\mathcal{S}_0$ des points (x,m) qui vérifient

$$\forall z \in \mathbb{Z}/p^M\mathbb{Z}, \quad \big[z \equiv x\ [p^m] \implies F(z) \equiv 0\ [p^M]\big].$$

Ceci vient de ce que notre définition de D_1 permet $D_1(y,m) < \min\{D_1(z,M)\ , z \equiv y\ [p^m]\}$ comme le montre l'exemple $F = X^2 - 2X$ modulo $2^M = 8$ et $2^m = 2$. Jusqu'à présent, la seule condition demandée à D_1 est de vérifier le lemme 5 ; d'autres définitions auraient pu convenir, certaines d'entre elles vérifiant la propriété juste mentionnée. Mais alors la possibilité d'avoir des amalgames rend la situation difficilement contrôlable.

Nous définissons les solutions minimales (y,m) par $D_1(y,m) \geq M > D_1(y,m-1)$. Soit $(y_1,m_1), \ldots, (y_r,m_r)$ leur collection (qui est non vide, puisque l'équation $F(x) \equiv 0\ [p^M]$ admet une solution). Il vient alors

$$\mathcal{N}(F,p^M) = \bigcup_{u=1}^{r} y_u + p^{m_u}\mathbb{Z} \tag{3.1}$$

et cette union est disjointe. Il nous faut à présent majorer r et minorer les m_u.

La croissance en m des fonctions $D_i(z,m)$ nous intéresse particulièrement. Pour tout $i \in \{1,\ldots,d_0\}$, nous posons

$$\begin{cases} \Delta_i(y,m) = D_i(y,m) - D_i(y,m-1) \geq 0 & (D_i(z,0)=0), \\ \Delta_i^*(y,m) = \mathrm{Card}\{\, j \geq i,\, \rho_j \equiv y\ [p^m]\,\}. \end{cases} \tag{3.2}$$

et $D_i^*(y,m) = \sum_{n=1}^m \Delta_i^*(y,n)$. Regardons à présent les points (ρ_i, M) et les chemins qui lient ces points à la racine de l'arbre $(0,0)$. Si un point (y,m) n'appartient pas à l'un de ces chemins, alors $D_1(y,m) = D_1(y,m-1)$ comme on le constate sur la définition (2.3). Par conséquent chaque solution minimale appartient à l'un de ces chemins ce qui nous donne déjà $r \leq d$. Le lemme suivant précise cette remarque.

Lemme 6. *Nous avons* $\Delta_i(y,m) \leq \Delta_i^*(y,m)$ *et* $\Delta_i(y,m+1) \leq \Delta_i(y,m)$ *pour* $1 \leq i \leq d_0$.

Preuve. Nous donnons tout d'abord une écriture plus explicite de Δ_i. Nous posons

$$\delta_m(z) = v_{p,m}(z) - v_{p,m-1}(z) \tag{3.3}$$

et vérifions que (avec $z = y - \rho_i$)

$$\Delta_i(y,m) = \begin{cases} \delta_m(z) + \Delta_{i+1}(y,m) \qquad \text{si } \ell_i \geq v_{p,m}(z) + D_{i+1}(y,m), \\ \delta_m(z) + \Delta_{i+1}(y,m) + \ell_i - v_{p,m}(z) - D_{i+1}(y,m) \\ \quad \text{si } v_{p,m}(z) + D_{i+1}(y,m) > \ell_i \geq v_{p,m-1}(z) + D_{i+1}(y,m-1), \\ 0 \qquad\qquad \text{si } v_{p,m-1}(z) + D_{i+1}(y,m-1) > \ell_i, \end{cases}$$

avec $\Delta_{d_0+1} = D_{d_0+1} = 0$. Une récurrence utilisant la suite d'inégalités

$$\Delta_i^*(y,m) = \delta_m(z) + \Delta_{i+1}^*(y,m) \geq \delta_m(z) + \Delta_{i+1}(y,m) \geq \Delta_i(y,m) \tag{3.4}$$

permet de conclure à la validité de la première inégalité.

Pour ce qui est de la seconde, notons tout d'abord que le cas $i = d_0$ est trivial. Pour i quelconque, nous avons trois cas à considérer. Si $\ell_i \geq v_{p,m+1}(z) + D_{i+1}(y,m+1)$ alors $\Delta_i(y,m) = \Delta_i(y,m+1)$. Si $v_{p,m}(z) + D_{i+1}(y,m+1) > \ell_i$, alors $\Delta_i(y,m+1) = 0$ ce qui règle aussi ce cas. Le dernier cas restant est $v_{p,m+1}(z) + D_{i+1}(y,m+1) > \ell_i \geq v_{p,m}(z) + D_{i+1}(y,m+1)$ auquel cas il nous suffit de vérifier que

$$\delta_m(z) + \Delta_{i+1}(y,m) \geq \delta_{m+1}(z) + \Delta_{i+1}(y,m+1)$$

ce qui est garantit par l'hypothèse de récurrence et l'inégalité $\delta_m(z) \geq \delta_{m+1}(z)$. $\square$

Les quantités $\Delta_1^*(y,m)$ sont beaucoup plus régulières que les quantités $\Delta_1(y,m)$ parce que $\Delta_1^*(y,m) = \sum \Delta_1^*(z,m+1)$ où la somme porte sur les classes z modulo p^{m+1} congrues à y modulo p^m. Comparativement nous ne savons que démontrer la seconde partie du lemme 6 pour les $\Delta_1(y,m)$.

Posons $\Delta_u^* = \Delta_1^*(y_u, m_u) \geq 1$. Nous obtenons alors

$$\sum_{u=1}^{r} \Delta_u^* = d_0 \tag{3.5}$$

parce que chaque ρ_i est compté dans au moins l'un des Δ_u^* et dans au plus un puisque sinon on aurait $y_u \equiv y_v\ [p^{\min(m_u,m_v)}]$ pour deux variables $u \neq v$, ce qui est impossible. Soit alors

$$m_{u,v} = \max\{m \leq m_u,\ y_u \equiv y_v\ [p^m]\} \geq 0. \tag{3.6}$$

Nous avons $m_{u,u} = m_u$ et $m_{v,u} = m_{u,v}$ et classiquement $m_{u,v} \geq \min(m_{u,w}, m_{w,v})$. Nous montrons facilement que

$$\Delta_1^*(y_u, m) = \sum_{v/m_{u,v} \geq m} \Delta_v^* \quad \text{pour } m \leq m_u \tag{3.7}$$

ce qui nous donne

$$D_1^*(y_u, m_u) = m_u \Delta_u^* + \sum_{v \neq u} m_{u,v} \Delta_v^*. \tag{3.8}$$

Nous ordonnons à présent les m_u de sorte à avoir $m_1 \leq m_2 \leq \cdots \leq m_r$. En utilisant le fait que $0 \leq m_{u,v} \leq m_v - 1$ si $v < u$, $0 \leq m_{u,v} \leq m_u - 1$ si $v \geq u$ et les inégalités $D_1^*(y_u, m_u) \geq D_1(y_u, m_u) \geq M$, nous obtenons

$$\sum_{v<u} \Delta_v m_v + \sum_{v \geq u} \Delta_u m_u \geq M + \sum_{v \neq u} \Delta_v. \tag{3.9}$$

Le théorème 1 en découle aisément.

4. Preuve du théorème 2

Nous considérons ici un module $q = p_1^{M(1)} \dots p_T^{M(T)}$ et utilisons le théorème 1. Il vient

$$\mathcal{N}(F,q) = \bigcap_{t=1}^{T} \bigcup_{i=1}^{r(t)} y_i(t) + p^{m_i(t)}\mathbb{Z} \tag{4.1}$$

avec des notations évidentes et où l'on a supposé qu'il existait une solution. Sinon $\mathcal{N}(F,q) = \emptyset$, cas que nous écartons. Définissons encore

$$\mathcal{Y} = \prod_{t=1}^{T} \{y_1(t), \dots, y_{r(t)}(t)\}. \tag{4.2}$$

Pour un point Y de $\mathcal{Y}$, nous définissons $m(Y,t)$ comme étant $m_i(t)$ si la t-ième coordonnée Y_t de Y est $y_i(t)$. Nous posons enfin

$$\mathcal{C}(Y) = \{z \in \mathbb{Z}, \forall t \in \{1,\dots,T\}, z \equiv Y_t\ [p_t^{m(Y,t)}]\} \tag{4.3}$$

et obtenons

$$\mathcal{N}(F,q) = \bigcup_{Y \in \mathcal{Y}} \mathcal{C}(Y). \tag{4.4}$$

Cette union est disjointe. En effet si $Y \neq Y'$, il existe un t pour lequel $Y_t \neq Y_t'$ et nous avons alors

$$\mathcal{C}(Y) \cap \mathcal{C}(Y') \subset \{z \in \mathbb{Z}, z \equiv Y_t\ [p_t^{m(Y,t)}]\} \cap \{z \in \mathbb{Z}, z \equiv Y_t'\ [p_t^{m(Y',t)}]\} = \emptyset. \tag{4.5}$$

Nous obtenons donc

$$\mathrm{N}(F,q,I) = \mathrm{Card}(\mathcal{N}(F,q) \cap I) = \sum_{Y \in \mathcal{Y}} \mathrm{Card}(\mathcal{C}(Y) \cap I). \tag{4.6}$$

Il est par ailleurs trivial de constater que

$$L \prod_{t=1}^{T} p_t^{-m(Y,t)} - 1 \leq \mathrm{Card}(\mathcal{C}(Y) \cap I) \leq L \prod_{t=1}^{T} p_t^{-m(Y,t)} + 1 \tag{4.7}$$

ce qui nous donne qu'il existe un $\theta \in [-1,1]$ tel que

$$\mathrm{N}(F,q,I) = L \prod_{t=1}^{T} (p_t^{-m_1(t)} + p_t^{-m_2(t)} + \cdots + p_t^{-m_{r(t)}(t)}) + \theta \sum_{Y \in \mathcal{Y}} 1. \tag{4.8}$$

Nous majorons le terme d'erreur par $d^T = d^{\omega(q)}$. Pour ce qui est du terme principal, nous utilisons deux approches. Tout d'abord ce terme principal est égal à $L\,\mathrm{N}(F,q,[1,q])/q$ ce qui nous permet d'utiliser la majoration de Konjagin et d'obtenir le théorème 2. Nous montrons à présent comment obtenir ce même résultat avec une constante plus élevée à l'aide du lemme suivant.

Lemme 7. *Nous avons*

$$p_t^{-m_1(t)} + p_t^{-m_2(t)} + \cdots + p_t^{-m_{r(t)}(t)} \leq \min(1, d\, p_t^{-\lceil M(t)/d \rceil}, C(p_t,d)\, p_t^{-M(t)/d}),$$

avec $C(p,d) = \max(1, d\, p^{-1+1/d})$ *et où* $\lceil x \rceil$ *désigne la partie entière par valeur supérieure du réel* x.

Preuve. Pour simplifier l'écriture nous n'indiquerons pas la dépendance des variables en t. Notre expression est inférieure à 1 puisqu'il s'agit d'une densité. Cette majoration est efficace lorsque p est petit. De plus chaque

m_i est supérieur à M/d et donc à $\lceil M/d \rceil$ puiqu'il s'agit d'entiers. Nous démontrons à présent la troisième inégalité. Nous avons

$$p^{-m_1} + p^{-m_2} + \cdots + p^{-m_r} \leq p^{-M/d_0} \sum_{i=1}^{r} p^{(d_0-\Delta_i)/d_0} = S(d_0; r; \Delta_1, \ldots, \Delta_r),$$

et nous souhaitons déterminer le maximum de cette quantité sur l'ensemble fini $\mathcal{V}$ des paramètres $V = (d_0; r; \Delta_1, \ldots, \Delta_r)$ vérifiant les contraintes du théorème 1. Tout d'abord, si $V \in \mathcal{V}$ est tel qu'il existe deux indices $i \neq j$ avec $\Delta_i \geq \Delta_j \geq 2$, alors le point V' obtenu à partir de V en remplaçant Δ_i par $\Delta_i + 1$ et Δ_j par $\Delta_j - 1$ vérifie $S(V) \leq S(V')$ puisque

$$S(V') - S(V) = p^{-M/d_0}(\alpha - 1)(\alpha^{\Delta_i} - \alpha^{\Delta_j - 1}) \geq 0 \qquad (\text{où } \alpha = p^{1/d_0}).$$

Nous pouvons donc prendre $\Delta_1 = d_0 - r + 1$ et $\Delta_i = 1$ si $i \geq 2$. Pour un tel point V, nous avons

$$S(V) = p^{-\frac{M}{d_0} - 1} \left(p^{\frac{d_0 - r + 1}{d_0}} + (r-1) p^{\frac{1}{d_0}} \right)$$

Nous vérifions sur cette expression qu'il suffit de prendre $d_0 = d$. Pour le point V correspondant, nous avons

$$S(V) = p^{-\frac{M}{d} + \frac{1}{d}} \left(p^{-\frac{r}{d}} + \frac{r}{p} - \frac{1}{p} \right).$$

Cette expression est décroissante puis croissante en r, ce qui fait qu'il suffit de considérer les valeurs $r = 1$ et $r = d$, d'où notre troisième majoration. $\square$

Nous obtenons alors

$$\text{(4.9)} \quad \mathrm{N}(F, q, I) \leq L\, q^{-1/d} \prod_{p^M \| q} \min \left(p^{M/d}, d p^{M/d - \lceil M/d \rceil}, C(p, d) \right) + d^{\omega(q)},$$

majoration qui est dans certains cas plus précise que celle du théorème 2. Posons

$$\text{(4.10)} \qquad C(d) = \prod_{p \geq 2} C(p, d).$$

En utilisant $\sum_{p \leq x} 1 \leq 1.26x/\operatorname{Log} x$ pour $x > 1$ (cf [RS] (3.6)), nous obtenons $\operatorname{Log} C(d) \leq 1.6d$ pour $d \geq 2$, ce qui conclut la preuve.

- *Deux questions.*

1— Pour obtenir le théorème 2, nous avons utilisé le procédé de crible le plus simple et il est légitime de penser qu'une amélioration de ce procédé réduise le terme d'erreur. Parmi les diverses façons d'aborder ce problème, nous signalons le problème annexe suivant : A-t-on $N(F, q, I) \gg d^{\omega(q)}$ si $\omega(q)$ est grand et $L = |I| = q^{1/d}$?

2— Peut-on caractériser les polynômes qui ne vérifient pas la propriété suivante où $k \geq 0$ est un entier : *Pour tout $x \in \mathbb{Z}$, il existe $y \equiv x$ $[p^k]$ tel que $F(y) \not\equiv 0$ $[p^{kd+1}]$?*

Pour $k = 0$, il suffit que $X^p - X$ ne divise pas F. Si l'on utilise le théorème 1 avec $M = kd + 1$, on obtient $m_u \geq k + 1$. Par conséquent, si les progressions $y_u + p^{m_u}\mathbb{Z}$ ne s'amalgament pas en une progression de module plus petit (ce qui est le cas si $d < p$), la propriété est vérifiée. Sinon après tous les amalgames, on atteint au pire une progression de module $p^{m_u - [d/p]}$, et donc nous pouvons trouver y modulo p puissance $k - [d/p]$ si $k \geq [d/p]$.

Bibliographie

[Hu] M.N. Huxley, *A note on polynomial congruences* , dans Recent progress in analytic number theory, vol.1 édité par H. Halberstam & C. Hooley (1981), 193–196.

[HS1] M.N. Huxley & P. Sargos *Points entiers au voisinage d'une courbe plane de classe C^n, I*, Acta Arith. **69** (1995), 359–366.

[HS2] M.N. Huxley & P. Sargos *Points entiers au voisinage d'une courbe plane de classe C^n, II*, En préparation.

[Ka] E. Kamke, *Zur Arithmetik der Polynome*, Math. Z. **19** (1923/1924), 247–264.

[Na] T. Nagell, An introduction to number theory, New-York (1964).

[Ko] S.V. Konjagin, *On the number of solutions of an nth degree congruence with one unknown*, Math. USSR Sbornik **37** (1980), no 2, 151–166.

[RS] J.B. Rosser & L. Schoenfeld, *Formulas for some functions of prime numbers*, Ill. J. of Math. **6** (1962), 64–94.

[Sa] G. Sándor, *Über die Anzahl der Lösungen einer Kongruenz*, Acta Math. **87** (1951-52), 13–16.

[Se] J.P. Serre, Corps locaux, Hermann, 1968.

[St] S.B. Stečkin, *Estimate of a complete rational trigonometric sum*, Trudy Mat. Inst. Steklov. **143** (1977), 188–207 ; English transl. in Proc. Steklov Inst. Math. **143** no 1 (1980).

Olivier Ramaré
Département de Mathématiques
Université Lille 1
59655 Villeneneuve d'Ascq Cedex
France