Sommes de deux carrés

Marc Lorenzi

6 janvier 2024

Nous désignons par $\mathcal{C}$ l'ensemble des entiers naturels qui sont la somme de deux carrés, c'est à dire qui s'écrivent sous la forme $a^2 + b^2$ où $a, b \in \mathbb{Z}$.

$$\mathcal{C} = \{n \in \mathbb{N} : \exists a, b \in \mathbb{Z}, n = a^2 + b^2\}$$

L'objectif de cet article est de déterminer quels sont les entiers qui appartiennent à $\mathcal{C}$. Dans un premier temps nous allons parler de l'*algorithme d'Euclide étendu*. Nous déterminerons ensuite quels sont les nombres premiers qui appartiennent à $\mathcal{C}$. Il est facile de voir que les entiers congrus à 3 modulo 4 n'appartiennent pas à $\mathcal{C}$. En utilisant de façon judicieuse l'algorithme d'Euclide étendu, il est possible, étant donné un nombre premier p congru à 1 modulo 4, de montrer que $p \in \mathcal{C}$ et de construire de façon quasi-effective deux entiers a et b tels que $p = a^2 + b^2$: c'est l'objet du *Lemme de Thue*. Enfin, nous passerons aux entiers quelconques.

1 L'algorithme d'Euclide étendu

1.1 Rappels sur l'algorithme d'Euclide - Notations

On désigne par $\perp$ un objet n'appartenant pas à $\mathbb{N}$.

Soient $a, b \in \mathbb{N}$ vérifiant $a \geq b \geq 0$. On définit par récurrence deux suites $(r_i)_{i\in\mathbb{N}}$ et $(q_i)_{i\in\mathbb{N}^*}$ d'éléments de $\mathbb{N} \cup \{\perp\}$ en posant $r_0 = a$ et $r_1 = b$. Puis, pour tout $i \in \mathbb{N}$, si $r_{i+1} \neq \perp$ et $r_{i+1} \neq 0$, alors q_{i+1} et r_{i+2} sont le quotient et le reste de la division euclidienne de r_i par r_{i+1}. Plus explicitement, $0 \leq r_{i+2} < r_{i+1}$ et

$$r_i = q_{i+1}r_{i+1} + r_{i+2}$$

Si $r_{i+1} = \perp$ ou $r_{i+1} = 0$, alors $q_{i+1} = \perp$ et $r_{i+2} = \perp$.

Nous ne redémontrerons pas le résultat classique ci-dessous.

Proposition 1. *Il existe un unique entier $n_0 \geq 1$ tel que*

- $r_{n_0} = 0$.
- *Pour tout $i \in [\![0, n_0]\!]$, $r_i \in \mathbb{N}$.*
- *Pour tout $i \in [\![1, n_0 - 1]\!]$, $q_i \in \mathbb{N}^*$.*

- *La suite* $(r_i)_{1\leq i\leq n_0}$ *est une suite strictement décroissante d'entiers naturels.*
- $r_{n_0-1} = pgcd(a, b)$.

Remarque. Insistons sur le fait que, par notre choix de a et b, les quotients q_i et les restes r_i sont des entiers naturels.

Nous conservons jusqu'à la fin de cette section les notations que nous venons de mettre en place.

1.2 L'algorithme étendu

Définissons deux suites $(u_i)_{0\leq i\leq n_0}$ et $(v_i)_{0\leq i\leq n_0}$ en posant

$$u_0 = 1, v_0 = 0$$

$$u_1 = 0, v_1 = 1$$

et pour tout $i \in [\![0, n_0 - 2]\!]$,

$$u_{i+2} = u_i - q_{i+1}u_{i+1}$$

$$v_{i+2} = v_i - q_{i+1}v_{i+1}$$

La suite $\text{EEA}(a, b) = ((u_i, v_i, r_i))_{0\leq i\leq n_0}$ est la suite de *l'algorithme d'Euclide étendu* (Extended Euclidean Algorithm) associée à a et b. Nous allons maintenant montrer quelques propriétés de cette suite.

Proposition 2. *Pour tout* $i \in [\![0, n_0]\!]$, $au_i + bv_i = r_i$.

Démonstration. Montrons-le par une récurrence à deux termes sur i. C'est clair pour $i = 0, 1$. Soit $i \in [\![0, n-2]\!]$. Supposons $au_i+bv_i = r_i$ et $au_{i+1}+bv_{i+1} = r_{i+1}$. On a alors

$$\begin{aligned} au_{i+2} + bv_{i+2} &= a(u_i - q_{i+1}u_{i+1}) + b(v_i - q_{i+1}v_{i+1}) \\ &= (au_i + bv_i) - q_{i+1}(au_{i+1} + bv_{i+1}) \\ &= r_i - q_{i+1}r_{i+1} \\ &= r_{i+2} \end{aligned}$$

□

Proposition 3. *Pour tout* $i \in [\![0, n_0 - 1]\!]$, $u_iv_{i+1} - u_{i+1}v_i = (-1)^i$.

Démonstration. Faisons une récurrence sur i. Tout d'abord,

$$u_0v_1 - u_1v_0 = 1 = (-1)^0$$

Soit $i \in [\![0, n_0 - 2]\!]$. Supposons $u_i v_{i+1} - u_{i+1} v_i = (-1)^i$. On a alors

$$\begin{aligned} u_{i+1}v_{i+2} - u_{i+2}v_{i+1} &= u_{i+1}(v_i - q_{i+1}v_{i+1}) - (u_i - q_{i+1}u_{i+1})v_{i+1} \\ &= u_{i+1}v_i - u_i v_{i+1} \\ &= (-1)^{i+1} \end{aligned}$$

□

Proposition 4. *Pour tout $i \in [\![0, n_0]\!]$, $pgcd(u_i, v_i) = 1$.*

Démonstration. C'est immédiat par la proposition 3 et le théorème de Bézout. □

Proposition 5. *Pour tout $i \in \mathbb{N}$,*

- *Si $2i \leq n_0$ alors $u_{2i} \geq 0$ et $v_{2i} \leq 0$.*
- *Si $2i + 1 \leq n_0$ alors $u_{2i+1} \leq 0$ et $v_{2i+1} \geq 0$.*

Démonstration. Montrons-le par récurrence sur i. Tout d'abord, $0 \leq n_0$, $u_0 = 1 \geq 0$, $v_0 = 0 \leq 0$, et aussi $1 \leq n_0$, $u_1 = 0 \leq 0$ et $v_1 = 1 \geq 0$. Soit $i \in \mathbb{N}$. Supposons la propriété vraie pour i.

Supposons $2i + 2 \leq n_0$. On a donc aussi $2i \leq n_0$ et $2i + 1 \leq n_0$ donc, par l'hypothèse de récurrence, $u_{2i} \geq 0$ et $u_{2i+1} \leq 0$. De là,

$$u_{2i+2} = u_{2i} - q_{2i+1}u_{2i+1} \geq 0$$

et

$$u_{2i+3} = u_{2i+1} - q_{2i+2}u_{2i+2} \leq 0$$

On procède de même pour v_{2i+2} et v_{2i+3}. □

Proposition 6. *Pour tout $i \in [\![0, n_0 - 1]\!]$, $|v_i| \leq |v_{i+1}|$. Si $i \geq 1$, $|u_i| \leq |u_{i+1}|$.*

Démonstration. Montrons par récurrence sur i que pour tout $i \in [\![1, n_0 - 1]\!]$, $|u_i| \leq |u_{i+1}|$. Comme $u_1 = 0$ c'est clair pour $i = 1$. Soit $i \in [\![1, n_0 - 2]\!]$. Supposons $|u_i| \leq |u_{i+1}|$. Si i est pair, on a par la proposition 5, $u_i \geq 0$, $u_{i+1} \leq 0$ et $u_{i+2} \geq 0$. On a également $q_{i+1} \geq 1$. De là,

$$\begin{aligned} |u_{i+2}| &= u_{i+2} \\ &= u_i - q_{i+1}u_{i+1} \\ &= |u_i| + q_{i+1}|u_{i+1}| \\ &\geq [u_{i+1}| \end{aligned}$$

et de même si i est impair. La preuve pour les v_i est identique. □

Proposition 7. *Pour tout $i \in [\![1, n_0]\!]$, $r_{i-1}|v_i| \leq a$ et $r_{i-1}|u_i| \leq b$.*

Démonstration. Soit $i \in [\![1, n_0]\!]$. On a

$$\begin{aligned} au_{i-1} + bv_{i-1} &= r_{i-1} \\ au_i + bv_i &= r_i \end{aligned}$$

Éliminons b de ces deux égalités :

$$a(u_{i-1}v_i - v_{i-1}u_i) = r_{i-1}v_i - r_iv_{i-1}$$

Par la proposition 3, $u_{i-1}v_i - v_{i-1}u_i = (-1)^{i-1}$ et donc

$$a = (-1)^{i-1}(r_{i-1}v_i - r_iv_{i-1})$$

Par la proposition 5, v_i et v_{i-1} sont de signes opposés. On a donc

$$a = |a| = |r_{i-1}v_i - r_iv_{i-1}| = r_{i-1}|v_i| + r_i|v_{i-1}|$$

Ainsi, $r_{i-1}|v_i| \leq a$. De même, $r_{i-1}|u_i| \leq b$. □

Proposition 8. *Si $a > 0$ alors pour tout $i \in [\![1, n_0]\!]$, $|v_i| \leq a$ et $|u_i| \leq b$.*

Démonstration. Supposons $a > 0$. Pour tout $i \in [\![1, n_0]\!]$, $r_{i-1} \geq 1$. D'où le résultat par la proposition précédente. □

Proposition 9. *Si $a > 1$ et $b > 0$ alors $|v_{n_0-1}| \leq a/2$ et $|u_{n_0-1}| \leq b/2$.*

Démonstration. Supposons $a > 1$ et $b > 0$. Alors, $n_0 \geq 2$. De plus, $r_{n_0-2} > r_{n_0-1} > r_{n_0} = 0$, donc $r_{n_0-2} \geq 2$. Par la proposition 7,

$$2|v_{n_0-1}| \leq r_{n_0-2}|v_{n_0-1}| \leq a$$

De même,

$$2|u_{n_0-1}| \leq r_{n_0-2}|u_{n_0-1}| \leq b$$

□

1.3 Un exemple

Prenons $a = 1317$ et $b = 315$. On a $n_0 = 9$ et $pgcd(a, b) = 3$. Le tableau ci-dessus donne les valeurs des termes de la suite EEA(a, b). On retrouve bien toutes les caractéristiques montrées dans les propositions précédentes : alternance des signes des u_i et des v_i, croissance des $|u_i|$ à partir du rang 1, croissance des v_i dès le rang 0.

i	u_i	v_i	r_i
0	1	0	1317
1	0	1	795
2	1	-1	522
3	-1	2	273
4	2	-3	249
5	-3	5	24
6	32	-53	9
7	-67	111	6
8	99	-164	3
9	-265	439	0

1.4 Le lemme de Thue

Venons-en au lemme de Thue qui sera la clé pour la décomposition en somme de carrés d'un nombre premier. Pour pouvoir nous y référer plus facilement, nous reprenons toutes les notations et les hypothèses nécessaires dans l'énoncé du lemme.

Proposition 10. [Lemme de Thue]

Soient $a, b, r^*, v^* \in \mathbb{Z}$. On suppose que $0 \leq b < a$ et $0 < r^* \leq a < r^* v^*$. Soit $\mathrm{EEA}(a,b) = ((u_i, v_i, r_i))_{0 \leq i \leq n_0}$ la suite de l'algorithme d'Euclide étendu associé à a et b. Alors,

- *Il existe $j \in [\![0, n_0]\!]$ tel que $0 \leq r_j < r^*$.*
- *En prenant un tel j minimal, on a*

$$\begin{cases} r_j \equiv bv_j \bmod a \\ 0 \leq r_j < r^* \\ 0 < |v_j| < v^* \end{cases}$$

Démonstration. Soit

$$E = \{j \in [\![0, n_0]\!] : r_j < r^*\}$$

$r_{n_0} = 0 < r^*$ donc $n_0 \in E$. Ainsi, E est une partie non vide de $\mathbb{N}$, donc possède un plus petit élément j. Comme $r_0 = a \geq r^*$, $0 \notin E$ donc $j \geq 1$. On a $0 \leq j - 1 < j$ donc $r_{j-1} \geq r^*$. Par la proposition 7,

$$|v_j| \leq \frac{a}{r_{j-1}} \leq \frac{a}{r^*} < v^*$$

Comme $j \geq 1$, on a $|v_j| \geq |v_1| > 0$. Enfin, par la proposition 2, $r_j = au_j + bv_j$ donc $r_j \equiv bv_j \bmod a$. □

2 Résidus quadratiques

2.1 Introduction

Dans cette section, p désigne un nombre premier impair. Nous noterons $\mathbb{Z}_p$ le corps des entiers modulo p et $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\}$ le groupe des inversibles de $\mathbb{Z}_p$. Enfin, pour tout $x \in \mathbb{Z}$, nous noterons $[x]$ la classe de x modulo p.

2.2 Résidus

Soit $f : \mathbb{Z}_p^\times \longrightarrow \mathbb{Z}_p^\times$ définie pour tout $x \in \mathbb{Z}_p^\times$ par $f(x) = x^2$.

Proposition 11. *f est un endomorphisme du groupe $\mathbb{Z}_p^\times$.*

Démonstration. Pour tous $x, y \in \mathbb{Z}_p^\times$,

$$f(xy) = (xy)^2 = x^2y^2 = f(x)f(y)$$

□

Nous noterons $Q_p = \mathrm{Im}(f)$. Q_p est l'ensemble des *résidus quadratiques*. Comme image d'un morphisme de groupes, Q_p est un sous-groupe de $\mathbb{Z}_p^\times$.

Exemple. Prenons $p = 11$. Voici les images par f des éléments de $\mathbb{Z}_{11}$.

x	1	2	3	4	5	6	7	8	9	10
$f(x)$	1	4	9	5	3	3	5	9	4	1

Q_{11} est donc de cardinal 5 et

$$Q_{11} = \{1, 3, 4, 5, 9\}$$

Exemple. Prenons $p = 17$. Les images par f des éléments de $\mathbb{Z}_{17}$ sont

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$f(x)$	1	4	9	16	8	2	15	13	13	15	2	8	16	9	4	1

Q_{17} est donc de cardinal 8 et

$$Q_{17} = \{1, 2, 4, 8, 9, 13, 15, 16\}$$

Remarquons une différence entre ces deux exemples qui s'avérera essentielle plus tard : $-1 = 16 \in Q_{17}$ alors que $-1 = 10 \notin Q_{11}$.

2.3 Caractérisation

Proposition 12. Ker(f) $= \{-1, 1\}$.

Démonstration. Soit $x \in \mathbb{Z}_p^\times$. On a $x \in \mathrm{Ker}(f)$ si et seulement si $x^2 = 1$, ou encore $(x-1)(x+1) = 0$. Comme $\mathbb{Z}_p$ est un corps, ceci équivaut à $x = \pm 1$. □

Proposition 13. $|Q_p| = (p-1)/2$.

Démonstration. On a la réunion dsjointe

$$\bigcup_{a \in Q_p} f^{-1}(\{a\}) = \mathbb{Z}_p^\times$$

et donc

$$\sum_{a \in Q_p} |f^{-1}(\{a\})| = |\mathbb{Z}_p^\times| = p-1$$

Soit $a \in \mathbb{Q}_p$. soit $x \in \mathbb{Z}_p^\times$ tel que $f(x) = a$. Soit $y \in \mathbb{Z}_p^\times$. On a $f(y) = a$ si et seulement si $y^2 = a = x^2$, ou encore $(y-x)(y+x) = 0$. Comme $\mathbb{Z}_p$ est intègre, ceci équivaut à $y = \pm x$. De plus, $p \neq 2$ donc $-1 \neq 1$. On en déduit que $|f^{-1}(\{a\})| = 2$. Ainsi,

$$\sum_{a \in Q_p} |f^{-1}(\{a\})| = 2|Q_p|$$

□

Proposition 14. *Soit $x \in \mathbb{Z}_p^\times$. On a $x \in Q_p$ si et seulement si $x^{(p-1)/2} = 1$.*

Démonstration. Supposons que $x \in Q_p$. Soit $y \in \mathbb{Z}_p^\times$ tel que $y^2 = x$. Par le petit théorème de Fermat, $x^{(p-1)/2} = y^{p-1} = 1$. Inversement, considérons le polynôme $P = X^{(p-1)/2} - 1 \in \mathbb{Z}_p[X]$. Le polynôme P est de degré $(p-1)/2$ donc P a au plus $(p-1)/2$ racines. Or, nous venons de montrer que les $(p-1)/2$ éléments de Q_p sont des racines de P. Nous avons donc trouvé toutes les racines de P ? Conséquence, si $x \notin Q_p$ alors $P(x) \neq 0$ donc $x^{(p-1)/2} \neq 1$. □

Proposition 15. *Soit $x \in \mathbb{Z}_p^\times$. On a $x \notin Q_p$ si et seulement si $x^{(p-1)/2} = -1$.*

Démonstration. Soit $y = x^{(p-1)/2}$. On a $y^2 = x^{p-1} = 1$ donc $y = \pm 1$. Comme $x \notin Q_p$, $y \neq 1$. □

Proposition 16. *Soient $x, y \in \mathbb{Z}_p^\times$.*

- *Si $x \in \mathbb{Q}_p$ et $y \in \mathbb{Q}_p$ alors $xy \in Q_p$.*
- *Si $x \in \mathbb{Q}_p$ et $y \notin \mathbb{Q}_p$ alors $xy \notin Q_p$.*
- *Si $x \notin \mathbb{Q}_p$ et $y \notin \mathbb{Q}_p$ alors $xy \in Q_p$.*

Démonstration. Les deux premiers points résultent immédiatement de la structure de groupe de Q_p. Supposons $x, y \notin Q_p$. Pour le dernier point,

$$(xy)^{(p-1)/2} = x^{(p-1)/2} y^{(p-1)/2} = (-1)^2 = 1$$

donc $xy \in Q_p$. $\square$

Remarque. Soit $x \in \mathbb{Z}_p^\times$. Nous disposons d'un algorithme simple pour déterminer si $x \in Q_p$. Il suffit de calculer $x^{(p-1)/2}$ par une exponentiation rapide. Si $x \in Q_p$, déterminer $y \in \mathbb{Z}_p^\times$ tel que $y^2 = x$ est une tout autre histoire. Il existe des algorithmes efficaces pour trouver un tel y, par exemple l'algorithme de *Tonnelli-Shanks*. Nous n'en parlerons pas ici.

2.4 Racines carrées de -1

Proposition 17. *$-1 \in Q_p$ si et seulement si $p \equiv 1 \bmod 4$.*

Démonstration. $-1 \in Q_p$ si et seulement si $(-1)^{(p-1)/2} \equiv 1 \bmod p$, c'est à dire $(p-1)/2$ est pair. $\square$

Remarque. Soit p un nombre premier congru à 1 modulo 4. Il existe un algorithme très simple pour trouver une racine carrée de -1 modulo p. L'algorithme consiste à prendre un nombre x aléatoire dans $[\![1, p-1]\!]$. Par la proposition 13, la probabilité que x soit un non-résidu est $\frac{1}{2}$. On obtient donc facilement un tel x (sauf grande malchance) en très peu de tirages aléatoires : la probabilité de ne pas avoir trouvé un tel x après n tirages est $1/2^n$. Une fois obtenu $x \notin Q_p$, soit $y = x^{(p-1)/4}$. On a alors $y^2 = x^{(p-1)/2} = -1$.

3 Sommes de deux carrés

3.1 Introduction

Rappelons que $\mathcal{C}$ l'ensemble des entiers naturels qui sont la somme de deux carrés.

$$\mathcal{C} = \{n \in \mathbb{N} : \exists a, b \in \mathbb{Z}, n = a^2 + b^2\}$$

Par exemple, 0, 1, 2, 4, 5, 8, 9 et 10 appartiennent à $\mathcal{C}$. En revanche, 3, 6 et 7 n'appartiennent pas à $\mathcal{C}$.

Commençons par quelques résultats faciles.

Proposition 18. *Soit n un entier impair. Si $n \in \mathcal{C}$ alors $n \equiv 1 \bmod 4$.*

Démonstration. Supposons que $n = a^2 + b^2$ où $a, b \in \mathbb{Z}$. On a $a^2 \equiv 0 \bmod 4$ ou $a^2 \equiv 1 \bmod 4$ et de même pour b^2. De là, n est congru à 0, 1 ou 2 modulo 4. Comme n est impair, $n \equiv 1 \bmod 4$. $\square$

Proposition 19. *L'ensemble $\mathcal{C}$ est stable pour la multiplication.*

Démonstration. Soient $a, b, c, d \in \mathbb{Z}$. Posons $z = a + ib$ et $z' = c + id$. On a

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

□

Proposition 20. *Soit $n \in \mathbb{N}^*$. Écrivons $n = 2^k m$ où $k \in \mathbb{N}$ et m est un entier impair. Alors, $n \in \mathcal{C}$ si et seulement si $m \in \mathcal{C}$.*

Démonstration. Remarquons que $2 = 1^2 + 1^2 \in \mathcal{C}$. Par la proposition 19, $2^k \in \mathcal{C}$.

Supposons que $m \in \mathcal{C}$. Toujours par la proposition 19, $n \in \mathcal{C}$.

Montrons par récurrence sur k que si $n \in \mathcal{C}$ alors $m \in \mathcal{C}$. C'est évident pour $k = 0$. Soit $k \geq 1$. Supposons la propriété vraie pour $k-1$ et supposons que $n = 2^k m \in \mathcal{C}$. Soient $a, b \in \mathbb{Z}$ tels que $n = a^2 + b^2$. Comme $k \geq 1$, n est pair donc a et b sont de même parité. Posons $\alpha = (a+b)/2$ et $\beta = (a-b)/2$. On a

$$\alpha^2 + \beta^2 = \frac{1}{4}((a+b)^2 + (a-b)^2) = \frac{1}{2}(a^2 + b^2) = \frac{n}{2}$$

Ainsi, $2^{k-1}m = n/2 \in \mathcal{C}$. Par l'hypothèse de récurrence, $m \in \mathcal{C}$. □

Pour résumer l'intérêt des trois propriétés précédentes, pour déterminer $\mathcal{C}$ il suffit de déterminer quels sont les entiers impairs congrus à 1 modulo 4 qui appartiennent à $\mathcal{C}$. Commençons par les nombres premiers.

3.2 Le cas des entiers premiers

La proposition ci-dessous montre que tous les nombres premiers p congrus à 1 modulo 4 appartiennent à $\mathcal{C}$. Elle fait même mieux que cela puisque, à condition de connaître une racine carrée de -1 modulo p, elle permet de calculer de façon effective au moyen de l'algorithme d'Euclide étendu une décomposition de p en somme de deux carrés.

Proposition 21. *Soit p un nombre premier impair congru à 1 modulo 4. Soit $b \in [|0, p-1|]$ tel que $[b]^2 = -1$. Soit j l'indice du théorème de Thue associé à $n = p$, b et $r^* = v^* = \lfloor \sqrt{p} \rfloor + 1$. Alors, $r_j^2 + v_j^2 = p$.*

Démonstration. Remarquons tout d'abord que les données vérifient les hypothèses du lemme de Thue. Tout d'abord, $0 \leq b < p$ et $0 < r^*$. Ensuite,

$$r^* \leq \sqrt{p} + 1 \leq p$$

Enfin,

$$r^* v^* = (\lfloor \sqrt{p} \rfloor + 1)^2 > \sqrt{p}^2 = p$$

On a $r_j \equiv b v_j \bmod p$. En élevant au carré, $r_j^2 \equiv b^2 v_j^2 \equiv -v_j^2 \bmod p$ et donc

$$r_j^2 + v_j^2 \equiv 0 \bmod p$$

De plus, $0 \leq r_j \leq \lfloor \sqrt{p} \rfloor$ et $0 < |v_j| \leq \lfloor \sqrt{p} \rfloor$. De là,

$$0 < r_j^2 + v_j^2 \leq 2\lfloor \sqrt{p} \rfloor^2 < 2p$$

Ainsi, $r_j^2 + v_j^2 = p$. $\square$

Exemple. Prenons $p = 1009$. Une racine carrée de -1 modulo p est $b = 469$ (l'autre est $p - b = 540$). On a $r^* = 32$. L'algorithme d'Euclide étendu appliqué à p et b fournit les résultats suivants.

j	u_j	v_j	r_j
0	1	0	1009
1	0	1	469
2	1	-2	71
3	-6	13	43
4	7	-15	28

Le plus petit indice j pour lequel $r_j < r^*$ est $j = 4$, pour lequel $r_4 = 28$ et $v_4 = -15$. On a donc

$$1009 = 28^2 + 15^2$$

3.3 Le cas général

Notons $\mathcal{P}$ l'ensemble des nombres premiers, $\mathcal{P}_1$ l'ensemble des nombres premiers congrus à 1 modulo 4 et $\mathcal{P}_3$ l'ensemble des nombres premiers congrus à 3 modulo 4. On a l'union disjointe

$$\mathcal{P} = \{2\} \cup \mathcal{P}_1 \cup \mathcal{P}_3$$

Lemme 22. *Soient $a, b \in \mathbb{N}$. Soit $p \in \mathcal{P}_3$. On suppose que p divise $a^2 + b^2$. Alors, p divise a et b.*

Démonstration. *Ici, je ne sais pas faire sans passer par l'anneau $\mathbb{Z}[i]$.* L'entier p divise $(a + ib)(a - ib)$. Comme $p \in \mathcal{P}_3$, p est premier dans $\mathbb{Z}[i]$ donc, dans cet anneau, p divise l'un des facteurs du produit. Par exemple, p divise $a + ib$. Il existe donc $u, v \in \mathbb{Z}$ tels que

$$a + ib = p(u + iv)$$

De là, $a = pu$ et $b = pv$, donc p divise a et b. $\square$

Proposition 23. *Soit $n \in \mathbb{N}^*$. On a $n \in \mathcal{C}$ si et seulement si pour tout $p \in \mathcal{P}_3$, $\nu_p(n)$ est pair.*

Démonstration. Supposons que pour tout $p \in \mathcal{P}_3$, $\nu_p(n)$ est pair. On a alors

$$n = 2^{\nu_2(n)} \prod_{p \in \mathcal{P}_1} p^{\nu_p(n)} \prod_{p \in \mathcal{P}_3} (p^2 + 0^2)^{\nu_p(n)/2}$$

Chacun des facteurs de ce produit appartient à $\mathcal{C}$. Comme $\mathcal{C}$ est stable pour la multiplication, $n \in \mathcal{C}$.

Inversement, soit $p \in \mathcal{P}_3$. Montrons par récurrence forte sur n que pour tout $n \in \mathbb{N}^*$, si $n \in \mathcal{C}$ alors $\nu_p(n)$ est pair. Si $n = 1$ c'est clair puisque $\nu_p(1) = 0$.

Soit $n \geq 2$. Supposons la propriété vérifiée pour tous les entiers strictement inférieurs à n. Supposons que $n \in \mathcal{C}$. On a donc $n = a^2 + b^2$ où $a, b \in \mathbb{N}$. Si p ne divise pas n alors $\nu_p(n) = 0$ est pair. Sinon, par le lemme 22, p divise a et b. Écrivons $a = pa'$ et $b = pb'$ où $a', b' \in \mathbb{N}$. On a donc $n = p^2(a'^2 + b'^2)$. Posons $n' = a'^2 + b'^2$. L'entier n' appartient à $\mathcal{C}$ et $n' < n$. Par l'hypothèse de récurrence, $\nu_p(n')$ est pair. De là, $\nu_p(n) = 2 + \nu_p(n')$ est pair. $\square$

Exemple. Les entiers $n \leq 100$ qui sont sommes de deux carrés sont 0, 1, 2, 4, 5, 8, 9, 10, 13, 16, 17, 18, 20, 25, 26, 29, 32, 34, 36, 37, 40, 41, 45, 49, 50, 52, 53, 58, 61, 64, 65, 68, 72, 73, 74, 80, 81, 82, 85, 89, 90, 97, 98, 100.

Ceux qui ne sont pas sommes de deux carrés sont 3, 6, 7, 11, 12, 14, 15, 19, 21, 22, 23, 24, 27, 28, 30, 31, 33, 35, 38, 39, 42, 43, 44, 46, 47, 48, 51, 54, 55, 56, 57, 59, 60, 62, 63, 66, 67, 69, 70, 71, 75, 76, 77, 78, 79, 83, 84, 86, 87, 88, 91, 92, 93, 94, 95, 96, 99.