Séminaire Delange-Pisot-Poitou. Théorie des nombres

Michel Langevin

Facteurs premiers d'entiers en progression arithmétique

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 19, n° 1 (1977-1978), exp. n° 4, p. 1-7

<http://www.numdam.org/item?id=SDPP_1977-1978__19_1_A3_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
19e année, 1977/78, n° 4, 7 p.

24 octobre 1977

FACTEURS PREMIERS D'ENTIERS EN PROGRESSION ARITHMÉTIQUE

par Michel LANGEVIN

Résumé. - L'application d'une forme détaillée d'un minorant pour les formes linéaires de logarithmes permet d'obtenir (avec améliorations) simultanément toutes les conséquences antérieurement établies de ces travaux sur les facteurs premiers d'entiers consécutifs. De plus, des arguments arithmétiques nouveaux permettent de généraliser ce résultat aux entiers consécutifs d'une progression arithmétique de raison > 1 .

Historique et résultats. - On désigne par P la fonction plus grand facteur premier. Autrement dit, en réservant la lettre p aux nombres premiers, on pose, pour tout entier n , $P(n) = \sup_{p|n} p$.

Une application simple des résultats de BAKER sur les minorations des formes linéaires de logarithmes est la suivante

(A) Pour tout entier $a \neq 0$,

$$\liminf_{n\to\infty} P(n(n+a))(\log\log n)^{-1} > 0 .$$

Joints à des arguments arithmétiques et combinatoires, les principes de la démonstration de (A) ont permis à trois mathématiciens K. RAMACHANDRA, T. N. SHOREY, R. TIJDEMAN d'obtenir des résultats nouveaux sur les facteurs premiers d'entiers consécutifs. Dans ce domaine de la théorie des nombres, ouvert par un théorème de Sylvester

$$P((n+1)(n+2)\ldots(n+k)) > \inf(n , k) ,$$

n'étaient acquis, il y a dix ans, que des renseignements de démonstrations élémentaires.

Les publications de ces auteurs se sont succédées à un rythme rapide entre 1970 et 1974 jusque survienne une stabilisation. Les meilleurs résultats obtenus concernent le nombre

$$P(n , k) = P((n+1)(n+2)\ldots(n+k))$$

et le problème de GRIMM (cf. [2]): Caractériser l'ensemble G des couples (n , k) tels qu'existe une injection f de l'ensemble $(n+1 , n+2 , \ldots , n+k)$ dans celui des nombres premiers pour laquelle $f(n+1)$ divise $n+1$, ... , $f(n+k)$ divise $n+k$ (GRIMM conjecture que le couple (n , k) appartient à G si aucun nombre premier ne figure parmi $n+1 , n+2 , \ldots , n+k$). Une condition nécessaire pour qu'un couple (n , k) appartienne à G est évidemment que le nombre des entiers $(n+i)$ vérifiant $P(n+i) \leqslant k$ soit au plus égal au nombre des entiers premiers inférieurs ou égaux à k .

Avant d'énoncer ces meilleurs résultats, quelques notations

$\pi(n) = \sum_{p \leq n} 1$,

$\omega(n) = \sum_{p \mid n} 1$,

$\log \log = \log_2$,

$\log \log \log = \log_3$,

C_1 , C_2 , ... désignent des constantes > 0 effectivement calculables. L'inégalité (immédiate sur les définitions)

$$\omega(n) \leqslant \pi(P(n)) \tag{1}$$

jouera un role important dans la suite.

THÉORÈME 1 (RAMACHANDRA, SHOREY [9], [12]). - Il existe une constante $C_1 > 0$, effectivement calculable, telle que, pour tout couple (n , k) vérifiant $n \geqslant \exp((\log k)^{5/4})$, $k \geqslant 2$ on ait

$$P(n , k) > C_1 \, k \log k \log_2 k (\log_3 k)^{-1} . \tag{2}$$

THÉORÈME 2 (SHOREY, TIJDEMAN [14]). - Soit B un réel > 0 , il existe un réel $C_2 > 0$, effectivement calculable en fonction de B , tel que, pour tout couple (n , k) vérifiant

$$n \geqslant \exp \exp(\log k)^B , \quad k \geqslant 2 ,$$

on ait

$$P(n , k) > C_2 \, k(\log k + \log_3 n)\log_2 n(\log_3 n)^{-1} . \tag{3}$$

Remarque. - Dans [14], le théorème 2 est un corollaire d'un résultat plus général. Pour une démonstration directe, voir [4].

THÉORÈME 3 (RAMACHANDRA, SHOREY, TIJDEMAN [7]) (voir aussi [6]). - Il existe une constante $C_3 > 0$, effectivement calculable, telle que tout couple (n , k) vérifiant

$$n \geqslant \exp(C_3 \, k^{1/3} \log k)$$

appartienne à G .

THÉORÈME 4 (RAMACHANDRA, SHOREY, TIJDEMAN [8]). - Il existe une constante $C_4 > 0$, effectivement calculable, telle que pour tout couple (n , k) vérifiant

$$n \geqslant \exp(C_4(\log k)^2) ,$$

le nombre des entiers i pour lesquels $P(n + i) \leqslant k$ soit au plus égal à $\pi(k)$.

le but de cet article est de montrer un théorème global admettant les théorèmes 1 à 4 pour corollaires. De plus, ce théorème généralise les résultats antérieurs aux entiers consécutifs d'une progression arithmétique.

La démonstration des théorèmes 1 à 4 a exigé la mise au point de variantes (dues principalement à SHOREY, cf. [11], [12], [13]) des énoncés de BAKER et notamment

l'étude des formes linéaires de logarithmes $\sum_i b_i \log a_i$, où les a_i sont des rationnels voisins de 1. Bien qu'on pourrait n'utiliser que ces résultats, on fera appel à un nouveau type d'énoncé, englobant les précédents, dû à M. WALDSCHMIDT. Pour ce qui suit, une forme affaiblie de ce théorème conviendra. A cela, il y a deux raisons :

- déduire un théorème global entièrement explicité d'un énoncé de même nature sur les formes linéaires de logarithmes est facile, et
- un théorème global, même non entièrement explicité, contient les théorèmes 1 à 4 comme corollaires.

On écrit d'abord cet unique théorème sur les formes linéaires de logarithmes dont on fera usage. Puis, on montrera comment en déduire (A), ce type de calcul étant la base de la démonstration du théorème global.

THÉORÈME 5 (WALDSCHMIDT [15]). - *Soient* $a_1 , a_2 , \ldots , a_m$ *des rationnels* > 0 *de hauteurs majorées respectivement par* $A_1 , A_2 , \ldots , A_m$ (*avec* $A_i \geq e$, $1 \leq i \leq m$), $b_1 , b_2 , \ldots , b_m$ *des entiers majorés en valeur absolue par* B (*avec* $B \geq e$) *tels que* $\Lambda = |\sum_{1\leq i\leq m} b_i \log a_i| \neq 0$. *On pose*

$$\Omega = \prod_{1\leq i\leq m} \log A_i , \quad \Omega' = \prod_{1\leq i<m} \log A_i ,$$

E *désigne un réel satisfaisant à*

$$e \leq E \leq \inf(B\Omega , e \log A_1 (\log a_1)^{-1} , \ldots , e \log A_m (\log a_m)^{-1}) .$$

Alors :

$$\Lambda > \exp(- C_0 m^{\gamma_0 m} \Omega \log(B\Omega)\log(E\Omega')(\log E)^{-(m+1)}) ,$$

où C_0 *et* γ_0 *désignent des constantes absolues explicitables.*

Dans l'énoncé précédent, on désigne par hauteur d'un rationnel positif, écrit sous forme irréductible, la borne supérieure du numérateur et du dénominateur.

Démonstration de (A). - Soient n et a deux entiers. On peut supposer $a > 0$ et $n > a^2$, ce qui entraîne $P(n(n + a)) \geq 3 > e$. On forme le logarithme du rationnel $n^{-1}(n + a)$ écrit comme produit de puissances de nombres premiers

$$\log(n^{-1}(n + a)) = \sum_{1\leq i\leq j} b_i \log p_i \quad \text{avec} \quad 2 \leq j \leq \omega(n(n + a)) .$$

Les entiers b_i sont majorés par $\log(n + a)(\log 2)^{-1}$, donc, pour $n \geq 3$, par $2 \log n$. On applique alors le théorème 5 avec $m = j$, $A_1 = A_2 = \ldots = A_m = P(n(n+a))$, $B = 2 \log n$, $E = e$. En majorant $\log(n^{-1}(n + a))$ par $n^{-1/2}$, on obtient

$$(4) \quad \tfrac{1}{2} \log n < C_0 j^{\gamma_0 j} (\log P(n(n + a)))^j \times \log(2 \log n(\log P(n(n + a)))^j)\log(e(\log P(n(n + a)))^j) .$$

Or, la quantité $\log(2 \log n(\log P(n(n + a)))^j)\log(e(\log P(n(n + a)))^j)$ peut être majorée par $2.10^6 \log_2 n(j \log_2 P(n(n + a)))^2$ comme le prouve le lemme facile suivant.

LEMME 1. - *Soient* $x_1 , x_2 , \ldots , x_m$ *des réels minorés par* $X \geq 0$, *alors*

$$x_1 + x_2 + \dots + x_m \leqslant m.X^{1-m}\, x_1\, x_2 \dots x_m .$$

De (4), se déduit alors l'inégalité

$$\log_2 n < \gamma_0\, j \log j + j \log_2 P(n(n+a)) + \log_3 n + 2 \log j + 2 \log_3 P(n(n+a)) + C_5 , \tag{5}$$

où C_5 est une constante convenable fonction de C_0 .
Dans le second membre de (5), j peut être majoré ainsi, à l'aide des inégalités

$$j \leqslant \omega(n(n+a)) \leqslant \pi(P(n(n+a))) \quad \text{(cf. (1))} \tag{6}$$

$$\pi(P(n(n+a))) \leqslant (1 + o(1))P(n(n+a))(\log P(n(n+a)))^{-1} \tag{7}$$

(théorème fondamental des nombres premiers), et il vient enfin, pour n infini,

$$\liminf P(n(n+a))(\log_2 n)^{-1} \geqslant \gamma_0^{-1} ,$$

c'est-à-dire l'inégalité (A) cherché.

On énonce maintenant le théorème global dont on déduira les théorèmes 1 à 4. Si X désigne un ensemble fini d'entiers, on désigne par $P(X)$ (resp. $\omega(X)$, ...) l'entier $P(\prod_{x\in X} x)$ resp. $\omega(\prod_{x\in X} x)$, ...). Quand $X = (n + a , n + 2a , \dots , n + ka)$, on écrit $P(n , k , a)$ (resp. $\omega(n , k , a)$) pour $P(X)$ (resp. $\omega(X)$). Dans toute la suite, on suppose (sans le répéter toujours) n et a premiers entre eux, $k \geqslant 2$, $n + a > k$.

THÉORÈME GLOBAL. - <u>Existent deux constantes effectivement calculables</u> C <u>et</u> γ <u>telle que, pour tout système</u> (n , k , a , ξ , j) (<u>où</u> n, k, a <u>sont des entiers avec</u> $(n , a) = 1$, $1 \leqslant a \leqslant n^{1/2}$, j <u>et</u> ξ <u>des réels avec</u> $j \geqslant 1$, $2 \leqslant \xi \leqslant k$) <u>vérifiant</u>

$$\log n/\log k > C j^{\gamma j} \inf(k^{1/3} , k/\xi) , \tag{8}$$

<u>aucune partie</u> X <u>de l'ensemble des entiers en progression arithmétique</u> $n + a$, $n + 2a$, ... , $n + ka$ <u>ne satisfait simultanément à :</u>

$$\operatorname{card} X \geqslant \inf(k , \sup(\xi , k^{2(j-1)})) \tag{9}$$

$$\pi(P(X)) \leqslant j.k \tag{10}$$

$$\omega(X) \leqslant j \operatorname{card} X \tag{11}$$

COROLLAIRE 1. - <u>Soit</u> ε <u>un réel positif. Pour tout triplet</u> (n , k , a) <u>d'entiers (avec</u> $(n , a) = 1$, $n^{1/2} \geqslant a$) <u>vérifiant</u> $n > k^{r(\varepsilon)}$ <u>où</u>

$$r(\varepsilon) = \sup(\exp((1 + \varepsilon^{-1}\gamma)\log C) , \exp\exp(\gamma + \varepsilon)^{-1}) ,$$

<u>on a :</u>

$$\pi(P(n , k , a)) > (\gamma + \varepsilon)^{-1} k \log(\log n/\log k)(\log_2(\log n/\log k))^{-1} . \tag{12}$$

(Dans cet énoncé, C et γ désignent les constantes du théorème global.)

<u>Démonstration du corollaire</u> 1. - On choisit

$$\xi = k \ , \quad j = (\gamma + \varepsilon)^{-1} \log(\log n/\log k)(\log_2(\log n/\log k))^{-1} \ ;$$

L'inégalité

$$\log n/\log k > \exp \exp(\gamma + \varepsilon)^{-1}$$

implique

$$\log j = \log_2(\log n/\log k) - (\log_3(\log n/\log k) + \log(\gamma + \varepsilon)) \leqslant \log_2(\log n/\log k) \ .$$

On en déduit que l'expression $j^{\gamma j} = \exp(\gamma j \log j)$, où l'on remplace j par sa valeur et où l'on majore $\log j$ comme ci-dessus, est inférieure ou égale à $(\log n/\log k)^{\gamma/(\gamma+\varepsilon)}$. Par suite,

$$Cj^{\gamma j} \inf(k^{1/3} \ , \ k/\xi) \leqslant C(\log n/\log k)^{\gamma/(\gamma+\varepsilon)}$$
$$\leqslant r(\varepsilon)^{\varepsilon/(\gamma+\varepsilon)}(\log n/\log k)^{\gamma/(\gamma+\varepsilon)} < (\log n/\log k) \ .$$

Le théorème global montre alors que, pour $X = (n+ a \ , \ n + 2a \ , \ \ldots \ , \ n + ka)$, l'une des inégalités (10) ou (11) est fausse, ce qui, joint à (1), prouve l'inégalité (12) annoncée.

L'équivalence $\pi(x) \sim x(\log x)^{-1}$ (et, plus précisément, l'inégalité (cf. [10]) $x > \pi(x).\log \pi(x)$) permet de déduire du corollaire 1 une minoration de $P(n \ , \ k \ , \ a)$. Quand $a = 1$, on retrouve les théorèmes 1 et 2. En effet, si $\log n/\log k > (\log k)^{1/4}$. on a

$$\pi(P(n \ , \ k \ , \ a)) > (4(\gamma + \varepsilon))^{-1} \ k \log_2 k(\log_3 k)^{-1} \ ,$$

d'où (2), et si $\log k < (\log_2 n)^{1/B}$,

$$\pi(P(n \ , \ k \ , \ a)) > (\gamma + \varepsilon)^{-1} \ k(\log_2 n - B^{-1} \log_3 n)(\log_3 n)^{-1} \ ,$$

d'où (3).

En fait, ce dernier calcul montre que le théorème 2 est vrai sous l'hypothèse plus faible $n > \exp(\log k)^B$ (avec $B > 1$).

Le corollaire 1 montre en particulier l'existence d'une constante r_0 telle que l'inégalité $P(n \ , \ k \ , \ a) \geqslant p'_k$, où p'_k désigne le k-ième nombre premier, soit réalisé lorsque n est supérieur à k^{r_0} (et, en outre, $(n \ , \ a) = 1$, $a \leqslant n^{1/2}$) . Dans le cas où a est égal à 1 , un meilleur résultat est connu, celui de JUTILA (cf. [3]), grâce à une toute autre technique (crible). On rappelle qu'une conséquence de la conjecture de GRIMM généralisée (cf. [5]) est

$$P(n \ , \ k \ , \ a) \geqslant \inf(n + a \ , \ p'_k) \ .$$

COROLLAIRE 2. - Pour tout triplet $(n \ , \ k \ , \ a)$ (avec $(n \ , \ a) = 1$, $a \leqslant n^{1/2}$) vérifiant $n > \exp(Ck^{1/3} \log k)$ (resp. $n > \exp(C(\log k)^2)$), où C désigne la constante du théorème global, on peut trouver k nombres premiers distincts divisant respectivement $n + a \ , \ n + 2a \ , \ \ldots \ , \ n + ka$ (resp. le nombre des entiers i pour lesquels $P(n + ia) \leqslant k$ est inférieur ou égal à $\pi(k)$).

Démonstration du corollaire 2. - On choisit $j = 1$, $\xi = 2$. L'inégalité (8) de-

vient

$$\log n/\log k > C.k^{1/3} .$$

Si cette dernière est réalisée, toute partie X (et même celles réduites à un élément) de $(n + a , n + 2a , \ldots , n + ka)$ pour laquelle $P(X) \leqslant k$ vérifie $\omega(X) \geqslant \text{card } X$. Le lemme des mariages (cf. [1], chap. 3, § 4, Exerc. 6(b)) montre alors l'existence d'une injection f de l'ensemble des entiers $n + ia$ avec $P(n + ia) \leqslant k$ dans celui des nombres premiers pour laquelle $f(n + ia)$ divise $n + ia$ $(i = 1, 2, \ldots, k)$. En prolongeant f par P , on obtient la première partie du corollaire. Pour prouver la seconde, on choisit $j = 1$, $\xi = \pi(k)$. On peut supposer $k \geqslant 17$ puisqu'on sait (cf. [5]) que la double conclusion du corollaire 2 est vraie, sauf peut-être lorsque l'un des entiers $n + ia$ $(1 \leqslant i \leqslant k)$ divise le plus petit commun multiple de $1, 2, \ldots, 15$ (i. e. 360360) (on peut d'ailleurs toujours écarter ce cas en augmentant au besoin C). L'inégalité $\log n > C(\log k)^2$ implique alors (8) puisque $\log k > k(\pi(k))^{-1}$ (pour $k \geqslant 17$, cf. [10]). Soit Y l'ensemble des entiers $n + ia$ vérifiant $P(n + ia) \leqslant k$ et appliquons le théorème global. L'inégalité (10) est vérifiée. Ou bien $\text{card } Y \leqslant \xi = \pi(k)$ et le résultat est acquis, ou bien $\text{card } Y > \xi$ (ce qui signifie que (9) est vérifiée), et donc $\omega(Y) > j\xi = \pi(k)$, d'où (d'après (1)) $\pi(P(Y)) > \pi(k)$, en contradiction avec la définition de Y .

Comme précédemment, il est clair que les théorèmes 3 et 4 sont des cas particuliers du corollaire 2.

Remarque. - Les inégalités montrant l'existence de C et γ sont liées (par ce qui suit, cf. démonstration, et parce qu'il en est de même des constantes C_0 et γ_0 du théorème 5). Suivant l'application recherchée, on choisira un couple (C , γ) avec C ou γ minimum.

On peut raffiner le théorème global. Ainsi, on peut remplacer l'hypothèse $a \leqslant n^{\frac{1}{2}}$ par $a \leqslant n^t$, où t est un réel strictement inférieur à 1, ou bien remplacer le coefficient 2 de l'inégalité (9) par un réel $t' > 1$, ou encore substituer dans (10), au majorant $j.k$, $j.k^{t''}$ (t'' réel $\geqslant 1$), voire une fonction de la forme $\exp(\log n)^{\theta}$ $(\theta < 1)$. Il convient évidemment alors de modifier convenablement les constantes C et γ .

Tout comme on a pu le faire pour le théorème 2, le théorème 4 peut être amélioré. Soit j_0 un réel tel que $1 \leqslant j_0 < 3/2$. Pour k assez grand, le choix $\xi = \pi(k)j_0^{-1}$, $j = j_0$ entraîne

$$\inf(k , \sup(\xi , k^{2(j-1)})) = \pi(k)j_0^{-1} .$$

Le théorème global montre alors que, pour de telles valeurs de k et pour n vérifiant $n > \exp(Cj_0^{\gamma j_0+1}(\log k)^2)$, on a $\text{card } Y \leqslant \pi(k)j_0^{-1}$ (Y conservant la même signification que dans la démonstration de la seconde partie du corollaire 2). Plus généralement, pour tout réel $\lambda > 1$, on peut montrer que $\text{card } Y \leqslant \pi(k)/\lambda$ pourvu que $n \geqslant \exp(C(\lambda)(\log k)^2)$.

BIBLIOGRAPHIE

[1] BOURBAKI (N.). - Théorie des ensembles. Nouvelle édition. - Paris, Hermann, 1970 (Elements de Mathématique).

[2] GRIMM (C. A.). - A conjecture on consecutive composite numbers, Amer. math. Monthly, t. 76, 1969, p. 1126-1128.

[3] JUTILA (M.). - On numbers with a large prime factor, II, J. Indian math. Soc., t. 38, 1974, p. 125-130.

[4] LANGEVIN (M.). - Quelques applications de nouveaux résultats de Van der Poorten, Séminaire Delange-Pisot-Poitou : Théorie des nombres, 17e année, 1975/76, n° G12, 11 p.

[5] LANGEVIN (M.). - Plus grand facteur premier d'entiers en progression arithmétique, Séminaire Delange-Pisot-Poitou : Théorie des nombres, 18e année, 1976/77, n° 3, 7 p.

[6] MIGNOTTE (M.). - Sur les facteurs premiers distincts d'entiers consécutifs, Séminaire Delange-Pisot-Poitou : Théorie des nombres, 16e année, 1974/75, n° G5, 6 p.

[7] RAMACHANDRA (K.), SHOREY (T. N.) and TIJDEMAN (R.). - On Grimm's problem relating to factorisation of a block of consecutive integers, I, J. für die reine und angew. Math., t. 273, 1975, p. 109-124.

[8] RAMACHANDRA (K.), SHOREY (T. N.) and TIJDEMAN (R.). - On Grimm's problem relating to factorisation of a block of consecutive integers, II, J. für die reine und angew. Math., t. 288, 1976, p. 192-201.

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

[10] ROSSER (B.) and SCHOENFELD (L.). - Approximate formulas for some functions of prime numbers, Illinois J. Math., t. 6, 1962, p. 64-94.

[11] SHOREY (T. N.). - Linear forms in the logarithms of algebraic numbers with small coefficients, II, J. Indian math. Soc., t. 38, 1974, p. 285-292.

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

[13] SHOREY (T. N.). - On linear forms in the logarithms of algebraic numbers, Acta Arithm., Warszawa, t. 25, 1974, p. 27-42.

[14] SHOREY (T. N.) and TIJDEMAN (R.). - On the greatest prime factors of polynomials at integer points, Compositio Math., Groningen, t. 33, 1976, p. 187-195.

[15] WALDSCHMIDT (M.). - A lower bound for linear forms in logarithms (à paraître).

(Texte reçu le 20 octobre 1977)

Michel LANGEVIN
Ecole normale supérieure
2 avenue du Palais
92210 SAINT CLOUD