ETRE OU NE PAS ETRE UN CARRE

On peut se demander si Hamlet possédait un bon algorithme pour résoudre son problème existenciel. J'espère que, docteur, Arjen saura construire pour lui-même un tel algorithme qui marche en temps réel. A défaut de lui proposer une solution, je vais parler d'un problème similaire, mais un peu moins profond.

Pour déterminer si un entier N est un carré parfait, on peut utiliser la racine carrée réelle de l'ordinateur en testant si N est égal à :

```
INT (SQRT (FLOAT (N) + .5)) ** 2
```

On peut aussi écrire un sous-programme de calcul de la racine carrée en nombres entiers par la méthode de Newton :

$$X_{k+1} = \frac{1}{2} (X_k + N/X_k)$$

On peut, pour gagner du temps, tester d'abord si N est un carré modulo M où M est un nombre que l'on se fixe. Si oui, on applique l'une des méthodes précédentes, sinon c'est terminé.

Comment choisir M ? Dans son article : " Factoring large integers " R. SHERMAN LEHMAN (Math. of comp. 28, 1974, p. 637-646) utilise M = 729. Ce n'est pas le meilleur choix.

Appelons q(n) le nombre de carrés mod n. La fonction q est multiplicative : si m et n sont premiers entre eux, on a :

$$q(m\,n) = q(m)\,q(n)$$

et l'on a :

$$q(2^\alpha) = [2^{\alpha/6}] + 2$$

et pour $p \neq 2$:

$$q(p^\alpha) = [\frac{p^{\alpha+1}}{2(p+1)}] + 1$$

où [x] désigne la partie entière de x. On dira que n est un nombre " de petit q " si la probabilité d'être un carré modulo n est plus faible que pour les nombres précédents, autrement dit si :

$$m < n \Rightarrow q(m)/m > q(n)/n$$

Les méthodes des nombres hautement composés s'appliquent à ce problème et l'on a la table où figure entre parenthèse la valeur n/q(n) :

Table des nombres " de petit q "

2	(1.)	3	(1.5)	*4	(2.)	8	(2.67)
12	(3.)	*16	(4.)	32	(4.57)	*48	(6.)
80	(6.67)	96	(6.86)	112	(7.)	*144	(9.)
240	(10.)	288	(10.29)	336	(10.5)	480	(11.43)
560	(11.67)	576	(12.)	*720	(15.)	1008	(15.75)
1440	(17.14)	1680	(17.5)	2016	(18.)	2640	(18.33)
2880	(20.)	3600	(20.45)	4032	(21.)	*5040	(26.25)

Avec l'accord du guide Michelin, nous avons signalé par une étoile les nombres analogues au nombres hautement composés supérieurs et qui sont particulièrement recommandés.

Il arrive dans certains cas que les nombres à tester ne sont pas distribués de façon aléatoire modulo 2 et que l'on préfère prendre M impair. Sont alors conseillés :

45	(3.75)	315	(6.56)	3465	(12.03)

Le choix de M dans ces tables dépend du nombre de mémoires dont on dispose. On construit alors un tableau T(1) ... T(M), où T(I) vaut 1 si I est un carré modulo M, et 0 sinon. Le nombre N ne sera pas un carré si T(MOD (N, M)) = 0.

J.L. NICOLAS

Département de Mathématiques
Université de Limoges
123, Avenue Albert Thomas
F-87060 LIMOGES CEDEX