Séminaire de philosophie et mathématiques

J. L. Nicolas

Utilisation des ordinateurs en théorie des nombres

Séminaire de Philosophie et Mathématiques, 1979, fascicule 6
« Utilisation des calculateurs en théorie des nombres », , p. 1-8

<http://www.numdam.org/item?id=SPHM_1979___6_A1_0>

UTILISATION DES ORDINATEURS EN THEORIE DES NOMBRES

par

J.L. NICOLAS (Limoges)*

De tout temps les arithméticiens ont calculé des familles de nombres et ont construit des tables numériques. A partir de ces calculs, ils établissaient des conjectures qu'ils démontraient ou qu'ils transmettaient à leurs descendants. Depuis quelques années, la puissance des ordinateurs a permis d'augmenter considérablement ces calculs qui sont souvent l'objet de publications. Le journal "Mathematics of computation" s'est spécialisé dans ce type d'article. On lira avec beaucoup d'intérêt le numéro 29 de Janvier 1975 qui recouvre une bonne part de cet exposé. Ce numéro est dédié à D. H. LEHMER qui fut un des pionniers et qui est un des maîtres de cette partie des mathématiques.

1) Calcul de π.

La formule de Machin, très connue des taupins,

$$\frac{\pi}{4} = 4 \operatorname{Arctg} \frac{1}{5} - \operatorname{Arctg} \frac{1}{239}$$

a été utilisée pour les premiers calculs de π :

1949	REITWEISNER	sur ENIAC,	2 000 décimales (70h)
1958	GENUYS	sur I.B.M. 704,	10 000 décimales (100mn).

On lui préféra ensuite la formule :

$$\frac{\pi}{4} = 6 \operatorname{Arctg} \frac{1}{8} + 2 \operatorname{Arctg} \frac{1}{57} + \operatorname{Arctg} \frac{1}{239}$$

(1961 SHANKS et WRENCH sur I.B.M. 7090, 100 000 décimales (8h), Math of comp. vol. 16, 1962, p. 76-99).

Monsieur BRETTE, professeur de mathématiques au Palais de la Découverte, a connaissance d'un calcul non publié d'un million de décimales de π, par cette formule.

Enfin E. SALAMIN donne la formule déduite de la théorie des intégrales elliptiques qui lui permettrait de calculer 10^7 décimales de π :

$$\frac{\pi}{4} = \frac{a\,g\,m\,(1,k)\;a\,g\,m\,(1,k')}{1 - \sum_{j \geq 1} 2^j (c_j^2 + c'^2_j)}$$

---

* (Conférence donnée au séminaire : Philosophie et mathématiques le 7 mai 1979)

où k et k' sont deux nombres réels vérifiant $k^2 + k'^2 = 1$, $a_o = 1$, $b_o = k$; $a'_o = 1$; $b'_o = k'$;

$$a_{n+1} = \frac{1}{2}(a_n + b_n) \qquad b_{n+1} = \sqrt{a_n b_n}$$

$$a'_{n+1} = \frac{1}{2}(a'_n + b'_n) \qquad b'_{n+1} = \sqrt{a'_n b'_n}$$

$$c_n = a_n^2 - b_n^2 \qquad c'_n = a'^2_n - b'^2_n$$

$a\ g\ m\ (1,k) = \lim a_n = \lim b_n$ est la moyenne arithmetico géométrique.

Une étude statistique a montré que les 10 000 premières décimales de π pouvaient être considérées comme une liste de chiffres au hasard.

L'étude des 21000 premières réduites du développement en fraction continue de π, a montré que π avait en ce domaine un comportement tout à fait normal.

BIBLIOGRAPHIE

M. MIGNOTTE, Séminaire de théorie des nombres D.P.P. 1972-1973, n° G. 12.
E. SALAMIN, Math of Comp. Vol. 30, 1976, p. 565-570.

2) Factorisation des nombres entiers.

a) Test de primalité.

Il est toujours plus facile de tester si un nombre est premier ou non, que d'obtenir sa décomposition en facteurs premiers. Les tests de primalité sont basés sur le théorème de Fermat :

$$p \text{ premier} \Rightarrow \forall a,\ a^p \equiv a \bmod p.$$

La réciproque n'est pas vraie : il existe des nombres m appelés nombres de Carmichael qui vérifient :

$$\forall a,\quad a^m \equiv a \bmod m$$

Le plus petit est $561 = 3.11.17$. Cependant il est possible d'obtenir des réciproques un peu plus compliquées du théorème de Fermat.

b) La méthode de division.

Pour factoriser n, on le divise par tous les nombres premiers $p \leq \sqrt{n}$. En fait on divise n par les nombres d'un ensemble contenant les nombres premiers et contenu dans l'ensemble des nombres impairs, par exemple les nombres premiers à 30 ou à 210.

Cette méthode est en $O(\sqrt{n})$ pas, c'est-à-dire comprend un nombre d'opérations de l'ordre de $\sqrt{n}$. On peut noter ici qu'un ordinateur rapide fait très approximativement un million d'opérations à la seconde. Par cette méthode, un nombre de 12 chiffres sera factorisé en 1 seconde ; un nombre de 18 chiffres en un quart d'heure ; un nombre de 24 chiffres en 250 heures, ce qui est irréaliste.

BIBLIOGRAPHIE

D.E. KNUTH, Fundamental algorithms t.2. Addison Wesley 1969.

c) La méthode de Fermat.

Grace à l'identité valable pour n impair :

$$n = pq = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2.$$

Fermat avait remarqué qu'il est équivalent de factoriser n, ou de l'écrire sous la forme $n = x^2-y^2$. Pour les $x > \sqrt{n}$, il regardait si x^2-n est un carré parfait. L'idée a été reprise par Sherman Lehman qui en déduit une méthode de factorisation en $O(n^{1/3})$ pas, assez facile à programmer. Il s'agit de résoudre l'équation $x^2-y^2 = 4kn$ pour les petites valeurs de k.

BIBLIOGRAPHIE

R. SHERMAN LEHMAN, Math of Comp., vol. 28, 1974, p. 637-646.

d) La méthode de Legendre.

Cette méthode consiste à développer en fractions continues $\sqrt{kn}$ pour de petites valeurs de k. Si $\frac{x}{d}$ est une réduite, $a = x^2-knd^2$ sera petit en valeur absolue et sera un carré modulo n. On peut ainsi trouver x et y tels que $x^2 \equiv y^2 \mod n$; p g c d $(n,x+y)$ et p g c d $(n,x-y)$ sont des diviseurs de n. Un autre avantage de la méthode, comme a est un carré modulo tous les diviseurs premiers de n, est de situer ces diviseurs premiers dans des progressions arithmétiques (par exemple $a=-1$ entraine $p\equiv 1 \mod 4$) ce qui facilite la méthode de factorisation par division.

BIBLIOGRAPHIE

KRAITCHIK, Recherches sur la théorie des nombres, Paris 1929
MORRISON et BRILLHART, Math of Comp., vol. 29, 1975, p. 183-205.

e) La méthode de Shanks.

Considérons l'ensemble $E(\Delta)$ des formes quadratiques $AX^2 + BXY + CY^2$ avec $A,B,C \in \mathbb{Z}$, de discriminant $\Delta = B^2 - 4AC$ fixé. Si l'on fait la transformation :

$$\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} X' \\ Y' \end{pmatrix} \qquad a,b,c,d \in \mathbb{Z}\ ,\ |ad-bc| = 1$$

la forme $AX^2 + BXY + CY^2$ se transforme en une forme $A'X'^2 + B'X'Y' + C'Y'^2$ de même discriminant Δ. La relation $(A,B,C) \sim (A',B',C')$ est une relation d'équivalence sur $E(\Delta)$. Le nombre de classes d'équivalences est fini et se note $h(\Delta)$. De plus, on peut mettre sur $E(\Delta)$ une loi de composition qui fait de l'ensemble quotient un groupe fini à $h(\Delta)$ éléments. On peut faire correspondre à chaque forme quadratique un idéal de l'anneau des entiers algébriques du corps de nombre $\mathbb{Q}(\sqrt{\Delta})$. La loi de composition des formes quadratiques s'interprète alors comme le produit des idéaux correspondants.

Pour factoriser n, Shanks calcule $h(\Delta)$ avec $\Delta=-n$, ou $\Delta=-4n$ et étudie le groupe fini à $h(\Delta)$ éléments de façon à trouver une forme (A,B,C) de discriminant Δ vérifiant $B=0$ ou $A=B$ ou $A=C$, ce qui donne une factorisation immédiate de Δ.

Cette méthode est d'une part très belle, puisqu'elle résoud un problème d'un énoncé très simple par des méthodes beaucoup plus profondes, et initialement développées dans d'autres but, et d'autre part très efficace pour des nombres de plus de 15 chiffres. (Le nombre de pas de l'algorithme est $O(n^{1/4+\varepsilon})$.

BIBLIOGRAPHIE

H. COHEN, Séminaire D.P.P. 1972-1973, n° G 7
D. SHANKS, Proc. of Symposia in pure mathematics, vol. XX, p. 415-440.

f) Un système de codage.

Un chef de réseau veut construire un codage de façon que n'importe qui puisse lui téléphoner un message qu'il est seul à savoir décrypter. A l'aide de tests de primalité, il choisit deux nombres premiers p et q d'une cinquantaine de chiffres. Il calcule $n=pq$; ce nombre n est trop grand pour être factorisé par les méthodes actuellement connues. Il calcule $\phi(n) = (p-1)(q-1)$ et choisit un nombre d, premier avec $\phi(n)$; $\phi(n)$ et d sont gardés secrets. Il calcule e, tel que $ed \equiv 1 \bmod \phi(n)$. Il envoie à ses correspondants la valeur de n et de e.

Un correspondant veut adresser au chef de réseau un message. Il le met d'abord sous la forme de nombres M, vérifiant $1 \leq M \leq n$, et envoie le message codé sous la forme du nombre $C \equiv M^e \bmod n$. Tout le monde peut connaître C, mais seul le chef de réseau peut reconstruire M par la formule $M \equiv C^d \bmod n$. Le calcul de d par un ennnemi est équivalent à la factorisation de n, et donc, pratiquement impossible.

BIBLIOGRAPHIE

R.L. RIVEST, A. SHAMIR, L. ADLEMAN, Com. A.C.M. vol. 21, 1978, p. 120 à 126.
M. MIGNOTTE, Publication du Séminaire d'Informatique de l'Université de Strasbourg.

3) Nombres de Mersenne et de Fermat.

La grande presse a annoncé en décembre 1978 que le plus grand nombre premier connu était $2^{21701}-1$, battant l'ancien record qui était $2^{19937}-1$. Les nombres de la forme 2^p-1, où p est premier sont appelés nombres de Mersenne. Actuellement 25 d'entre eux ont été montrés premiers, correspondant aux valeurs de $p = 2,3,5,7,13,17,19,31,61,89,107,127,521,607,1279,2203,2281,3217,4253,4423,9689,9941,11213,19937,21701$. Pour ce type de nombre, il existe un test de primalité particulier.

Test de Lucas-Lehmer : Soit q premier $\neq 2$, $L_o=4$, $L_{n+1} \equiv L_n^2 - 2 \bmod (2^q-1)$, alors :

$$(2^q-1) \text{ premier} \iff L_{q-2} = 0.$$

En 1876, à l'aide de ce test, Lucas avait montré que $2^{127}-1$ était premier, et ceci à la main.

Fermat avait conjecturé que les nombres $F_m = 2^{2^m}+1$ étaient tous premiers, et l'avait montré pour $m \leq 4$. Malheureusement on ne connait pas de nombres F_m premiers avec $m \geq 5$. Ils sont tous composés pour $5 \leq m \leq 16$. Le premier cas non connu est m=17. Il existe deux méthodes pour tester les nombres de Fermat. D'abord on sait démontrer que si p premier divise F_m, alors $p \equiv 1 \bmod 2^{m+2}$. Ainsi pour m=5, on divise F_5 par les nombres de la forme 128k+1 ; on constate rapidement que 641 divise F_5. Cette technique permet de trouver des diviseurs des nombres de Fermat.

La seconde méthode est un test de primalité : si $p=F_m$ est premier, on peut démontrer que 3 est un générateur du groupe cyclique $(\mathbb{Z}/p\mathbb{Z})^*$ et l'on a le critère :

$$F_m = p \text{ premier} \iff 3^{\frac{p-1}{2}} \equiv -1 \bmod p.$$

BIBLIOGRAPHIE.

W. SIERPINSKI, Elementary theory of numbers.
D.E. KNUTH., Fundamental algorithms, vol. 2.
J.C. HALLYBURTON and J. BRILLHART, Math of Comp., vol 29, 1975, p. 109-112.

4) Théorème de Fermat.

Soit $n \geq 3$. Peut-on trouver des nombres entiers non nuls x,y,z tels que $x^n + y^n = z^n$?

Pour n = 4, Fermat avait démontré que c'est impossible, on peut donc se restreindre au cas n=p premier.

Si p est un nombre premier régulier, Kummer a démontré en 1850, que l'équation de Fermat $x^p + y^p = z^p$ n'a pas de solution. Un nombre premier est régulier s'il ne divise pas le numérateur des nombres de Bernouilli $B_2, B_4, \ldots, B_{p-3}$. Les nombres de Bernouilli sont définis par :

$$\frac{x}{e^x-1} = 1 - \frac{x}{2} + \frac{B_2}{2} x^2 + \frac{B_4}{4!} x^4 + \ldots + \frac{B_{2k}}{2k!} x^{2k} + \ldots$$

ou par :
$$1 + \sum_{k=1}^{m-1} \binom{m}{k} B_k = 0 \qquad \text{avec} \qquad \binom{m}{k} = \frac{m!}{k!(m-k)!}$$

On a : $B_1 = -\frac{1}{2}$, $B_2 = \frac{1}{6}$, $B_4 = -\frac{1}{30}$, $B_6 = \frac{1}{42}$, $B_8 = -\frac{1}{30}$, $B_{10} = \frac{5}{66}$, $B_{12} = \frac{-691}{2730}$, $B_{14} = \frac{7}{6}$ etc ...

Le plus petit nombre premier irrégulier est 37 qui divise le numérateur de B_{32}.

Lorsque p est irrégulier, un test toujours efficient jusqu'à présent (cf. Math of Comp. vol 29, 1975, p. 114) permet de montrer que l'équation de Fermat n'a pas de solution et ainsi Wagstaff a démontré qu'il n'y avait pas de solutions pour $3 \leq n \leq 125\,000$.

BIBLIOGRAPHIE

Z.I. BOREVITCH et I.R. CHAFAREVITCH, Théorie des nombres Gauthiers Villars 1967.
S. WAGSTAFF, Math of Comp. vol 32, 1978, p. 583-591.

5) Hypothèse de Riemann.

La fonction ζ de Riemann est définie pour $s \in \mathbb{C}$, $\mathcal{R}e\ s > 1$, par la série : $\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s}$. Elle se prolonge en une fonction analytique dans $\mathbb{C} - \{1\}$ et a des zéros dans la bande $0 < \mathcal{R}e\ s < 1$ qui sont symétriques par rapport à l'axe réel et à la droite $\mathcal{R}e\ s = \frac{1}{2}$. Riemann a conjecturé que tous ces zéros (dont le plus petit en module est $\frac{1}{2} \pm 14{,}1\ i$) sont situés sur la droite $\mathcal{R}e\ s = \frac{1}{2}$. Rosser et Schoenfeld ont calculé plus de 3.500 000 zéros vérifiant $0 \leq \mathrm{Im}\ s \leq 1.894\ 438$. Ils vérifient tous l'hypothèse de Riemann.

La fonction ζ de Riemann intervient largement dans la distribution des nombres premiers. Les calculs précédents ont permis de démontrer certaines inégalités; par exemple pour la fonction $\pi(x)$ égale au nombre de nombres premiers $\leq x$, on a ; pour $x \geq 67$:

$$\frac{x}{\log x - 1/2} \leq \pi(x) \leq \frac{x}{\log x - 3/2}$$

BIBLIOGRAPHIE

W.J. ELLISON et M. MENDES-FRANCE, les nombres premiers, Hermann, 1975.

J.B. ROSSER et L.S. SCHOENFELD, Math of Comp., vol 29, 1975, p. 243-269

" " Math of Comp., vol 30, 1976, p. 337-360.

EDWARDS : Riemann zeta function, Acad. Press.

6) Une démonstration achevée par des calculs.

Dans ce domaine, l'exemple le plus célèbre est certainement le théorème des 4 couleurs. En arithmétique, un résultat important a été aussi obtenu par ordinateur : On sait démontrer que si Δ est négatif et si le nombre de classes (défini au paragraphe 2e) vérifie $h(\Delta) = 2$, alors $|\Delta| < 10^{1030}$. Il reste donc à regarder les "petites" valeurs de $|\Delta|$, (ce qui ne peut se faire par une recherche systématique), pour montrer qu'il n'y a que 18 valeurs de Δ comprises entre -15 et -427 qui sont solution de $h(\Delta) = 2$.

L'équation $h(\Delta) = 1$ avait été résolue ainsi, mais aussi par une autre démonstration n'utilisant pas les calculs numériques. D'autres résultats illustrent cette méthode, notamment la résolution des équations $x^2 - y^3 = k$ pour certaines valeurs de k.

BIBLIOGRAPHIE

H.M. STARK, Math of Comp., vol 29, 1975, p. 289-302.

7) Quelques exemples ou contre exemples.

a) Euler avait conjecturé, comme généralisation du théorème de Fermat que pour $n \geq 3$ l'équation :

$$x_1^n + x_2^n + \ldots + x_{n-1}^n = x_n^n$$

n'avait pas de solution.

Lander et Parkin (Math of Comp. vol 21, 1967, p. 101-103) ont fourni le contre exemple :

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5.$$

b) Dans leur important travail sur les groupes finis, Feit et Thompson avaient conjecturé que si p et q étaient premiers, alors

$$\frac{p^q-1}{q-1} \quad \text{et} \quad \frac{q^p-1}{p-1}$$

étaient premiers entre eux. N.M. Stephens (Math of Comp. t. 25, 1971, p. 625) a montré que pour $p=17$ et $q=3313$, $112\,643=2pq+1$ était un facteur commun aux deux nombres.

c) Un vieux problème d'arithmétique, encore irrésolu est le suivant : Pour tout n, existe-t-il une progression arithmétique dont tous les termes $a+kb$, $0 \leqslant k \leqslant n-1$ soient des nombres premiers ? Le record actuel $n=17$ est dû à S. Weintraub, Math of Comp. vol 31, 1977, p. 1030.

d) Cassells et Guy (Mathematika t. 13, 1966, p. 11-120) ont démontré que l'équation :

$$5x^3 + 12y^3 + 9z^3 + 10w^3 = 0$$

a des solutions dans tous les corps p-adiques $\mathbb{Q}_p$, mais pas dans $\mathbb{Q}$. L'ordinateur leur a servi à trier parmi les formes qui avaient des zéros dans tous les $\mathbb{Q}_p$, celles qui n'avaient pas dans $\mathbb{Q}$ de racines $\frac{a}{b}$, avec a et b petit.

e) Soit $\mu(n)$ la fonction de Möbius. (Si n se décompose en facteurs premiers $n = \prod_{i=1}^{k} p_i^{a_i}$, on a $\mu(n) = \prod_{i=1}^{k} \mu(p_i^{a_i})$, $\mu(p) = -1$ et $\mu(p^a) = 0$ si $a \geqslant 2$, $\mu(1) = 1$). On pose $M(x) = \sum_{n \leqslant x} \mu(n)$. Van Sternek a conjecturé que $|M(x)| \leqslant \frac{\sqrt{x}}{2}$. H. Cohen et F. Dress ont montré que cette conjecture était vraie pour $x \leqslant n_o = 7725038628$, et fausse pour $x = n_o+1$. (Astérisque 61, p. 57-61).

8) Quelques problèmes à résoudre.

a) Soit $\pi(x)$ le nombre de nombres premiers $\leqslant x$. Le théorème des nombres premiers s'énonce : $\pi(x) \sim \frac{x}{\log x}$. En fait une meilleure approximation de $\pi(x)$ est le logarithme intégral de x, $\mathrm{li}\, x = \int_2^x \frac{dt}{\log t}$. Les tables de nombres premiers montrent que $\pi(x) < \mathrm{li}\, x$ pour $x \leqslant 10^8$. Cependant on peut démontrer que la différence $\pi(x)-\mathrm{li}\, x$ change de signe pour une infinité de valeurs de x. Sherman Lehman a montré (Acta Arithmetica, t. 11, 1966, p. 397-410) que $\pi(x_o) > \mathrm{li}(x_o)$ pour $x_o \leqslant 1{,}65.10^{1165{,}4}$. Mais cette borne est encore beaucoup trop grande pour pouvoir calculer la plus petite racine de l'équation $\pi(x) = \mathrm{li}\, x$. Cela montre également que dans ce type de problèmes, comme dans l'hypothèse de Riemann, il est dangereux d'extrapoler des résultats, mêmes s'ils sont obtenus pour un grand nombre de valeurs.

b) Vinogradov a démontré que tout nombre $n > 3^{3^{15}}$ et impair s'écrivait comme une somme de 3 nombres premiers. Là aussi la borne est trop grande pour montrer que la propriété est vraie pour $n > 7$.

c) Catalan avait conjecturé que l'équation $a^x - b^y = 1$ avec $a,b,x,y, \geq 2$ n'avait comme solution que $3^2 - 2^3 = 1$. Tijdeman (Acta Arithmetica, t. 24, 1976, p. 197-209) a démontré que l'équation de Catalan n'avait qu'un nombre fini de solutions. Cependant les calculs restant à faire sont beaucoup trop longs pour achever la démonstration de la conjecture.

d) Soit $f : \mathbb{N} \to \mathbb{N}$ définie par :

$$f(n) = n/2 \quad \text{si} \quad n \quad \text{est pair}$$
$$f(n) = 3n+1 \quad \text{si} \quad n \quad \text{est impair.}$$

On construit la suite $a_o, \ldots, a_{n+1} = f(a_n)$. On conjecture que cette suite vaut 1 à partir d'un certain rang quel que soit la valeur de départ a_o. C'est un problème très simple à programmer, même sur une petite machine, et de nombreux calculs ont été faits pour mettre en défaut cette conjecture. Dans ce cas c'est la théorie qui est un peu en retard sur l'ordinateur.

BIBLIOGRAPHIE

R.E. CRANDALL, Math of Comp., vol 32, 1978, p. 1281-1292.

J.L. NICOLAS
Département de Mathématiques
123 rue Albert Thomas
87060 LIMOGES