L7 CRM

Sommes de deux et quatre carrés

Alexandre Junod, Lycée Denis-de-Rougemont (Neuchâtel), alexandre.junod@rpn.ch

1 Sommes de deux carrés

Charles Hermite (1822-1901) a montré que si m divise r^2+1 (avec des entiers $m > r > 0$), alors $\frac{m}{r}$ admet une fraction continue palindromique de longueur paire, disons $\frac{m}{r} = [a_0, a_1, \ldots, a_n, a_n, \ldots, a_1, a_0]$, et la fraction irréductible $\frac{a}{b} = [a_n, \ldots, a_1, a_0]$ est telle que $m = a^2 + b^2$. Si on veut éviter la référence aux fractions continues, on peut dire qu'en itérant la transformation $(a; b) \longrightarrow (a'; b') = (b; a - b\lfloor a/b \rfloor)$ à partir de $(m; r)$ jusqu'à ce que $a' < \sqrt{m}$, on obtient finalement $m = (a')^2 + (b')^2$.

Exemples

- Avec $m = 274$ et $r = 237$, l'algorithme donne $(274; 237) \longrightarrow (237; 37) \longrightarrow (37; 15) \longrightarrow (15; 7)$ et on s'arrête car $15^2 < 274$. On a alors la décomposition $274 = 15^2 + 7^2$.
- Soit $p = 4k + 1$ un nombre premier. Si on le soustrait à chaque facteur de $(2k)! = 1 \cdot 2 \cdots 2k$, on obtient modulo p la congruence $(2k)! \equiv (4k)(4k-1)\cdots(2k+1)(-1)^{2k}$. En la multipliant par $(2k)!$, on trouve $[(2k)!]^2 \equiv (4k)! = (p-1)! \equiv -1$ grâce au théorème de Wilson [1]. Ainsi p divise $r^2 + 1$ avec $r = (2k)!$ et est donc une somme de deux carrés (Fermat, ∼1607-1665).

Cherchant une généralisation pour traiter les sommes de quatre carrés, nous avons découvert un algorithme (a priori original) relié à des fractions continues dont les "coefficients" sont des entiers de Gauss. Les fidèles lecteurs du bulletin retrouveront donc sans surprise les matrices $\mathcal{M}(\cdot)$ utilisées dans nos différents articles traitant des fractions continues.

2 Algorithme

On considère trois nombres entiers $m > 0$, r et s tels que m divise $r^2 + s^2 + 1$. Pour $k = 0$, on pose

$$\begin{array}{|ccccc|} \hline & & & a_{k-1} & b_{k-1} \\ m_k & r_k & s_k & a_k & b_k \\ \hline \end{array} = \begin{array}{|ccccc|} \hline & & & 0 & 0 \\ m & r & s & 1 & 0 \\ \hline \end{array}$$

et on définit inductivement

$$m_{k+1} = \frac{r_k^2 + s_k^2 + 1}{m_k}, \quad r_{k+1} = r_k - m_{k+1}\left[\frac{r_k}{m_{k+1}}\right], \quad s_{k+1} = m_{k+1}\left[\frac{s_k}{m_{k+1}}\right] - s_k$$

$$a_{k+1} = a_{k-1} + a_k\left[\frac{r_k}{m_{k+1}}\right] - b_k\left[\frac{s_k}{m_{k+1}}\right], \quad b_{k+1} = b_{k-1} + b_k\left[\frac{r_k}{m_{k+1}}\right] + a_k\left[\frac{s_k}{m_{k+1}}\right]$$

où $[x]$ est l'entier le plus proche de x. La fonction $x \mapsto [x]$ est impaire si on convient d'arrondir tout demi-entier positif à l'entier inférieur et tout demi-entier négatif à l'entier supérieur.

1. Alors que les nombres 1 et $p-1$ sont leurs propres inverses modulo p, les éléments de l'ensemble $\{2, 3, \ldots, p-2\}$ peuvent être regroupés en $\frac{p-3}{2}$ paires $(x; y)$ avec $x \cdot y \equiv 1 \pmod{p}$, donc leur produit vaut 1 (modulo p).

Nous allons montrer que cet algorithme conduit forcément à un indice $N > 0$ tel que $m_N = 1$ et que l'on obtient alors la décomposition $m = a_{N-1}^2 + b_{N-1}^2 + a_N^2 + b_N^2$.

Exemple : Avec $m = 534$, $r = 323$ et $s = 134$, l'algorithme (détaillé ci-contre) donne $534 = 5^2 + 12^2 + 19^2 + (-2)^2$.

k	m_k	r_k	s_k	a_k	b_k
-1				0	0
0	534	323	134	1	0
1	229	94	95	1	1
2	78	16	-17	1	2
3	7	2	3	7	3
4	2	0	-1	5	12
5	1	0	0	19	-2

Proposition 1. Il existe un indice minimal N tel que $m_N = 1$. Plus précisément, on a une suite décroissante d'entiers $m_1 > m_2 > \ldots > m_N = 1$ et $m_k = 1$ si $k \geqslant N$.

Preuve. Les nombres m_0, m_1, r_0 et s_0 sont entiers non nuls et on procède par induction. Le nombre $m_{k+1}m_{k+2} = r_{k+1}^2 + s_{k+1}^2 + 1$ est égal à

$$\underbrace{(r_k^2 + s_k^2 + 1)}_{m_k m_{k+1}} + m_{k+1}^2 \left(\left[\frac{r_k}{m_{k+1}}\right]^2 + \left[\frac{s_k}{m_{k+1}}\right]^2 \right) - 2m_{k+1} \left(r_k \left[\frac{r_k}{m_{k+1}}\right] + s_k \left[\frac{s_k}{m_{k+1}}\right] \right).$$

Comme $m_{k+1} \neq 0$, on en déduit la relation $(*)$:

$$m_{k+2} = m_k + m_{k+1} \left(\left[\frac{r_k}{m_{k+1}}\right]^2 + \left[\frac{s_k}{m_{k+1}}\right]^2 \right) - 2 \left(r_k \left[\frac{r_k}{m_{k+1}}\right] + s_k \left[\frac{s_k}{m_{k+1}}\right] \right)$$

et donc m_{k+2} est un entier. Comme $|r_{k+1}| = \left| \dfrac{r_k}{m_{k+1}} - \left[\dfrac{r_k}{m_{k+1}}\right] \right| \cdot |m_{k+1}| \leqslant \dfrac{1}{2}|m_{k+1}|$ et de manière similaire $|s_{k+1}| \leqslant \dfrac{1}{2}|m_{k+1}|$, on peut écrire

$$m_{k+2} = \frac{r_{k+1}^2 + s_{k+1}^2 + 1}{m_{k+1}} \leqslant \frac{0.5m_{k+1}^2 + 1}{m_{k+1}} = \frac{m_{k+1}}{2} + \frac{1}{m_{k+1}}.$$

Si $m_{k+1} \geqslant 2$, alors $m_{k+2} < \frac{1}{2}m_{k+1} + 1 \leqslant m_{k+1}$. Ainsi $m_{k+1} > m_{k+2} > 0$. Il existe un indice minimal N tel que $m_N = 1$ et on a alors $r_N = s_N = 0$, $m_{N+1} = 1$. □

Proposition 2. Si $m_N = 1$, alors $m = a_{N-1}^2 + b_{N-1}^2 + a_N^2 + b_N^2$.

Preuve. Nous adoptons les notations suivantes :

$$\mathcal{M}(\alpha) = \begin{pmatrix} \alpha & 1 \\ 1 & 0 \end{pmatrix} \quad , \quad \alpha_k = \left[\frac{r_k}{m_{k+1}}\right] + i\left[\frac{s_k}{m_{k+1}}\right] \quad , \quad \beta_k = r_k + is_k.$$

On a la relation $m_{k+1}\alpha_k + \overline{\beta_{k+1}} = \beta_k$ et, par conjugaison complexe, $m_{k+1}\overline{\alpha_k} + \beta_{k+1} = \overline{\beta_k}$. De plus, la relation $(*)$ dans la preuve précédente se reformule $m_{k+2} = m_k + m_{k+1}|\alpha_k|^2 - 2\,\mathrm{Re}(\alpha_k\overline{\beta_k})$. On vérifie alors que

$$\mathcal{M}(\overline{\alpha_k}) \begin{pmatrix} m_{k+1} & \overline{\beta_{k+1}} \\ \beta_{k+1} & m_{k+2} \end{pmatrix} \mathcal{M}(\alpha_k) = \begin{pmatrix} m_k & \overline{\beta_k} \\ \beta_k & m_{k+1} \end{pmatrix}.$$

En itérant cette formule dans le membre de gauche et en utilisant les valeurs $m_N = m_{N+1} = 1$ et $\beta_N = 0$, on obtient la relation matricielle $(**)$:

$$\begin{pmatrix} m_k & \overline{\beta_k} \\ \beta_k & m_{k+1} \end{pmatrix} = \mathcal{M}(\overline{\alpha_k})\mathcal{M}(\overline{\alpha_{k+1}}) \cdots \mathcal{M}(\overline{\alpha_{N-1}})\mathcal{M}(\alpha_{N-1}) \cdots \mathcal{M}(\alpha_{k+1})\mathcal{M}(\alpha_k).$$

Si on pose $\theta_k = a_k + ib_k$, on a $\alpha_k\theta_k + \theta_{k-1} = \theta_{k+1}$ et

$$\begin{pmatrix}\theta_N\\ \theta_{N-1}\end{pmatrix} = \mathcal{M}(\alpha_{N-1})\begin{pmatrix}\theta_{N-1}\\ \theta_{N-2}\end{pmatrix} = \ldots = \mathcal{M}(\alpha_{N-1})\mathcal{M}(\alpha_{N-2})\cdots\mathcal{M}(\alpha_0)\begin{pmatrix}1\\ 0\end{pmatrix}$$

car $\theta_0 = 1$ and $\theta_{-1} = 0$. Après transposition et conjugaison complexe, on obtient

$$(\overline{\theta_N} \quad \overline{\theta_{N-1}}) = (1 \quad 0)\mathcal{M}(\overline{\alpha_0})\mathcal{M}(\overline{\alpha_1})\cdots\mathcal{M}(\overline{\alpha_{N-1}}).$$

Ainsi, la relation $(**)$ avec $k = 0$ se reformule

$$\begin{pmatrix} m & \overline{\beta_0}\\ \beta_0 & m_1\end{pmatrix} = \begin{pmatrix} \overline{\theta_N} & \overline{\theta_{N-1}}\\ \cdots & \cdots\end{pmatrix}\begin{pmatrix}\theta_N & \cdots\\ \theta_{N-1} & \cdots\end{pmatrix}$$

et on conclut en comparant les coefficients dans le coin supérieur gauche. □

Sommes de deux carrés. Si un nombre m divise r^2+1 (comme c'est le cas pour tout nombre premier $p \equiv 1 \pmod 4$), on peut considérer $s = 0$ dans l'algorithme. On a alors $s_k = 0$ et $b_k = 0$ pour tout indice k si bien que lorsque $m_N = 1$, on trouve la décomposition $m = a_{N-1}^2 + a_N^2$. Toujours dans ce cas, on peut montrer qu'on peut remplacer $[\,\cdot\,]$ par $\lfloor\,\cdot\,\rfloor$, que l'algorithme fournit la fraction continue de m/r et qu'il démontre le résultat d'Hermite évoqué dans le premier paragraphe.

3 Sommes de quatre carrés

Le théorème de Lagrange (1736 – 1813) affirme que tout nombre naturel est la somme d'au plus quatre carrés d'entiers. Il découle immédiatement de notre algorithme et du résultat suivant.

Proposition 3. Soit m un entier positif. Alors il existe deux entiers r et s tels que m divise r^2+s^2+1 si, et seulement si m n'est pas divisible par 4.

Preuve. Modulo 4, $r^2 + s^2 + 1$ ne peut être congru qu'à 1 (si r et s sont pairs), 2 (si r et s ont des parités différentes) ou 3 (si r et s sont impairs). Ainsi, aucun diviseur de $r^2 + s^2 + 1$ ne peut être divisible par 4. On peut démontrer la réciproque avec le théorème de la progression arithmétique de Dirichlet (1805-1859).

- Si $m \equiv 2 \pmod 4$, alors $4m$ et $m - 1$ sont premiers entre eux car tout diviseur commun divise $4m - 4(m - 1) = 4$ alors que $m - 1$ est impair. Par le théorème de Dirichlet, il existe un nombre premier $p = (m - 1) + n \cdot 4m$. Il est congru à 1 modulo 4 et on a $p = qm - 1$ avec $q = 4n + 1$.
- Si m est impair (c'est-à-dire si $m \equiv \pm 1 \pmod 4$), alors $4m$ et $2m^2 - 1$ sont premiers entre eux car tout diviseur commun divise $m(4m) - 2(2m^2 - 1) = 2$ alors que $2m^2 - 1$ est impair. Par le théorème de Dirichlet, il existe un nombre premier $p = (2m^2-1)+n\cdot 4m$. Il est congru à 1 modulo 4 et on peut écrire $p = qm - 1$ avec $q = 4n + 2m$.

Dans tous les cas, on a trouvé un nombre premier $p = 4k + 1$. Ce nombre divise $r^2 + 1$ avec $r = (2k)!$ (selon l'exemple du premier paragraphe) et l'algorithme (avec $s = 0$) permet de l'exprimer comme une somme de deux carrés : $p = qm - 1 = r^2 + s^2$. Il s'ensuit que m divise $qm = r^2 + s^2 + 1$. □

Remarque. Le recours au théorème de Dirichlet dont la preuve est compliquée peut déplaire. Habituellement, on démontre la proposition lorsque $m = p$ est un nombre premier impair avec le principe des tiroirs. Les ensembles $\{r^2 : r = 0, 1, 2, \ldots, \frac{p-1}{2}\}$ et $\{-1 - s^2 : s = 0, 1, 2, \ldots, \frac{p-1}{2}\}$ admettent chacun $\frac{p+1}{2}$ éléments distincts [2] modulo p. Comme on dénombre $p+1$ éléments au total, deux éléments

2. Si $r_1^2 \equiv r_2^2 \pmod p$, alors p divise $r_1^2 - r_2^2 = (r_1 - r_2)(r_1 + r_2)$, donc p divise $r_1 + r_2 \in \{0, 1, \ldots, p - 1\}$, ce qui n'est possible que si $r_1 = r_2 = 0$, ou p divise $|r_1 - r_2| \in \{0, 1, \ldots, \frac{p-1}{2}\}$, auquel cas $r_1 = r_2$ également.

coïncident modulo p : il existe r et s tels que $r^2 \equiv -1 - s^2 \pmod{p}$, autrement dit p divise r^2+s^2+1. On montre ensuite par l'absurde (ou historiquement par une descente infinie) que p est une somme de quatre carrés (on peut maintenant simplement invoquer notre algorithme) et on conclut avec la relation $(|a|^2+|b|^2)(|\alpha|^2+|\beta|^2) = |a\alpha+b\beta|^2+|b\alpha-a\beta|^2$, valable pour tous les entiers de Gauss a, b, α, β : si deux nombres sont des sommes de quatre carrés, il en est alors de même de leur produit.

4 Vers des sommes de trois carrés

Notre algorithme fournit une preuve constructive du fait qu'un nombre m qui divise r^2+s^2+1 est une somme de quatre carrés. De nombreux essais laissent à penser que si m n'a aucun facteur carré et si $m+1$ n'est pas divisible par 8, alors il existe un couple $(r;s)$ pour lequel la décomposition obtenue comportera au moins un carré nul.

Nous pouvons énoncer trois cas où l'algorithme fournit une décomposition avec un carré nul.

- Si $s=0$ (autrement dit si m divise un nombre de la forme r^2+1), alors tous les nombres s_k et b_k sont nuls de sorte que lorsque $m_N=1$, on a $m = a_{N-1}^2 + a_N^2$.
- Si $s=1$ (autrement dit si m divise un nombre de la forme r^2+2), alors $s_k=(-1)^k$ et $b_k=0$ tant que $m_k>1$. Lorsque $m_N=1$, on a $b_N=(-1)^{N-1}a_{N-1}$, de sorte que $m = a_N^2 + 2a_{N-1}^2$.
- Si $s=r$ (autrement dit si m divise un nombre de la forme $2r^2+1$), on a $s_k=(-1)^k r_k$ alors que $b_k=0$ si k est pair et $b_k=a_k$ sinon (rappelons que la fonction $[\,\cdot\,]$ est impaire). Lorsque $m_N=1$, on trouve ainsi $m=2a_{N-1}^2+a_N^2$ si N est pair et $m=a_{N-1}^2+2a_N$ sinon.

De plus, dans tous ces cas, les nombres a_N et a_{N-1} sont premiers entre eux. Cela provient du fait que si un entier de Gauss divise $\theta_N = a_N + ib_N$ et θ_{N-1}, alors il divise également $\theta_{N-2} = \theta_N - \alpha_{N-1}\theta_{N-1}$ (avec les notations de la proposition 2) et, en itérant le raisonnement, il divise $\theta_1 = 1$.

697 divise 132^2+1

k	m_k	r_k	s_k	a_k	b_k
0	697	132	0	1	0
1	25	7	0	5	0
2	2	1	0	16	0
3	1	0	0	21	0

$697 = 16^2 + 21^2$

697 divise 585^2+2

m_k	r_k	s_k	a_k	b_k
697	585	1	1	0
491	94	−1	1	0
18	4	1	6	0
1	0	0	25	6

$697 = 25^2 + 2\cdot 6^2$

697 divise $2\cdot 97^2+1$

m_k	r_k	s_k	a_k	b_k
697	97	97	1	0
27	−11	11	4	4
9	−2	−2	−7	0
1	0	0	18	18

$697 = 2\cdot 18^2 + 7^2$

Proposition 4. Etant donné un entier $m \geqslant 2$, les assertions suivantes sont équivalentes.

1) il existe un entier r tel que r^2+1 est divisible par m,
2) il existe deux entiers a et b premiers entre eux tels que $m=a^2+b^2$,
3) m n'est pas divisible par 4 et tous ses diviseurs impairs sont congrus à 1 modulo 4.

On a aussi les équivalences suivantes.

1) il existe un entier r tel que r^2+2 est divisible par m,
2) il existe deux entiers a et b premiers entre eux tels que $m=a^2+2b^2$,
3) m n'est pas divisible par 4 et tous ses diviseurs impairs sont congrus à 1 ou à 3 modulo 8.

Preuve. On pose $D=1$ ou $D=2$ selon les équivalences que l'on cherche à démontrer. Les implications 1) $\Rightarrow$ 2) découlent directement de l'algorithme alors que leurs réciproques proviennent de la relation $(a^2+Db^2)(D\alpha^2+\beta^2) = (a\beta - Db\alpha)^2 + D$ si α et β vérifient l'identité de Bézout $\alpha a + \beta b = 1$ (valable si a et b sont premiers entre eux). Les implications 1) $\Rightarrow$ 3) sont faciles à établir : si m divise

$r^2 + D$, il en est de même pour tout diviseur d et on peut écrire $d = a^2 + Db^2$ (car 1) $\Rightarrow$ 2)), ce qui ne peut être congru modulo 8 qu'à 1, D, $1 + D$, $1 + 4D$ ou $4 + D$ lorsque a et b ne sont pas tous les deux pairs (modulo 8, un carré ne peut être congru qu'à 0, 1 ou 4). Les implications 3) $\Rightarrow$ 1) sont plus délicates à démontrer, par induction sur le nombre de facteurs premiers de m.

Ancrage. Montrons que si $m = p$ est un nombre premier vérifiant 3), alors il vérifie également 1).

- Il est clair que $p = 2$ vérifie les assertions 1).
- On a déjà vu que si $p \equiv 1 \pmod 4$, disons $p = 4k + 1$, alors p divise $[(2k)!]^2 + 1$.
- Si $p \equiv 3 \pmod 8$, disons $p = 8k + 3$, alors on considère le produit

$$\begin{aligned} 2^{4k+1}(4k+1)! &= 2^{4k+1}1 \cdot 2 \cdot 3 \cdots (4k+1) \\ &= 2 \cdot 4 \cdot 6 \cdots (4k) \cdot (4k+2) \cdot (4k+4) \cdots (8k+2). \end{aligned}$$

  En soustrayant p à chacun des $2k + 1$ facteurs plus grands que $4k$, on obtient modulo p

$$\begin{aligned} 2^{4k+1}(4k+1)! &\equiv 2 \cdot 4 \cdot 6 \cdots (4k) \cdot (-4k-1) \cdot (-4k+1) \cdots (-1) \\ &\equiv 2 \cdot 4 \cdot 6 \cdots (4k) \cdot (-1)^{2k+1}(4k+1) \cdot (4k-1) \cdots 1 \\ &\equiv (-1)^{2k+1}(4k+1)! \end{aligned}$$

  On en déduit que $2^{4k+1} \equiv -1 \pmod p$, et donc p divise $2(2^{4k+1} + 1) = (2^{2k+1})^2 + 2$.

- Si $p \equiv 1 \pmod 8$, disons $p = 8k + 1$, on peut procéder comme ci-dessus pour établir que $2^{4k}(4k)! \equiv (-1)^{2k}(4k)!$, c'est-à-dire $2^{4k} \equiv 1 \pmod p$. Le polynôme $P(x) = x^{(p-1)/2} - 1$ s'annule donc (modulo p) en $x = 2$.

  Remarquons que pour tout nombre $a \in \{1, 2, \ldots, \frac{p-1}{2}\}$, les ensembles $\{a, 2a, \ldots, (p-1)a\}$ et $\{1, 2, \ldots, p-1\}$ coïncident modulo p car chacun d'eux contient $p - 1$ éléments non nuls différents (modulo p). Le produit de leurs éléments est donc $a^{p-1}(p-1)! \equiv (p-1)! \pmod p$. Ainsi $a^{p-1} \equiv 1$ et le polynôme $P(x) = x^{(p-1)/2} - 1$ s'annule (modulo p) en $x = a^2$.

  Comme les nombres a^2 avec $a \in \{1, 2, \ldots, \frac{p-1}{2}\}$ sont tous différents modulo p (voir la note [2] du paragraphe 3) et qu'il y en a autant que le degré du polynôme, on a recensé exactement toutes les racines de $P(x)$ et on a vu que $x = 2$ est l'une d'elles. Il existe donc un nombre a tel que $a^2 \equiv 2 \pmod p$. Comme $p = 4(2k) + 1 \equiv 1 \pmod 4$, on a encore $[(4k)!]^2 \equiv -1 \pmod p$, donc $[a(4k)!]^2 = a^2[(4k)!]^2 \equiv -2 \pmod p$, autrement dit p divise $[a(4k)!]^2 + 2$.

Induction. Considérons un entier m et un nombre premier impair p qui vérifient l'assertion 3). Par hypothèse d'induction, il existe deux entiers r et k tels que $r^2 + D = km$. De plus, avec les considérations ci-dessus et le fait que 1) implique 2), on peut également trouver des entiers $a, b \geqslant 1$ tels que $p = a^2 + Db^2$. Ce nombre premier ne peut pas diviser à la fois $a + br$ et $a - br$ car sinon il diviserait $(a + br) + (a - br) = 2a \in \{2, \ldots, p - 1\}$ (la majoration $2a < p$ est évidente si $a = 1$ et si $a \geqslant 2$, on a $2a \leqslant a^2 < p$). En changeant le signe de b au besoin, on peut supposer que $a + br$ n'est pas divisible par p et on écrit $kmp = (r^2 + D)(a^2 + Db^2) = (ar - Db)^2 + D(a + br)^2$. Les nombres $ar - Db$ et $a + br$ sont premiers entre eux car tout diviseur commun divise $a(a + br) - b(ar - Db) = p$ alors que $a + br$ n'est pas divisible par p. Ainsi kmp vérifie l'assertion 2) qui implique 1) et mp vérifie également l'assertion 1). □

Références

[1] G. AURIOL, "*Sur les sommes de carrés*"
`http://auriolg.free.fr/doc/sommes_carres.pdf`

[2] P-J. HORMIÈRE, "*Théorèmes des deux, trois et quatre carrés*"
`https://lescoursdemathsdepjh.monsite-orange.fr`, rubrique "Algèbre générale"