Collect. Math. **40**, 1 (1989), 1–11

Plus petit commun multiple des termes consécutifs d'une suite récurrente linéaire

JEAN-PAUL BÉZIVIN

Université Paris VI, Mathématiques, 4 Place Jussieu, 75005 Paris, France

Received 16/JUN/89

ABSTRACT

Let a, b be coprime rational integers, and $u(n)$ the binary recurrent sequence $u(n+2) = au(n+1) + bu(n)$, with the initial values $u(0) = 0$ and $u(1) = 1$. It is proved in [4] that the quotient of the logarithm of the product of the $u(k)$, $1 \leq k \leq n$, and of the logarithm of the least common multiple of the $u(k)$, $1 \leq k \leq n$, converges to $\pi^2/6$ when n goes to infinity. In this paper, we generalize this result to other recurrent sequences. As an example, for the binary sequence above with initial values $u(0) = 2$ and $u(1) = a$, the limit is $\pi^2/8$.

1. Introduction

Soient a et b deux éléments de $\mathbb{Z}$, avec b non nul et a et b premiers entre eux. On considère la suite récurrente linéaire $u(n)$, vérifiant la récurrence

$$u(n+2) = au(n+1) + bu(n) \tag{1}$$

pour tout n dans $\mathbb{N}$, les valeurs initiales étant $u(0) = 0$ et $u(1) = 1$.

Nous supposerons dans toute la suite que le polynôme caractéristique $Q(X) = X^2 - aX - b$ de la suite $u(n)$ a ses racines distinctes dans une clôture algébrique $\bar{\mathbb{Q}}$ de $\mathbb{Q}$, racines que nous noterons α et β.

Il est alors bien connu que la suite $u(n)$ a l'expression:

$$u(n) = \frac{\alpha^n - \beta^n}{\alpha - \beta}\ . \tag{2}$$

Nous supposerons aussi dans toute la suite que le quotient α/β n'est pas une racine de l'unité et que $|\alpha| \geq |\beta|$, de sorte que l'on a $|\alpha| > 1$.

Nous notons enfin $P(n)$ le plus petit commun multiple des termes $u(k)$, k variant entre 1 et n.

On a alors le résultat suivant:

Théorème A

La suite

$$w(n) = \frac{\log(u(1)\cdots u(n))}{\log P(n)}$$

a pour limite la quantité $\pi^2/6$ quand n tend vers $+\infty$.

Le théorème A est du à Matiyasevitch et Guy [5] dans le cas de la suite de Fibonacci (cas $a = b = 1$), à Davis [3] pour le cas ($a \in \mathbb{Z}$, $b = 1$) et ($a \in \mathbb{Z}$, a pair, $b = -1$) et enfin à Kiss et Matyas [4] dans le cas général.

Dans cet article nous nous proposons de généraliser le théorème A, à d'autres suites récurrentes linéaires, possédant comme la suite $u(n)$ donnée par (2) de bonnes propriétés de factorisation.

Soit n un entier naturel positif, nous notons si $m = 1$ par $u_1(n)$ la suite $u(n)$ et pour m plus grand que 1, par $u_m(n)$ la suite

$$u_m(n) = \frac{\alpha^{mn} - \beta^{mn}}{\alpha^n - \beta^n}$$

pour n non nul.

Nous notons $P_m(n)$ le plus petit commun multiple des termes $u_m(k)$ pour k variant entre 1 et n.

Nous allons démontrer le résultat suivant, où φ est la fonction d'Euler:

Théorème

La suite

$$w_m(n) = \frac{\log(u_m(1)\cdots u_m(n))}{\log P_m(n)}$$

a pour limite $\pi^2/6$ si m est égal à 1 et sinon la quantité

$$C(m) = \frac{(m-1)L(M)\pi^2}{6H(m)}$$

où nous avons noté $L(m)$ le produit des $1 - 1/p^2$ pour p premier divisant m, $H(m)$ la somme des termes $\varphi(d)\varphi(m/d)d/m$ pour d divisant m, d plus grand que 1.

EXEMPLES. 1) Considérons le cas $m = 2$. qui correspond à la suite récurrente binaire $u_2(n) = \alpha^n + \beta^n$. La limite est alors $\pi^2/8$.

2) Pour la suite $u_3(n) = \alpha^{2n} + (\alpha\beta)^n + \beta^{2n}$. qui vérifie une récurrence d'ordre 3, la limite est $4\pi^2/27$.

Nous suivrons une méthode différente de celle utilisée dans [4[ou [5]; celle-ci utilisait assez largement les propriétés arithmétiques de la suite $u(n)$ donnée par (2). En fait il semble que ce soit surtout les propriétés de factorisation assez formelles de la suite $u(n)$ qui interviennent. Pour le voir, nous allons décrire rapidement un problème analogue pour les polynômes.

Nous considérons le plus petit commun multiple dans $\mathbb{Q}[X]$ des polynômes $X^k - 1$, où k varie entre 1 et n, que nous notons $Q_n(X)$, et le produit des $X^k - 1$, que nous notons $S_n(X)$. Nous voulons comparer les degrés de Q_n et S_n.

Notons pour cela que l'on a la formule

$$X^k - 1 = \prod_{d|k} \phi_d(X),$$

où ϕ_d est le d ième polynôme cyclotomique; on en déduit facilement que le polynôme $Q_n(X)$ est le produit des $\phi_d(X)$ où d est inférieur où égal à n. On a donc les résultats suivants: le degré de S_n est égal à $n(n+1)/2$, et le degré de Q_n est égal à la somme des $\varphi(d)$ pour d inférieur ou égal à n. On sait que cette dernière somme est équivalente a $3n^2/\pi^2$ si n tend vers $+\infty$, de sorte que le rapport des degrés tend vers $\pi^2/6$.

Il s'agit de démontrer que cette propriété de nature formelle se conserve quand on spécialise la variable X, et donc que finalement les propriétés arithmétiques de la suite $u(n)$ interviennent peu.

REMARQUE. L'analogue formel du problème que nous étudions suggère la question plus générale suivante:

Soit $\mathbb{K}$ un corps commutatif de caractéristique nulle et algébriquement clos. Soit $P(X)$ un polynôme unitaire de degré non nul. et de terme constant non nul. On note $Q_n(X)$ le plus petit commun multiple des polynômes $P(X^k)$ pour $1 \leq k \leq n$, et $S_n(X)$ le produit des $P(X^k)$ pour $1 \leq k \leq n$. Comparer les degrés de Q_n et de S_n.

Ce que nous allons démontrer dans les lignes qui suivent permet de donner la solution à cette question dans le cas des polynômes $X - 1$ et pour $m \geq 2$ de $(X^m - 1)/(X - 1)$.

Il est d'autre part assez facile de voir que si aucune des racines de $P(X)$ n'est une racine de l'unité et s'il n'y a pas de relation multiplicative entre deux racines de $P(X)$, alors $Q_n = S_n$.

Il serait intéressant d'avoir la réponse dans le cas général: on peut envisager aussi de regarder le même type de question pour des polynômes à plusieurs variables.

2. Résultats préliminaires

Nous aurons besoin des résultats suivants:

Lemme 1 (Schinzel [6])

Soit $\mathbf{K}$ *un corps de nombres et* α *et* β *deux entiers algébriques de* $\mathbf{K}$, *de même valeur absolue, mais tels que* α/β *ne soit pas une racine de l'unité. Alors on a:*

$$\log \left| \left(\frac{\alpha^n}{\beta} \right)^n - 1 \right| = O(\log n)$$

si n *tend vers* $+\infty$.

Lemme 2 (Apostol [1])

Soient q *et* n *deux entiers positifs distincts. On note* $R(\phi_q, \phi_n)$ *le résultant de* ϕ_q *et* ϕ_n. *Alors on a les résultats suivants:*

1) Si $q > 1$, $R(\phi_q, \phi_n) = p$ *ou* 1 *suivant que* q *est une puissance de* p *ou non.*

2) Si q *et* n *sont premiers entre eux, le résultant de* ϕ_q *et de* ϕ_n *est égal à un.*

3) Si $q > n$ *et* q *et* n *ne sont pas premiers entre eux,* $R(\phi_q, \phi_n)$ *est égal à* $p^{\varphi(n)}$ *ou* 1 *suivant que* q/n *est une puissance de* p *ou non.*

Lemme 3

Soit m *un entier naturel plus grand que* 1, *et* h *un diviseur de* m *différent de* 1. *On note* $S(h, m)$ *la somme*

$$\sum \frac{(h \wedge k)\mu(k)}{k^2},$$

où $h \wedge k$ est le plus grand commun diviseur de h et de k, $\mu(k)$ est la fonction de Moebius, et où la sommation a lieu sur les indices k tels que $k/(k \wedge h)$ et m/h soient premiers entre eux. Alors on a

$$S(h,m) = \frac{6}{\pi^2} \prod_{p|m} \left(1 - \frac{1}{p^2}\right)^{-1} \left(\sum_{d|h} \frac{\mu(d)}{d}\right).$$

Preuve. Tout d'abord l'ensemble de sommation peut être remplacé par l'ensemble des k tels que aucun premier p divisant m/h, mais ne divisant pas h, ne divise k. En effet si k appartient à l'ensemble de sommation du départ, il est clair que si p premier divise m/h et ne divise pas h, p ne peut diviser k; l'ensemble de sommation du départ est donc inclus dans le second. Soit maintenant un indice k appartenant au second ensemble et pas au premier. Alors, puisque $k/(k \wedge h)$ et m/h ne sont pas premiers entre eux, on peut trouver un nombre premier p tel que p divise ces deux nombres. Puisque k appartient au second ensemble de sommation, on voit que le nombre premier p divise le nombre h. Donc p divise $h \wedge k$, et par suite p^2 divise k; mais alors $\mu(k)$ est nul, de sorte que le terme correspondant dans la somme est lui aussi nul. Nous supposerons dans la suite que les indices k sont sans facteurs carrés.

Nous séparons ensuite les indices k suivant les différentes possibilités pour $h \wedge k = d$.

On a donc:

$$S(h,m) = \sum d \sum \frac{\mu(k)}{k^2},$$

où la première sommation a lieu sur les diviseurs d sans facteurs carrés de h, et la seconde sur les indices k tels que pour tout p premier: a) $p|k$ si $p|d$, b) $p \nmid k$ si $p|h$ et $p \nmid d$, et enfin c) $p \nmid k$ si $p|m/h$ et $p \nmid h$.

Tout entier k satisfaisant aux conditions précédentes et sans facteurs carré peut se mettre sous la forme $k = dk_1$, où k_1 est tel que $p \nmid k_1$ si $p|d$, si $p|h$ et $p \nmid d$, ou si $p|m/h$ et $p \nmid h$. Cet ensemble de nombres premiers est exactement l'ensemble des diviseurs premiers de m de sorte que l'on a:

$$\sum \frac{(k \wedge h)\mu(k)}{k^2} = \left(\sum \frac{\mu(d)}{d}\right)\left(\sum \frac{\mu(k_1)}{k_1^2}\right),$$

où la première sommation a lieu sur les diviseurs de h, et la seconde sur les indices k_1 tels que pour p premier divisant m, p ne divise pas k_1.

On sait que l'on a

$$\sum \frac{\mu(n)}{n^s} = \prod \left(1 - \frac{1}{p^s}\right) = \frac{1}{\zeta(s)},$$

où $\zeta(s)$ est la fonction dzéta de Riemann, d'où on déduit facilement le résultat. □

Nous notons maintenant pour d entier positif par $\psi_d(\alpha,\beta)$ la quantité $\alpha^{\varphi(d)}\phi_d(\beta/\alpha)$. Pour $d>1$, $\psi_d(\alpha,\beta)$ est un élément de $\mathbb{Z}$.

On a alors le résultat suivant:

Lemme 4

Notons $Q_1(n)$ le produit des $\psi_d(\alpha,\beta)$ pour d parcourant les entiers entre 2 et n, et pour $m\geq 2$, par $Q_m(n)$ le produit $\prod\prod\psi_{dh}(\alpha,\beta)$, où le premier produit porte sur les $h\geq 2$ tels que $h|m$ et le second sur les $d\leq n$ tels que d soit premier à m/h. Alors, pour tout $n\geq 2$ et pour tout m, $P_m(n)$ (on rappelle que c'est le ppcm des $u_m(k)$, $1\leq k\leq n$) divise $Q_m(n)$ et de plus, pour tout p premier tel que $p\nmid m$ on a $v_p(P_m(n))=v_p(Q_m(n))$ pour tout n, où v_p est la valuation p-adique. En particulier, si $m=1$ on a $P_1(n)=Q_1(n)$.

Preuve. Nous considérons d'abord le cas de $m=1$; on a immédiatement la formule

$$u_1(n)=\frac{\alpha^n-\beta^n}{\alpha-\beta}=\prod\psi_d(\alpha,\beta),$$

où le produit est étendu aux diviseurs de n différents de 1. Il est donc immédiat que $P_1(n)$ divise $Q_1(n)$. Nous estimons maintenant les valuations p-adiques. On a

$$v_p(P_1(n))=\max\left(\sum v_p(\psi_d(\alpha,\beta))\right),$$

où le maximum est pris sur les $k\leq n$ et la sommation sur les d divisant k, différents de 1 et

$$v_p(Q_1(n))=\sum v_p(\psi_d(\alpha,\beta)),$$

où la sommation a lieu sur les d inférieurs ou égaux à n, différents de 1.

Soit s le plus petit entier inférieur ou égal à n tel que $v_p(\psi_s(\alpha,\beta))$ soit non nul (s'il en existe; sinon la propriété est évidente) et t un autre entier tel que $v_p(\psi_t(\alpha,\beta))$ soit non nul. On peut considérer que l'on s'est placé dans le corps p-adique $\mathbb{C}_p$; remarquons que si on a alors $|\alpha|_p$ ou $|\beta|_p$ plus petit que 1 (où nous avons noté $|x|_p$ la valeur absolue p-adique de $x\in\mathbb{C}_p$), alors les deux le sont puisque $|\psi_s(\alpha,\beta)|_p<1$, ce qui est impossible puisque les entiers a et b sont supposés premiers entre eux. Donc α et β sont des unités p-adiques. Il en résulte que l'on a $|\phi_s(\beta/\alpha)|_p<1$ et $|\phi_t(\beta/\alpha)|_p<1$. Soient $U(X)$ et $V(X)$ deux polynômes de $\mathbb{Z}[X]$ tels que l'on ait la relation

$$U(X)\phi_s(X)+V(X)\phi_t(X)=R(\phi_s,\phi_t).$$

En remplaçant X par β/α dans cette égalité, on voit que $|R(\phi_s,\phi_t)|_p<1$.

D'après le lemme 2, on a alors que t/s est une puissance de p.

Considérons alors l'entier e défini par: $sp^e \leq n$ et $sp^{e+1} > n$. On a immédiatement

$$v_p(u_1(sp^e)) = \sum v_p(\psi_d(\alpha, \beta)),$$

où la dernière sommation a lieu sur les $d \leq n$, donc $v_p(P_1(n)) = v_p(Q_1(n))$, d'où l'assertion.

On a facilement la formule:

$$u_m(n) = \prod \psi_d(\alpha, \beta)$$

où le produit est fait sur les d divisant mn et ne divisant pas n.

Nous considérons tout d'abord l'ensemble E_n des d tels qu'il existe k, avec $k \leq n$ et $d|km$, $d \nmid k$, et l'ensemble F_n, réunion des ensembles $\{d : d \wedge (m/h) = 1,\ d \leq n\}$, pour h diviseur de m différent de 1.

Montrons que $E_n = F_n$.

Soit d dans E_n; il existe donc k tel que $k \leq n$ et $d|mk$, $d \nmid k$; par suite $h = d \wedge m$ est différent de 1; on a $m = hm_1$ et $d = hd_1$ avec m_1 et d_1 premiers entre eux. Le nombre d divise mk, donc hd_1 divise hm_1k et par suite d_1 divise k. On pose $k = d_1k_1$; comme $k \leq n$, on a $d_1 \leq n$ et $d_1 \wedge (m/h) = 1$. Par suite, d appartient bien à F_n.

Soit maintenant d dans F_n. On peut donc écrire $d = d_1h$, avec $h|m$, $h \geq 2$ et $d_1 \wedge (m/h) = 1$. Soit $k = d_1$; on a $d|mk$ et $d \nmid k$ car $h \geq 2$, donc d appartient à E_n.

Il est alors clair d'après ce qui précède que $P_m(n)$ divise $Q_m(n)$. Il reste à regarder les valuations p-adiques.

Soit donc p un nombre premier ne divisant pas m.

On a les formules suivantes:

$$v_p(P_m(n)) = \max\left(\sum v_p(\psi_d(\alpha, \beta))\right),$$

où le maximum, se fait sur les indices $k \leq n$ et la sommation sur les $d|mk$ et $d \nmid k$, et

$$v_p(Q_m(n)) = \sum\sum v_p(\psi_{dh}(\alpha, \beta)),$$

où la première sommation a lieu sur les diviseurs h de m différents de 1 et la seconde sur les $d \leq n$ tels que $d \wedge (m/h) = 1$. S'il n'y a aucun $d \leq mn$ tel que $v_p(\psi_d(\alpha, \beta))$ soit non nul, l'égalité à démontrer est claire. Sinon on note s le plus petit de ces entiers, et un raisonnement déjà fait montre que tout autre entier possédant cette propriété est de la forme sp^a où a est dans $\mathbb{N}$.

On définit l'entier e comme précédemment: soit $h = s \wedge m$, on pose $s = s_1 h$, et on définit l'entier k par $k = s_1 p^e$ où e est tel que $s_1 p^e \leq n$ et $s_1 p^{e+1} > 1$. On a $k \leq n$, et d'autre part, si d est un entier de la forme sp^a avec $a \leq e$, alors d divise mk, mais ne divise pas k; en effet, si c'était le cas, h diviserait p^{e-a}, et par suite puisque $h \geq 2$, p diviserait h, donc m, ce qui est contraire à l'hypothèse faite; on a donc

$$v_p(Q_m(n)) = v_p(u_m(s_1 p^e)) = v_p(P_m(n)),$$

ce qui termine la démonstration du lemme 4. □

Remarque. Si on prend $m = 2$, $a = b = 1$, on voit que $P_2(6) = 2^2 \cdot 3^2 \cdot 7 \cdot 11$ et $Q_2(6) = 2^3 \cdot 3^2 \cdot 7 \cdot 11$, de sorte que $v_2(P_2(6)) < v_2(Q_2(6))$. La restriction $p \nmid m$ ne peut donc être évitée.

Lemme 5

On note $T_n = \sum \varphi(d)$ où la sommation a lieu sur les éléments d de F_n (cf la démonstration du lemme 4). Alors T_n est équivalent à $C(m)n^2$ si n tend vers l'infini, avec

$$C(m) = \frac{3}{\pi^2} \left(\sum \varphi(h) \varphi\left(\frac{m}{h}\right) \frac{h}{m} \right) \prod \left(1 - \frac{1}{p^2}\right)^{-1},$$

où la sommation a lieu sur les diviseurs h de m différents de 1, et le produit sur les nombres premiers divisant m.

Preuve. Notons $F_{n,h} = \{dh : d \leq n,\ d \wedge (m/h) = 1\}$; la réunion des ensembles disjoints $F_{n,h}$ pour h diviseur différent de 1 et de m est égale à F_n.

Nous notons $T_{n,h}$ la somme des $\varphi(d)$ pour d dans $F_{n,h}$. De la formule

$$\varphi(d) = \sum \mu(k) \frac{d}{k},$$

où k parcourt les diviseurs de d, on déduit que

$$T_{n,h} = \sum c(k) \mu(k)$$

où $k \leq mn$ et où on a posé

$$c(k) = \sum \frac{d}{k},$$

où la sommation se fait sur les d appartenant à $F_{n,h}$ tels que k divise d.

Pour un tel d, il existe donc d_1 tel que $d = d_1 h$, $d_1 \wedge (m/h) = 1$ et tel que $k | d$, avec $d_1 \leq n$.

Supposons $(k/k\wedge h)\wedge(m/h)$ différent de 1, et soit p un facteur premier commun à ces deux nombres. On voit facilement que p^2 divise k, de sorte que $\mu(k)$ est nul et donc que le terme correspondant n'apparaît pas dans la somme. On se limite donc à calculer $c(k)$ pour les k tels que

$$\left(\frac{k}{k\wedge h}\right)\wedge\left(\frac{m}{h}\right)=1.$$

Posons $d=kk'$. On a

$$\left(\frac{k}{k\wedge h}\right)k'=d_1\left(\frac{h}{h\wedge k}\right),$$

d'où on déduit que d_1 s'écrit $d_2(k/k\wedge h)$ et k' s'écrit $d_2(h/k\wedge h)$.

Donc finalement

$$c(k)=\sum\frac{d_2h}{k\wedge h}$$

avec ces restrictions sur d_2. On regarde la somme sur chacune des progressions arithmétiques $(tm/h)+r$, où r parcourt les entiers premiers à m/h, $r\le m/h$, et on trouve facilement que l'on a:

$$c(k)=h^2\,\varphi\left(\frac{m}{h}\right)\frac{n^2(k\wedge h)}{2mk^2}+B(n,k)$$

où $B(n,k)$ est $O(n/k)$.

La somme $\sum B(n,k)\mu(k)$ est en valeur absolue inférieure, à une constante multiplicative près, à $n\sum 1/k$ où la sommation a lieu sur les entiers inférieurs ou égaux à mn, donc cette somme est $o(n^2)$ si n tend vers $+\infty$. Finalement, en rassemblant ces estimations, utilisant les lemmes précédents et la formule

$$\frac{\varphi(k)}{k}=\sum\frac{\mu(d)}{d}$$

où d parcourt les diviseurs de k, on trouve la formule annoncée. □

3. Démonstration du théorème

Nous regardons tout d'abord le cas $m = 1$.

D'après le lemme 4, on a

$$P_1(n) = Q_1(n) = \prod v_d(\alpha, \beta)$$

où d parcourt les entiers plus grands que 1 et inférieurs à n.

On a d'autre part $v_d(\alpha, \beta) = \alpha^{\varphi(d)}\phi_d(\beta/\alpha)$; rappelons que nous avons supposé que β/α est de module plus petit que 1. Nous allons d'abord majorer et minorer $|\phi_d(\beta/\alpha)|$.

On a

$$|\phi_d(\beta/\alpha)| = \prod |(\beta/\alpha)^k - 1|^{\mu(d/k)},$$

où le produit est fait sur les diviseurs de d. Si $|\beta/\alpha| < 1$, on voit facilement que la famille des $|\phi_d(\beta/\alpha)|$ est majorée et minorée par une constante positive.

Nous examinons maintenant le cas où β/α est de module 1. On peut alors appliquer le lemme 1, d'où on déduit que:

$$\left|\log|\phi_d(\beta/\alpha)|\right| \leq \sum c_1 |\mu(d/k)| \log k$$

où c_1 est une constante et où l'on somme sur les diviseurs de d.

Comme $\mu(d/k)$ est toujours de valeur absolue ≤ 1, on a donc la majoration:

$$\left|\log|\phi_d(\beta/\alpha)|\right| \leq c_2 N(d) \log d$$

où c_2 est une constante, et $N(d)$ le nombre de diviseurs de d. Une estimation de cette forme est donc vraie dans tous les cas, que β/α soit de module 1 ou non.

Maintenant, $\log P_1(n)$ se présente comme la somme de deux termes: l'un est le terme

$$\sum \varphi(d) \log|\alpha|.$$

l'autre

$$\sum \log|\phi_d(\beta/\alpha)|.$$

Le premier est équivalent à $3n^2 \log \alpha/\pi^2$ comme on l'a déjà vu, et le second majoré à une constante multiplicative près par la somme $\sum N(d) \log d$ où d parcourt les entiers $\leq mn$. D'après [2, th. 7.8, p. 109] on a

$$\sum_{d \leq n} N(d) = O(n \log n),$$

de sorte ce deuxième terme est $o(n^2)$.

Donc $\log P_1(n)$ est équivalent à $3\log|\alpha|\,n^2/\pi^2$. Il nous reste à estimer $\log(u_1(1)\cdots u_1(n))$; on a d'après le lemme 1

$$\log(u_1(k)) = k\log|\alpha| + O(\log k),$$

d'où on tire facilement que $\log(u_1(1)\cdots u_1(n))$ est équivalent à $n^2\log|\alpha|/2$, ce qui termine la démonstration dans ce cas.

Nous passons maintenant au cas $m \geq 2$.

Nous allons tout d'abord comparer $\log P_m(n)$ et $\log Q_m(n)$. D'après le lemme 4, ces deux expressions ne diffèrent que par une somme de la forme $\sum a_p(n)\log p$ où p parcourt les diviseurs premiers de m et où $a_p(n)$ appartenant à $\mathbb{N}$ est inférieur à la valuation p-adique de $Q_m(n)$. On voit facilement que $Q_m(n)$ est un diviseur de $Q_1(mn)$, qui est le plus petit commun multiple des $u_1(k)$, $k \leq mn$. Par suite, on a $a_p(n) = O(n)$ pour tout p et donc:

$$\log Q_m(n) = \log P_m(n) + O(n).$$

Nous estimons maintenant $\log Q_m(n)$. Cette quantité est la somme des deux expressions

$$A(n) = \sum\sum \varphi(dh)\log|\alpha|$$

et

$$B(n) = \sum\sum \log|\delta_d(\beta/\alpha)|$$

où dans les deux cas la première sommation a lieu sur les diviseurs h de m différents de 1 et la seconde sur les $d \leq n$ tels que d soit premier à m/h.

On montre exactement comme dans le cas de $m = 1$ que $B(n)$ est $o(n^2)$ si n tend vers $+\infty$ et d'après le lemme 5 on a $A(n)$ équivalent à $C(m)\log|\alpha|\,n^2$ ($C(m)$ a été défini dans le lemme 5). Finalement, on a donc $\log P_m(n)$ équivalent à $n^2C(m)\log|\alpha|/2$ si n tend vers l'infini.

Enfin, on montre comme précédemment que $\log(u_m(1)\cdots u_m(n))$ est équivalent à $(m-1)n^2\log|\alpha|/2$, et la réunion de ces deux estimations prouve le théorème. □

Bibliographie

1. T. Apostol, Resultants of cyclotomic polynomials, *Proc. Amer. Math. Soc.* **24** (1970), 457–462.
2. R. Ayoub, *An Introduction to the Analytic Number Theory*, AMS Mathematical Surveys 10, American Mathematical Society, Providence, 1963.
3. M. Davis, Hilbert's tenth problem is unsolvable, *Amer. Math. Monthly* **80** (1973), 233–269.
4. P. Kiss and F. Matyas, An asymptotic formula for π, *J. Number Theory* **31** (1989), 255–259.
5. Y. Matiyasevitch and R. Guy, A new formula for π, *Amer. Math. Monthly* **93** (1986), 631–635.
6. A. Schinzel, Primitive divisors of $A^n - B^n$, *J. Reine Angew. Math.* **268–269** (1974), 27–33.