Concours SMF Junior 2017

Sujet 9. Théorie des nombres

Sommes de carrés dans $\mathbb{Z}/n\mathbb{Z}$

Rapport de correction

Bruno Deschamps (Université du Maine)

Il y a eu beaucoup de propositions de solutions, justes du point de vue mathématique, et il a été difficile de classer les meilleures. Les critères d'excellence retenus ont été l'originalité et le caractère élémentaire des arguments. Plusieurs solutions proposées utilisaient de gros (voire très gros) théorèmes tels que les théorèmes des deux et trois carrés, le lemme de Hensel, le théorème de progression arithmétique de Dirichlet. Nous avons donc considéré que *l'utilisation de bulldozers pour écraser une mouche* était un critère discriminant pour le palmarès, car peu en accord avec la tradition de subtilité en théorie des nombres. Comme nous allons le voir, il existait plusieurs façons totalement élémentaires d'arriver au résultat, et plusieurs d'entre elles étaient concises et élégantes. Certaines de ces solutions sont même présentables à un niveau L1-L2, ce qui est remarquable. Pour la notation, trois groupes ont été retenus :

0	• Preuve incomplète. • Erreur dans la preuve (sauf s'il y avait une idée très originale.) • Utilisation des théorèmes des deux et trois carrés, du lemme de Hensel ou du théorème de Dirichlet (sauf s'il y avait une idée très originale.)
5 – 8	• Preuve élémentaire faisant intervenir le théorème des quatre carrés ou ayant échappé au groupe précédent pour des raisons d'originalité.
9 – 10	• Preuve totalement élémentaire.

et le classement dans chaque groupe s'est fait au gré de la sensibilité du correcteur.

Pour ce qui est des preuves proposées, elles ont toutes, peu ou prou, suivi la même stratégie. Nous avons toutefois été à la fois surpris et ravis de découvrir une grande diversité d'idées avancées pour la résolution du problème. C'est sur les points clé qu'il y a eu des variantes d'arguments. Nous avons essayé dans la suite de synthétiser et présenter les différentes bonnes idées que nous avons rencontrées. Les participants au concours devraient ainsi tous pouvoir se retrouver dans ce qui suit.

Étape 1 : si $f : A \longrightarrow B$ est un morphisme d'anneaux et si $A_0 \subset A$ est une partie où tout élément est une somme de k carrés d'éléments de A et telle que $f(A_0) = B$, alors tout élément de B est une somme de k carrés.

Une conséquence immédiate de ce résultat est que la suite $(\sigma(n))_n$ est croissante (pour l'ordre de divisibilité sur $\mathbb{N}^*$).

Étape 2 : le théorème des quatre carrés "*tout entier naturel est somme de quatre carrés*". En combinant ce résultat avec celui de l'étape 1, on en déduit que $\sigma(n) \leq 4$ pour tout $n \geq 2$. Nous verrons plus loin que l'utilisation du théorème des quatre carrés (qui est loin d'être trivial) n'était en fait pas nécessaire pour montrer que $\sigma(n) \leq 4$.

Étape 3 : le théorème des restes chinois "*si $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ désigne la décomposition en facteurs premiers de l'entier $n \geq 2$ alors les anneaux $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}$ sont isomorphes*". Une conséquence pour notre problème est alors que $\sigma(n) = \max_i \sigma(p_i^{\alpha_i})$. Le problème se ramenait donc à étudier $\sigma(p^n)$ pour tout premier p et tout entier $n \geq 1$.

Étape 4 : le cas $p = 2$. Un petit calcul montre que $\sigma(2) = 1$, $\sigma(4) = 3$ (3 n'est pas somme de deux carrés dans $\mathbb{Z}/4\mathbb{Z}$), $\sigma(8) = 4$ (7 n'est pas somme de trois carrés dans $\mathbb{Z}/8\mathbb{Z}$). Les résultats des étapes 1 et 2 montrent que l'on a ensuite $\sigma(2^n) = 4$ pour $n \geq 2$.

Étape 5 : le cas $p \neq 2$.

5.1. Cas $n = 1$. Le dénombrement classique des carrés de $\mathbb{F}_p$ montre qu'il existe des éléments de $\mathbb{F}_p$ qui ne sont pas des carrés mais que tout élément de $\mathbb{F}_p$ est une somme de deux carrés. Ainsi, $\sigma(p) = 2$ et, en vertu du résultat de l'étape 1, $\sigma(p^n) \geq 2$ pour tout $n \geq 1$.

5.2. Etude de $(\mathbb{Z}/p^n\mathbb{Z})^*$. Ce point est le cœur de la preuve. Même si cela n'a pas été toujours mentionné clairement, tout le monde a tenté de démontrer que

Tout élément de $(\mathbb{Z}/p^n\mathbb{Z})^*$ est une somme de deux carrés.

Pour démontrer cette propriété, beaucoup ont invoqué une propriété de relèvement pour affirmer que *si $a \in \mathbb{Z}$ est tel que p ne divise pas a alors $a \bmod(p)$ est un carré si est seulement si $a \bmod(p^n)$ l'est aussi*. Il y eu trois écoles :

L'école hensélienne : on considère le polynôme $P(x) = x^2 - a \in \mathbb{Z}_p[x]$ qui, une fois réduit modulo p, possède par hypothèse une racine $y \in \mathbb{Z}/p\mathbb{Z}$. Puisque $P'(y) = 2y \neq 0$, le lemme d'Hensel permet d'affirmer qu'il existe $\alpha \in \mathbb{Z}_p$ tel que $P(\alpha) = 0$. Si pour $n \geq 2$, on note α_n l'image de α par l'épimorphisme $\mathbb{Z}_p \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$, alors $\alpha_n^2 = a \bmod(p^n)$.

———

L'école élémentaire : on opère une récurrence sur $n \geq 1$. Supposons qu'il existe $y \in \mathbb{Z}$ tel que $y^2 \equiv a \bmod(p^n)$. Il existe donc $k \in \mathbb{Z}$ tel que $a = y^2 + kp^n$ et puisque p ne divise visiblement pas y (par hypothèse p ne divise pas a) l'élément $y \bmod(p^{n+1})$ est inversible dans $\mathbb{Z}/p^{n+1}\mathbb{Z}$. Puisque $p \neq 2$, $2y \bmod(p^{n+1})$ est aussi inversible. On a alors

$$\left(y \bmod(p^{n+1}) + \left(2y \bmod(p^{n+1})\right)^{-1} \left(kp^n \bmod(p^{n+1})\right)\right)^2 = a \bmod(p^{n+1})$$

———

L'école combinatoire : il s'agit de montrer que, pour $n \geq 2$,

$$(\mathbb{Z}/p^n\mathbb{Z})^{*2} = \left\{a \bmod(p^n) / \ a \bmod(p) \in (\mathbb{Z}/p\mathbb{Z})^{*2}\right\}$$

(ici le carré d'ensemble désigne l'ensemble des carrés et non le produit cartésien). L'inclusion directe est claire. Puisque les fibres de l'épimorphisme $\mathbb{Z}/p^n\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}$ compte exactement p^{n-1} éléments et que $(\mathbb{Z}/p\mathbb{Z})^{*2}$ en compte $\frac{p-1}{2}$, il vient que

$$\sharp\left\{a \bmod(p^n) / \ a \bmod(p) \in (\mathbb{Z}/p\mathbb{Z})^{*2}\right\} = \frac{p^{n-1}(p-1)}{2}$$

On va voir un peu plus loin que $\sharp(\mathbb{Z}/p^n\mathbb{Z})^{*2} = \frac{p^{n-1}(p-1)}{2}$. L'égalité annoncée en découle alors.

———

Scholie. *Les arithméticiens des corps en herbe verront que cette propriété de relèvement permet de montrer que le niveau du corps $\mathbb{Q}_p$ (le nombre minimal $\nu(\mathbb{Q}_p)$ tel que -1 soit une somme de $\nu(\mathbb{Q}_p)$ carrés dans $\mathbb{Q}_p$) vaut 1 ou 2.*

Une fois établie cette propriété de relèvement, on considère un entier x tel que $p \nmid x$. Il existe $a, b \in \mathbb{Z}$ tels que $x \equiv a^2 + b^2 \bmod(p)$. Si $b \equiv 0 \bmod(p)$ alors x est un carré non nul modulo p et il

l'est donc modulo p^n en vertu de ce qui précède. Si $b \not\equiv 0 \bmod(p)$ alors $x - a^2$ est un carré non nul modulo p et il l'est donc modulo p^n. Ainsi, il existe $c \in \mathbb{Z}$ tel que $x \equiv a^2 + c^2 \bmod(p^n)$. Ceci prouve finalement que $x \bmod(p^n)$ est bien une somme de deux carrés.

———

Il était possible de montrer que tout inversible modulo p^n est une somme de deux carrés sans utiliser un lemme de relèvement. Dans sa solution initiale, l'auteur du sujet avait proposé une preuve combinatoire directe, preuve dont les idées ne sont pas d'intersection vide avec celles de l'école combinatoire citée plus haut.

Une preuve combinatoire directe : On note respectivement $\boxed{1}$ et $\boxed{2}$ les carrés et les sommes de deux carrés d'éléments de $\mathbb{Z}/p^n\mathbb{Z}$.

Commençons par dénombrer les carrés dans $(\mathbb{Z}/p^n\mathbb{Z})^*$. L'application $c : x \longmapsto x^2$ est un endomorphisme du groupe $(\mathbb{Z}/p^n\mathbb{Z})^*$ et son image est bien évidemment égale à $(\mathbb{Z}/p^n\mathbb{Z})^* \cap \boxed{1}$.

Puisque $(\mathbb{Z}/p^n\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{n-1}\mathbb{Z}$, on voit que $(\mathbb{Z}/p^n\mathbb{Z})^*$ possède un unique élément d'ordre 2 et donc, le noyau $\ker(c)$ est composé de seulement deux éléments. Le premier théorème d'isomorphisme nous permet alors d'affirmer que

$$\sharp(\mathbb{Z}/p^n\mathbb{Z})^* \cap \boxed{1} = \frac{(p-1)p^{n-1}}{2}$$

Considérons maintenant l'ensemble $G = (\mathbb{Z}/p^n\mathbb{Z})^* \cap \boxed{2}$. L'ensemble $\boxed{2}$ est un monoïde multiplicatif, mais puisque, si $x^2 + y^2$ est inversible, alors

$$\frac{1}{x^2+y^2} = \frac{x^2}{(x^2+y^2)^2} + \frac{y^2}{(x^2+y^2)^2} \in \boxed{2}$$

on en déduit que G est un sous-groupe de $(\mathbb{Z}/p^n\mathbb{Z})^*$. Il est clair que $(\mathbb{Z}/p^n\mathbb{Z})^* \cap \boxed{1} \subset (\mathbb{Z}/p^n\mathbb{Z})^* \cap \boxed{2}$ et donc l'on a donc $o(G) \geq \frac{(p-1)p^{n-1}}{2}$. Il vient alors

$$[(\mathbb{Z}/p^n\mathbb{Z})^* : G] \leq 2$$

Si $[(\mathbb{Z}/p^n\mathbb{Z})^* : G] = 2$, on a alors $G = (\mathbb{Z}/p^n\mathbb{Z})^* \cap \boxed{1}$ et, puisque $1^2 + 1^2 = 2 \in \boxed{1}$, on en déduit par récurrence que, pour tout $i = 1, \cdots, p-1$, on a $i = 1 + (i-1) \in \boxed{1}$. Maintenant, $p+1 = (p-1)+2$ et donc $(p+1) \in \boxed{1}$. Par récurrence, on montre ainsi que pour tout k premier à p, $k \in \boxed{1}$, c'est-à-dire que $(\mathbb{Z}/p^n\mathbb{Z})^* \subset \boxed{1}$. Ceci est absurde d'après ce qui précède.

Ainsi, $[(\mathbb{Z}/p^n\mathbb{Z})^* : G] = 1$ et donc $(\mathbb{Z}/p^n\mathbb{Z})^* = (\mathbb{Z}/p^n\mathbb{Z})^* \cap \boxed{2}$, ce qui prouve finalement que $(\mathbb{Z}/p^n\mathbb{Z})^* \subset \boxed{2}$.

———

Remarque : On peut appliquer l'idée précédente pour le cas $p = 2$ et montrer que $\sigma(2^n) \leq 4$ sans utiliser le théorème des quatre carrés. Notons $\boxed{4}$ l'ensemble des sommes de quatre carrés d'éléments de $\mathbb{Z}/2^n\mathbb{Z}$. L'identité quaternionique de Hamilton montre que cet ensemble est stable par produit si bien que, en appliquant le même argument que précédemment, l'ensemble $(\mathbb{Z}/2^n\mathbb{Z})^* \cap \boxed{4}$ est un sous-groupe de $(\mathbb{Z}/2^n\mathbb{Z})^*$ et l'on a

$$(\mathbb{Z}/2^n\mathbb{Z}) \cap \boxed{1} \subsetneq (\mathbb{Z}/2^n\mathbb{Z})^* \cap \boxed{2} \subsetneq (\mathbb{Z}/2^n\mathbb{Z})^* \cap \boxed{4} \subset (\mathbb{Z}/2^n\mathbb{Z})^*$$

Pour voir que les deux premières inclusions sont strictes, il suffit de remarquer que pour $n = 3$, l'élément 5 est un inversible qui est somme de deux carrés sans être un carré et 7 est un inversible qui est somme de quatre carrés sans être une somme de deux carrés.

On considère à nouveau l'épimorphisme $c : x \longmapsto x^2$ de $(\mathbb{Z}/2^n\mathbb{Z})^*$ sur $(\mathbb{Z}/2^n\mathbb{Z}) \cap \boxed{1}$. Puisque $(\mathbb{Z}/2^n\mathbb{Z})^* \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}$, on voit que ce groupe compte exactement trois éléments d'ordre 2 et donc $\mathrm{Im}(c) = (\mathbb{Z}/2^n\mathbb{Z}) \cap \boxed{1}$ est d'indice $o(\ker(c)) = 4$ dans $(\mathbb{Z}/2^n\mathbb{Z})^*$. Les inclusions précédentes

assure alors que $(\mathbb{Z}/2^n\mathbb{Z})^* \cap \boxed{4}$ est d'indice 1 dans $(\mathbb{Z}/2^n\mathbb{Z})^*$, c'est-à-dire que $(\mathbb{Z}/2^n\mathbb{Z})^* \cap \boxed{4} = (\mathbb{Z}/2^n\mathbb{Z})^*$.

Pour finir de montrer que $\sigma(2^n) \leq 4$, on voit qu'une puissance de 2 dans $\mathbb{Z}/2^n\mathbb{Z}$ est soit un carré, soit une somme de deux carrés et donc dans tous les cas une somme de quatre carrés. L'identité quaternionique permet alors d'en déduire que $\sigma(2^n) \leq 4$.

———

D'autres preuves directes ont été proposées :

Une autre preuve combinatoire directe : Comme vu précédemment, $(\mathbb{Z}/p^n\mathbb{Z})^{*2}$ est un sous-groupe d'indice 2 de $(\mathbb{Z}/p^n\mathbb{Z})^*$. Ainsi, en regardant les images des éléments de $(\mathbb{Z}/p^n\mathbb{Z})^*$ dans le groupe quotient $(\mathbb{Z}/p^n\mathbb{Z})^*/(\mathbb{Z}/p^n\mathbb{Z})^{*2}$, on en déduit que dans $(\mathbb{Z}/p^n\mathbb{Z})^*$, le produit de deux éléments dont aucun n'est un carré, est un carré.

Une fois cette remarque faite, on raisonne par l'absurde en supposant qu'il existe un élément $x \in (\mathbb{Z}/p^n\mathbb{Z})^*$ qui ne soit pas somme de deux carrés (x n'est en particulier pas un carré). On a donc, pour tout $a, b \in \mathbb{Z}/p^n\mathbb{Z}$, $x \neq a^2(1+b^2) = a^2 + (ab)^2$. Ainsi,

$$\forall b \in \mathbb{Z}/p^n\mathbb{Z},\ 1 + b^2 \in (\mathbb{Z}/p^n\mathbb{Z})^* \Longrightarrow 1 + b^2 \in (\mathbb{Z}/p^n\mathbb{Z})^{*2}$$

car si $1 + b^2 \in (\mathbb{Z}/p^n\mathbb{Z})^* - (\mathbb{Z}/p^n\mathbb{Z})^{*2}$ alors $x(1+b^2)^{-1} \in (\mathbb{Z}/p^n\mathbb{Z})^{*2}$ d'après la remarque précédente.

Puisque $2 = 1 + 1^2$, 2 est un carré et, par récurrence, on en déduit que tout $r = 1, \cdots, p-1$ est un carré. Par ailleurs, puisque 2 est un carré, pour tout $a, b \in \mathbb{Z}/p^n\mathbb{Z}$, on a $x \neq a^2(2+b^2) = (\sqrt{2}a)^2 + (ab)^2$. Comme précédemment, on en déduit que

$$\forall b \in \mathbb{Z}/p^n\mathbb{Z},\ 2 + b^2 \in (\mathbb{Z}/p^n\mathbb{Z})^* \Longrightarrow 2 + b^2 \in (\mathbb{Z}/p^n\mathbb{Z})^{*2}$$

Comme $p + 1 = 2 + (p-1)$, on en déduit que $p+1$ est un carré et, par récurrence, que tout $r = p+1, \cdots, 2p-1$ est un carré. En appliquant p^{n-1}-fois ce raisonnement, on en déduit finalement que $(\mathbb{Z}/p^n\mathbb{Z})^* = (\mathbb{Z}/p^n\mathbb{Z})^{*2}$, ce qui est absurde.

———

Remarques : 1/ On peut appliquer l'idée développée ici pour donner une nouvelle preuve du fait que les éléments de $(\mathbb{Z}/2^n\mathbb{Z})^*$ sont des sommes de quatre carrés.

Les inclusions strictes établies dans le paragraphe précédent montrent que $(\mathbb{Z}/2^n\mathbb{Z})^* \cap \boxed{2}$ est un sous-groupe d'indice 2 de $(\mathbb{Z}/2^n\mathbb{Z})^*$ et l'on en déduit la propriété suivante : si $x, y \in (\mathbb{Z}/2^n\mathbb{Z})^*$ désignent deux éléments dont aucun n'est une somme de deux carrés, alors le produit xy est une somme de deux carrés.

On raisonne maintenant par l'absurde en supposant qu'il existe $x \in (\mathbb{Z}/2^n\mathbb{Z})^*$ qui ne puisse s'écrire comme somme de quatre carrés. Pour tout $a, b, c, d \in \mathbb{Z}/2^n\mathbb{Z}$, on a donc $x \neq (a^2+b^2)(1 + (c^2+d^2)) = a^2 + b^2 + (a^2+b^2)(c^2+d^2)$ (somme de quatre carrés d'après l'identité de Jacobi). On en déduit que pour tout $c, d \in \mathbb{Z}/2^n\mathbb{Z}$, si $1 + (c^2+d^2)$ est inversible alors il est somme de deux carrés. Pour $c = d = 1$ on en déduit que 3 est somme de deux carrés dans $\mathbb{Z}/2^n\mathbb{Z}$, et donc dans $\mathbb{Z}/4\mathbb{Z}$, ce qui est absurde.

———

2/ Nous avons rencontré une autre preuve, totalement élémentaire, pour la majoration $\sigma(2^n) \leq 4$. Elle repose sur la propriété suivante : *si $a \in \mathbb{Z}$ est tel que $a \equiv 1 \bmod(8)$, alors a est un carré modulo 2^n pour tout $n \geq 3$.* Pour $a = 1 + 8k$, la preuve se fait par récurrence. Pour $n = 3$ la proposition est claire. Si la propriété est vraie pour $n \geq 3$ alors, il existe $b, l \in \mathbb{Z}$ tel que $b^2 = a + l2^n$ et, pour un entier h quelconque, on a alors $(b + h2^{n-1})^2 \equiv a + (l + bh)2^n \bmod(2^{n+1})$. L'entier b étant impair, on peut choisir l'entier $h = 0, 1$ pour que $2|(l + bh)$ et donc a est bien un carré modulo 2^{n+1}.

Une fois établi ce résultat, supposons par l'absurde qu'il existe un plus petit entier $a > 0$ tel que $a \bmod(2^n)$ ne soit pas une somme de quatre carrés. On a nécessairement $a \not\equiv 0 \bmod(4)$, car

sinon $a/4 < a$ est une somme de quatre carrés et donc a est somme de quatre carrés. Donc $a \equiv 1, 2, 3, 5, 6, 7 \bmod(8)$ et donc il existe un entier $b \equiv 1 \bmod(8)$ tel que $a = b, b+1, b+2, b+4, b+5, b+6$. L'élément $b \bmod(2^n)$ est un carré, mais les éléments $1, 2, 3, 5, 6, 7 \bmod(2^n)$ étant tous des sommes de trois carrés, on en déduit une contradiction.

———

Une preuve dirichletienne : Soit $a \in \mathbb{Z}$ premier à p. Puisque 4 et p sont premier entre eux, le théorème des restes chinois assure qu'il existe $b \in \mathbb{Z}$ tel que $b \equiv 1 \bmod(4)$ et $b \equiv a \bmod(p^n)$. Puisque b est premier avec $4p^n$, le théorème de progression arithmétique de Dirichlet assure qu'il existe un premier q tel que $q \equiv b \bmod(4p^n)$. Puisque $q \equiv 1 \bmod(4)$ il est somme de deux carrés (théorème des deux carrés) et comme $q \equiv a \bmod(p^n)$, a est bien somme de deux carrés modulo p^n.

———

Une preuve hensélienne : C'est exactement la même idée que pour relever les carrés. Si $a \in \mathbb{Z}$ est premier à p alors il existe $c, d \in \mathbb{Z}$ tel que $a \equiv b^2 + c^2 \bmod(p)$. Les entiers b et c ne peuvent être simultanément divisibles par p, donc par exemple, $b \not\equiv 0 \bmod(p)$. On considère alors le polynôme $P(x) = x^2 + (b^2 - a)$ et l'on applique le lemme de Hensel comme précédemment.

Certains membres de l'école hensélienne ont même utilisé une variante à plusieurs variables du lemme de Hensel, en considérant le polynôme $P(x, y) = x^2 + y^2 - a$.

———

Une fois établi le fait que tout inversible modulo p^n est une somme de deux carrés, on constate que si $x \in \mathbb{Z}$ est tel que $p \nmid x$ alors $x \bmod(p^n)$ est une somme de deux carrés et si $p|x$ alors $p \nmid (x-1)$ et donc $(x-1) \bmod(p^n)$ est une somme de deux carrés, donc $x \bmod(p^n)$ est une somme de trois carrés. En conclusion, on a $2 \leq \sigma(p^n) \leq 3$.

Remarque : Il est donc possible de n'utiliser que des propriétés élémentaires pour montrer que $\sigma(p^n) \leq 4$ pour tout premier p et donc que $\sigma(n) \leq 4$ pour tout $n \geq 2$.

5.3. Détermination de $\sigma(p^n) = 2, 3$ pour $n \geq 2$. La fin de la preuve consistait à montrer que la valeur de $\sigma(p^n)$ est entièrement déterminée par la congruence modulo 4 du premier p.

5.3.1. Cas $p \equiv 1 \bmod(4)$. Dans cette situation il fallait remarquer que $p \bmod(p^n)$ était une somme de deux carrés. Il y a eu deux écoles pour démontrer ce résultat :

L'école du théorème des deux carrés, qui invoque le fait qu'un premier p vérifiant $p \equiv 1 \bmod(4)$ est somme de deux carrés dans $\mathbb{Z}$, donc dans $\mathbb{Z}/p^n\mathbb{Z}$.

L'école élémentaire : si $p \equiv 1 \bmod(4)$ alors $(-1)^{(p-1)/2} \equiv 1 \bmod(4)$ et donc -1 est un carré modulo p (propriété classique et élémentaire du symbôle de Legendre). Il existe donc $a \in \mathbb{Z}$ tel que $p \equiv 1 + a^2 \bmod(p)$ et l'on écrit $p = 1 + a^2 + \lambda p$. Comme $p \neq 2$, 2 est inversible modulo p^2 et il existe $d \in \mathbb{Z}$ tel que $2d \equiv 1 \bmod(p^2)$. On a alors

$$(1 + d\lambda p)^2 + a^2 \equiv 1 + \lambda p + a^2 \equiv p \bmod(p^2)$$

et donc $p \bmod(p^2)$ est une somme de deux carrés dont l'un au moins est inversible. En appliquant alors la propriété de relèvement détaillée dans la partie 5.2. on en déduit que p est une somme de deux carrés modulo p^n.

Une fois établi ce résultat il convenait de se rappeler que, eu égard à l'identité de Jacobi

$$(a_1^2 + a_2^2)(b_1^2 + b_2^2) = (a_1 b_1 + a_2 b_2)^2 + (a_1 b_2 - a_2 b_1)^2$$

les sommes de deux carrés dans un anneau sont stables par produit. Tout élément de $\mathbb{Z}/p^n\mathbb{Z}$ est le produit d'un élément de $(\mathbb{Z}/p^n\mathbb{Z})^*$ et d'une puissance de p modulo p^n. Il est donc somme de deux carrés vu ce qui précède.

On constate réciproquement que, si $p \bmod(p^n) = (a^2 + b^2) \bmod(p^n)$ est une somme de deux carrés, alors $a^2 + b^2 \equiv 0 \bmod(p)$. L'un des deux entiers a ou b n'est pas divisible par p, sinon les deux le seraient et, pour $n = 2$, on aurait $p \equiv a^2 + b^2 \equiv 0 \bmod(p^2)$, ce qui est absurde. On a donc, par exemple, $a \not\equiv 0 \bmod(p)$ (et a est alors inversible modulo p^2). On a alors

$$-1 \bmod(p) = \left((b \bmod(p))(a \bmod(p))^{-1}\right)^2$$

ce qui implique que $p \equiv 1 \bmod(4)$ (réciproque de la propriété du symbôle de Legendre rappelée plus haut).

En conclusion, on a $\sigma(p^n) = 2 \Longleftrightarrow p \equiv 1 \bmod(4)$.

5.3.2 Cas $p \equiv -1 \bmod(4)$**.** Si $p \not\equiv 1 \bmod(4)$ alors comme $p \neq 2$ on a $p \equiv -1 \bmod(4)$. Ce qui précède prouve que $\sigma(p^n) = 3 \Longleftrightarrow p \equiv -1 \bmod(4)$.

Étape 6 : Conclusion. On déduit de ce qui précède que

Théorème.— *Si* $n = 2^h p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ *désigne la décomposition en facteurs premiers de l'entier* $n \geq 2$ *alors on a* $\sigma(n) \leq 4$ *et*

$\sigma(n) = 1$ *si et seulement si* $n = 2$.

$\sigma(n) = 2$ *si et seulement si* $h \leq 1$ *et, pour tout* $i = 1, \cdots, k$, $p_i \equiv -1\ (4) \Longrightarrow \alpha_i = 1$.

$\sigma(n) = 3$ *si et seulement si [*$h = 2$*] ou [*$(h \leq 1)$ *et (il existe* $i = 1, \cdots, k$ *tel que* $p_i \equiv -1\ (4)$ *et* $\alpha_i \geq 2$*)].*

$\sigma(n) = 4$ *si et seulement si* $h \geq 3$.

Quelques valeurs :

n	$\sigma(n)$	n	$\sigma(n)$	n	$\sigma(n)$	n	$\sigma(n)$
2	1	12	3	22	2	32	4
3	2	13	2	23	2	33	2
4	3	14	2	24	4	34	2
5	2	15	2	25	2	35	2
6	2	16	4	26	2	36	3
7	2	17	2	27	3	37	2
8	4	18	3	28	3	38	2
9	3	19	2	29	2	39	2
10	2	20	3	30	2	40	4
11	2	21	2	31	2	41	2