Séminaire Delange-Pisot-Poitou. Théorie des nombres

Michel Langevin

Sur la fonction plus grand facteur premier

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 16, n° 2 (1974-1975), exp. n° G22, p. G1-G29

<http://www.numdam.org/item?id=SDPP_1974-1975__16_2_A18_0>

Séminaire DELANGE-PISOT-POITOU
(Groupe d'étude de théorie des nombres)
16e année, 1974/75, n° G3, G7, G10, G12, G22, 29 p.

SUR LA FONCTION PLUS GRAND FACTEUR PREMIER (*)

par Michel LANGEVIN

0. Résumé.

P désigne la fonction plus grand facteur premier. On recherche des minorants effectifs pour les suites $P(n(n+k))$, $P(\prod_{0\leq i<k}(n+i))$, k étant un entier >0 donné et, plus généralement, pour $P(f(n))$, f étant un polynôme à coefficients entiers ayant au moins deux zéros distincts ; on s'intéressera aussi aux cas particuliers suivants : f cyclotomique, homogène à deux variables, de la forme $aX^m + bY^n$. Ces résultats, joints à quelques théorèmes sur les fractions continues, permettent d'étudier les suites d'entiers de facteurs premiers donnés. Les techniques utilisées sont essentiellement basées sur la méthode de Baker pour laquelle on renvoie aux chapitres 2, 3, 4 de son livre : Transcendental number theory (Cambridge, Cambridge University Press, 1975).

1. Résultats élémentaires et résultats non effectifs.

(1.0) La lettre p est réservée aux nombres premiers. On note, pour tout entier n , $\omega(n) = \sum_{p|n} 1$; $\Omega(n) = \sum_{p^a|n} 1$; $u(n) = \prod_{p|n} p$; $\pi(n) = \sum_{p\leq n} 1$; $\theta(n) = \sum_{p\leq n} \log p$; $\nu(n) =$ p. p. c. m. $(1, 2, \ldots, n)$;

$$\psi(n) = \log \nu(n) = \sum_{p^a|n} \log p ;$$

$v_p(n) = \sup(a , p^a|n)$; et, comme prévu, $P(n) = \sup_{p|n} p$. On désigne par (p_n) la suite croissante des nombres premiers. On écrit $\log_2$ pour log.log , $\log_3$ pour log.log.log ...

(1.1) La double inégalité $\theta(p_{\omega(n)-1}) + \log P(n) \leq \log n \leq \Omega(n).\log P(n)$, et les théorèmes classiques sur les fonctions ω et Ω (cf. [22], ch. 22) montrent que,

---

(*) Exposé des conférences prononcées au Groupe d'étude de Théorie des nombres les 25 novembre 1974, 13 et 20 janvier, 24 février, 10 mars et 9 juin 1975.

pour tout réel $\varepsilon > 0$, la densité de l'ensemble des entiers n vérifiant

(1.1.1) $\quad (1-\varepsilon)\log n/\log_2 n < \log P(n) \leq \log n - (1-\varepsilon)\log_2 n \log_3 n$

est égale à 1 (la densité considérée est la densité naturelle, il en sera toujours de même dans la suite).

Remarque : Le résultat précédent ne donne aucun renseignement sur le réel $\log P(n)/\log n$; en fait, l'ensemble de ces réels est partout dense dans $[0 , 1]$; on le voit aisément en associant, à tout réel x $(0 < x < 1)$ et à tout nombre premier p , l'entier $p \exp([(1 - x)\log p/x \log 2]\log 2)$.

(1.2) Les autres inégalités $\omega(n) \leq \pi(P(n))$ et $\log n \leq (\sup_p v_p(n)).\theta(P(n))$ fournissent de moins bons résultats mais joueront un rôle essentiel dans la suite. Signalons toutefois que l'inégalité, vraie pour presque tout n ,

(1.2.1) $\quad \log_2 n - a_n(\log_2 n)^{\frac{1}{2}} \leq \omega(n) \leq \log_2 n + a_n(\log_2 n)^{\frac{1}{2}}$

(où a_n désigne une suite quelconque de limite infinie) reste valable quand on y remplace n par $f(n)$, f étant un polynôme quelconque à coefficients entiers (cf. [18]) ; ainsi, pour tout réel $\varepsilon > 0$, l'inégalité

$$P(f(n)) > (1 - \varepsilon).\log_2 n.\log_3 n$$

est vraie au moins pour presque tout n .

(1.3) Soit f un polynôme à coefficients entiers ayant au moins deux zéros distincts. Les théorèmes de Thue et Siegel ont permis de prouver, d'abord dans le cas $d^0 f = 2$, puis dans le cas général, que $P(f(n))$ tend vers l'infini avec n (cf. [37], [52] et [53]). Plus généralement, mais avec des méthodes comparables, MAHLER (cf. [30]) a montré que, lorsque $\sup(n , n')$ tend vers l'infini (n , n' entiers premiers entre eux), il en est de même de $P(f(n , n'))$, f désignant maintenant un polynôme homogène à deux variables et à coefficients entiers comportant au moins trois facteurs linéaires non proportionnels. Vingt ans plus tard, MAHLER prouvait le même résultat avec $f(X , Y) = aX^m + bY^n$ $(m \geq 2 , n \geq 3 ; a \neq 0 , b \neq 0$ entiers) (cf. [33]). Tous ces énoncés sont malheureusement ineffectifs. Hormis les théorèmes du §2, les seuls résultats effectifs antérieurs aux travaux de GEL'FOND et BAKER concernent $\sup_{n \leq x} P(f(n))$ $(f \in Z[X])$ et non $P(f(n))$; ainsi, ERDÖS a prouvé l'inégalité

$$\sup_{n \leq x} P(f(n)) \gg x.\exp((\log x)^c) \qquad (c \text{ cte } > 0)$$

(non publié, un résultat un peu moins fort et les références relatives aux travaux antérieurs se trouvent dans [12]) ; les méthodes utilisées sont le crible de Selberg et ses extensions aux corps de nombres ; le cas $f(X) = X^2 + 1$ avait déjà été étudié par ČEBIČEV et LANDAU (cf. [26], §147).

(1.4) Soit $f \in Z[X]$; des majorations de $\inf_{n \geq x} P(f(n))$ ont été obtenues par SCHINZEL (cf. [44]). L'idée est la suivante : si d désigne le degré de f , SCHINZEL prouve l'existence d'un polynôme f' $(\in Z[X])$ de degré $d - 1$ tel que

$f \circ f'$ ait dans $Z[X]$ un facteur de degré $d^2 - 2d$. En poursuivant cette construction, on voit qu'existe, pour tout entier $m > 0$, un polynôme $f^{(m)} \in Z[X]$ de degré $u_1 u_2 \dots u_m$ (avec $u_1 = d - 1$, $u_{i+1} = u_i^2 - 2$) tel que $f \circ f^{(m)}$ ait un facteur $g^{(m)}$ de degré u_{m+1}. Il suffit alors de donner à n des valeurs de la forme $f^{(m)}(n')$ pour majorer $P(f(n))$ par

$$\sup(P(g^{(m)}(n')) , P(f \circ f^{(m)}(n')/g^{(m)}(n')))$$

et obtenir

$$\underline{\lim}_{n\infty} \log P(f(n))/\log f(n) < \infty .$$

Dans le cas de polynômes de la forme $aX^d + b$ (a, b entiers $\neq 0$), on obtient un meilleur résultat :

$$\underline{\lim}_{n\infty} \log P(an^d + b).\log_3 n/\log n < \infty$$

en se ramenant au polynôme $X^d - 1$ de factorisation immédiate.

(1.5) Soit k un entier non nul, du résultat précité [37] de POLYA, on déduit aussitôt que la suite $P(n(n + k))$ tend vers l'infini avec n. En d'autres termes, si l'on désigne par (n_i) la suite croissante des entiers dont les facteurs premiers appartiennent à un ensemble fini donné, on voit que la différence $n_{i+1} - n_i$ tend vers l'infini avec i. Les travaux de SIEGEL et MAHLER (cf. [29] et [51]) permettent de donner une formulation plus précise de ce résultat : pour tout réel $t < 1$, l'inégalité $n_{i+1} - n_i > n_i^t$ est vraie à partir d'un certain rang (non effectivement calculable). Signalons enfin qu'on établit aisément que

$$\lim_{i\infty} n_{i+1}/n_i = 1$$

(cf. [37] ou §4).

(1.6) Pour tout entier $k > 1$, soit $P(n , k) = P((n + 1)(n + 2)\dots(n + k))$; le théorème de Sylvester établit l'inégalité $P(n , k) > k$ (pour tout entier $n \geq k$) ; historiquement, cela est apparu comme une généralisation du résultat de ČEBIČEV sur la conjecture de Bertrand ($\pi(2n) > \pi(n)$). On trouvera une démonstration du théorème de Sylvester (ainsi que divers corollaires élémentaires utilisés dans des travaux récents) dans l'annexe 1.

La fonction $(n , k) \longmapsto P(n , k)$ a fait l'objet, ces dernières années, d'actives recherches liées à une conjecture d'ERDÖS. Soit ε un réel > 0, on sait (cf. [23]) que l'inégalité $p_{n+1} - p_n < p_n^{(7/12)+\varepsilon}$ est vraie à partir d'un certain rang et que la conjecture de CRAMER [7] s'écrit

$$\overline{\lim}_{n\infty} (p_{n+1} - p_n)/(\log n)^2 = 1 .$$

D'autre part, on montre que, pour tout entier $k > 0$, on peut trouver un entier n vérifiant $k < p_n < p_{n+1} < 2k$ et $p_{n+1} - p_n \gg \log n.\log_2 n.\log_4 n.(\log_3 n)^{-2}$ (cf. [43] et [47] pour ce résultat et les diverses valeurs de la constante). Soient m un entier > 0, $(u_n(m))$ la suite croissante des entiers vérifiant $P(u_n(m)) > m$ et $g(m) = \sup_n u_{n+1}(m) - u_n(m)$ (pour les valeurs prises par $g(m)$ quand m est

un entier petit, voir [13]) ; comme $\lim_{n\infty} P(n(n+1)) = \infty$, à partir d'un certain rang (déterminé ultérieurement, cf. (2.4.1)) n_0 , on a $u_{n+1}(m) = u_n(m) + 1$, c'est-à-dire $g(m) = \sup_{n\leqslant n_0} u_{n+1}(m) - u_n(m)$. Soient m_0 le plus petit entier tel que $p_{m_0} > m$ (donc $p_{m_0} = u_1(m)$), et n_1 l'entier défini par $u_{n_1}(m) = 2p_{m_0}$, ERDÖS conjecture que

$$g(m) = \sup_{n<n_1} u_{n+1}(m) - u_n(m) = \sup_{m<p_n<p_{n+1}<2m}(p_{n+1} - p_n) ,$$

soit, en appliquant la conjecture de Cramer, $g(m) = (1 + o(1))(\log m)^2$ (cf. [10]). L'étude de la fonction g se ramène à celle de $(n , k) \longmapsto P(n , k)$. En effet, il est clair qu'on a $\inf_{n>u_1(m)} P(n , g(m)) > m$; réciproquement, soit h une fonction continue strictement croissante telle que

$$\overline{\lim}_{k\infty}(\inf_{n\geqslant h(k)} P(n , k))(h(k))^{-1} \geqslant 1 ,$$

on vérifie alors aisément qu'on a $\overline{\lim}_{m\infty} g(m)(h^{-1}(m))^{-1} \leqslant 1$. Par exemple, le théorème de Sylvester montre que $\overline{\lim}\, g(m)/m \leqslant 1$. En fait, on peut déduire des calculs de Sylvester l'inégalité (pour $n \geqslant k$) (cf. Annexe 1) :

$$k.(1 - \log k/\log(n + k)) \leqslant \pi(P(n , k)) ;$$

soient alors r et r' deux réels vérifiant $7/12 < r < r' < 1$, on voit facilement que, si $k \leqslant n^r < (n + k)^r$, l'on a, pour k assez grand,

$$P(n , k) \geqslant (1 - r').k.\log k$$

tandis que, si $k > n^r$, l'on a, pour k assez grand, $P(n , k) > n$. En d'autres termes, on a prouvé l'inégalité $\overline{\lim}_{m\infty} g(m).(\log m)/m \leqslant 5/12$ (poser

$$h(x) = (1 - r').k.\log k).$$

La minoration donnée précédemment de l'écart $p_{n+1} - p_n$ permet d'écrire l'inégalité $g(m) \gg \log m.\log_2 m.\log_4 m.(\log_3 m)^{-2}$ puisque $u_1(m) = p_{m_0}$ et $u_2(m)=p_{m_0+1}$.

(1.7) J. M. DESHOUILLERS [8] a dressé une liste avec références bibliographiques des diverses majorations obtenues pour l'infiniment grand $g(m)$ $(m\infty)$; on trouvera dans [60] un exposé historique détaillé valable pour les résultats antérieurs à 1972 ; on peut aussi consulter [39]. Aujourd'hui, deux méthodes sont utilisées pour minorer $P(n , k)$:

1° des méthodes de crible (par exemple, effectuer une double évaluation de $\sum_{i>0} \theta((n + k)/i) - \theta(n/i)$ puisqu'on a $P(n , k) > n/i$ si $\pi((n + k)/i) > \pi(n/i)$) qui donnent un minorant de $P(n , k)$ en fonction de k seul, valable pour n vérifiant $k^{3/2} \leqslant n \leqslant n_1(k)$ (quand $n \leqslant k^{3/2}$, on a $P(n , k) > n$ puisque $(2/3) > (7/12)$ (cf. (1.6))), minorant d'autant meilleur que $n_1(k)$ est petit. Ainsi, on prouve (cf. [24]) que, pour k assez grand, $P(n , k) \geqslant k.\log^2 k$ avec $n_1(k) = \exp((\log k)^{5/4})$.

2° des méthodes effectives détaillées dans les §2 et 3, qui fournissent des minorants de $P(n , k)$ en fonction de n et k , bons surtout quand n est grand devant k . Ainsi, on prouve (cf. [28]) que $\underline{\lim}_{n\infty} P(n,k)(\log_2 n)^{-1} \geqslant k$.

La taille des intervalles sur lesquels ces minorations sont valables est aussi importante que la valeur des minorants eux-mêmes. En effet, pour obtenir des résultats sur la fonction g, il est nécessaire d'avoir une minoration de $P(n , k)$ en fonction de k valable uniformément en n. Par exemple, l'apparition du résultat précité [24] a permis de prouver $g(k) = O(k.\log_3 k.(\log k.\log_2 k)^{-1})$ non à cause de l'amélioration apportée par le minorant $k.\log^2 k$ mais à cause de la plus grande valeur de $n_1(k)$ que celle $(\exp(\log k.\log_2 k))$ utilisée auparavant, ce qui a permis de substituer à l'inégalité $P(n , k) \gg k.\log k.\log_3 k.(\log_4 k)^{-1}$ (pour $n \geqslant \exp(\log k.\log_2 k)$) l'inégalité $P(n , k) \gg k.\log k.\log_2 k.(\log_3 k)^{-1}$ (pour $n \geqslant \exp((\log k)^{5/4})$) qui s'obtient pareillement.

2. La méthode de Størmer.

(2.1) Le lemme suivant, relatif à l'équation de Pell-Fermat, a été prouvé par STØRMER en 1897 (cf. [58]).

(2.1.1) LEMME. - *Soient d un entier > 0 non carré parfait, (x_0 , y_0) la solution fondamentale de l'équation de Pell-Fermat $x^2 - dy^2 = 1$ (ou -1) ; alors, ou bien l'ensemble des diviseurs premiers de y_0 est inclus dans l'ensemble des diviseurs premiers de d, ou bien il n'existe aucune solution (x , y) de l'équation satisfaisant à cette condition.*

(2.2) Montrons les conséquences de ce lemme en prouvant le théorème suivant.

(2.2.1) THÉORÈME. - $\lim_{n\infty} P(n^2 \pm 1) = \infty$.

Avant de prouver ce théorème, remarquons que cet énoncé implique

$$\lim_{n\infty} \sup(P(n) , P(n + 2)) = \infty$$

et donc, en prenant n pair, $\lim_{n\infty} \sup(P(n) , P(n + 1)) = \infty$ énoncés dont Størmer, le premier, a donné les démonstrations. Soient $q_1 , q_2 \dots q_r$ des entiers premiers, prouver le théorème revient à montrer la finitude de l'ensemble des solutions de l'équation

$$(E) \qquad q_1^{x_1}.q_2^{x_2}. \dots .q_r^{x_r} = x^2 \pm 1 .$$

Soit D l'ensemble de cardinal $s = 3^r$ formé par les entiers de la forme $\prod_i q_i^{a_i}$ avec $0 \leqslant a_i \leqslant 2$. Il est clair que le membre de gauche de (E) peut être écrit de façon unique sous la forme $d.m^2$, avec $d \in D$, quand on impose la condition supplémentaire : p divise m implique p divise d . On est donc ramené à résoudre s équations de Pell-Fermat $x^2 - dm^2 = \pm 1$ avec la condition supplémentaire précédente ; le théorème suit alors aussitôt du lemme. Le théorème précédent est effectif puisque la recherche de la solution de l'équation de Pell-Fermat se ramène au calcul du développement en fraction continue de $d^{1/2}$.

(2.3) En 1934, S. CHOWLA redécouvrait le lemme (2.2.1), et prouvait l'inégalité $P(n^2 + 1) \geqslant c.\log_2 n$ (cf. [6]) grâce au lemme ci-dessous.

(2.3.1) LEMME (SCHUR). - La solution fondamentale (quand elle existe) (x_0 , y_0) de l'équation de Pell-Fermat $x^2 - dy^2 = -1$ satisfait à l'inégalité

$$\log \sup(x_0 , y_0) \ll d^{1/2}.\log d .$$

Le même résultat concernant $P(n^2 \pm 1)$ a été prouvé indépendamment par MAHLER (cf. [31]).

(2.4) Soient $m_1 , m_2 , \dots , m_r , n_1 , n_2 , \dots , n_s , a , b$ des entiers > 0, et c un entier égal à ± 1 ou ± 2. La démonstration du théorème (2.2.1) montre que l'équation

$$am_1^{x_1} m_2^{x_2} \dots m_r^{x_r} - bn_1^{y_1} n_2^{y_2} \dots n_s^{y_s} = c$$

n'a qu'un nombre fini de solutions (effectivement calculables). D. H. LEHMER a repris cette question, et a étudié en outre le cas $c = \pm 4$; en d'autres termes, D. H. LEHMER cherche à déterminer tous les entiers de la forme $n(n + 1)$, $n(n+2)$ ou $n(n + 4)$ ayant des facteurs premiers donnés $q_1 , q_2 , \dots , q_t$. Pour cela, il remplace le lemme (2.1.1) par des résultats voisins de la théorie des fonctions de Lucas et, pour le cas des entiers de la forme $n(n + 4)$, utilise une extension de (2.3.1) due à HUA (les références concernant ces lemmes sont données dans [29]). Dans le même article [29], D. H. LEHMER obtient des majorants pour l'ensemble des entiers n tels que $n(n + i)$ $(i = 1 , 2 , 4)$ ait tous ses facteurs premiers parmi $q_1 , q_2 , \dots , q_t$. Par exemple,

(2.4.1) pour $i = 1$, $\log n \leqslant M.(2 + \log(8Q))(2Q)^{1/2} - 2 \log 2$

(2.4.2) pour $i = 2$, $\log n \leqslant M.(2 + \log(4Q))\, Q^{1/2} - \log 2$

avec $M = \sup(3 , (1 + \sup_j q_j)/2)$, $Q = \prod_{1\leqslant j\leqslant t} q_j$. En particulier, on voit que $\varlimsup_{n\infty} \sup(P(n) , P(n + i)).(\log_2 n)^{-1} \geqslant 2$ (avec $i = 1 , 2$). Toute cette théorie est accessible au calcul ; on trouvera, toujours dans [29], des tables numériques dressées pour les petites valeurs de $q_1 , q_2 , \dots , q_t$.

(2.5) Des inégalités (2.4.1) et (2.4.2), on va déduire une minoration de $P(n,k)$ (cf. (1.6)). On va montrer en effet que toute inégalité de la forme $u(n(n+1))\geqslant h(n)$ (où h désigne une fonction tendant vers l'infini avec la variable) fournit une minoration pour $P(n , k)$. Il suffit de remarquer qu'on a l'inégalité

(2.5.1) $\sum_{1\leqslant i\leqslant k} \log u((n+2i-1)(n+2i)) \leqslant \theta(P(n,2k)) + 2k.\log k + O(k)$,

ce qui implique l'existence d'un entier i tel que $u((n + 2i - 1)(n + 2i))$ soit majoré par $\theta(P(n , 2k))/k + O(\log k)$, d'où l'inégalité

$$P(n , 2k) > (1 - \varepsilon).k.h(n) \quad \text{pour} \quad n \geqslant n_0(\varepsilon , k) .$$

Prouvons maintenant (2.5.1) ; si $p \geqslant 2k$, p ne peut diviser qu'au plus un entier parmi $n + 1 , n + 2 , \dots , n + 2k$, par conséquent, on peut écrire

$$\sum_{1\leqslant i\leqslant 2k} \sum_{p\mid n+i, p\geqslant 2k} \log p \leqslant \theta(P(n , 2k)) - \theta(2k) ;$$

d'autre part,

$$\sum_{1\leq i\leq 2k}\sum_{p\mid n+i,\,p<2k}\log p=\sum_{p<2k}\log p.\left(\left[\frac{n+2k}{p}\right]-\left[\frac{n}{p}\right]\right)\leq 2k.\log k+\theta(2k)+O(k)$$

d'où l'on déduit le résultat puisque

$$\sum_{1\leq i\leq k}\log u((n+2i-1)(n+2i))=\sum_{1\leq i\leq 2k}\sum_{p\mid n+i}\log p\ .$$

Par exemple, les inégalités (2.4.1) et (2.4.2) étant de la forme

$$\log n \ll (P(n(n+i))).(\log u(n(n+i))).u^{1/2}(n(n+i))\ ,$$

et le terme prépondérant du membre de droite étant le terme en $u(n(n+i))$, on obtient, en modifiant convenablement l'argument précédent, l'inégalité

$$\varliminf_{n\infty} P(n\ ,\ k)/\log_2 n \geq k \quad \text{(cf. [28])}.$$

3. La méthode de Baker.

(3.1) Les travaux de BAKER concernent avant tout la minoration des formes linéaires de logarithmes (pour un historique de ces minorations, consulter [67]) ; on sait que ces calculs ont permis de donner des majorants effectifs pour les valeurs absolues des solutions des équations diophantiennes de la forme $y^n = f(x)$ $(n \geq 2$, $f \in \mathbb{Z}[X]$ ayant au moins deux (ou trois suivant les énoncés) zéros distincts) et $g(x\ ,\ y) = m$ $(g \in \mathbb{Z}[X\ ,\ Y]$ homogène de degré $3)$. Ces différents aspects des résultats de BAKER vont intervenir dans les applications à l'étude de la fonction P. Par exemple, on a le théorème suivant :

(3.1.1) THÉORÈME. - *Soient* t *un réel* < 1, *et* (k_n) *une suite d'entiers* $\neq 0$ *telle que*

1° $|k_n| \leq n^t$, *alors* $\sup(P(n)\ ,\ P(n+k_n)).(\log_2 n)^{-1}$ *reste supérieur à une constante strictement positive effectivement calculable* ;

2° $|k_n| \leq (\log n)^t$, *alors, pour tout réel* $\varepsilon > 0$, $\sup(P(n),P(n+k_n)).(\log_2 n)^{-1}$ *est supérieur à* $(1-t)/(5+\varepsilon)$ *à partir d'un rang effectivement calculable.*

Pour prouver 1°, on forme le logarithme du rationnel $(n+k_n)/n$ écrit sous la forme d'un produit de puissances de nombres premiers, et on applique à la forme linéaire ainsi obtenue la nouvelle minoration obtenue par SHOREY (cf. [50]). Il vient :

$$|\log(n+k_n)/n| = |\sum_{1\leq i\leq\omega} b_i \log p_i| = |b_\omega|\ |\sum_{1\leq i<\omega}(-b_i/b_\omega)\log p_i-\log p_\omega|$$
$$\geq \exp(-\omega^{C\omega}(\Lambda\log\Lambda B)^2\ (\log(\Lambda\log B))^{3\omega})\ ,$$

où $\omega = \omega(n(n+K_n))$, C constante, $\Lambda = \prod_i \log p_i \leq (\log P)^\omega$ avec $P=P(n(n+k_n))$, $B = \sup_{1\leq i<\omega}(\text{hauteur } b_i/b_\omega) \ll \log n$.

Il suffit alors d'appliquer l'inégalité $\omega \leq \pi(P)$, et d'observer que

$$|\log(n+k_n)/n| \ll n^{t-1}$$

pour obtenir le résultat cherché.

La deuxième partie du théorème dépend de la majoration trouvée par STARK (cf. [56]) pour les solutions de l'équation diophantienne $y^2 = x^3 + k$ $(k \neq 0)$. En appliquant le lemme chinois, on voit qu'existent des entiers m , x , y tels que $0 < m \leqslant (\prod_{p \mid n(n+k_n)} p)^5$, $mn = x^3$, $m(n + k_n) = y^2$; on en déduit l'inégalité

$$\log n \ll (mk_n)^{1+\varepsilon'} \quad (\varepsilon' \text{ réel } > 0),$$

d'où aisément le résultat. En modifiant un peu l'argument précédent, on voit qu'on peut remplacer le minorant $(1 - t)/5$ par $(1 - t)/4$ avec l'hypothèse $|k_n| < (\log n)^{t/2}$ (cf. [28]). En particulier, quand k_n est constante, on obtient

$$\underline{\lim}_{n\infty} \sup(P(n) , P(n + k_n)).(\log_2 n)^{-1} \geqslant 1/4$$

soit un moins bon résultat que celui donné dans (2.4) quand $k_n = \pm 1$ ou ± 2 . Remarquons cependant que cette technique fait apparaître $u(n(n + k))$ seul et non associé avec $P(n(n + k))$; plus précisément, on a déduit le résultat de (3.1.1)-2° de l'inégalité

$$\log_2 n \leqslant (1 + \varepsilon').(5 \log u(n(n + k_n)) + t \log_2 n) + \text{Cte} ,$$

d'où

$$\underline{\lim}_{n\infty} \log u(n(n + k_n)).(\log_2 n)^{-1} \geqslant (1 - t)/5 ,$$

alors que la technique de (2.4) donne, dans le cas où k_n ne prend que les valeurs ± 1 et ± 2 , en majorant $P(n(n + k_n))$ par $u(n(n + k_n))$,

$$\underline{\lim}_{n\infty} \log u(n(n + k_n)).(\log_2 n)^{-1} \geqslant 2/3 .$$

(3.2) Comme on l'a vu dans (2.5), il est naturel d'attendre de nouveaux résultats sur $P(n , k)$ déduits de (3.1) ; par exemple, on prouve l'inégalité

$$\underline{\lim}_{n\infty} P(n , k).(\log_2 n)^{-1} \geqslant k/8$$

grâce à (3.1.1)-2°. De la même manière, la première partie de (3.1.1) peut être utilisée : en formant le logarithme du rationnel $(n + 1)/n$, on obtient une relation de la forme $\log_2 n \leqslant F(\omega , \log P)$ avec $\omega = \omega(n(n + 1))$, $P = P(n(n + 1))$, où F est une fonction croissante de limite infinie en chacune des variables, et d'ordre plus élevé en la première qu'en la seconde. Or, en remarquant, comme dans (2.5), qu'un diviseur premier $p \geqslant 2k$ de $\prod_{1\leqslant i\leqslant 2k}(n + i)$ ne peut diviser qu'au plus un terme du produit, on voit que

$$\sum_{1\leqslant i\leqslant k} \omega((n+2i-1)(n+2i)) \leqslant \pi(P(n,2k)) - \pi(2k) + \sum_{p<2k} [\tfrac{n+2k}{p}] - [\tfrac{n}{p}]$$
$$\leqslant \pi(P(n , 2k)) + 2k.\log_2 k + O(k) ,$$

ce qui prouve l'existence d'un entier i pour lequel $\omega((n + 2i - 1)(n + 2i))$ est majoré par $\pi(P(n , 2k))/k + O(\log_2 k)$. Il suffit alors d'appliquer l'inégalité initiale à $n + 2i - 1$, et de développer F par rapport à la première variable (prépondérante) pour conclure. Il est en fait préférable d'utiliser dans ce cas une variante de l'argument précédent due à RAMACHANDRA (cf. [40]). On écrit chacun des entiers $n + i$ $(1 \leqslant i \leqslant k)$ sous la forme $m_i m_i'$ en posant $m_i = \prod_{p\leqslant k} p^{v_p(n+i)}$,

de sorte qu'il est clair que $\sum_{1\leqslant i\leqslant k} \omega(m_i') \leqslant \pi(P(n\ ,\ k)) - \pi(k)$. D'autre part, en désignant par $\prod_i^0 m_i$ le produit $\prod m_i$ où l'on a oublié, pour tout $r \leqslant k$, un terme m_i tel que $v_p(m_i) = \sup_j v_p(m_j)$, on a $\prod_i^0 m_i \leqslant (k-1)!$ (cf. Annexe 1). On vérifie aisément que $(k-1)! < (k/e)^k$ à partir d'un certain rang. Le produit $\prod^0$ comporte au moins $k - \pi(k)$ termes, c'est-à-dire, pour tout $\varepsilon > 0$, au moins $(1-\varepsilon)k = k'$ termes dès que k est assez grand ; on prendra cependant $k' = k/2$ pour simplifier les notations. Soit I l'ensemble des entiers i $(1 \leqslant i \leqslant k)$ tels que m_i figure effectivement dans $\prod^0$, et soit majoré par $(k/e)^4$; le complémentaire de I ayant au plus $k/4$ éléments, card I est au moins $k/4$. Le même argument montre l'existence d'une partie I' de I ayant au moins $k/8$ éléments vérifiant tous $\omega(m_i') \leqslant (8/k)(\pi(P(n\ ,\ k)) - \pi(k))$. Soient $i_1 < i_2 < \ldots < i_\ell$ les éléments de I' , comme $\sum_{1\leqslant j<\ell} i_{j+1} - i_j < k$, il existe un entier j tel que $i_{j+1} - i_j \leqslant 8$. En résumé, on a mis en évidence un couple $n' = n + i_j$, $n'' = n + i_{j+1}$ où $n'' - n' \leqslant 8$ tel qu'on puisse écrire (n'/n'') sous la forme $(m_1/m_2).(m_1'/m_2')$ avec hauteur $(m_1/m_2) \leqslant (k/e)^4$ et $\omega(m_1') + \omega(m_2') \leqslant (16/k)(\pi(P(n\ ,\ k)) - \pi(k))$, ce qui permet, en décomposant m_1'/m_2' en produit de puissances de nombres premiers, d'appliquer le résultat précité de SHOREY dans des conditions plus favorables. On obtient ainsi l'inégalité $P(n\ ,\ k) \gg k.\log_2 n$ pour $n > e^k$ ce qui, joint au résultat élémentaire $P(n\ ,\ k) \gg k.\log k$, permet de voir que l'inégalité $P(n\ ,\ k) \gg k.\log_2 n$ est vraie pour tout couple $(n\ ,\ k)$ tel que $n > k^{3/2}$. La même technique peut être appliquée aux résultats de (2.4) ou de (3.1.1)-1°, on obtient alors des inégalités valables dans le domaine plus vaste défini précédemment (mais moins bonnes pour n infini et k fixe).

(3.3) Un perfectionnement de l'argument précédent (dû à RAMACHANDRA, cf. [42]) et un énoncé "type Baker" sur les expressions de la forme $|\sum_{1\leqslant i\leqslant \omega} b_i.\log q_i|$, où les b_i sont entiers et les q_i rationnels voisins de 1 (dû à SHOREY, cf. [42] et [49]) permettent d'obtenir une minoration de $P(n\ ,\ k)$ lorsqu'on impose une condition de la forme $n_1(k) \leqslant n \leqslant n_2(k)$. Comme dans (3.2), on recherche un couple $(n'\ ,\ n'')$ $(n < n'' < n' \leqslant n + k)$ tel qu'en formant $\log n'/n''$ $(\leqslant k/n)$ on tire le meilleur parti de cet autre résultat de SHOREY (lequel a été d'ailleurs conçu plus particulièrement pour cet usage).

On écrit comme précédemment chaque entier $n + i$ $(1 \leqslant i \leqslant k)$ sous la forme $m_i\, m_i'$ afin de limiter au maximum le nombre de termes figurant dans la forme linéaire de logarithmes. On raisonne ensuite ainsi : si $P(n\ ,\ k)$ est assez petit, on peut trouver $k/16$ (par exemple) entiers i tels que les ensembles non ordonnés d'exposants obtenus en écrivant les m_i' sous la forme de produits de puissances de nombres premiers soient tous les mêmes (observer qu'il y a au plus

$$\exp((8/k)(\pi(P(n\ ,\ k)) - \pi(k))(\log_2(n_2(k)) - \log_2 k)) \tag{3.3.1}$$

tels ensembles d'exposants, et que ce nombre est un $o(k)$ si $P(n\ ,\ k)$ est suffisamment petit). On est alors ramené à choisir deux entiers i_1 et i_2 parmi les précédents tels que m_{i_1}/m_{i_2} soit voisin de 1 et m_{i_1}'/m_{i_2}' de la forme

$\prod_j p_j^{(1)}/p_j^{(2)}$ où les $p_j^{(1)}$, $p_j^{(2)}$ sont des nombres premiers, ce choix étant fait de sorte que les rationnels $p_j^{(1)}/p_j^{(2)}$ soient le plus proches possible de 1 . On applique alors le résultat de SHOREY qui montre que $P(n , k)$ ne peut être trop petit ; par ce procédé, on est limité par la condition : expression (3.3.1) $= o(k)$; toutefois, on obtient des résultats intéressants : si $n_1(k) = \exp(\log k.\log_2 k)$ (resp. $\exp(\exp((\log k)^{1+a})\log k)$) et $n_2(k) = \exp(\exp((\log k)^{5/4}))$ (resp. $\exp(\exp((\log k)^{1+b}).\log k)$ avec $0 < a < b < 1 - a$) , $P(n , k)$ est minoré par $c.\log k.\log_3 k.(\log_4 k)^{-1}$ (resp. $c.(\log k)^{1+a}.(\log_2 k)^{-1}$) où c est une constante absolue effectivement calculable.

(3.4) Soit f un polynôme à coefficients entiers ayant au moins deux zéros distincts. On va montrer que les résultats de BAKER et STARK sur les équations diophantiennes fournissent très simplement des minorants pour la suite $u(f(n))$. Par exemple, quand $f(X) = aX^2 + bX + c$, soit v_n le plus petit entier > 0 tel que $4af(n) = (2an + b)^2 + 4ac - b^2 = v_n y^3$ avec y entier, ce qu'on peut écrire $(v_n y)^3 - (v_n(2an + b))^2 = v_n^2(4ac - b^2)$, permettant ainsi d'appliquer le résultat de STARK (cf. [56]) sur l'équation $X^3 - Y^2 = k$, il vient

$$\log_2(2an + b) < (1 + \varepsilon').2 \log v_n + \text{Cte} \quad (\varepsilon' \text{ réel } > 0) ,$$

d'où, comme $v_n \leq u^2(f(n))$, l'inégalité $\log u(f(n)) \geq ((1 - \varepsilon)/4).\log_2 n$ valable à partir d'un certain rang effectivement calculable en fonction de ε (quelconque $> \varepsilon'$). La même technique convient pour les équations de degré ≥ 2 : on obtient

$$\log u(f(n)) \gg \log_2 n \quad \text{pour le degré } 3 ,$$

(3.4.1)

$$\log u(f(n)) \gg \log_3 n \quad \text{pour les degrés } > 3 ,$$

les constantes sous-entendues dans (3.4.1) étant explicites. En modifiant un peu les résultats de BAKER et par des arguments moins simples, SPRINDŽUK a montré (cf. [55]) que, f étant un polynôme à coefficients entiers de degré ≥ 3 ayant au moins trois zéros simples, l'inégalité

$$\log u(f(n)) \geq (3(2d)^9 + \varepsilon)^{-1} \log_2 n \quad (\text{où } d = d^0 f)$$

était valable à partir d'un certain rang effectivement calculable. Dans le cas de polynômes f de la forme $aX^d + b$ $(d \geq 3)$, ces résultats peuvent être améliorés par des arguments aussi élémentaires que ceux décrits au début de cet alinéa (3.4) : en envisageant le plus petit entier v_n tel qu'on puisse écrire $v_n y^d - an^d = b$, et en utilisant les majorations obtenues par STARK pour les solutions de l'équation de THUE $g(x , y) = m$ (g homogène), on trouve l'inégalité

$$\log u(f(n)) \geq (2d^2 + \varepsilon)^{-1} \log_2 n \quad (\text{pour } n \text{ assez grand}) \text{ (cf. [27])}.$$

(3.5) Les résultats de (3.4) sur $u(f(n))$ permettent d'en obtenir d'autres sur $P(f(n))$ grâce à l'inégalité $\log u(f(n)) \leqslant \theta(P(f(n)))$. Les formes p-adiques des travaux de BAKER dues à COATES et SPRINDŽUK (qui ont en fait déjà été utilisées dans l'article de Sprindžuk cité dans l'alinéa précédent) permettent d'obtenir directement des inégalités concernant $P(f(n))$ et plus généralement $P(g(n , n'))$, où g est un polynôme homogène irréductible à coefficients entiers et n , n' premiers entre eux. Il est clair en effet, que toute majoration des solutions de l'équation $g(x , y) = mp_1^{x_1} \dots p_r^{x_r}$ (m , $p_1 \dots p_r$ donnés) fournit une minoration pour les entiers de la forme $g(n , n')$ (cf. [54]). On prouve notamment les inégalités $P(g(n , n')) \gg (\log_2(n + n'))^{1/4}$ quand g est de degré 4 et

$$P(g(n , n')) \gg \log_2(n + n').(\log_3(n + n'))^{-1}$$

quand g est de degré > 4 (pour ces résultats et la bibliographie correspondante, consulter le "survey" de W. SCHMIDT [46]). Une modification de la démonstration donnée par SPRINDŽUK des résultats précédents a permis à KOTOV (cf. [25]) de montrer, dans le cas d'un polynôme f d'une seule variable, l'inégalité $P(f(n)) \gg \log_2 n$. Cette dernière inégalité peut encore être déduite du résultat précité de SHOREY (cf. démonstration (3.1.1)-1°) ; plus généralement, SHOREY a montré, avec TIJDEMAN, l'inégalité (cf. [51]) :

$$P(\textstyle\prod_{1\leqslant i\leqslant k} f(n + i)) \geqslant \varepsilon(f , a).k.\log_2 n.\log(k.\log_2 n).(\log_3 n)^{-1}$$

avec $k \leqslant (\log n)^a$, $a > 0$, $\varepsilon(f , a)$ effectivement calculable (cf. [51]). Dans le cas de polynômes de degré 2 , on a, par les méthodes très simples exposées au début de (3.4), le résultat meilleur suivant : Soient (f_i) $(1 \leqslant i \leqslant k)$ des polynômes du second degré premiers entre eux deux à deux et un réel $\varepsilon > 0$, alors, l'inégalité $P(\prod_{1\leqslant i\leqslant k} f_i(n)) \geqslant ((k - \varepsilon)/4).(\log_2 n)$ est vraie pour $n \geqslant n_0(f_1,\dots,f_k)$ effectivement calculable (cf. [27]).

(3.6) On sait que les premiers résultats sur les formes linéaires en logarithmes sont dus à GEL'FOND (cf. [17]), et l'application de ces idées à l'étude de suites comme $P(f(n))$ a été aperçue avant les développements donnés par BAKER. Ainsi, SCHINZEL, dans un important article (cf. [44]) a, entre autres choses, résolu effectivement les équations : $q_1^{y_1} \dots q_i^{y_i} \pm r_1^{z_1} \dots r_j^{z_j} = s^x$ ($q_1 \dots q_i$, $r_1 \dots r_j$ nombres premiers donnés, s entier $\neq 0$ donné) soit un problème un peu plus général que celui résolu par STØRMER, amélioré des résultats de MAHLER [32] et NAGELL [35], relatifs à $P(ax^2 + bx + c)$ et $P(ax^3 + b)$, certaines de ces améliorations étant toujours actuelles.

4. Suite des nombres ayant des facteurs premiers donnés.

(4.1) Soient a et b deux entiers ayant les mêmes facteurs premiers. ERDÖS et SELFRIDGE ont conjecturé (cf. [14]) que l'écart $a - b$ était supérieur à une fonction croissante de a ou b , plus précisément qu'il existait une constante absolue c telle qu'on ait $a - b \geqslant (\log b)^c$ pour tout couple (a , b) ; cette con-

jecture a été récemment démontrée à partir du résultat déjà cité ([50], cf. (3.1.1)-1° et (3.5)) de SHOREY sur les formes linéaires de logarithmes ; on va en donner une autre démonstration basée sur les résultats de STARK sur l'équation diophantienne $x^3 - y^2 = k$. Soient donc a et b deux entiers tels que $u(a) = u(b)$; comme dans (3.1.1)-2°, on voit qu'il existe un entier $v \leqslant u^5(a)$ tel que va (resp. vb) soit un carré (resp. cube) ; par suite, $v(a - b)$ est de la forme $x^3 - y^2$ et donc, pour tout réel $\varepsilon' > 0$, $\log a \leqslant C(\varepsilon').(v(a - b))^{1+\varepsilon'}$, d'où, puisque $v \leqslant u^5(a) \leqslant (a - b)^5$, $\log a \leqslant C(\varepsilon).(a - b)^{6+\varepsilon}$. Une variante de cette démonstration se trouve dans [28] ; en combinant les deux, on peut, si l'on dispose de renseignements sur les classes modulo 6 des entiers $v_p(a)$ et $v_p(b)$, améliorer l'exposant $6 + \varepsilon$. L'avantage de cette démonstration sur celle (cf. [15]) basée sur les travaux de SHOREY est de fournir une valeur explicite pour l'exposant; elle est toutefois insuffisante pour donner une réponse à une autre question, posée par ERDÖS et SELFRIDGE : existe-t-il toujours un nombre premier compris entre deux entiers a et b tels que $u(a) = u(b)$? En effet, si l'on pouvait substituer à l'exposant $6 + \varepsilon$ un nombre inférieur à $1/2$, on pourrait répondre par l'affirmative (en appliquant la conjecture de CRAMER (cf. (1.6))) . Signalons cependant qu'il en est ainsi si l'on admet les conjectures de HALL sur la courbe $x^3 - y^2 = k$ (cf. [20]), et PILTZ sur l'écart $p_{n+1} - p_n$ (pour tout $\varepsilon > 0$, l'inégalité $p_{n+1} - p_n < (p_n)^{\varepsilon}$ est vraie pour n assez grand), car on prouve alors l'inégalité $a - b \gg (a + b)^{1/16}$ (cf. [28]).

(4.2) Soient S un ensemble fini de nombres premiers, de cardinal $\geqslant 2$, et (n_i) la suite croissante des entiers engendrés par S , c'est-à-dire la suite des nombres dont les facteurs appartiennent à S (cf. (1.5)). Les résultats qui suivent sont dus, pour la plupart, à TIJDEMAN (cf. [61], [62], [63]) ; signalons cependant qu'avant les développements apportés par BAKER, CASSELS [4] avait déduit des travaux de GEL'FOND la possibilité effective de calculer un rang $n_0(t)$ à partir duquel l'inégalité $n_{i+1} - n_i \geqslant (n_i)^t$ est valable (t réel < 1), rang dont l'existence avait été prouvée antérieurement par SIEGEL (cf. (1.5)). Montrons que l'inégalité $n_{i+1} - n_i \geqslant n_i.(\log n_i)^s$ (s constante < 0 effectivement calculable dépendant de S) est une conséquence facile des résultats de BAKER. Il suffit de remarquer que :

$$(n_{i+1} - n_i)/n_i \geqslant \log n_{i+1}/n_i = |\Sigma_{p \in S}\, b_p.\log p| \geqslant \exp(-\, C(S).\log \sup b_p) ,$$

où pour tout $k \in S$, $|b_p| \leqslant \log k n_i/\log 2$. Un calcul analogue peut être fait pour déterminer le rang $n_0(t)$ défini précédemment ; on trouvera ces deux démonstrations complètes dans TIJDEMAN [61], mais il conviendra de reprendre les calculs en utilisant les résultats de SHOREY (précité [50]) ou RAMACHANDRA (cf. [41]) de préférence à ceux de FEL'DMAN [16] et BAKER (Mathematika, t. 15). Toujours dans [61], TIJDEMAN, grâce au principe des tiroirs, prouve que la constante s ne peut être supérieure à $1 - \operatorname{card} S$. Ce même principe et les résultats de BAKER lui permettent également de prouver l'existence, pour tout réel $t < 1$, d'un ensemble

$S(t)$ infini d'entiers tel que la suite croissante (n_i) engendrée satisfasse, pour i assez grand, à l'inégalité $n_{i+1} - n_i \geqslant (n_i)^t$; la construction de $S(t)$ se fait par récurrence, les $k-1$ premiers éléments de $S(t)$ étant définis, et n_0 étant un rang tel que, n'_i désignant la suite engendrée par ces $k-1$ éléments, l'inégalité $n'_{i+1} - n'_i \geqslant (n'_i)^t$ soit vérifiée pour $n'_i \geqslant n_0$: on construit un k-ième élément de sorte que la même inégalité soit vraie à partir du même rang n_0 pour la suite engendrée par ces k éléments. Ce résultat résout une conjecture de WINTNER et est en quelque sorte le meilleur possible ; en effet, la démonstration de l'inégalité $s > 1-\text{card } S$ permet de prouver qu'étant donné un ensemble infini de nombres premiers S' engendrant une suite (n'_i), l'inégalité

$$n'_{i+1} - n'_i \geqslant n'_i.(\log n'_i)^a \quad (a \text{ réel quelconque})$$

est fausse une infinité de fois.

(4.3) Cet alinéa est consacré à des rappels relatifs aux fractions continues. Soit x un réel irrationnel, un rationnel r/s sera dit une bonne approximation à gauche (resp. à droite) de x si $r - sx < 0$ (> 0) et si $r'/s' < x$ $(> x)$ avec $s' < s$ implique $|r - sx| < |r' - s' x|$. Une bonne approximation est un rationnel r/s tel que $|r - sx| < \inf_{s'<s} |r' - s' x|$; une bonne approximation r/s est donc une bonne approximation à gauche ou à droite suivant le signe de $r - sx$, la réciproque étant en général fausse comme on le verra. Comme x est irrationnel, si l'entier $s > 0$ est donné, il y a un unique entier r tel que

$$|r - sx| = \inf_{r' \in \mathbb{Z}} |r' - sx|$$

en d'autres termes, si l'on note $\|y\| = \inf_{n \in \mathbb{Z}} |y - n|$, on peut caractériser les dénominateurs s des bonnes approximations par la propriété $\|sx\| < \inf_{s'<s} \|s' x\|$. L'application classique de Dirichlet du principe des tiroirs montre que, pour tout réel ε $(0 < \varepsilon < 1)$, il existe un entier positif $s < 1/\varepsilon$ tel que $\|sx\| < \varepsilon$, ce qui prouve l'existence d'une infinité de dénominateurs de bonnes approximations. Soient s_n cette suite croissante ainsi attachée à x , et r_n la suite des numérateurs associés ; la suite r_n/s_n converge vers x , et on montre qu'elle coïncide avec la suite obtenue à partir du classique développement en fraction continue de x (si $x = [a_0 , a_1 , \ldots , a_n , \ldots]$, avec $a_0 = [x]$, $a_1 = [(x - a_0)^{-1}]$, ... on a $r_n/s_n = [a_0 , \ldots , a_n]$ si $x - [x] < 1/2$, et $r_n/s_n = [a_0 , \ldots , a_{n+1}]$ si $x - [x] > 1/2$) ; c'est d'ailleurs ainsi que CASSELS introduit les fractions continues dans [3] (pour la présentation "classique", voir par exemple PERRON [36]). Si $x - [x] < 1/2$ (resp. $> 1/2$) , la suite r_{2n}/s_{2n} croît (décroît) vers x tandis que r_{2n+1}/s_{2n+1} décroît (croît) vers la même limite, ce que traduit la relation $s_{n+1} r_n - s_n r_{n+1} = (-1)^n$ (resp. $(-1)^{n+1}$) . De cette dernière égalité, on déduit aisément $s_n \|s_{n+1} x\| + s_{n+1} \|s_n x\| = 1$, et les relations $s_{n+1} = a_n s_n + s_{n-1}$, $r_{n+1} = a_n r_n + r_{n-1}$, lesquelles permettent de retrouver la suite a_n précédemment définie (à un décalage éventuel de 1 près) (on peut encore écrire

$$a_n = [\|s_{n-1} x\| / \|s_n x\|]).$$

Soit n un entier tel que $r_n/s_n < x < r_{n+1}/s_{n+1}$, et considérons les fractions $(ar_{n+1} + r_n)/(as_{n+1} + s_n)$ quand a décrit les entiers de 0 à a_{n+1}, on obtient une suite de rationnels dont on démontre qu'ils sont de bonnes approximations à gauche de x ; réciproquement, on prouve que toutes les bonnes approximations à gauche peuvent être ainsi obtenues. On caractériserait de même les bonnes approximations à droite. Tous ces résultats sont contenus (certains implicitement) dans l'ouvrage de PERRON, quelques uns d'entre eux sont rappelés dans [63].

(4.4) Soient p et q deux nombres premiers $(p \neq q)$, et n_i la suite croissante des entiers de la forme $p^u q^v$ (u, v entiers $\geqslant 0$). Supposons $n_i = p^u q^v$ et $p^u \geqslant (n_i)^{1/2}$, soit r_n/s_n la suite des bonnes approximations attachée à l'irrationnel (et même transcendant) $\log p/\log q$, et désignons plus précisément par n l'entier tel que $s_n \leqslant u < s_{n+1}$. Le nombre $n' = p^{u-s_n}.q^{v+r_n}$ est entier et tel que $|\log n'/n_i| = \log q.|r_n - s_n(\log p/\log q)|$; par conséquent, d'après (4.3),

$$|\log n'/n_i| < (\log q)/s_{n+1} < (\log q)/u < 2(\log p)(\log q)/\log n_i .$$

On a donc prouvé l'inégalité $|n' - n_i| \ll n_i/\log n_i$, c'est-à-dire

$$\inf(n_{i+1} - n_i , n_i - n_{i-1}) \ll n_i/\log n_i .$$

Montrons maintenant l'existence d'une constante c', fonction de p et q, telle que $s_{n+1} < (s_n)^{c'}$, ce qui permettra de prouver qu'on a toujours

$$(n_{i+1} - n_i) \leqslant n_i(\log n_i)^t \quad (t \text{ constante} < 0).$$

(Si $n' > n_i$, c'est clair ; si $n' < n_i$, envisager $n'' = p^{u-s_{n-1}}.q^{v+r_{n-1}}$ $(> n_i)$ et écrire

$$0 < \log(n''/n_i) < (\log q)/s_n < (\log q).s_{n+1}^{-1/c'} < (\log q).u^{-1/c'} \ll (\log n_i)^{-1/c'}) .$$

C'est en effet une conséquence de l'inégalité (où h et k désignent des entiers)

$$|h.\log p - k.\log q| > \exp(- c''.\log \sup(|h| , |k|))$$

puisqu'en particulier,

$$(\log q)/s_n > (\log q)\|s_{n+1}(\log p/\log q)\| > \exp(- c'' \log s_{n+1}) .$$

L'inégalité $(n_{i+1} - n_i) \leqslant n_i/(\log n_i)^t$ étant vraie pour une suite engendrée par deux entiers p et q, elle l'est a fortiori pour toute suite engendrée par un ensemble d'entiers de cardinal > 2. En résumé, S désignant un ensemble fini de nombres premiers, et (n_i) la suite engendrée par S, ce qui précède et (4.2) montrent l'existence de deux constantes < 0, s et t telles qu'on ait, pour tout i,

$$n_i.(\log n_i)^s \leqslant n_{i+1} - n_i \leqslant n_i.(\log n_i)^t .$$

(4.5) Revenons au cas d'une suite n_i engendrée par deux éléments p et q. On a majoré $\inf(n_{i+1}/n_i , n_i/n_{i-1})$ par $\sup(p^{s_n} q^{-r_n} , p^{-s_n}.q^{r_n})$. Plus généralement,

on prouve (cf. [63], §4) que l'ensemble des quotients n_{i+1}/n_i coïncide avec celui des valeurs prises par $\sup(p^{-s} q^{r} , p^{s} q^{-r})$ quand r/s décrit l'ensemble des bonnes approximations de $(\log p)/(\log q)$ à gauche ou à droite ; c'est une conséquence facile des définitions données dans (4.3).

(4.6) Les notations sont celles de (4.2). On va montrer que l'ensemble des entiers i tels que $(n_i , n_{i+1}) = 1$ est infini. Soient d le p. g. c. d. de n_i et n_{i+1} , j et j' les entiers définis par $n_j = n_i/d$, $n_{j'} = n_{i+1}/d$; on vérifie aisément que $j' = j + 1$ (sinon $n_i < dn_j < n_{i+1}$). Prouvons alors la propriété par l'absurde ; si, au-delà d'un rang i_0 , on avait toujours $(n_i , n_{i+1}) = d > 1$, alors $(n_{i+1} - n_i)/n_i = (n_{i+1}/d - n_i/d)/(n_i/d)$ appartiendrait à un ensemble fini ce qui est en contradiction avec l'inégalité $(n_{i+1} - n_i)/n_i \leqslant (\log n_i)^t$ prouvée dans (4.3). Soit S' une partie de S , différente de S , le même raisonnement que précédemment permet de prouver, si S' est réduit à un seul élément, que l'ensemble des entiers i tels que n_i soit engendré par S' et $(n_{i+1} , n_i) = 1$ est infini ; dans le cas où $S' = \{p , q\}$, ce résultat reste vrai, ce qui a été prouvé par TIJDEMAN et MEIJER (cf. [63], §6) mais la démonstration n'est plus immédiate : Comme $\operatorname{card} S' = 2$, on sait, d'après (4.4), que la suite des entiers engendrée par S' est assez bien connue. On raisonne par l'absurde, c'est-à-dire qu'on suppose que si $n_i = p^u q^v$, alors n_{i+1} est divisible par p ou q (pour i assez grand). Cette hypothèse montre qu'à partir d'un certain rang, soit n_{i-1} , soit n_{i+1} est nécessairement de la forme $p^{u'} q^{v'}$; on prouve alors l'existence d'intervalles $(\ell_m , \inf(p , q)\ell_m)$ (où ℓ_m est une suite tendant vers l'infini) tels que les éléments n_i qui y sont situés soient tous engendrés par S' . Or, si $r \in S - S'$, la suite (rn_i) ne contient aucun élément engendré par S' ; par conséquent, pour tout réel $L > 0$, il existe un entier i tel que

$$rn_i < L < \inf(p , q)L < rn_{i+1}$$

ce qui est en contradiction avec $\lim_{i\infty} n_{i+1}/n_i = 1$ (conséquence de

$$(n_{i+1} - n_i) \leqslant n_i(\log n_i)^t).$$

Cette démonstration, basée sur une analyse fine des rapports n_{i+1}/n_i à l'aide de considérations de fractions continues ne semble pas pouvoir être prolongée au cas $\operatorname{card} S > 2$ lequel reste ouvert ; TIJDEMAN et MEIJER conjecturent que la propriété (laquelle est en fait une propriété additive de géométrie des nombres) demeure exacte.

5. Plus grand facteur premier de $C_n(a , b)$ (C_n cyclotomique).

(5.1) Pour tout entier $n \geqslant 1$, on désigne par C_n le n-ième polynôme cyclotomique, c'est-à-dire $C_n(X) = \prod_{x \in R_n}(X - x)$, où R_n est l'ensemble des $\varphi(n)$ racines de 1 d'ordre n . Etant donnés deux entiers a et b $(0 < b < a)$ premiers entre eux, on note $C_n(a , b)$ l'entier $b^{\varphi(n)} C_n(a/b)$. La propriété fondamentale sur laquelle reposent tous les résultats de ce paragraphe est due à BIRKHOFF et

VANDIVER (cf. [2], ces auteurs ont en fait amélioré des résultats antérieurs de ZSIGMONDY [68]) ; elle s'énonce ainsi : les diviseurs premiers de $C_n(a , b)$ (pour $n > 2$) sont tous (sauf peut-être un qui est alors $P(n)$) congrus à 1 modulo n (démonstration dans l'annexe 2).

(5.2) L'intérêt de l'étude des facteurs premiers de nombres comme $C_n(a , b)$ a été perçu depuis longtemps. Les nombres de Fermat $(F_m = 2^{2^m} + 1)$ sont de cette forme $(F_m = C_{2^{m+1}}(2 , 1))$, et si l'on conjecture qu'aucun de ces nombres n'est premier (pour $m > 4$) , on sait par des vérifications numériques qu'ils ont de "grands" facteurs premiers (au sens de (1.1)) ; de même, les nombres de Mersenne ($M_p = 2^p - 1$ avec p premier) sont de cette forme ($M_p = C_p(2 , 1)$), et possèdent tous de "grands" facteurs premiers ; les plus grands nombres premiers connus explicitement sont des nombres de Mersenne : $2^{11213} - 1$, $2^{19937} - 1$ (respectivement les 23e et 24e nombres M_p premiers, cf. [65]).

(5.3) Les résultats prouvés concernant $P(C_n(a , b))$ sont très en deçà de ce que peuvent laisser supposer les investigations numériques. Avant 1962, le meilleur résultat connu était $P(C_n(a , b)) > n$ (cf. Annexe 2) ; SCHINZEL, par des moyens élémentaires (mais longs et techniques), a montré l'inégalité $P(a^n - b^n) > 2n$ quand ab est un carré ou deux fois un carré et hormis certains cas particuliers (cf. [45]). Voyons maintenant pourquoi les méthodes de (3.1) permettent naturellement d'améliorer ces résultats. Etant donnés deux entiers voisins n et $n + k$, on a obtenu, à l'aide des travaux de BAKER, une relation entre $P(n(n + k))$, $\omega(n(n + k))$ et n , d'où l'on a déduit une minoration de $P(n(n + k))$ grâce à l'inégalité $\omega(n(n + k)) \leqslant \pi(P(n(n + k)))$. Or, dans le cas des entiers tels que $C_n(a , b)$, on a vu dans (5.1) qu'on pouvait remplacer cette inégalité par

$$\omega(C_n(a , b)) \leqslant 1 + \pi_{1,n}(P(C_n(a , b))) ,$$

où $\pi_{1,n}(x) = \sum_{p \leqslant x, p \equiv 1 (\mathrm{mod}\ n)} 1$ (on verra dans l'annexe 2 que c'est cette inégalité qui est aussi à la base des résultats antérieurs relatifs à $P(C_n(a , b))$ cités ci-dessus) ; l'évaluation de $\pi_{1,n}(x)$ se fait, comme x n'est pas très "grand" devant n , suivant les méthodes de BRUN-TITSCHMARCH (cf. [38]) ; rappelons qu'on déduit de l'hypothèse de Riemann la relation (valable uniformément en x) :

$$\pi_{1,n}(x) = (\varphi(n))^{-1} \int_2^x \frac{dy}{\log y} + O(x^{1/2} . \log x) .$$

Pour x infini, on a, d'après le théorème de la progression arithmétique,

$$\pi_{1,n}(x) = (1 + o(1))(\varphi(n))^{-1}(x/\log x) .$$

(5.4) D'après ce que l'on a vu dans (5.3), il suffit donc de savoir approcher $C_n(a , b)$ par un nombre n'ayant que de petits facteurs premiers pour obtenir des résultats sur $P(C_n(a , b))$. Si $n = p$ premier, $C_p(a , b) = (a^p - b^p)/(a - b)$ peut évidemment être approché par $a^p/(a - b)$ et, de même, si $n = 2p$, $C_{2p}(a , b) = (a^p + b^p)/(a + b)$ peut être approché par $a^p/(a + b)$; on va d'abord traiter ces deux premiers cas qui sont faciles, le cas général faisant l'objet de l'alinéa suivant. Pour cela, il suffit de reprendre la démonstration de (3.1.1)-1°

pour déduire du résultat [50] de SHOREY l'inégalité (pour p assez grand)

$$P(a^p - b^p) = P(C_p(a , b)) \gg p.\log p$$

(et de même $P(a^p + b^p) = P(C_{2p}(a , b)) \gg p.\log p$) ; de plus, la même méthode, jointe à un résultat de crible d'Erdös [11] sur $\omega(2^p - 1)$, permet de prouver que, pour presque tout nombre premier (au sens de la densité naturelle dans cet ensemble), l'inégalité $P(2^p - 1) \geqslant p.(\log p)^2 (\log_2 p)^{-3}$ est vraie (cf. [15]). Les méthodes ayant permis de prouver (3.1.1)-2° qui utilisaient les travaux de BAKER et STARK sur les équations diophantiennes ne donnent pas de résultats ici, mais, si l'on admet la conjecture de HALL [20] et l'hypothèse de Riemann généralisée, on peut prouver par ces moyens que les inégalités (pour tout entier donné a)

$$P(a^p - 1) \geqslant p^2.(\log p)^{-4-\varepsilon} \quad \text{et} \quad P(a^{2^m} + 1) \geqslant 2^{2^m}.m^{-4-\varepsilon}$$

sont vraies à partir d'un certain rang (fonction de ε , nombre > 0 donné).

(5.5) L'approximation de $C_n(a , b)$ par un nombre n'ayant que de petits facteurs premiers reste possible pour presque tout entier (au sens de la densité naturelle) grâce à une méthode due à STEWART [57] ; plus précisément, cette méthode s'applique à tous les entiers n tels que $\omega(n) \leqslant k.\log_2 n.(\log 2)^{-1}$ (où k est un réel < 1), entiers qui forment un ensemble de densité 1 dès que $k > \log 2 \simeq 0{,}69$. Soient $d_1 < d_2 < \ldots < d_t$ les diviseurs de n tels que $\mu(n/d) \neq 0$ (μ fonction de Möbius) de sorte qu'en posant $d_0 = 1$, on ait $n = \prod_{0 \leqslant i < t}(d_{i+1}/d_i)$; on voit donc qu'existe un entier s $(0 \leqslant s < t)$ tel que $d_{s+1}/d_s \geqslant n^{1/t}$, c'est-à-dire, puisque $t = 2^{\omega(n)}$, tel que $\log(d_{s+1}/d_s) \geqslant (\log n)^{1-k}$; le (ou les) entier(s) d_{s+1} ainsi défini(s) tend(ent) donc vers l'infini avec n . On écrit $C_n(a , b)$ sous la forme $\prod_{1 \leqslant i \leqslant t}(a^{d_i} - b^{d_i})^{\mu(n/d_i)}$ et plus précisément :

$$\prod_{1 \leqslant i \leqslant s}(a^{d_i} - b^{d_i})^{\mu(n/d_i)} . \exp\Big(\Big(\sum_{s < i \leqslant t} d_i \, \mu(n/d_i)\Big).\log a\Big) . \prod_{s < i \leqslant t}(1 - (b/a)^{d_i})^{\mu(n/d_i)} ;$$

ce dernier terme est un produit composé :

1° d'un rationnel R_1 de hauteur majorée par

$$\exp\Big(\Big(\sum_{1 \leqslant i \leqslant s} |d_i|\Big).\log a\Big) < a^{td_s} \leqslant \exp((\log n)^k \log a) ,$$

2° d'un rationnel R_2 n'ayant que des facteurs premiers indépendants de n de hauteur majorée par $\exp((\log n)^k \, n \log a)$,

3° d'un rationnel R_3 voisin de 1 puisque

$$\Big|\log \prod_{s < i \leqslant t}(1 - (b/a)^{d_i})\Big| \leqslant K(a , b)(b/a)^{d_{s+1}} \quad (K(a , b) \text{ constante}).$$

En d'autres termes, on approche $C_n(a , b)$ par le rationnel $(R_1 \, R_2)$ de sorte qu'en décomposant $C_n(a , b)$ en produit de puissances de nombres premiers, et en formant comme dans (3.1)

$$\log R_3 = \log\Big((R_1 \, R_2)^{-1} \prod_{1 \leqslant j \leqslant \ell} p_j^{b_j}\Big) ,$$

on obtient, grâce au résultat [50] de SHOREY, l'inégalité :

$$P(C_n(a , b)) \gg n(\log n)^{1-k}(\log_2 n)^{-1} \quad \text{(cf. [15])}.$$

6. L'équation de Catalan.

(6.1) Au siècle dernier, CATALAN a conjecturé que l'équation diophantienne $x^p - y^q = 1$ avait pour unique solution la solution évidente $x = 3$, $p = 2$, $y = 2$, $q = 3$ (cf. [5]). On trouvera dans le dernier chapitre du livre de MORDELL [34] un résumé, avec référence, des principaux résultats (de nature purement arithmétique) relatifs à cette conjecture. R. TIJDEMAN [64] vient de déduire des nouvelles formes des inégalités de BAKER ("Sharpening", Acta Arithm., t. 24 et 27) une variante lui permettant de donner un majorant effectif pour les solutions de l'équation de Catalan, ramenant la conjecture de ce dernier à un nombre fini déterminé de vérifications numériques (irréalisables avec les valeurs actuelles des divers majorants). On va exposer la démonstration de TIJDEMAN, mais on ne détaillera ni la variante en question, ni les résultats de BAKER qui lui ont donné naissance, car A. VAN DER POORTEN vient de prouver un résultat plus fort englobant le tout (valable en outre en p-adique) (cf. [66]). On se borne donc à énoncer le lemme qui nous sera directement utile :

(6.1.1) LEMME. - *Il existe deux constantes strictement positives* c' *et* c'', *effectivement calculables, telles que, pour tout triplet* (a, b, c) *de nombres rationnels* $\neq 0$, *et tout triplet* (i, j, k) *d'entiers relatifs satisfaisant à* $L = |i \log a + j \log b + k \log c| \neq 0$, *on ait*

$$L \geqslant \exp(-c' \log A(\log A')^{c''} \log B)$$

avec, h désignant la fonction hauteur,

$$A \geqslant \sup(2, h(a)),\ A' \geqslant \sup(2, h(b), h(c)),\ B \geqslant \sup(2, |i|, |j|, |k|).$$

(6.2) Soient S l'ensemble des quadruplets (x, y, p, q) d'entiers $\geqslant 2$ vérifiant $x^p - y^q = 1$, T l'ensemble des éléments de S tels que $p > q$ et p, q premiers. On va d'abord prouver que s'il existe une constante M telle que $(x, y, p, q) \in T$ implique $\sup(p, q) \leqslant M$, alors, pour une constante M' convenable, $(x, y, p, q) \in S$ implique $\sup(x, y, p, q) \leqslant M'$. Soient $(x, y, p, q) \in S$, p', q', deux facteurs premiers de p et q respectivement, le quadruplet $(x^{p/p'}, y^{q/q'}, p', q')$ appartient donc à T, ce qui entraîne $\sup(p', q') \leqslant M$; or, on sait (cf. [1], ch. 4) qu'une telle condition implique la majoration de $x^{p/p'}$ et $y^{q/q'}$ (donc de x, y, p/p', q/q') par une fonction effectivement calculable de M, d'où le résultat. Soit T' la partie de T formée des éléments (x, y, p, q) où $p > q > 2$; on va prouver l'existence d'une constante M majorant p pour tout $(x, y, p, q) \in T'$, la même démonstration, à d'évidentes modifications près, montrera un résultat analogue pour les quadruplets (x, y, p, q) tels que $2 \leqslant p < q$. Ne restent donc que les cas $p = q$ (immédiat) et $q = 2$ (réglé deux ans après que CATALAN ait émis sa conjecture, ce cas est traité (d'après une démonstration de CASSELS basée sur la factorialité des entiers de Gauss) dans le livre de MORDELL [34]) où l'on voit qu'il n'existe aucune solution.

(6.3) On prouve maintenant un résultat arithmétique préparatoire. L'équation de Catalan peut être écrite $(x - 1).C_p(x) = y^q$ avec les notations du §5 et de l'annexe 2 ; comme $C_p(1) = p$, le p. g. c. d. de $(x - 1)$ et de $C_p(x)$ est 1 ou p ; d'autre part, d'après l'annexe 2, $v_p(C_p(x)) = 1$ (si $x \equiv 1 \pmod p$) ou 0 (si $x \not\equiv 1 \pmod p$) ; on voit donc que ou $(x - 1)$ ou $p(x - 1)$ est de la forme a^q , où a est un entier non divisible par p dans le premier cas, divisible dans le second. De même, on peut écrire l'équation de Catalan sous la forme

$$(y + 1).C_{2q}(y) = x^p \quad \text{(puisqu'on a supposé } q \neq 2 \text{)},$$

et déduire des relations $C_{2q}(-1) = q$ et $v_q(C_{2q}(y)) \leqslant 1$ que $(y + 1)$ ou $q(y + 1)$ est de la forme b . D'autre part, CASSELS a prouvé que, pour tout $(x , y , p , q) \in T$, p (resp. q) divise y (resp. x) ; cela exclut donc les possibilités $x - 1 = a^q$, $y + 1 = b^p$. Signalons qu'il est possible d'utiliser des résultats arithmétiques plus simples (notamment de ne pas faire appel à l'annexe 2 ou au résultat de Cassels) au prix d'un allongement de la suite de la démonstration (cf. TIJDEMAN [64]).

(6.4) On est maintenant ramené à la situation suivante : $x = 1 + a^q/p$, $y = -1 + b^p/q$, d'où

$$a^{pq}\, p^{-p}(1 + pa^{-q})^p = b^{pq}\, q^{-q}((1 - qb^{-p})^q + (qb^{-p})^q) .$$

Comme $qb^{-p} \leqslant 1/3$, $|\log(1 - qb^{-p})^q + (qb^{-p})^q)| \leqslant (4/3)q(qb^{-p})$ et donc

$$|pq \log(a/b) - p \log p + q \log q| \leqslant p^2\, a^{-q} + (4/3)(q^2\, b^{-p}) .$$

On a supposé $p > q$ donc $x < y$, on peut alors majorer $q^2\, b^{-p}$ par $p^2\, a^{-q}$, c'est-à-dire que si p est tel que $10 \log p \leqslant q$, on a $3p^2 \leqslant (a^{-q})^{1/2}$ et donc $p^2\, a^{-q} + (4/3)(q^2\, b^{-p}) \leqslant a^{-q/2}$. En particulier, on en déduit :

$$|\log(a/b)| \leqslant (\log p)/q + (\log q)/p + 1/pq < 1 ,$$

ce qui montre qu'on peut majorer la hauteur de a/b par $3a$. En résumé, on a prouvé que l'on a soit $q < 10 \log p$, soit $|pq \log(a/b) - p \log p + q \log q| \leqslant a^{-q/2}$ d'où l'on déduit, grâce au lemme (6.1.1),

$$q \log a \leqslant \log a (\log p)^{c''} \log pq$$

et donc $q \leqslant (\log p)^k$, où k est une constante convenable. On écrit maintenant l'équation de Catalan sous la forme suivante :

$$x^p(qb^{-p})^q = (1 - qb^{-p})^q + (qb^{-p})^q ;$$

en faisant apparaître dans le premier membre le quotient x/b^q , et en formant le logarithme, on obtient

$$p \log(x/b^q) + q \log q = \log((1 - qb^{-p})^q + (qb^{-p})^q)$$

qu'on majore comme précédemment par $(4/3)q^2\, b^{-p}$, quantité $\leqslant b^{-p/2}$ pour p assez grand. De là, on déduit, toujours comme précédemment,

$$|\log(x/b^q)| \leqslant (q \log q)/p + 1 ,$$

ce qu'on peut majorer par 2 pour p assez grand d'après la première partie de la démonstration ; la hauteur de x/b^q est donc au plus $2b^q$. Il n'y a alors plus qu'à appliquer le lemme (6.1.1) pour obtenir, comme ci-dessus,

$$p \log b \leqslant q(\log b)(\log p)(\log q)^{c''} ,$$

ce qui implique, d'après ce qui a déjà été prouvé, $p \leqslant (\log p)^{k'}$ (k' constante) d'où la majoration de p .

(6.5) La démonstration précédente ne permet pas de donner des majorants pour les solutions de l'équation $x^p - y^q = c$, c entier donné ; il semble toutefois que ČUDNOWSKI ait des résultats dans ce sens (non encore publiés). Plus généralement, le problème suivant : Est-ce que $\lim P(x^p - y^q) = \infty$, lorsque $\sup(x , y , p , q)$ (avec x , y , p , q entiers, $(x , y) = 1$, $x^p \neq y^q$) , tend vers l'infini ? est ouvert ; il résulte des travaux de MAHLER que la réponse est affirmative quand (x et y) ou (p et q) sont fixés, certains cas particuliers peuvent être ramenés aux résultats de [28].

Annexe 1 : Le théorème de Sylvester

(A.0) Les notations définies en (1.0) restent valables. Etant donnés deux entiers n ($\geqslant 0$) et k (> 0) , on désigne par $\nu(n , k)$ le p. p. c. m. de $n + 1 , n + 2 , \ldots , n + k$; quand $n = 0$, on note $\nu(k)$ au lieu de $\nu(0 , k)$. Si $k \geqslant n$, il est clair que $\nu(n , k) = \nu(n + k)$; cette annexe est consacrée à l'étude, par des moyens élémentaires, de $\nu(n , k)$; on obtiendra en particulier ainsi le théorème de Sylvester.

(A.1) *Soient* n , k *deux entiers* $\geqslant 1$ *et, pour tout nombre premier* p , i_p *un entier compris entre* 1 *et* k *réalisant* $v_p(n + i_p) = \sup_{1 \leqslant i \leqslant k} v_p(n + i)$. *Alors, pour tout entier* $j \neq 0$ *tel qu'on ait* $n + 1 \leqslant n + i_p + j \leqslant n + k$,

$$v_p(n + i_p + j) = v_p(j) .$$

Démonstration. - Il est clair qu'il suffit de prouver que les relations :

$$v_p(n + i_p + j) = v_p(n + i_p) \quad \text{et} \quad v_p(j) > v_p(n + i_p)$$

ne peuvent avoir lieu simultanément. En effet, en supposant par exemple $j > 0$, on pourrait alors écrire

$$n + i_p + j = p^{v_p(n+i_p)}(a + bp^c)$$

avec $a > 0$, $b > 0$, $c > 0$, $(a , p) = (b , p) = 1$; comme il existe un multiple de p compris strictement entre a et $a + bp^c$, il y aurait entre $n + i_p$ et $n + i_p + j$ un élément n' tel que $v_p(n') > v_p(n + i_p)$, ce qui est impossible. Le cas $j < 0$ se traite de façon analogue en écrivant

$$n + i_p = p^{v_p(n+i_p+j)}(a + bp^c) .$$

(A.2) THÉORÈME.

1° $k\binom{n+k}{k}$ *divise* $\nu(n,k)$; $\nu(n,k)$ *divise* $\nu(k)\binom{n+k}{k}$.

2° *Les inégalités précédentes sont les meilleures possibles.*

Démonstration. - On conserve les notations de (A.1) ; par définition de i_p , on a $v_p(n+i_p) = v_p(\nu(n,k))$; en appliquant (A.1), il vient donc :

$$v_p(\nu(n,k)) = \sum_{1\leqslant i\leqslant k} v_p(n+i) - v_p((i_p-1)!) - v_p((k-i_p)!)$$

ou

$$v_p(\nu(n,k)) = v_p(\binom{n+k}{k}) + v_p(k) + v_p(\binom{k-1}{i_p-1}) ,$$

d'où la première relation.

Si l'on pose $n+k=n'$, et si l'on remarque que $\nu(n,k)$ divise $\nu(n')$, on déduit de la première partie de la démonstration que, pour tout entier $k' \leqslant n'$, $k'\binom{n'}{k'}$ divise $\nu(n')$; en particulier, $k\binom{k-1}{i_p-1} = i_p\binom{k}{i_p}$ divise $\nu(k)$, ce qui achève de prouver 1°. Pour montrer 2°, il suffit de vérifier que tout entier n de la forme $a\prod_{p\leqslant k} p^{a_p} - 1$ avec a entier >0 , a_p entier tel que $k < p^{a_p}$, possède les propriétés suivantes :

$$k\binom{n+k}{k} = \nu(n,k) , \quad \nu(n+1,k) = \nu(k)\binom{n+1+k}{k} .$$

(A.3) THÉORÈME (SYLVESTER). - $P(n,k) > k$ *lorsque* $n \geqslant k$.

Démonstration. - De $p^{v_p(\nu(n,k))} \leqslant n + i_p \leqslant n+k$, on déduit l'inégalité

$$\nu(n,k) \leqslant (n+k)^{\pi(P(n,k))} .$$

On est donc ramené à infirmer $\nu(n,k) \leqslant (n+k)^{\pi(k)}$. Tout ensemble de la forme $m+1, m+2, \ldots, m+6$ (où $m \geqslant 2$) contenant au plus deux nombres premiers, on vérifie aisément que $\pi(k) \leqslant k/3$ à partir de $k = 33$; d'autre part, $\binom{n+k}{k}$ s'écrit $((n+k)/k)^k \cdot \prod_{0\leqslant i<k}(1 - i/(n+k))/(1-i/k)$ donc est supérieur à $((n+k)/k)^k$. Le résultat est par suite clair lorsque $(n+k) > k^{3/2}$ et $k \geqslant 33$, cette dernière restriction pouvant être levée par une suite de vérifications convenables. Le cas $(n+k) \leqslant k^{3/2}$ (d'où $k \geqslant (n+n^{2/3})^{2/3}$) se traite aisément comme dans (1.6) et se ramène à un petit nombre de vérifications numériques.

(A.4) La démonstration donnée, en 1892, par SYLVESTER [59] était basée sur l'inégalité naturelle $\nu(n,k) \leqslant (n+k)^{\pi(P(n,k))}$ et sur une évaluation originale du premier membre, le second étant majoré grâce aux calculs de ČEBIČEV sur la fonction π . Comme on l'a vu, ce procédé n'est commode que lorsque n est grand devant k , aussi, la démonstration de SYLVESTER est-elle longue. En 1929, SCHUR [48] donnait une nouvelle démonstration utilisant également les travaux de ČEBIČEV. Grâce à un usage répété de la relation $v_p(n!) = \sum_{i\geqslant 1} np^{-i}$, ERDÖS [9], en 1934, prouve à nouveau le théorème en partageant son étude en deux parties

1° $(n+k) \geqslant k^{3/2}$: cas traité de façon analogue à celle de SYLVESTER en montrant

directement l'inégalité $\binom{n+k}{k} \leqslant (n+k)^{\pi(P(n,k))}$.

2° $(n+k) < k^{3/2}$: cas non traité par l'emploi d'inégalités de la forme $p_{n+1} - p_n \geqslant (p_n)^a$ (ce que fera ERDÖS en 1955 dans [10]) mais de façon entièrement élémentaire grâce à la démonstration préalable de l'inégalité $\nu(n) \leqslant 4^n$; ERDÖS déduit ensuite, de l'hypothèse $P(n , k) \leqslant k$, une relation analogue à

$$\nu(n , k) \leqslant \prod_{p\leqslant k} p^{v_p(\nu(n+k))} \leqslant \prod_{p\leqslant k} p . \prod_{p^\alpha \leqslant n+k, \alpha\geqslant 2} p ,$$

mais en utilisant $\binom{n+k}{k}$ au lieu de $\nu(n , k)$, relation qu'il infirme grâce au lemme préalablement établi $\nu(n) = \prod_{p^\alpha\leqslant n} p \leqslant 4^n$.

(Cela revient à montrer que l'inégalité ci-dessous est fausse à partir d'un certain rang

$$k.\log 4 \leqslant k.\log(2(n+k)/k) \leqslant \theta(k) + \psi(n+k) - \theta(n+k) \leqslant \theta(k) + O(k^{3/4}) .)$$

Signalons que l'inégalité $\nu(n) \leqslant 4^n$ a été récemment améliorée de façon élémentaire en $\nu(n) \leqslant 3^n$ (cf. [21]), et que la démonstration d'ERDÖS a suscité de nombreuses recherches sur les facteurs premiers des coefficients binômiaux (une liste (et des problèmes ouverts) se trouve dans un survey d'ERDÖS [13]).

(A.5) Dans la suite de cette Annexe, on n'utilise que les résultats de (A.1) et (A.2). On va montrer maintenant que le théorème (A.2) permet de retrouver les classiques résultats de ČEBIČEV. On vérifie facilement par récurrence qu'on a $\binom{2n}{n} \geqslant 2^{2n-1}/n$ (resp. $\geqslant 2^{2n}/n$) pour $n \geqslant 1$ ($\geqslant 4$) et, par conséquent, $2^{2n} \leqslant \nu(2n)$ pour $n \geqslant 4$), d'où $2^{n-1} \leqslant \nu(n)$ (pour tout n). D'autre part, on voit de même qu'on a, pour tout $n \geqslant 5$, $\binom{2n}{n} \leqslant 4^{n-1}$, et donc, en désignant par a la fonction associant au réel x l'entier immédiatement supérieur (au sens large) à $x/2$, et en utilisant l'inégalité $\nu(2n)/\nu(n) \leqslant \binom{2n}{n}$, il vient :

$$\nu(n) \leqslant \nu(2a(n)) \leqslant \frac{\nu(2a(n)).\nu(a(n)).\nu(a^{(2)}(n)) \ldots}{\nu(a(n)).\nu(a^{(2)}(n)).\nu(a^{(3)}(n)) \ldots}$$

$$\leqslant \prod_{1\leqslant i\leqslant i_0} \frac{\nu(2a^{(i)}(n))}{\nu(a^{(i)}(n))} \leqslant \prod_{1\leqslant i\leqslant i_0} \binom{2a^{(i)}(n)}{a^{(i)}(n)} \leqslant 4^{2a(n)-2} \quad (< 4^n)$$

(où i_0 désigne le premier entier tel que $a^{(i_0)} = 1$) pour $a(n) \geqslant 3$, la dernière inégalité s'obtenant aisément par récurrence sur $a(n)$; il est alors immédiat de vérifier que l'inégalité $\nu(n) \leqslant 4^n$ est vraie pour tout n . En remarquant que $\binom{2n}{n} = o(4^n)$, on prouve aisément, par récurrence sur $a(n)$, l'inégalité

$$\prod_{1\leqslant i\leqslant i_0} \binom{2a^{(i)}(n)}{a^{(i)}(n)} = o(4^n) ,$$

d'où l'on déduit de même $\nu(n) = o(4^n)$. De façon analogue, la première partie de la démonstration permet de voir que $2^n.n^{1/2} = O(\nu(n))$.

(A.6) On donne maintenant une amélioration d'un lemme d'ERDÖS utilisé fréquemment dans l'étude de $P(n , k)$ par RAMACHANDRA, SHOREY, TIJDEMAN (et ERDÖS) comme on l'a vu dans (3.2). Soit ℓ un entier $\geqslant k$; on désigne par $I(\ell)$ l'ensemble

décrit par i_p (pour n'importe quelle détermination de i_p, cf. (A.1)) quand p parcourt l'ensemble des nombres premiers $\leqslant \ell$. Pour tout $i = 1, 2, \ldots, k$; soit $m_i(\ell) = \prod_{p\leqslant\ell} p^{v_p(n+i)}$; on note $\prod_i^0 m_i(\ell)$ le produit des $m_i(\ell)$ quand i décrit l'ensemble $\{1, 2, \ldots, k\} - I(\ell)$. Quand $\ell = k$, on retrouve le produit envisagé dans (3.2) dont ERDÖS a prouvé qu'il était inférieur ou égal à k^k. On va prouver l'inégalité, pour tout ℓ, $\prod_i^0 m_i(\ell) \leqslant (k-1)!$ laquelle est la meilleure possible. Pour $p \leqslant \ell$, on a

$$v_p(\prod\nolimits^0 m_i(\ell)) \leqslant \Sigma_{1\leqslant i\leqslant k}\, v_p(n+i) - v_p(n+i_p)$$
$$= v_p((i_p-1)!) + v_p((k-i_p)!) = v_p((k-1)!) - v_p(\binom{k-1}{i_p-1})$$

ce qui prouve le résultat annoncé, le meilleur possible pour les entiers n définis comme dans (A.2)-2°.

(A.7) On a vu dans (A.0) que l'inégalité naturelle $\nu(n, k) \leqslant \nu(n+k)$ était une égalité pour $k \geqslant n$; on sait donc évaluer $\nu(n, k)$ de façon précise dans ce cas puisque $\nu(n+k) = \exp(\psi(n+k))$. On suppose maintenant $4 \leqslant k < n$, et on va prouver les inégalités suivantes qui précisent celles utilisées par BAKER dans [1] (ch. 3, §2) :

$$(2(n+k)/k)^k < \nu(n, k) < (8(n+k)/k)^k \quad \text{(pour } 4 \leqslant k < n\text{)}.$$

Remarquons d'abord que

$$\binom{n+k}{k} = \binom{2k}{k}.\prod_{k\leqslant i<2k}((n+k-i)/(2k-i)) > ((2^{2k})/k).((n+k)/2k)^k$$

(pour $4 \leqslant k < n$, ce qu'on a supposé par hypothèse) ce qui, d'après (A.2)-1°, montre la première inégalité ; d'autre part, on a

$$\nu(n,k) \leqslant \nu(k)\binom{n+k}{k} \leqslant (2{,}83)^k(n+k)^k(k!)^{-1} \leqslant (2{,}83e(n+k)/k)^k \leqslant (7{,}7(n+k)/k)^k$$

en appliquant l'inégalité (non élémentaire) $\nu(k) \leqslant (2{,}83)^k$ déduite des évaluations bien connues de ROSSER et SCHOENFELD.

Annexe 2 : Le théorème de Birkhoff et Vandiver.

(A'.0) On conserve les notations de (1.0) et du §5 ; pour tout entier $n > 0$, R_n désigne l'ensemble des racines de 1 d'ordre n, et $C_n = \prod_{x\in R_n}(X - x)$ le n-ième polynôme cyclotomique. On rappelle les identités :

$$X^n - 1 = \prod_{d|n} C_d \quad \text{et} \quad C_n = \prod_{d|n}(X^d - 1)^{\mu(n/d)}$$

où μ désigne la fonction de Möbius ; pour tout couple (a, b) (avec $0 < b < a$) d'entiers premiers entre eux, on note $C_n(a, b)$ l'entier

$$\prod_{x\in R_n}(a - bx) = b^{\varphi(n)}.C_n(a/b),$$

φ étant l'indicateur d'Euler. Le théorème de Birkhoff et Vandiver dont on rappelle l'énoncé ci-après (cf. (A'.1)) est une extension du résultat suivant permettant de prouver simplement l'irréductibilité des polynômes cyclotomiques : pour tout

nombre premier p et tout entier n non congru à 1 modulo p, les diviseurs premiers de $C_p(n)$ sont tous congrus à 1 modulo p. En effet, soit p' un diviseur premier de $C_p(n)$; p' est différent de p puisqu'il est clair que $C_p(n)$ est congru à 1 modulo p ; l'ordre de n modulo p' est donc $\neq 1$, et par suite égal à p, autrement dit, $p' - 1$ divise p d'où le résultat.

Déduisons de cela l'irréductibilité dans $Z[X]$ des polynômes cyclotomiques ; on sait qu'il suffit d'établir la propriété pour C_n avec n premier impair ; posons $n = p$, et soit $D \in Z[X]$ un diviseur strict de C_p ; comme les facteurs premiers de $C_p(i)$ pour $i = 0, 2, 3, \ldots, p - 1$ sont égaux à 1 modulo p, il en est de même de ceux de $D(i)$; en d'autres termes, dans Z/pZ, l'équation $D(x) = 1$ a 0 ou $p - 1$ racines, la deuxième éventualité étant impossible par hypothèse, on en déduit $D = 1$

C. Q. F. D.

(A'.1) THÉORÈME. - Pour tout entier $n > 2$, les facteurs premiers de $C_n(a, b)$ sont congrus à 1 modulo n sauf peut-être un qui est alors $P(n)$.

Démonstration. - Soit p un diviseur premier de $C_n(a, b)$. On suppose d'abord que p ne divise aucun nombre $C_d(a, b)$ lorsque d parcourt l'ensemble des diviseurs stricts de n. En d'autres termes, l'ordre modulo p de a/b (défini puisque $(a, b) = 1$ implique $(b, p) = 1$) est n, et, dans ce cas, n divise $p - 1$, d'où $p \equiv 1 \pmod{n}$. Pour traiter le cas résiduel, on aura besoin du lemme suivant.

(A'1.1) LEMME. - $v_p(a - b) > 0$ et $v_p(n) = 0$ impliquent $v_p(a^n - b^n) = v_p(a - b)$.

Démonstration. - $v_p(a^n - b^n) = v_p(a - b) + v_p(\sum_{0 \leqslant i < n} a^i b^{n-1-i})$; or, puisque $a \equiv b \pmod{p}$, $\sum_{0 \leqslant i < n} a^i b^{n-1-i} \equiv n a^{n-1} \pmod{p}$, d'où le résultat.

On revient à la démonstration de (A'.1). Soit $d < n$ un diviseur de n tel que p divise $C_d(a, b)$; on a donc $v_p(a^n - b^n) > v_p(a^d - b^d) > 0$; il résulte alors aussitôt du lemme que p divise n/d, donc n. Soient a et n' tels que $(n', p) = 1$ et $n = p^a n'$; montrons alors la congruence

$$C_n(a, b) \equiv (C_{n'}(a, b))^{\varphi(p^a)} \pmod{p} ;$$

en effet, en remarquant que $v_p(d) < a - 1$ implique $\mu(n/d) = 0$, on voit que (dans $Q(X, Y)$)

$$C_n(X, Y) = \prod_{d' | n'} (X^{p^a d'} - Y^{p^a d'})^{\mu(n'/d')} \cdot \prod_{d' | n'} (X^{p^{a-1} d'} - Y^{p^{a-1} d'})^{-\mu(n'/d')}$$

d'où, dans $Z[X, Y]$,

$$C_n(X, Y) \cdot C_{n'}(X^{p^{a-1}}, Y^{p^{a-1}}) = C_{n'}(X^{p^a}, Y^{p^a})$$

c'est-à-dire, dans $(Z/pZ)[X, Y]$,

$$C_n(X, Y) \cdot (C_{n'}(X, Y))^{p^{a-1}} = (C_{n'}(X, Y))^{p^a} ,$$

et le résultat cherché est alors clair. La congruence qu'on vient de prouver nous montre que p divise $C_{n'}(a , b)$; or, comme p ne divise pas n' , on voit, d'après la partie précédente de la démonstration, que $v_p(C_d(a , b)) = 0$ pour tout diviseur strict d de n' . La première partie de la démonstration prouve alors que n' divise $p - 1$, ce qui montre que les facteurs premiers de n' sont strictement inférieurs à p , et donc que $p = P(n)$. C'est ce théorème (A'.1), dû à BIRKHOFF et VANDIVER, qui est à la base des résultats du §5.

(A'.2) THÉORÈME. - Si $n > 2$, $v_{P(n)}(C_n(a , b)) \leqslant 1$.

Démonstration. - Dans cet alinéa, p désigne $P(n)$. Soit d un diviseur de n tel que $\mu(n/d) \neq 0$ et $C_d(a , b)$ soit divisible par p ; d est donc de la forme $n'' p^b$ avec $b = a$ ou $a - 1$ (on rappelle que $v_p(n)$ a été noté a , cf. (A'.1)) et $(p , n'') = 1$, si $b > 0$, alors p divise $C_{n''}(a , b)$ et, puisque $P(n'') < p$, on a donc $n'' = n'$, si $b = 0$, de même, la divisibilité de $C_{n''}(a,b)$ par p implique $n'' = n'$; en résumé, on a donc prouvé que d est égal à n ou n/p ; autrement dit,

$$v_p(C_n(a , b)) = v_p(a^n - b^n) - v_p(a^{n/p} - b^{n/p}) .$$

Prouvons alors le lemme suivant :

LEMME. - Pour tout nombre premier impair q tel que $v_q(a - b) > 0$, on a $v_q(a^q - b^q) = v_q(a - b) + 1$. De plus, la même relation reste valable pour $q = 2$ si $v_q(a - b) > 1$.

Démonstration. - $a^q - b^q = (b + (a - b))^q - b^q = \sum_{0<i\leqslant q} \binom{q}{i} (a - b)^i b^{q-i}$, or, la valuation q-adique de chacun des termes de la somme vaut $1 + iv_q(a - b)$ pour $i < q$ et $qv_q(a - b)$ pour $i = q$; donc, comme on a supposé q impair, la borne inférieure des valeurs prises par cette valuation est atteinte une seule fois pour $i = 1$, d'où le résultat. La démonstration est la même à d'évidentes modifications près quand $q = 2$. Si $v_q(a - b) = 0$, alors $v_q(a^q - b^q) = 0$.

Le lemme qui vient d'être prouvé termine la démonstration de (A'.2) quand p est $\neq 2$ ou bien quand $v_2(a - b) = 0$ ou $v_2(a - b) > 1$; reste seulement le cas $a - b = 2c$ avec c impair, mais, $v_2(a^2 - b^2) = v_2(4c(c + b)) \geqslant 3$, et le lemme précédent peut s'appliquer à nouveau puisque, par hypothèse, $n > 2$.

(A'.3) THÉORÈME. - Si $n \neq 6$, $P(C_n(a , b)) > n$.

Démonstration. - Il suffit de prouver que l'égalité $C_n(a , b) = P(n)$ est impossible. La restriction $n \neq 6$ est indispensable car $C_6(2 , 1) = 2^2 - 1.2 + 1 = 3$. La démonstration est immédiate dans deux cas particuliers :

$a - b \geqslant 2$, car alors $C_n(a , b) > 2^{\varphi(n)} \geqslant 2^{P(n)-1} \geqslant P(n)$,

n premier, car alors $C_n(a , b) = \sum_{0\leqslant i<n} a^i b^{n-i-1} > nb^{n-1} \geqslant P(n)$.

Plus généralement, soit D (resp. D') l'ensemble des diviseurs d de n tels

que $\mu(n/d) = 1(-1)$; il est clair que card D = card D' = $2^{\omega(n)-1}$ ainsi que $\sum_{d\in D} d - \sum_{d\in D'} d = \varphi(n)$. De $a^{d-1}(a-1) \geqslant a^{d-1} b > b^d$, on déduit $a^d - b^d > a^{d-1}$ et $\prod_{d\in D}(a^d - b^d) > \exp((\sum_{d\in D} d - \text{card } D).\log a)$; de même, $a^d - b^d < a^d$ implique $\prod_{d\in D'}(a^d - b^d) < \exp((\sum_{d\in D'} d).\log a)$. On voit donc que

$$C_n(a , b) > \exp(\varphi(n).2^{-\omega(n)+1}(2^{\omega(n)-1} - 1).\log 2) ;$$

or, si l'on pose $n = \prod_{1\leqslant i\leqslant k} q_i^{a_i}$, les facteurs premiers q_i étant rangés dans l'ordre croissant, on a $\varphi(n).2^{-\omega(n)} \geqslant \prod_{1\leqslant i\leqslant k}(q_i - 1)/2$, de sorte qu'on est ramené à prouver l'inégalité $(1 - 2^{1-k}).\prod_{1<i\leqslant k}(q_i - 1) \geqslant q_k - 1$ dont on voit aisément qu'elle est vraie sauf pour $n = 6$.

BIBLIOGRAPHIE

[1] BAKER (A.). - Transcendental number theory. - Cambridge, Cambridge University Press, 1975.

[2] BIRKHOFF (G. D.) and VANDIVER (H. S.). - On the integral divisors of $a^n - b^n$, Annals of Math., Series 2, t. 5, 1904, p. 173-180.

[3] CASSELS (J. W. S.). - An introduction to diophantine approximation. 2nd edition. - Cambridge, Cambridge University Press, 1965.

[4] CASSELS (J. W. S.). - On a class of exponential equations, Arkiv. für Math., t. 4, 1963, p. 231-233.

[5] CATALAN (E.). - Note extraite d'une lettre adressée à l'éditeur, J. reine angew. Math., t. 27, 1844, p. 192.

[6] CHOWLA (S.). - The greastest prime factor of $x^2 + 1$, J. London math. Soc., t. 10, 1935, p. 117-120.

[7] CRAMER (H.). - On the order of magnitude of the difference between consecutive prime numbers, Acta Arithm., Warszawa, t. 2, 1937, p. 23-46.

[8] DESHOUILLERS (J. M.). - Le théorème de Sylvester et Schur (dactylographié).

[9] ERDÖS (P.). - A theorem of Sylvester and Schur, J. London math. Soc., t. 9, 1934, p. 282-288.

[10] ERDÖS (P.). - On consecutive integers, Nieuw Arch. voor Wisk., t. 3, 1955, p. 124-128.

[11] ERDÖS (P.). - On the normal number of prime factors of p - 1 and some related problems concerning Euler ∅-function, Quaterly J. of Math., t. 6, 1935, p. 203-213.

[12] ERDÖS (P.). - On the greatest prime factor of $\prod_{k=1}^{x} f(k)$, J. London math. Soc., t. 27, 1952, p. 379-384.

[13] ERDÖS (P.). - Some problems in number theory, "Computers in number theory", Proceedings of a symposium held at Oxford, 1969, p. 405-414. - London, New York, Academic Press, 1971.

[14] ERDÖS (P.) and SELFRIDGE (J. L.). - Some problems on the prime factors of consecutive integers, II, "Proceedings Washington State University Conference of number theory, Pullman 1971"(à paraître).

[15] ERDÖS (P.) and SHOREY (T. N.). - On the greastest prime factor of $2^P - 1$ for a prime p and other expressions, Acta Arithm., Warszawa (à paraître).

[16] FEL'DMAN (N. I.). - Improved estimate for a linear form of the logarithms of algebraic numbers, Math. of the USSR-Sbornik, t. 6, 1968, p. 393-406 ; [en russe] Mat. Sbornik, N. S., t. 77, 1968, p. 423-436.

[17] GEL'FOND (A. O.). - Transcendental and algebraic numbers. - New York, Dover Publications, 1960.

[18] HALBERSTAM (H.). - On the distribution of additive number theoretic function, II and III., J. London math. Soc., t. 31, 1956, p. 1-11, 14-31.

[19] HALBERSTAM (H.). - Numbers with a large prime factors, Séminaire de Théorie des nombres de l'Université de Bordeaux, 1971/72, exp. 23.

[20] HALL (Marshall Jr.). - The diophantine equation $x^3 - y^2 = k$, "Computers in number theory", Proceedings of a symposium held at Oxford, 1969, p. 173-198. - London, New York, Academic Press, 1971.

[21] HANSON (D.). - On the product of the primes, Canad. math. Bull., t. 15, 1972, p. 33-37.

[22] HARDY (G. H.) and WRIGHT (E. M.). - An introduction to the theory of numbers, 4th edition. - Oxford, Clarendon Press, 1959.

[23] HUXLEY (M. N.). - On the difference between consecutive primes, Inventiones Math., Berlin, t. 15, 1972, p. 164-170.

[24] JUTILA (M.). - On numbers with a large prime factor, Indian J. of Math. (à paraître).

[25] KOTOV (S. V.). - The greatest prime factor of a polynomial, Math. Notes, t. 13, 1973, p. 313-317 ; [en russe], Mat. Zametki, t. 13, 1973, p. 515-522.

[26] LANDAU (E.). - Primzahlen. - New York, Chelsea publishing Company, 1953.

[27] LANGEVIN (M.). - Plus grand facteur premier d'entiers consécutifs, C. R. Acad. Sc. Paris, t. 280, 1975, Série A, p. 1567-1570.

[28] LANGEVIN (M.). - Plus grand facteur premier d'entiers voisins, C. R. Acad. Sc. Paris (à paraître).

[29] LEHMER (D. H.). - On a problem of Störmer, Illinois J. Math., t. 8, 1964, p. 57-79.

[30] MAHLER (K.). - Zur approximation algebraischer Zahlen, I und II., Math. Annalen, t. 107, 1933, p. 691-730, t. 108,1933, p. 37-55.

[31] MAHLER (K.). - Über den grössten Primteiler der Polynome $x^2 \mp 1$, Archiv for Math. og Naturvid, t. 41, 1935, n° 1, 8 p.

[32] MAHLER (K.). - Über den grössten Primteiler spezieller Polynome zweiten Grades, Arch. for Math. og Naturvid., t. 41, 1935, n° 6, 26 p.

[33] MAHLER (K.). - On the greatest prime factor of $ax^m + by^n$, Nieuw Archief voor Wiskunde, 3e série, t. 1, 1953, p. 113-122.

[34] MORDELL (L. J.). - Diophantine Equations. - London, New York, Academic Press, 1969 (Pure and applied Mathematics, Academic Press, 30).

[35] NAGELL (T.). - Über den grössten Primteiler gewisser Polynome dritten Grades, Math. Annalen, t. 114, 1937, p. 284-292.

[36] PERRON (O.). - Die Lehre von den Kettenbruchen, 3te Auflage. Band 1. - Stuttgart, B. G. Teubner, 1954.

[37] POLYA (G.). - Zur arithmetischen Untersuchung der Polynome, Math. Z., t. 1, 1918, p. 143-148.

[38] PRACHAR (K.). - Primzahlverteilung. - Berlin, Springer-Verlag, 1957 (Grundlehren der mathematischen Wissenschaften, 91).

[39] RAMACHANDRA (K.). - Largest prime factor of the product of k-consecutive integers, "Proceedings of the international conference on number theory, Moscou, 1971"(à paraître).

[40] RAMACHANDRA (K.). - A note on numbers with a large prime factor, III., Acta Arithm., Warszawa, t. 19, 1971, p. 49-62.

[41] RAMACHANDRA (K.). - Application of Baker's theory to two problems considered by Erdös and Selfridge, J. Indian math. Soc., t. 37, 1973, p. 25-34.

[42] RAMACHANDRA (K.) and SHOREY (T. N.). - On gaps between numbers with a large prime factor, Acta Arithm., Warszawa, t. 24, 1973, p. 99-111.

[43] RANKIN (R. A.). - The difference between consecutive prime numbers, J. London math. Soc., t. 13, 1938, p. 232-247 ; et Proc. Edinburgh math. Soc., t. 13, 1963, p. 331-332.

[44] SCHINZEL (A.). - On two theorems of Gel'fond and some of their applications, Acta Arithm., Warszawa, t. 13, 1967, p. 177-236.

[45] SCHINZEL (A.). - On primitive prime factors of $a^n - b^n$, Proc. Cambridge phil. Soc., t. 58, 1962, p. 555-562.

[46] SCHMIDT (W.). - Approximation to algebraic numbers. - Genève, l'Enseignement mathématique, 1972 (Monographies de l'Enseignement mathématique, 19).

[47] SCHÖNHAGE (A.). - Eine Bemerkung zur Konstruktion grosser Primzahllücken, Arch. der Math., t. 14, 1963, p. 29-30.

[48] SCHUR (J.). - Einige Sätze über Primzahlen mit Anwendung auf Irreduzibilitätsfragen, Sitz. der Preuss. Akad. Wiss., Phys. Math. Klasse, t. 23, 1929, p. 1-24.

[49] SHOREY (T. N.). - On gaps between numbers with a large prime factor, II., Acta Arithm., Warszawa, t. 25, 1974, p. 365-373.

[50] SHOREY (T. N.). - On linear forms in the logarithms of algebraic numbers, Acta Arithm., Warszawa (à paraître).

[51] SHOREY (T. N.) and TIJDEMAN (R.). - On the greatest prime factor of polynomials at integer points, Acta Arithm., Warszawa (à paraître).

[52] SIEGEL (C. L.). - Approximation algebraischen Zahlen, Math. Z., t. 10, 1921, p. 173-213.

[53] SIEGEL (C. L.). - The integer solutions of the equation $y^2=ax^n+bx^{n-1}+\ldots+k$, (extrait d'une lettre à L. J. Mordell), J. London math. Soc., t. 1, 1926, p. 66-68.

[54] SPRINDŽUK (V. G.). - An improvement of the estimate of rational approximations to algebraic numbers, Dokl. Akad. Nauk Belorusskoj SSR, t. 15, 1971, p. 101-104.

[55] SPRINDŽUK (V. G.). - Diviseurs sans facteurs carrés des polynômes et nombre de classes des corps de nombres algébriques [en russe], Acta Arithm., Warszawa, t. 24, 1973, p. 143-149.

[56] STARK (H. M.). - Effective estimates of solutions of some diophantine equations, Acta Arithm., Warszawa, t. 24, 1973, p. 251-259.

[57] STEWART (C. L.). - The greatest prime factor of $a^n - b^n$, Acta Arithm., Warszawa, (à paraître).

[58] STØRMER (C.). - Quelques théorèmes sur l'équation de Pell $x^2-Dy^2=\pm 1$ et leurs applications, Christiana Videnskabsselskabs Skrifter, Mat. Naturv. Kl., 1897, n° 2, 48 p.

[59] SYLVESTER (J. J.). - On arithmetical series, Messenger of Math., t. 21, 1892, p. 1-19, 87-120.

[60] TIJDEMAN (R.). - Old and new in number theory, Nieuw Arch. voor Wiskunde, 3e série, t. 20, 1972, p. 20-30.

[61] TIJDEMAN (R.). - On integers with many small prime factors, Comp. Math., Groningen, t. 26, 1973, p. 319-330.

[62] TIJDEMAN (R.). - On the maximal distance between integers composed of small primes, Comp. Math., Groningen, t. 28, 1974, p. 159-162.

[63] TIJDEMAN (R.) and MEIJER (H. G.). - On integers generated by a finite number of fixed primes, Comp. Math., Groningen, t. 29, 1974, p. 273-286.

[64] TIJDEMAN (R.). - On the equation of Catalan, Acta Arithm., Warszawa (à paraître).

[65] TUCKERMAN (B.). - The 24th Mersenne prime, Notices Amer. math. Soc., t. 18, 1971, p. 608.

[66] VAN DER POORTEN (A.). - A p-adic analogue of an inequality of Baker for linear forms in the logarithms of algebraic numbers, Austral. J. of Math (à paraître).

[67] WALDSCHMIDT (M.). - Minorations effectives de formes linéaires de logarithmes, Séminaire Delange-Pisot-Poitou : Groupe d'étude de théorie des nombres, 15e année, 1973/74, n° G3, 8 p.

[68] ZSIGMONDY (K.). - Zur Theorie der Potenzreste, Monatsh. Math., t. 3, 1892, p. 265-284.

(Texte reçu le 3 septembre 1975)

Michel LANGEVIN
Ecole Normale Supérieure de Saint-Cloud
2 avenue du Palais
92211 SAINT-CLOUD