Séminaire Delange-Pisot-Poitou. Théorie des nombres

Michel Langevin

Plus grand facteur premier d'entiers en progression arithmétique

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 18, n° 1 (1976-1977), exp. n° 3, p. 1-7

<http://www.numdam.org/item?id=SDPP_1976-1977__18_1_A3_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
18e année, 1976/77, n° 3, 7 p.

18 octobre 1976

PLUS GRAND FACTEUR PREMIER D'ENTIERS EN PROGRESSION ARITHMÉTIQUE

par Michel LANGEVIN

I. Historique et résultats.

1. - En 1969, GRIMM fait la conjecture suivante [3] :

(G) : Etant donnés k entiers consécutifs non premiers $n + 1$, $n + 2$, ... , $n + k$, il existe une injection f de cet ensemble à valeurs dans celui des nombres premiers telle que $f(n + i)$ divise $n + i$ pour $i = 1 , 2 , \dots , k$.

Autrement dit, si $n_1 , n_2 , \dots , n_\ell$ forment une suite croissante d'entiers telle que le nombre de facteurs premiers du produit $n_1 n_2 \dots n_\ell$ soit inférieur à ℓ, alors il existe un nombre premier dans l'intervalle (n_1 , n_ℓ) (appliquer le lemme des mariages).

La conjecture (G) a d'intéressantes conséquences ; ainsi, ERDÖS et SELFRIDGE en ont déduit l'existence d'un nombre premier dans tout intervalle $(n^2 , (n + 1)^2)$.

(G) peut être étendue aux entiers consécutifs d'une progression arithmétique sous la forme

(GG) : Etant donnés k entiers non premiers $n + a$, $n + 2a$, ... , $n + ka$ (avec $n > 0$, $(n , a) = 1$), il existe une injection f de cet ensemble à valeurs dans celui des nombres premiers telle que $f(n + ia)$ divise $n + ia$ pour $i = 1 , 2 , \dots , k$.

De même, d'intéressantes conséquences, par exemple vers la conjecture de Landau sur l'existence d'un nombre premier congru à n modulo a dans l'intervalle $((ma)^2 , ((m + 1)a)^2)$.

Un procédé pratique de vérification numérique de (GG) pour k inférieur à une valeur donnée est fourni par le théorème suivant :

THÉORÈME 1. - La conclusion de (GG) est vraie lorsqu'aucun des entiers $(n + ia)$ $(i = 1 , 2 , \dots , k)$ ne divise le plus petit commun multiple (p. p. c. m.) de $1 , 2 , \dots , k - 1$.

En particulier, (GG) est établie sous l'hypothèse

$$n + a > \text{p. p. c. m. } (1 , 2 , \dots , k - 1) = \exp(\Psi(k - 1)) ,$$

où Ψ désigne l'habituelle fonction de ČEBIČEV, équivalente à k d'après le théorème fondamental des nombres premiers.

2. - Soit $P(n , k , a)$ le plus grand facteur premier de $(n + a)(n + 2a) \ldots (n + ka)$; on suppose dans tout ce qui suit $n > 0$, $(n , a) = 1$, $k \geqslant 2$; $P(n , k , 1)$ sera abrégé en $P(n , k)$. De (GG), on déduit aisément l'inégalité conjecturale :

$$P(n , k , a) \geqslant \inf(n + a , p_k) ,$$

où p_k désigne le k-ième nombre premier. En particulier,

$$P(n , k) \geqslant \inf(n + 1 , p_k) .$$

Cette dernière inégalité n'est pas encore établie, mais l'étude de la fonction $P(n , k)$ a été entreprise depuis bientôt un siècle.

En 1892, SYLVESTER prouve l'inégalité, pour $n \geqslant k$, $P(n , k) > k$ (i. e. $P(n , k) \geqslant \inf((n + 1) , (k + 1)))$, résultat retrouvé et étendu aux progressions arithmétiques de raison 2 par SCHUR, en 1929. Cinq ans plus tard, sans introduire d'idée nouvelle, ERDÖS donne une démonstration plus rapide et plus efficace ($P(n , k) > 1{,}1\, k$ avec $n \geqslant k$) comme le remarque MOSER en 1963. Cette démonstration est également à la base de l'assez récente amélioration de HANSON (1973) : $P(n , k) > 1{,}5\, k$ avec $n \geqslant k$ et $(n , k) \neq (2 , 2) , (7 , 2) , (5 , 5)$ (Cf. [13], [1], [4]).

Le meilleur résultat qu'on puisse espérer avec la condition $n \geqslant k$ est clairement :

$$\lim_{k \infty} \inf_{n \geqslant k} P(n , k)/k = 2 .$$

Ce sera une conséquence du théorème suivant.

THÉORÈME 2. - Si $(n , k) \neq (7 , 2) , (7 , 3)$,

$$P(n , k) \geqslant \inf(n + 1 , 13k/6) .$$

La démonstration du théorème 2 est complètement élémentaire, au même titre que celles des résultats antérieurs, de SYLVESTER à HANSON. De plus, cette démonstration est assez brève, mais, au prix d'un sensible allongement des calculs, on peut prouver, toujours élémentairement, le théorème suivant.

THÉORÈME 2'. - Si $k \geqslant 4$ et $(n , k) \neq (23 , 5)$,

$$P(n , k) \geqslant \inf(n + 1 , 19k/7) .$$

Plus précisément, en ce qui concerne les petites valeurs de k , on peut prouver élémentairement que les inégalités suivantes sont vraies pour n assez grand (les exceptions sont aussi faciles à expliciter) :

$$P(n , 2) \geqslant 7 , \quad P(n , 3) \geqslant 11 , \quad P(n , 4) \geqslant 13 , \quad P(n , 5) \geqslant 17 ,$$

$$P(n , 6) \geqslant 19 , \quad P(n , 8) \geqslant 23 , \quad P(n , 9) \geqslant 29 , \quad \ldots$$

En adoptant la forme d'énoncé des auteurs antérieurs, on déduit du théorème 2, en n'utilisant que les (petits) moyens nécessaires à sa démonstration, le corollaire

suivant.

COROLLAIRE 1. - Si $n \geqslant k$ et $(n , k) \neq (2 , 2) , (7 , 2) , (5 , 5)$,

$$P(n , k) > 1{,}6\, k .$$

Si l'on utilise le théorème fondamental des nombres premiers, on peut remplacer le coefficient 1,6 par un quelconque réel inférieur à 2 (en modifiant convenablement l'ensemble des exceptions, bien sûr) ; par exemple, on peut montrer le nouveau corollaire.

COROLLAIRE 2. - Si $n \geqslant k > 659504$,

$$P(n , k) > 1{,}995169\, k .$$

3. - Dans le travail de SYLVESTER est implicitement prouvée l'existence, pour tout réel $c > 0$, d'un réel b et d'un entier K tels que les inégalités $K < bk < n$ assurent $P(n , k) > ck$ (Cf. [8]). D'autre part, du théorème fondamental des nombres premiers (prouvé vers la même époque), on déduit aisément que les inégalités $ck \leqslant n < bk$ impliquent $P(n , k) \geqslant ck$ pour k assez grand (observer que $\pi(n + k) \geqslant \pi((1 + b^{-1})n) > \pi(n)$ pour n , donc pour k , assez grand). Or, toujours vers la même époque, STØRMER montrait que $P(n , 2)$ tend vers l'infini avec n ; il en résulte donc que l'ensemble des couples (n , k) avec $n \geqslant ck$ et $P(n , k) < ck$ est fini. Autrement dit, le rapprochement des trois précédents résultats permet d'établir que l'inégalité $P(n , k) \geqslant \inf(n + 1 , ck)$ est vraie à un nombre fini d'exceptions près, et ce, pour tout réel c .

Lorsque c est petit, des formes très affaiblies des deux derniers résultats suffisent pour expliciter l'ensemble des exceptions ; ce travail a été mené à bien, lorsque $c = 2$, par FAULKNER (Cf. [2]), mais le théorème 1 montre que, pour une telle valeur de c , il n'était pas même nécessaire d'y avoir recours. En fait, avec les moyens utilisés par FAULKNER, on peut montrer le théorème ci-après.

THÉORÈME 3. - Si $(n , k) \neq (23 , 5)$ et $k \geqslant 4$,

$$P(n , k) \leqslant \inf(n , 3k) .$$

De plus, la démonstration du théorème 3 montre comment déterminer, pour tout réel c , l'ensemble des exceptions (i. e. les couples (n , k) avec

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

ce n'est qu'affaire de moyens numériques (le cas $c = 3$ correspond à un problème résoluble par les tables numériques existantes) ; en effet, pour les grandes valeurs de k , le coefficient 3 peut facilement être amélioré :

THÉORÈME 3'. - Si $k \geqslant 10^4$ (resp. 10^6),

$$P(n , k) > \inf(n , 6k) \quad (\text{resp. } \inf(n , 7k)).$$

THÉORÈME 3". - $P(n , k) > \inf(n , k \log\log k)$.

4. - On est encore assez loin de l'inégalité conjecturée $P(n,k) \geqslant \inf(n+1, p_k)$, cependant, on peut montrer que ce résultat est vrai pour k assez grand. Quand $n + 1 \leqslant p_k$, cela est une conséquence de l'inégalité $p_{m+1} - p_m \leqslant m$ (pour tout entier m) qu'on peut déduire des travaux numériques de ROSSER et SCHOENFELD. Quand $p_k \leqslant n < k^{3/2}$, l'inégalité $P(n , k) \geqslant n + 1$ est réalisée pour k assez grand d'après le théorème de Hoheisel-Ingham- ... -Huxley ($p_{m+1} - p_m = o(p_m^{2/3})$; actuellement, $p_{m+1} - p_m = o(p_m^h)$ avec $h > 7/12$) . Quand $k^{3/2} \leqslant n < 3^k$, le résultat est acquis grâce à un résultat dû à JUTILA et SHOREY, établissant que

$$P(n , k) \gg k \log k \log\log k \, (\log\log\log k)^{-1} ;$$

enfin, quand $n \geqslant 3^k$, le résultat est vrai pour toute valeur de k d'après le théorème 1.

D'autres résultats, relatifs à (G) ou à la fonction $P(n , k)$, ont été récemment obtenus grâce à la méthode de Baker par RAMACHANDRA, SHOREY, TIJDEMAN ; nous renvoyons pour toutes précisions aux exposés [11] et [7] du groupe d'étude.

5. - On étudie maintenant comment généraliser les précédents résultats aux entiers consécutifs d'une progression arithmétique. Une telle généralisation pour le théorème fondamental des nombres premiers existe, comme il est bien connu, mais il ne peut être recherché un analogue pour les travaux numériques de ROSSER et SCHOENFELD valable uniformément en la raison a . De même, on voit, grâce à la méthode de Baker que $\lim_{n\infty} P(n(n + a)) = \infty$ quand a est fixé ou, du moins, petit devant n ($\lim_{n\infty} \inf P(n(n + a))/\log\log n \geqslant 1/6$ si $a \leqslant n^t$ avec $t < 1$, Cf. [9]) . Enfin, on montre dans [10], dont cet exposé donne les principaux résultats, que le théorème de Sylvester du § 3 se généralise entièrement et uniformément en a .

Ceux des résultats des paragraphes précédents dont la démonstration n'exige pas l'emploi de tables numériques peuvent donc être généralisés. Par exemple, le théorème de Sylvester, établissant que $P(n , k) > k$ (quand $n \geqslant k$) dont la démonstration est d'autant plus rapide qu'on dispose d'une bonne majoration de $\pi(x)$ ou de $\psi(x)$ (Cf. [8]), mais qui peut être prouvé sans cela, peut être étendu ainsi :

THÉORÈME 4. - Soient k entiers $n + a$, $n + 2a$, ... , $n + ka$ ($n > 0$, $(n , a) = 1$) supérieurs à k , il existe un nombre premier supérieur à k divisant l'un d'entre eux.

Ce théorème est en fait la conséquence de l'inégalité suivante, où $I_A(k)$ désigne la borne inférieure de $\pi(P(n , k , a))\log k/k$ quand $n + a > k$, $(n , a) = 1$, $a \geqslant A$.

THÉORÈME 5. - $\lim_{k\infty} \inf I_A(k) \geqslant \log(A + 1)$.

Signalons d'autre part que tous les résultats récents obtenus sur ces sujets grâce à la méthode de Baker (non décrits ici, Cf. § 4) peuvent être étendus aux progressions arithmétiques pourvu que la raison soit fixe (ou du moins reste petite devant n).

II. Quelques démonstrations.

Toutes les démonstrations des théorèmes précédents figurent dans [10]. On se bornera donc ici aux preuves des théorèmes 1 et 4 ainsi que d'un résultat faisant intervenir la théorie de Baker.

Soient k entiers $n + a$, $n + 2a$, ... , $n + ka$ avec $n > 0$, $(n , a) = 1$. Pour tout facteur premier p du produit $(n + a)...(n + ka)$, soit $I(p)$ l'ensemble des entiers i $(1 \leqslant i \leqslant k)$ pour lesquels $v_p(n + ia)$ est maximal (v_p désigne la valuation p-adique).

Ou, pour tout entier $i = 1 , 2 , ... , k$, existe un nombre premier p vérifiant $I(p) = \{i\}$, et l'injection f , dont on cherche à prouver l'existence, est toute trouvée, ou, pour un entier i , l'on a $I(p) \neq \{i\}$ pour tout facteur premier de $n + ia$ et donc, en désignant par j $(\neq i)$ un élément de $I(p)$,

$$v_p(n + ia) = \inf(v_p(n + ia) , v_p(n + ja)) \leqslant v_p((i - j)a) = v_p(i - j) ,$$

ce qui est majoré par la valuation p-adique du p. p. c. m. de $1 , 2 , ... , k - 1$. Le théorème 1 est maintenant clair.

De plus, si l'on choisit, pour tout facteur premier du produit $(n + a)...(n + ka)$, un élément $i(p)$ appartenant à $I(p)$, et si l'on note J l'ensemble des entiers i $(1 \leqslant i \leqslant k)$ qui ne sont pas de la forme $i(p)$, on obtient :

$$v_p(\textstyle\prod_{i\in J} (n + ia)) \leqslant v_p(\prod_{i\neq i(p)} (n + ia))$$

$$\leqslant v_p(\textstyle\prod_{i\neq i(p)} (i - i(p))) \leqslant v_p((k - 1)!) ,$$

d'où

$$\prod_{i\in J} (n + ia) \mid (k - 1)! \quad . \tag{1}$$

On prouve maintenant le théorème 4 ; il est clair qu'il suffit de le montrer dans le cas où k est premier ; grâce au théorème 1, il suffirait également de le prouver dès que k est assez grand ; toutefois, cette dernière possibilité n'est indispensable que lorsqu'on cherche à raffiner le théorème 4, et on ne l'utilisera pas ici. D'autre part, à l'aide des résultats antérieurs, on voit aussi qu'on peut supposer $a > 2$ (en fait, on peut traiter les cas $a = 1$ et $a = 2$ simultanément). On fait la démonstration par l'absurde ; soit donc (n , k , a) un triplet vérifiant $n + a > k$, $k = p_m$, p_m désignant le m-ième nombre premier, $a \geqslant 3$, $P(n , k , a) \leqslant k$. En appliquant l'inégalité (1), en minorant a par 3, $n + a$ par $1 + p_m$, et en observant que J a au moins $p_m - m$ éléments, il vient

$$(1 + p_m)(4 + p_m)...(1 + 3(p_m - m - 1) + p_m) \leqslant (p_m - 1)! \ ;$$

on vérifie alors directement que cette inégalité implique $m \geqslant 32$; de plus, s'en déduit la relation

$$(4p_m - 3m - 1)! \leqslant ((p_m - 1)!)^4 .$$

On forme le logarithme des deux membres, et on applique les inégalités de Stirling ainsi que le lemme suivant :

LEMME. - Soient $0 < t < s$ deux réels, on a

$$(s - t)\log(s - t) + t > (s - t)\log s + t^2/2s$$

de sorte qu'on obtienne

$$(8 \log 2)p_m < 3m \log(4p_m) ,$$

inégalité impossible pour $m \geqslant 32$ puisqu'on peut alors encadrer p_m ainsi (Cf. [12])

$$m \log m < p_m < m(\log m + \log\log m) .$$

THÉORÈME 6. - Pour tout couple d'entiers (k , a) ,

$$\lim_n \inf P(n , k , a)/\log\log n \geqslant k/8 .$$

Démonstration. - En observant que $\sum_{1 \leqslant i \leqslant k} \sum_{p | (n + ia)} \log p$ peut être majoré par $k \log k + \theta(P(n , k , a))$ (avec $\theta(x) = \sum_{p \leqslant x} \log p$) (distinguer le cas $p \leqslant k$ du cas $p > k$), on voit, comme dans [6], qu'on peut trouver deux entiers i' , i'' vérifiant $1 \leqslant i' < i'' \leqslant i' + 2 \leqslant k + 1$, et

$$\sum_{p | (n+i'a)(n+i''a)} \log p \leqslant 2(\log k + \theta(P(n , k , a))/k) .$$

On pose alors $n + i'a = x$, de sorte que $n + i''a = x + a'$ avec $a' = a$ ou $2a$; on applique la méthode de [5] en introduisant un entier sans facteur cubique u tel que $4x(x + a') = uy^3$ et, en se ramenant à la courbe $X^2 - Y^3 = C$ par $(u(2x + a'))^2 - (uy)^3 = (ua')^2$, ce qui permet d'appliquer les résultats de BAKER-STARK, on obtient le résultat cherché. Quand $a = 1$ ou 2, on peut montrer, par une généralisation facile de [6], que le membre de droite de l'inégalité du théorème 6 peut être amélioré en k .

BIBLIOGRAPHIE

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

[2] FAULKNER (M.). - On a theorem of Sylvester and Schur, J. London math. Soc., t. 41, 1966, p. 107-110.

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

[4] HANSON (D.). - On a theorem of Sylvester and Schur, Canad. math. Bull., t. 16, 1973, p. 195-199.

[5] LANGEVIN (M.). - Plus grand facteur premier d'entiers consécutifs, C. R. Acad.

Sc. Paris, Série A, t. 280, 1975, p. 1567-1570.

[6] LANGEVIN (M.). - Plus grand facteur premier d'entiers voisins, C. R. Acad. Sc. Paris, Série A, t. 281, 1975, p. 491-493.

[7] LANGEVIN (M.). - Sur la fonction plus grand facteur premier, Séminaire Delange-Pisot-Poitou : Groupe d'étude de théorie des nombres, 16e année, 1974/75, n° G22, 29 p.

[8] LANGEVIN (M.). - Méthodes élémentaires en vue du théorème de Sylvester, Séminaire Delange-Pisot-Poitou : Groupe d'étude de théorie des nombres, 17e année, 1975/76, n° G2, 9 p.

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

[10] LANGEVIN (M.). - Plus grand facteur premier d'entiers en progression arithmétique (à paraître).

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

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

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

(Texte reçu le 16 décembre 1976)

Michel LANGEVIN
E. N. S. Saint-Cloud
2 avenue du Palais
92210 SAINT CLOUD