Astérisque

H. COHEN

Arithmétique et informatique

Astérisque, tome 61 (1979), p. 57-61

<http://www.numdam.org/item?id=AST_1979__61__57_0>

Société Mathématique de France
Astérisque 61 (1979) p. 57-61

ARITHMÉTIQUE ET INFORMATIQUE

par H. COHEN

Le but de mon exposé est d'attirer encore une fois l'attention sur les liens existant entre l'arithmétique et l'informatique, ces liens allant dans les deux sens.

§ 1. UTILISATION DE MOYENS INFORMATIQUES EN ARITHMÉTIQUE.

De nombreux exposés et conférences ont eu lieu à ce sujet. Je voudrais simplement parler de trois problèmes qui m'ont intéressé.

a) Nombres sociables.

Posons $s(n) = \sum_{\substack{d \mid n \\ d \neq n}} d = \sigma_1(n) - n$.

On s'intéresse au comportement des itérés successifs de la fonction s . Ce comportement peut être de trois types :

(i) $s^{(k)}(n)$ converge, c'est-à-dire qu'il existe un k tel que $s^{(k)}(n) = 1$ $\left(s^{(k)}(n) = s\left(s^{(k-1)}(n)\right)\right)$

(ii) $s^{(k)}(n)$ est périodique à partir d'un certain rang

(iii) $s^{(k)}(n)$ est non bornée.

Les exemples de (i) abondent. On ne connaît pas d'exemple de (iii). Le plus petit n qui pourrait être du type (iii) est $n = 276$. Lenstra a toutefois démontré que la suite $s^{(k)}(n)$ peut être arbitrairement longtemps strictement croissante.

Les exemples de (ii) sont les plus intéressants. Si la suite $s^{(k)}(n)$ est purement périodique de période k_o , on appelle $\left(n, s(n), \ldots, s^{(k_o-1)}(n)\right)$ un groupe sociable d'ordre k_o . Les résultats connus sont les suivants :

$k_o = 1$: n est alors dit parfait. On sait que si n est pair, n est de la forme $2^{p-1}(2^p-1)$ où 2^p-1 est premier ; on connaît 25 tels nombres, le plus grand étant $2^{21700}(2^{21701}-1)$. On conjecture qu'il n'y a

pas de nombres parfaits impairs. S'il en existe, ils doivent être supérieurs à 10^{50}.

$k_o = 2$: $(n,s(n))$ est un couple de nombres amiables. On en connaît plus de 1100, le plus petit étant le couple $(220,284)$. Tous les couples pour lesquels $n \leq 10^8$ ont été trouvés (voir [1]).

$k_o > 2$: les seuls exemples connus avant 1968 étaient dus à Poulet avec un groupe sociable d'ordre 5 et un d'ordre 28. En 1968, W. Borho a construit un groupe d'ordre 4, et indépendamment j'ai trouvé 9 groupes d'ordre 4 (voir [1]). Depuis, 5 autres groupes d'ordre 4 ont été trouvés. Les problèmes principaux sur le sujet sont les suivants :

- Existe-t-il un groupe sociable dont la somme des termes soit impair ?
- Existe-t-il un groupe sociable d'ordre 3 ?
- Existe-t-il une infinité de nombres amiables, et si oui peut-on donner une estimation asymptotique ?

b) Fonctions L de caractères quadratiques aux entiers négatifs.

Soit N un entier positif ou nul. Si $r \geq 1$ on pose

$$H(r,N) = \zeta(1-2r) \quad \text{si} \quad N = 0$$

$$H(r,N) = L\left(1-r, \left(\frac{D}{\cdot}\right)\right) \sum_{d|f} \mu(d)\left(\frac{D}{d}\right) d^{r-1}\sigma_{2r-1}(f/d)$$

où on a écrit $(-1)^r N = Df^2$ avec D discriminant de corps quadratique. Ceci est un analogue supérieur de la fonction $H(N) = H(1,N)$ introduite par Hurwitz et comptant le nombre de classes de formes quadratiques de discriminant $-N$ modulo l'ordre de leur groupe d'automorphismes. Ces fonctions $H(r,N)$ interviennent dans différents problèmes (voir [2] et [5]) et j'ai jugé utile d'en faire une table assez étendue, pour $r > 1$ (pour $r = 1$ une telle table existe). Pour cela, j'ai utilisé le fait que la série

$$\mathcal{H}_r(\tau) = \sum_{N\geq 0} H(r,N)e^{2i\pi N\tau} = \sum_{N\geq 0} H(r,N)q^N \qquad (q = e^{2i\pi\tau})$$

est une forme modulaire de poids $r+\frac{1}{2}$ sur $\Gamma_o(4)$. Ceci entraîne que

$\mathcal{H}_r$ est un polynôme en $\theta = \sum_{n\in\mathbb{Z}} q^{n^2}$ et $F_2 = \sum_{\substack{n\geq 1\\ n \text{ impair}}} \sigma_1(n)q^n$ dont les coefficients se déterminent aisément.

Toutefois, le calcul de F_2^2, F_2^3 etc... est très long si on veut aller jusqu'à $N = 1000$. Il a donc fallu employer une méthode (déjà utilisée par Atkin) pour accélérer les calculs. Cette méthode était la suivante :

Posons $\theta_1 = \sum_{n\geq 0} q^{(2n+1)^2}$, $\theta_2 = \sum_{n\in\mathbb{Z}} q^{(2n)^2}$. On démontre que $F_2 = \theta_1\theta_2(\theta_2^2 + 4\theta_1^2)$ et $\theta = 2\theta_1 + \theta_2$ donc on peut exprimer $\mathcal{H}_r$ comme polynôme en θ_1 et θ_2. L'avantage énorme est que les séries θ_1 et θ_2 sont très lacunaires, donc que la multiplication par une telle série est très rapide.

J'ai ainsi pu calculer une table de $H(r,N)$ avec $2 \leq r \leq 11$, $0 \leq N \leq 1020$ en 16 mn d'IRIS 80. Il m'a fallu employer une bibliothèque maison de multiprécision car le plus grand nombre de la table est

$$-3036\,H(11,1020) = 142369924502364047754513095232000 0.$$

Cette table a été déposée aux U.M.T. de Mathematics of Computation [3].

c) Contre-exemple à la conjecture de von Sterneck. (Travail fait en collaboration avec F. Dress)

Posons $M(x) = \sum_{n\leq x} \mu(n)$, où μ est la fonction de Möbius. Von Sterneck a conjecturé que $|M(x)| \leq \frac{\sqrt{x}}{2}$ pour tout $x > 200$. En calculant des valeurs particulières de $M(x)$ Neubauer a montré que cette conjecture était fausse pour $x = 7{,}77 \times 10^9$.

J'ai programmé en assembleur un miniordinateur TI 980 B acheté grâce à l'ATP du CNRS Mathématiques-Informatique, pour faire le calcul systématique de $M(x)$ jusqu'à $7{,}8.10^9$. Le temps de calcul initial pour arriver à $7{,}8.10^9$ aurait été de quelques mois. J'ai réussi en optimisant le programme au maximum à ramener la durée à moins d'une semaine, temps raisonnable. Je dispose ainsi d'une table de $M(x)$ de 10^7 en 10^7 jusqu'à $7{,}8.10^9$ et j'ai trouvé que le plus petit x pour lequel la conjecture de von Sterneck est fausse est $x = 7725038629$ pour lequel on a

$M(7725038629) = 43947$.

Remarque. On conjecture en fait que

$$\overline{\lim} \frac{|M(x)|}{\sqrt{x}} = +\infty$$

et même que

$$\overline{\lim} \frac{|M(x)|}{\sqrt{x}\ \mathrm{Log}\ \mathrm{Log}\ x} > 0 .$$

§ 2. UTILISATION DE L'ARITHMÉTIQUE EN INFORMATIQUE.

Je voudrais ici énoncer un problème non encore résolu à ma connaissance, et qui se trouve dans l'excellent livre de Knuth ([4]) auquel on pourra se référer pour les détails de ce qui suit.

Ce problème est l'analyse de l'algorithme binaire de calcul du PGCD. Cet algorithme est basé sur les remarques suivantes : si u et v sont pairs, $(u,v) = 2(u/2, v/2)$. Si u est pair et v est impair, $(u,v) = (u/2, v)$ (et inversement). Enfin si u et v sont impairs, $(u,v) = (u-v, v)$ et $u-v$ est pair. On peut aisément déduire de ces remarques un algorithme de calcul du PGCD ne nécessitant pas de division (la division par 2 se faisant beaucoup plus rapidement qu'une division arbitraire dans la grande majorité des ordinateurs) et cet algorithme se trouve être en pratique plus rapide que l'algorithme d'Euclide. En ce qui concerne l'algorithme d'Euclide, on sait que le nombre de divisions pour calculer (a,n) est en moyenne de l'ordre de $\frac{12\ \mathrm{Log}\ 2}{\pi^2}\ \mathrm{Log}\ n$. En ce qui concerne l'algorithme binaire, certains calculs heuristiques et des expérimentations ont été faites, mais on ne connaît pas en moyenne le nombre de pas nécessaire pour calculer (a,n) , et ceci pose un problème à mon avis très intéressant aux mathématiciens.

BIBLIOGRAPHIE.

[1] H. COHEN. - On amicable and sociable numbers, Math. Comp. 24 (1970) pp. 423-429.

[2] H. COHEN. - Sums involving the values at negative integers of L functions of quadratic characters, Math. Ann. 217 (1975) pp. 271-285.

[3] H. COHEN. - A table of values at negative integers of L functions of quadratic characters, Math. Comp., UMT file.

[4] D. KNUTH. - The Art of Computer Programming, vol. 2, ch. 4, § 4.5.2 (Addison Wesley, 1969).

[5] D. ZAGIER. - Modular forms whose Fourier coefficients involve zeta-functions of quadratic fields, Lecture Notes n° 627, pp. 106-169.

-:-:-:-

Henri COHEN
Laboratoire de Mathématiques Pures - Institut Fourier
dépendant de l'Université Scientifique et Médicale de Grenoble
associé au C.N.R.S.
B.P. 116
38402 ST MARTIN D'HERES (France)

(décembre 1978)