Sur la division euclidienne d'un nombre premier par son rang

Nik Lygerōs(1), Michel Mizony(1) et Paul Zimmermann(2)

(1) Institut Girard Desargues UPRESA 5028, Lyon
(2) Inria Lorraine, Technopole de Nancy-Brabois
lygeros et mizony@desargues.univ-lyon1.fr, zimmerma@loria.fr

Notons p_n le n-e nombre premier et n son rang. A. Vavoda a posé une série de questions sur l'ensemble des restes de la division euclidienne d'un nombre premier par son rang, parmi lesquelles celle sur sa finitude. C'est à M. Balazard qu'il revient d'avoir démontré que cet ensemble est infini. Par ailleurs A. Vavoda a demandé si l'on peut trouver trois (ou plus) nombres premiers consécutifs ayant le même reste pour cette division ? Cette question a été résolue par M. Balazard de manière affirmative en donnant la solution suivante : 1181=6·194+17, 1187=6·195+17, 1193=6·196+17. Cette solution, comme nous allons le montrer par la suite est la plus petite solution du problème de A. Vavoda.

Notre but est de préciser un peu plus cette réponse en décrivant explicitement l'ensemble des solutions du problème posé pour trois nombres premiers et de donner des exemples explicites jusqu'à sept nombres premiers en progression arithmétique.

Lemme 1 : Soient m nombres premiers consécutifs $p_n, p_{n+1}, p_{n+2}, ..., p_{n+m-1}$ de la forme $p_k = a_k k + r$, où p_n est le n-e nombre premier et r le reste de la division euclidienne du nombre premier par son rang alors tous les a_k sont égaux.

Preuve : Comme a_k est le quotient de la division euclidienne de p_k par k, on a $p_k/k-1 < a_k \leq p_k/k$. Soit $\delta = a_{k+1} - a_k$. Alors $p_{k+1} - p_k = a_k + \delta k + \delta$. Si a_{k+1} est inférieur à a_k, alors $\delta \leq -1$, et $p_{k+1} - p_k \leq a_k - k - 1 \leq p_k/k - k - 1 \leq \log k + \log\log k - k - 1$ grâce au lemme suivant :

Lemme (Rosser et Schoenfeld) Pour $k \geq 6$, $p_k \leq k(\log k + \log\log k)$.

Cela donnerait $p_{k+1} - p_k \leq 0$ pour $k \geq 6$, d'où contradiction.

Si a_{k+1} est supérieur à a_k, alors $\delta \geq 1$, et $p_{k+1} - p_k \geq k + a_k + 1 \geq k \geq \frac{p_k}{\log p_k}$ pour $k \geq 4$ grâce au lemme suivant :

Lemme (Dusart) Pour $k \geq 2$, $p_k \geq k(\log k + \log\log k - 1)$

Ce qui est incompatible avec le lemme suivant :

Lemme (Dusart) L'intervalle $[x, x + \frac{x}{2\log^2 x}]$ contient au moins un nombre premier pour $x \geq 3275$.

Lemme 2 : Soient m nombres premiers consécutifs $p_n, p_{n+1}, p_{n+2}, ..., p_{n+m-1}$ de la forme $p_k = ak + r$, où p_n est le n-e nombre premier et r le reste de la division euclidienne du nombre premier par son rang alors, pour $n > 2$, a est congru à 0 modulo 6.

Preuve : Il est trivial que a est pair car il faut au moins 3 nombres premiers. Pour $n > 2$, le produit $p_{n+1}p_{n+2}$ ne doit pas être congru à 0 modulo 3, cela impose à $2a^2 + 1$ de ne pas être congru à 0 modulo 3 donc a est un multiple de 3.

Lemme 3 : Soient m nombres premiers consécutifs $p_n, p_{n+1}, p_{n+2}, ..., p_{n+m-1}$ de la forme $p_k = ak + r$, où p_n est le n-e nombre premier et r le reste de la division euclidienne du nombre premier par son rang alors pour a congru à 2, 4, 6, 8 modulo 10, le problème n'a pas de solution pour un nombre supérieur ou égal à cinq nombres premiers consécutifs.

Preuve : Pour $n > 3$, un nombre premier impair, dans la base 10, ne peut avoir pour chiffre des unités que 1, 3, 5, 7 ou 9. Pour a congru à 2, 4, 6 ou 8 modulo 10, quel que soit le chiffre des unités de p_n, il y aura un 5 parmi les chiffres des unités des nombres $p_{n+1}, p_{n+2}, p_{n+3}, p_{n+4}$.

Ainsi pour trois et quatre nombres premiers consécutifs a est congru à 0 modulo 6. Et pour cinq (et plus) nombres premiers consécutifs, a est congru à 0 modulo 30. Ces deux lemmes sont optimaux ainsi que le montrent les résultats que nous avons obtenus à l'aide de Maple, MuPAD et Pari.

nombre de k − uplets	$a = 6$	$a = 12$	$a = 18$
nombre de triplets	11	531	59253
nombre de quadruplets	1	28	2463

rang et nombre premier	$a = 6$	$a = 12$	$a = 18$	$a = 24$	$a = 30$
premier triplet	194	40123	10553419	3140422032	1003652348061
	1181	481489	189961591	75370128893	30109570442659
premier quadruplet	271	41181	10556627	3140440470	1003652378080
	1741	495377	190021963	75370590959	30109571372759
premier quintuplet	–	–	–	–	1003652392516
	–	–	–	–	30109571823599
premier sextuplet	–	–	–	–	1003653970688
	–	–	–	–	30109620819077

Pour $a = 6$, il y a un seul quadruplet à savoir : $1741 = 6{\cdot}271{+}115$, $1747 = 6{\cdot}272{+}115$, $1753 = 6{\cdot}273{+}115$, $1759 = 6{\cdot}274{+}115$ (solution que nous noterons par 271) et 11 triplets notés : 194, 199, 218, 271, 272, 291, 339, 358, 387, 419 et 426.

Pour $a = 18$, le dernier triplet correspond à $n = 27067108$ avec $p_n = 514274993$ et le dernier quadruplet à $n = 27066411$ avec $p_n = 514261273$.

Pour $a = 30$, le deuxieme quintuplet correspond à $n = 1003653943255$ avec $p_n = 30109619964181$. Quant au dernier sextuplet de la fenêtre il correspond à $n = 2636892436268$ avec $p_n = 81743644268701$.

Nous pouvons être plus précis sur la condition nécessaire pour l'obtention de solutions.

Théorème : Soit k un nombre premier, s'il existe un k-uplet de nombres premiers consécutifs, dont le premier est strictement supérieur à a, tels que les restes des divisions des nombres premiers par leur rang respectif soient égaux alors a est congru à 0 modulo $\prod_{q=2}^{k} q$ pour q premier.

Preuve : Dans un corps fini de caractéristique j, nous avons la formule suivante :

$$X^j - X \equiv \prod_{i=1}^{j} (X - i) \mod j$$

D'où :

$$X^{j-1} - 1 \equiv \prod_{i=1}^{j-1} (X - i) \mod j$$

Comme a est inversible on peut remplacer X par p/a on obtient :

$$(p/a)^{j-1} - 1 \equiv \prod_{i=1}^{j-1} (p/a - i) \mod j$$

,

ce qui après simplification donne :

$$\prod_{i=1}^{j-1}(p-ia) \equiv p^{j-1} - a^{j-1} \mod j$$

or $\prod_{i=1}^{j-1}(p+ia) = \prod_{i=1}^{j-1}(p-ia)$ car i parcourt tous les inversibles modulo j, ainsi nous avons :

$$\prod_{i=1}^{j-1}(p+ia) \equiv p^{j-1} - a^{j-1} \mod j$$

ou encore :

$$\prod_{i=1}^{j-1}p_i \equiv p^{j-1} - a^{j-1} \mod j$$

or pour $p > j$, $p^{j-1} \equiv 1 \mod j$ et comme $\prod_{i=1}^{j-1}p_i$ n'est pas un multiple de j on a : $a \equiv 0 \mod j$. Comme ce raisonnement est valable pour tout j-uplet de nombres premiers consécutifs, avec j premier inférieur ou égal à k nous en déduisons que : $a \equiv 0 \mod \prod_{q=2}^{k}q$.

De fait, ce théorème représente une généralisation des lemmes 2 et 3.

Remarque : en utilisant le théorème de Wilson nous pouvons obtenir directement le coefficient de a^{k-1}. En effet un calcul explicite du produit des nombres premiers consécutifs donne le résultat suivant : $(k-1)!$. Ce qui, correspond bien à -1.

Nous avons répondu ici complètement à la question posée initialement pour trois nombres premiers consécutifs, mais pas à celle générale pour k nombres premiers. Il semble difficile de montrer l'existence de telles suites pour n'importe quel k. En effet, si on supprime la condition sur les restes, cela revient à chercher k nombres premiers consécutifs en progression arithmétique, problème qui lui-même est jugé très difficile (cf. Guy chapitre A6). Cependant l'analyse probabiliste de Dubner et Nelson semble indiquer qu'il existe bien des k-uplets pour tout k. En effet, soit $a = \prod_{p \leq k}$ la plus petite distance possible entre les nombres premiers. Par analogie avec l'hypothèse de Schinzel, en supposant une indépendance totale, la probabilité pour que $x, x+a, \ldots, x+(k-1)a$ soit solution est :

$$\pi_{k,a}(x) = (C_{k,a} + o(1)) \left(\frac{1}{\ln x}\right)^k \left(1 - \frac{1}{\ln x}\right)^{(k-1)(a-1)}.$$

D'autre part, la ¡¡fenêtre¿¿ où l'on a $a \leq p_n/n < a+1$ est environ $ae^{a+1}/W(e^{a+1}) \ldots (a+1)e^{a+2}/W(e^{a+2})$ en partant de $p_n \simeq n(\ln n + \ln \ln n)$ et où W est la fonction de Lambert.

Le tableau ci-dessous indique les nombres ¡¡attendus¿¿ de solutions pour chaque paire (k, a) en multipliant la longueur de la fenêtre par $\pi_{k,a}(x)$.

a	6	6	12	12	18	18	30	30	210	210	210	210
k	3	4	3	4	3	4	5	6	7	8	9	10
esp.	1	0	60	2	7365	154	40328	501	10^{73}	10^{70}	10^{67}	10^{64}

Remarque : Les nombres attendus de solutions semblent indiquer que le problème de trouver ¡¡une¿¿ solution pour m donné n'est pas plus difficile que sans la condition de division par le rang.

En combinant notre méthode avec celle de Dubner et Nelson nous avons trouvés neuf 7-uplets, chacun de la forme $p = x + Nm + 1$ où x est égal à :
19131958978991812690857851677439676683450969104871876729265869238520629522129O
et m égal au produit des 44 premiers nombres premiers :
198962376391690981640415251545285153602734402721821058212203976095413910572270

avec $N \in \{220022677473575, 220026679078214, 220035980192096, 221056059553958, 222046548586683, 223515937652402, 224037093127486, 225074304777884, 225117563124254\}$

Actuellement, il n'est pas possible de trouver la valeur exacte du rang de ces nombres premiers néanmoins la formule de Riemann-Siegel nous permet d'affirmer que nous sommes bien dans la bonne fenêtre à savoir celle où le quotient du nombre premier par son rang est égal à 210.

Remerciements

Nous tenons à remercier Marc Deleglise et Joël Rivat pour nous avoir permis de vérifier nos résultats de manière indépendante grâce à leur programme de calcul du rang $\pi(x)$ de nombres premiers.

Références

M. Balazard et A. Vavoda : *Division euclidienne.* Pour la Science no 239, septembre 1997.

P. J. Davis et R. Hersh : *L'univers mathématique.* Editions Gauthier-Villars 1985

M. Deleglise et J. Rivat : *Computing of $\pi(x)$: The Meissel, Lehmer, Lagarias, Miller, Odlyzko method.* Mathematics of Computation, volume 65, number 213, p. 235-245, 1996.

H. Dubner et H. Nelson : *Seven consecutive primes in arithmetic progression.* Mathematics of Computation 1997.

P. Dusart : *Le kième nombre premier est plus grand que* $k(\ln k + \ln\ln k - 1)$ *pour* $k \geq 2$. Mathematics of Computation 1997.

W. et F. Ellison : *Prime numbers.* Editions Hermann 1985.

R. K. Guy : *Unsolved Problems in Number Theory.* Springer-Verlag New York 1981.

K. *Λάκκη* : *Θεωρία Αριθμών.* Εκδόσεις *Ζήτη*, *Θεσσαλονίκη* 1984.

F. Le Lionnais : *Les nombres remarquables.* Editions Hermann 1983.

Σ. *Περσίδης* : *Μαθηματικό τυπολόγιο.* ΕΣΠΙ, *Αθήνα* 1976.

C. Pomerance : *The Prime Number Graph.* Mathematics of Computation, volume 33, number 145, p. 399-408, 1979.

G. Robin : *Estimation de la fonction de Tchebychef.* Acta Arithmetica, volume 52, p. 367-389, 1983.

H. Riesel : *Prime numbers and computer method for factorization.* Birkäuser 1985.

J. B. Rosser et L. Schoenfeld : *Approximate Formulas for some functions of prime numbers.* Illinois J. Math. vol 6, p. 64-94, 1962.

J. B. Rosser et L. Schoenfeld : *A Sharper Bounds for the Chebyshev Functions* $\theta(x)$ *and* $\psi(x)$, Math. of Computation, Vol. 29, Number 129, pp. 243-269. 1975

L. Schoenfeld : *Sharper Bounds for the Chebyshev Functions* $\theta(x)$ *and* $\psi(x)$*.II*, Mathematics of Computation, Vol. 30, n. 134, pp. 337-360. 1976

J.-P. Serre : *Corps locaux.* Publications de l'Institut de Mathématiques de l'Université de Nancago VIII. Editions Hermann 1962.