31

Nombres de Carmichael

Daniel Guillaume
Vélizy, France

[résumé par Philippe Dumas]

Le nombre de Carmichael est le Canada Dry du nombre premier. Il en a le goût, il en a l'odeur, mais il n'est pas premier.

D'après le petit théorème de Fermat, si p est un nombre premier et a un entier, le nombre $a^p - a$ est divisible par p. Ceci donne une condition nécessaire pour que p soit premier, mais la réciproque est fausse et certains nombres composés passent ce test de primalité. Comme l'a remarqué Lucas, le nombre 2^{341} est congru à 2 modulo 341 alors que 341 égale 11×31 et ceci fournit un exemple de nombre pseudopremier en base 2. Qui plus est, il existe des nombres qui sont pseudopremiers dans n'importe quelle base, comme $561 = 3 \times 11 \times 17$, qui vérifie $a^{561} \equiv a \bmod 561$ pour tout entier a. Ces nombres sont les nombres de Carmichael [3], qui les a définis en 1909, et 561 est le plus petit d'entre eux.

1 Propriétés des nombres de Carmichael

Pour décrire les nombres de Carmichael, il faut introduire deux outils : l'indicateur d'Euler, φ, et la fonction de Carmichael, λ. Pour un entier $N \geq 1$, son indicateur d'Euler, $\varphi(N)$, est le nombre d'entiers compris entre 1 et N et premiers avec N. On peut aussi dire que $\varphi(N)$ est l'ordre du groupe des entiers inversibles modulo N. Par ailleurs Carmichael a défini [2] la fonction λ, qui porte son nom, de la façon suivante. Elle coïncide avec φ sur les nombres primaires p^α, si p est un nombre premier impair ou si p égale 2 et α est inférieur ou égal à 2. Par contre $\lambda\left(2^\alpha\right) = 2^{\alpha-2}$ si α vaut au moins 3. La propriété remarquable de $\lambda(N)$ est d'être le plus petit exposant $\Lambda > 0$ tel que $a^\Lambda \equiv 1 \bmod N$ pour tout entier a premier avec N. Autrement dit $\lambda(N)$ est le ppcm des ordres des inversibles modulo N, ce qui fait que $\lambda(N)$ divise $\varphi(N)$.
Revenons aux nombres de Carmichael : dire que C est un tel nombre signifie que C est composé et que

$$a^{C-1} \equiv 1 \bmod C$$

pour tout entier a premier avec C. Ceci s'énonce encore : pour tout diviseur premier p de C, le nombre $p - 1$ divise $C - 1$. On en tire les propriétés fondamentales suivantes pour un nombre de Carmichael C :

- C est impair,

- C est sans carré,
- C a au moins trois facteurs premiers,
- si p et q sont deux facteurs premiers de C, alors p n'est pas congru à 1 modulo q,
- $\lambda(C)$ divise $C-1$.

Cette dernière propriété est caractéristique des nombres de Carmichael. Donnons quelques exemples. Tout d'abord le plus petit nombre de Carmichael, 561, vérifie bien la propriété caractéristique car $\lambda(561) = \mathrm{ppcm}(2,10,16) = 80$ et 80 divise 560. Ensuite [9] les nombres $C = (6m+1)(12m+1)(18m+1)$, où les trois facteurs sont premiers, sont des nombres de Carmichael, car $\lambda(C) = 36m$ divise $C-1 = 36m(36m^2+11m+1)$. Le nombre $1729 = 7\times 13\times 19$ entre dans cette famille. Enfin indiquons la méthode d'extension [4] de Chernik : si $C = k\lambda(C)+1$ est un nombre de Carmichael et si le nombre $p = d\lambda(C)+1$, dans lequel d est un diviseur de k, est premier, alors $C' = pC$ est un nombre de Carmichael.

Les deux questions importantes qui se posent sont les suivantes.

- Existe-t-il une infinité de nombres de Carmichael ? Pour essayer de répondre à cette question, on a établi des tables de ces nombres dont la plus importante [8] s'étend jusqu'à 10^{15}. C. Pomerance, R. Alford et A. Granville [1] viennent de prouver l'infinitude de l'ensemble des nombres de Carmichael. Antérieurement P. Erdős, C. Pomerance et E. Schmutz avaient proposé la conjecture suivante : le nombre $C(x)$ de nombres de Carmichael inférieurs à x vérifie
$$C(x) \underset{x\to\infty}{=} x \exp\left(-\frac{\ln x}{\ln_2 x}\left(\ln_3 x + \ln_4 x + \frac{\ln_4 x - 1}{\ln_3 x} + \cdots\right)\right).$$
Maintenant on sait que
$$C(x) > x^{1/8}$$
pour x assez grand.
- Existe-t-il des nombres de Carmichael avec un nombre de facteurs premiers arbitrairement grand ?

  Jusqu'ici toutes les études s'appuyaient sur la formule $(6m+1)(12m+1)(18m+1)$ et ses variantes, ce qui fournissait au mieux des nombres d'une quinzaine de facteurs. Récemment Zhang [11] a obtenu des nombres de Carmichael à 1300 facteurs et plus de 8300 chiffres décimaux. Le record précédent était tenu par Dubner [5], qui avait exhibé des nombres de 3000 chiffres.

2 Recherche de grands nombres de Carmichael

Pour obtenir des nombres N de Carmichael, D. Guillaume et F. Morain [6] partent de la valeur Λ de $\lambda(N)$. Ils construisent d'abord un Λ, hautement composé mais dont l'indicateur d'Euler ne dépasse pas le plus grand entier permis, typiquement 2^{32}. Puis ils cherchent tous les nombres premiers p tels que $p-1$ divise Λ, ce qui assure que le ppcm de ces $p-1$ divise Λ. Ensuite ils calculent tous les produits congrus à 1 modulo Λ de ces nombres premiers et obtiennent ainsi des nombres de Carmichael ayant une vingtaine de facteurs.

Donnons un exemple volontairement simplet pour rester lisible. Avec $\Lambda = 2^4 3^2$ on obtient l'ensemble de nombres premiers $\{5, 7, 13, 17, 19, 37, 73\}$ et les deux nombres de Carmichael $1729 = 7 \times 13 \times 19$ et $825265 = 5 \times 7 \times 17 \times 19 \times 73$.
Mais ceci n'est encore pas assez efficace à leurs yeux et ils améliorent leur méthode de différentes façons. Pour éviter de calculer de gros produits, il vaut mieux calculer d'abord le produit complet, P, de tous les p puis chercher ensuite des produits partiels à 3, 4 ou 5 facteurs, qui sont congrus à P modulo Λ. Par simplification, on trouve des nombres de Carmichael à une quarantaine de facteurs. En procédant ainsi, on traite des Λ de plus en plus grands et on évite la croissance des données en utilisant le théorème des restes chinois, ce qui permet d'atteindre la centaine de facteurs en quelques heures de temps de calcul.
Pour éviter des essais inutiles, on regarde la forme a priori du dernier facteur utilisé dans le produit partiel et on ne teste que les nombres premiers p qui vérifient cette congruence. Ceci permet d'atteindre le millier de facteurs. Évidemment on peut pousser cette idée plus loin et regarder la forme a priori des deux derniers facteurs p du produit partiel, mais ceci complique la programmation. On peut ainsi obtenir des nombres de Carmichael ayant presque 2000 facteurs en 24 heures sur une station SPARC (pourvue de 50 Mo de mémoire). A l'aide de quelques heuristiques supplémentaires, D. Guillaume et F. Morain [6] ont obtenu leur record de **3075 facteurs et 21163 chiffres décimaux**.

3 Conclusion

Revenons sur la démarche employée. Appelons t le nombre d'entiers premiers p, pour lesquels $p-1$ divise le nombre Λ choisi, et notons S_u l'ensemble des produits partiels de u facteurs p pris dans ces t nombres premiers. Si l'un de ces produits partiels vaut 1 modulo Λ, on trouve un nombre de Carmichael. On peut aussi demander que ces produits partiels de u facteurs fournissent tous les résidus inversibles modulo Λ. Pour ceci il est nécessaire que le binomial $\binom{t}{u}$ vérifie

$$\binom{t}{u} > \varphi(\Lambda). \qquad (1)$$

En pratique, il semble que cette condition soit suffisante et que les résidus soient également répartis modulo Λ, ce qui signifie que l'on a une chance sur $\varphi(\Lambda)$ d'obtenir le résidu 1 et donc un nombre de Carmichael à u facteurs. Cette constatation empirique amène D. Guillaume et F. Morain à conjecturer que[7]

$$S_u = (\mathbf{Z}/\Lambda\mathbf{Z})^\times$$

si l'inégalité (1) est vérifiée pour un $u > 2$. Cette conjecture est étroitement liée au problème de Davenport :

> Si G est un groupe abélien, il existe un entier d tel que pour tout $s > d$ et toute suite $g_1, \ldots, g_s$ d'éléments de G, l'un des produits partiels $g_{i_1} g_{i_2} \cdots g_{i_l}$ ($i_1 < i_2 < \cdots < i_l$, $1 \leq l \leq s$) soit égal à 1.

[7] On note $A^\times$ le groupe des éléments inversibles d'un anneau A.

Cependant il faut remarquer que les bornes connues sont trop grandes pour être utilisables ici. Précisément van Emde Boas et Kruyswijk [10] ont montré que

$$d \leq m\left(1+\log\frac{|G|}{m}\right)$$

en notant m le ppcm des ordres des éléments de G. Avec $G = (\mathbf{Z}/\Lambda\mathbf{Z})^\times$ on voit que si le nombre t vérifie

$$t > \lambda(\Lambda)\left(1+\log\frac{\varphi(\Lambda)}{\lambda(\Lambda)}\right) \tag{2}$$

alors on peut affirmer que Λ fournit un nombre de Carmichael. Mais l'inégalité (2) n'a pas lieu en général.
L'idée de Pomerance *et alii* [1] est de faire croître t en modifiant peu la borne de (2). Pour cela on remplace un p par de nouveaux facteurs premiers q tels que $q-1$ divise $p\Lambda$. Autrement dit on a changé Λ en $p\Lambda$ et le majorant de (2) n'est pas trop modifié car $\lambda(p\Lambda) = \lambda(\Lambda)$. On parvient ainsi à inverser l'inégalité pour obtenir (2) puis l'infinitude de l'ensemble des nombres de Carmichael.

Signalons enfin que la méthode utilisée dans cette construction de grands nombres de Carmichael peut s'étendre à d'autres classes de nombres pseudopremiers comme les nombres Δ-Lucas pseudopremiers, les nombres pseudopremiers elliptiques et permet d'étudier le problème de Williams, le problème de Giuga, par exemple. Ces différents points figurent dans [7].

Références

[1] W. R. Alford, A. Granville, and C. Pomerance. There are infinitely many Carmichael numbers. In preparation, February 1992.

[2] R. D. Carmichael. Note on a new number theory function. *Bull. AMS*, XVI:232–238, 1910.

[3] R. D. Carmichael. On composite numbers P which satisfy the Fermat congruence $a^{P-1} \equiv 1 \bmod P$. *American Mathematical Monthly*, XIX:22–27, 1912.

[4] J. Chernick. On Fermat's simple theorem. *Bull. AMS*, 45:269–274, April 1939.

[5] H. Dubner. A new method for producing large Carmichael numbers. *Math. Comp.*, 53(187):411–414, July 1989.

[6] D. Guillaume and F. Morain. Building Carmichael numbers with a large number of prime factors. Research Report LIX/RR/92/01, Ecole Polytechnique–LIX, February 1992.

[7] D. Guillaume and F. Morain. Carmichael-like numbers with a large number of prime factors. Preprint, submitted to Eurocrypt'92, January 1992.

[8] R. Pinch. The Carmichael numbers to 10^{15}. In preparation, January 1992.

[9] P. Ribenboim. *The book of prime number records.* Springer, 2nd edition, 1989.

[10] P. van Emde Boas and D. Kruyswijk. A combinatorial problem on finite abelian groups, III. Technical Report ZW–008, Math. Centrum Amsterdam Afd. Zuivere Wisk., 1969.

[11] M. Zhang. Searching for large Carmichael numbers. Submitted to Mathematic of Computation, December 1991.