Représentation d'un nombre par une somme de quatres carrés

PRIMES Switzerland

The Higher Arithmetic, H. Davenport's

Yunshu Ouyang Juraj Rosinsky

Tuteurs : Alan Morier et Charlotte Baumgart

Samedi 16 juin 2017

Table des matières

Nombre de la forme $4k + 3$

$n \pmod 4$	0	1	2	3
$n^2 \pmod 4$	0	1	$4 \equiv 0$	$9 \equiv 1$

Il y a trois possibilités pour $x^2 + y^2$:

- $x^2 \equiv y^2 \equiv 0 \pmod 4 \Longrightarrow x^2 + y^2 \equiv 0 \pmod 4$
- $x^2 \equiv y^2 \equiv 1 \pmod 4 \Longrightarrow x^2 + y^2 \equiv 2 \pmod 4$
- $x^2 \equiv 0 \pmod 4, y^2 \equiv 1 \pmod 4 \Longrightarrow x^2 + y^2 \equiv 1 \pmod 4$
  Par conséquent, un nombre de la forme $4k + 3$ ne peut pas être représenté par la somme de deux carrés.

Nombre pouvant être représenté par la somme de deux carrés

Lemme

Soit $N = x^2 + y^2$.
Soit $p_1^{\alpha_1} p_2^{\alpha_1} \cdots p_r^{\alpha_r}$ *la décomposition en facteurs premiers de* N.
Alors,

$$\forall p_i \equiv 3 \pmod 4,\ \alpha_i \equiv 0 \pmod 2$$

Nombre pouvant être représenté par la somme de deux carrés

Démonstration.

Soit N un nombre naturel. Soit q un facteur de N de la forme $4k+3$. Alors,

$$x^2 + y^2 \equiv 0 \pmod{N} \Longrightarrow x^2 \equiv -y^2 \pmod{q}$$

-1 est un non-residu quadratique de q, donc la seule solution à cette équivalence est $x \equiv y \equiv 0 \pmod{q}$.

$$q \mid x \text{ et } q \mid y \Longrightarrow q^2 \mid x^2 + y^2$$

Donc, $N = q^2 N_1$. Par répétition de cet argument, on trouve que la puissance de q qui divise N doit être pair. □

Représentation d'un premier de la forme $4k + 1$ par deux carrés

Théorème

Tout nombre premier p de la forme $4k + 1$ peut être représenté par la somme de deux carrés.

Lemme

Un multiple d'un premier p peut être représenté sous la forme z^2+1, cad. l'équation

$$z^2 + 1 \equiv 0 \pmod{p}$$

est soluble.

Démonstration.

Soit $p = 4k+1$.

$$z^2 \equiv -1 \pmod{p}$$

Or, d'après le critère d'Euler,

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{1}{2}(4k+1-1)} = (-1)^{2k} = 1$$

Donc, -1 est un résidu quadratique modulo p donc l'équation est soluble.

Lemme

$p = 4k + 1$ peut être représenté par la somme de deux carrés

Démonstration.

Soit $p = 4k + 1$. Par le lemme précédent, il existe un m tel que $mp = z^2 + 1$. SPGD, supposons que $-\frac{1}{2}p < z < \frac{1}{2}p$. Alors,

$$m = \frac{1}{p}(z^2 + 1) < \frac{1}{p}(\frac{1}{4}p^2 + 1) < p$$

$mp = x^2 + y^2$ est soluble pour $m < p$.

Démonstration (Cont.)

$mp = x^2 + y^2$ est soluble pour $m < p$.
Soit $-\frac{1}{2}m < u, v < \frac{1}{2}m$ tel que $u \equiv x \pmod{m}$ et $v \equiv y \pmod{m}$. Alors,

$$u^2 + v^2 \equiv x^2 + y^2 \equiv 0 \pmod{m}$$

$$\Longrightarrow \exists r, mr = u^2 + v^2$$

r ne peut pas être nul car cela impliquerait que $x \equiv y \equiv 0 \pmod{m}$, ce qui contredit $mp = x^2 + y^2$.

$$r = \frac{1}{m}(u^2 + v^2) \leq \frac{1}{m}(\frac{1}{4}m^2 + \frac{1}{4}m^2) < m$$

Démonstration (Cont.)

On a donc :

$$mp = x^2 + y^2$$
$$mr = u^2 + v^2$$

De plus, l'identité ci-dessous nous dit que le produit de deux sommes de deux carrés peut être représenté comme une somme de deux carrés :

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$$

Par conséquent,

$$\begin{aligned} m^2 rp &= mp \cdot mr \\ &= (x^2 + y^2)(u^2 + v^2) \\ &= (xu + yv)^2 + (xv - yu)^2 \end{aligned}$$

Démonstration (Cont.)

$$m^2 rp = (xu + yv)^2 + (xv - yu)^2$$

Or, $u \equiv x, v \equiv y \pmod{m}$,

$$\begin{aligned} xu + yv &\equiv x^2 + y^2 \equiv 0 \pmod{m} \\ xv - yu &\equiv xy - yx \equiv 0 \pmod{m} \end{aligned}$$

Par conséquent, en divisant l'équation par m^2, on obtient :

$$rp = X^2 + Y^2$$

Démonstration (Cont.)

$$rp = X^2 + Y^2$$

Nous avons donc prouver qu'il existe un $r < m$, pour tout m satisfaisant l'équation de base, tel que rp peut être représenté par la somme de deux carrés.
Par conséquent, il existe un $r = 1$ et donc, p peut être représenté par la somme de deux carrés. La représentation de p par une somme de deux carrés est unique. □

Représentation d'un nombre par deux carrés

- Tout nombre premier de la forme $4k + 1$ peut être représenté par la somme de deux carrés.
- Toute puissance paire d'un nombre premier de la forme $4k + 3$ peut être représenté par la somme de deux carrés : $(4k + 3)^{2l} = (4k + 3)^{2l} + 0^2$
- 2 peut être représenté comme la somme de deux carrés : $2 = 1^2 + 1^2$

Conséquence : un nombre $N = p_1^{\alpha_1} \cdot p_r^{\alpha_r}$ peut être représenté comme la somme de deux carrés si pour tout $p_i \equiv 3 \pmod 4$, $a_i \equiv 0 \pmod 2$.

Exemple (Représentation du nombre premier 277)

$$z^2 + 1 \equiv 0 \pmod{277}$$
$$60^2 + 1 = 3601 = 277 \cdot 13$$

$$mp = x^2 + y^2$$
$$13 \cdot 277 = 60^2 + 1^2$$
$$60^2 + 1^2 \equiv (-5)^2 + 1^2 \pmod{13}$$

$$mr = u^2 + v^2$$
$$13 \cdot 2 = 25 + 1 = (-5)^2 + 1^2$$

$$\begin{aligned} m^2 rp &= 13^2 \cdot 2 \cdot 277 \\ &= (x^2 + y^2)(u^2 + v^2) \\ &= (60^2 + 1^2)((-5)^2 + 1^2) \\ &= (xu + yv)^2 + (xv - yu)^2 \\ &= (-299)^2 + 65^2 \end{aligned}$$

On obtient alors,

$$2 \cdot 277 = (-23)^2 + 5^2$$

On refait la même chose ($m = 2$) :

$$(-23)^2 + 5^2 \equiv 1^2 + 1^2 \pmod 2$$
$$2 \cdot 1 = 1^2 + 1^2$$
$$2^2 \cdot 1 \cdot 277 = (-18)^2 + (-28)^2$$
$$277 = 9^2 + 14^2$$

Par conséquent,

$$277 = 9^2 + 14^2$$

Représentation d'un premier de la forme $4k + 3$ par quatre carrés

Théorème

Tout nombre premier p de la forme $4k + 3$ peut être représenté par la somme de quatre carrés.

Lemme

Un multiple d'un premier p peut être représenté sous la forme $x^2 + y^2 + 1$, c'est à dire que l'équation

$$x^2 + y^2 + 1 \equiv 0 \pmod{p}$$

est soluble.

Démonstration.

Soit $p = 4k + 3$.

$$x^2 + 1 \equiv -y^2 \pmod{p}$$

Cette équation est soluble car $-y^2$ est toujours un non-résidu quadratique. x^2 étant un résidu quadratique, pour trouver une solution, il suffit de trouver un résidu quadratique Y et un non-résidu quadratique X tel que $X + 1 = Y$, ce qui est le cas pour les premiers de la forme $4k + 3$.

Lemme

p peut être représenté par la somme quatre carrés

Démonstration.

Soit $p = 4k + 3$ Par le lemme précédent, il existe un m tel que $mp = x^2 + y^2 + 1$. SPDG, supposons que $-\frac{1}{2}p < x, y < \frac{1}{2}p$. Alors,

$$m = \frac{1}{p}(x^2 + y^2 + 1) < \frac{1}{p}(\frac{1}{4}p^2 + \frac{1}{4}p^2 + 1) < p$$

$mp = x^2 + y^2 + z^2$ est soluble pour $m < p$. Donc
$mp = x^2 + y^2 + z^2 + w^2$ est également soluble en mettant $w = 0$.

Démonstration (Cont.)

$mp = x^2 + y^2 + z^2 + w^2$ est soluble pour $m < p$.
Soit $-\frac{1}{2}m < a, b, c, d < \frac{1}{2}m$ tel que $a \equiv x \pmod{m}$, $b \equiv y \pmod{m}$, $c \equiv z \pmod{m}$ et $d \equiv w \pmod{m}$. Alors,

$$a^2 + b^2 + c^2 + d^2 \equiv x^2 + y^2 + z^2 + w^2 \equiv 0 \pmod{m}$$

$$\Longrightarrow \exists r, mr = a^2 + b^2 + c^2 + d^2$$

Démonstration (Cont.)

r ne peut pas être nul car cela impliquerait que $x \equiv y \equiv z \equiv w \equiv 0 \pmod{m}$, ce qui contredit $mp = x^2 + y^2 + z^2 + w^2$.

$$r = \frac{1}{m}(a^2 + b^2 + c^2 + d^2) \leq \frac{1}{m}(\frac{1}{4}m^2 + \frac{1}{4}m^2 + \frac{1}{4}m^2 + \frac{1}{4}m^2) = m$$

$r = m$ seulement si $a, b, c, d \equiv \frac{m}{2} \pmod{m}$ et donc
$x, y, z, w \equiv \frac{m^2}{4} \pmod{m}$ et $mp \equiv 0 \pmod{m^2}$.
Donc m divise p, ce qui est impossible et $r < m$.

Démonstration (Cont.)

On a donc :

$$mp = x^2 + y^2 + z^2 + w^2$$
$$mr = a^2 + b^2 + c^2 + d^2$$

De plus, nous connaissons l'identité d'Euler qui permet d'écrire un produit de deux sommes de quatre carrés sous la forme d'une somme de quatre carré :

$$(x^2 + y^2 + z^2 + w^2)(a^2 + b^2 + c^2 + d^2)$$

$$= (ax + by + cz + dw)^2 + (ay - bx - cw + dz)^2$$

$$+(az + bw - cx - dy)^2 + (aw - bz + cy - dx)^2$$

Démonstration (Cont.)

Par conséquent,

$$m^2 rp = mp \cdot mr$$

$$= (x^2 + y^2 + z^2 + w^2)(a^2 + b^2 + c^2 + d^2)$$

$$= (ax + by + cz + dw)^2 + (ay - bx - cw + dz)^2$$

$$+(az + bw - cx - dy)^2 + (aw - bz + cy - dx)^2$$

$$= X^2 + Y^2 + Z^2 + W^2$$

Démonstration (Cont.)

$$m^2 rp = X^2 + Y^2 + Z^2 + W^2$$

Or, $a \equiv x \pmod{m}$, $b \equiv y \pmod{m}$, $c \equiv z \pmod{m}$ et $d \equiv w \pmod{m}$.
Donc $X, Y, Z, W \equiv 0 \pmod{m}$
Par conséquent, en divisant l'équation par m^2, on obtient :

$$rp = X^2 + Y^2 + Z^2 + W^2$$

Démonstration (Cont.)

$$rp = X^2 + Y^2 + Z^2 + W^2$$

Nous avons donc prouver qu'il existe un $r < m$, pour tout m satisfaisant l'équation de base, tel que rp peut être représenté par la somme de quatre carrés.
Par conséquent, il existe un $r = 1$ et donc, tout p peut être représenté par la somme de quatre carrés.

□

Démonstration (Cont.)

Grâce à l'identité d'Euler, on sait que le produit de deux sommes de quatre carrés est aussi une somme de quatre carrés.
Donc tout nombre entier peut être écrit comme une somme de quatre carrés.

Exemple (Représentation de 103 avec une somme de quatre carrés)

Tout d'abord, il faut trouver deux nombres x et y tels que

$$x^2 + y^2 + 1 \equiv 0 \pmod{103}$$

On trouve $x = 10, y = 38$.
On a donc $10^2 + 38^2 + 1 = 15 \cdot 103$
On regarde l'équation modulo 15 :

$$(-7)^2 + (-5)^2 + 1^2 + 0^2 = 15 \cdot 5$$

Exemple

On utilise l'identité d'Euler avec les quadruplets (38 ;10 ;1 ;0) et (-5 ;-7 ;1 ;0) :

$$[38^2 + 10^2 + 1^2 + 0^2][(-7)^2 + (-5)^2 + 1^2 + 0^2]$$

$$= (38\cdot(-7)+10\cdot(-5)+1\cdot 1+0\cdot 0)^2+(38\cdot(-5)-10\cdot(-7)-1\cdot 0+0\cdot 1)^2$$

$$+(38\cdot 1+10\cdot 0-1\cdot(-7)-0\cdot(-5))^2+(38\cdot 0-10\cdot 1+1\cdot(-5)-0\cdot(-7))^2$$

$$(-315)^2 + (-120)^2 + 45^2 + (-15)^2$$

Exemple

Chacun des 4 carrés est divisible par m^2, donc par 15^2 :

$$103 \cdot 5 = 21^2 + 8^2 + 3^2 + 1^2$$

On regarde l'équation modulo 5 et on obtient :

$$5 \cdot 2 = 1^2 + (-2)^2 + (-2)^2 + 1^2$$

En appliquant l'identité de Euler, on obtient :

$$103 \cdot 5^2 \cdot 2 = 0^2 + (-55)^2 + (-35)^2 + 30^2$$

$$103 \cdot 2 = 0^2 + 11^2 + 7^2 + 6^2$$

Exemple

En appliquant une dernière fois cette méthode, on trouve que 103 s'écrit sous la forme de 4 carrés de cette manière :

$$103 = 9^2 + 3^2 + 3^2 + 2^2$$

Remerciements

Nous sommes très heureux de remercier le MIT et en particulier Claude Eicher qui nous a fait l'honneur de regarder nos présentations. Nous sommes également redevables à l'Unige de nous avoir proposé ce projet à la suite du programme Athéna ainsi que à Alan Morier et Charlotte Baumgart pour leur investissement autour de ce projet qui nous a permis de beaucoup progresser en mathématiques.