Le développement en fraction continue d'un réel

Soit x un réel positif. On définit les suites (α_n), et (a_n) par $\alpha_0 = x$, $a_0 = [x]$, et, tant que α_n n'est pas un entier,

$$\alpha_{n+1} = \frac{1}{\{\alpha_n\}}, \qquad a_{n+1} = [\alpha_{n+1}]\,.$$

ou, de manière équivalente,

$$\alpha_n = a_n + \frac{1}{\alpha_{n+1}}, \qquad a_n \in \mathbb{N},\ \alpha_{n+1} > 1,$$

et on a succesivement

$$x = a_0 + \frac{1}{\alpha_1} = a_0 + \frac{1}{a_1 + \dfrac{1}{\alpha_2}} = a_0 + \frac{1}{a_1 + \dfrac{1}{a_2 + \dfrac{1}{\alpha_3}}} = \dots$$

Les (a_n), qui sont des entiers ≥ 1 pour $n \geq 1$, sont appelé les *quotients* du développement en fraction continue de x. On note $[a_0, a_1, \dots, a_n]$ la fraction

$$[a_0, a_1, \dots, a_n] = a_0 + \frac{1}{a_1 + \dfrac{1}{a_2 + \dots \dfrac{1}{a_n}}} = \frac{p_n}{q_n}$$

est appelée la n^{eme} *réduite* du développement de x. Les suites (p_n) et (q_n) vérifient la relation de récurrence

$$p_{-2} = 0, \quad p_{-1} = 1, \quad p_n = a_n p_{n-1} + p_{n-2}. \qquad q_{-2} = 1, \quad q_{-1} = 0, \quad q_n = a_n q_{n-1} + q_{n-2}$$

Une propriété essentielle des réduites de x est que ce sont de bonnes approximations rationelles de x, en ce sens que, pour tout entier n on a

$$\left| x - \frac{p_n}{q_n} \right| \leq \frac{1}{q_n\, q_{n+1}} < \frac{1}{q_n^2}$$

La condition ci-dessus est nécessaire, mais non suffisante, pour que la fraction $\dfrac{p_n}{q_n}$ soit l'une des réduites de x. On a cependant la réciproque suivante

Si la fraction $\dfrac{p_n}{q_n}$ *vérifie* $\left| x - \dfrac{p_n}{q_n} \right| \leq \dfrac{1}{2\, q_n^2}$ *alors, elle est une des réduites du développement en fraction continue de* x.

Pour obtenir à l'aide de Maple le développement en fraction continue de x on utilise, par exemple la fonction prédéfinie `cfrac(x,n,reduites)`, qui reçoit le nombre `x`, et l'entier `n`, et renvoie dans la variable dont le nom est `reduites` la liste des n premières réduites de x.

Une attaque contre RSA

Ce paragraphe, extrait d'un sujet d'examen de Maitrise d'Arithmétique, montre comment casser un code RSA, si l'exposant de décodage, d est plus petit que $\frac{1}{3}\sqrt[4]{n}$.

Alice choisit deux nombres premiers p et q vérifiant $q < p < 2q$, et calcule $n = pq$. Elle choisit ensuite la clef d'encodage e, e premier avec $\varphi(n)$, $2 \leq e < \varphi(n)$, où φ est la fonction d'Euler. Puis elle calcule d tel que $ed \equiv 1 \pmod{\varphi(n)}$, qui est la clef de décodage. Alice publie n et e comme clé publique du protocole RSA.

On suppose que l'entier d vérifie

$$2 \leq d \leq \frac{1}{3} n^{\frac{1}{4}}.$$

1. Montrer que l'on a $q \leq \sqrt{n}$, $p \leq 2\sqrt{n}$ et $n - \varphi(n) \leq 3\sqrt{n}$.

2. On pose $k = \dfrac{ed-1}{\varphi(n)}$. Montrer que k et d sont premiers entre eux, et que l'on a $1 \leq k \leq d$.

3. Montrer que
$$\left| \frac{k}{d} - \frac{e}{n} \right| \leq \frac{1}{3d^2}. \tag{1}$$

4. Soit la fraction continue $[a_0, a_1, \ldots, a_r] = \dfrac{p_r}{q_r}$, où les a_i sont des nombres entiers vérifiant $a_i \geq 1$ pour $i \geq 1$. On pose $\theta = \dfrac{1+\sqrt{5}}{2} = 1.618\ldots$. Montrer que $q_r \geq \theta^{r-1}$. On pourra utiliser, par la suite, l'inégalité $\theta > e^{1/4}$.

5. Montrer que, pour n et e donnés, le nombre de couples (d, k) solutions de l'inégalité (1), et vérifiant $2 \leq d \leq \frac{1}{3}n^{\frac{1}{4}}$ et $(k, d) = 1$ est inférieur à $\log n$. Donner un algorithme permettant de lister ces solutions.

6. Montrer comment un ennemi malicieux peut, à partir de la clé publique n et e, retrouver la clé de déchiffrement d parmi les solutions de (1).

Application :

Alice a choisi, et rendus publics, n et e,

$$n := 19525955760372385323658485866229443955978756 17$$

et

$$e := 155684402792930107560089282757296928825343 1945.$$

Bob, utilisant ces données, fait parvenir à Alice le message codé :

$$mc := 166441680900404906436818333800906458549994 4056.$$

Décoder le message mc et retrouver l'original m.