Concours SMF Junior

Équipe TiSaNe

Problème 9

Auteurs :
Chloé Papin
Etienne Perrot
Victor Quach

May 11, 2017

1 Problème 9

Pour ce problème, on utilisera les trois théorèmes suivants.

Théorème 1.1 (Théorème des quatre carrés)**.** *Soit $n \in \mathbb{N}$. Alors n est une somme de quatre carrés.*

Théorème 1.2 (Théorème des deux carrés)**.** *Soit $n \in \mathbb{N}$. Alors n est une somme de deux carrés si et seulement si chacun de ses facteurs premiers de la forme $4k+3$ intervient à une puissance paire.*

Théorème 1.3 (Théorème des trois carrés)**.** *Soit $n \in \mathbb{N}$. Alors n est somme de trois carrés d'entiers si il n'est pas de la forme $4^j \times (8k-1)$ avec j et k entiers positifs.*

Corollaire 1.1. *Soit $n \in \mathbb{N}$ impair tel que $n \not\equiv -1[8]$. Alors n est somme de trois carrés d'entiers.*

Remarquons pour commencer que 0 est un carré, donc toute somme de a carrés est une somme de b carrés pour tout $b \geq a$.

Proposition 1.1. *Pour tout $n \in \mathbb{N}, n \geq 2$, on a $2 \leq \sigma(n) \leq 4$.*

Preuve : Soit $n \geq 3$ et $z \in \mathbb{N}$.
D'après le théorème 1.1, il existe $a, b, c, d \in \mathbb{N}$ tel que $z = a^2 + b^2 + c^2 + d^2$. Cette égalité est encore vraie dans $\mathbb{Z}/n\mathbb{Z}$, ce qui donne la majoration. D'autre part, pour $n \geq 3$, la fonction carré n'est pas injective dans $\mathbb{Z}/n\mathbb{Z}$ ($1 \neq -1$), donc elle n'est pas surjective, et il existe z qui n'est pas un carré dans $\mathbb{Z}/n\mathbb{Z}$, ce qui donne la minoration. □

Proposition 1.2. *Pour tout $m, n \in \mathbb{N}, m, n \geq 2$, si $m \mid n$, alors $\sigma(m) \leq \sigma(n)$.*

Preuve : Notons $s = \sigma(n)$. Soit $z \in \mathbb{N}$. Il existe alors $a_1, a_2, \ldots, a_s$ tel que $z \equiv \sum a_{i^2}[n]$, c'est-à-dire n divise $z - \sum a_i^2$. Par transitivité de la divisibilité, m divise $z - \sum a_i^2$, donc z est une somme de s carrés. Ainsi, $\sigma(m) \leq \sigma(n)$. □

Proposition 1.3. $\sigma(2) = 1, \sigma(4) = 3, \sigma(8) = 4$.

Preuve :

- **Modulo 2.** Tous les entiers ($0 = 0^2$ et $1 = 1^2$) sont des carrés. Donc $\sigma(2) = 1$.
- **Modulo 4.** Les carrés sont 0 et 1, donc 3 ne peut pas s'écrire comme somme de moins de 3 carrés. Or, $3 = 1^2 + 1^2 + 1^2$ et $2 = 1^2 + 1^2$. Donc $\sigma(4) = 3$.
- **Modulo 8.** Les carrés sont 0, 1 et 4, donc 7 ne peut pas s'écrire comme somme de moins de 4 carrés. Or, $7 = 2^2 + 1^2 + 1^2 + 1^2$ et on écrit facilement $3, 5, 6$ comme somme de 3 carrés ou moins. Donc $\sigma(8) = 4$.

□

Proposition 1.4 (Multiplicativité)**.** *Soit $m, n \in \mathbb{N}$ deux entiers premiers entre eux tels que $\sigma(m) = \sigma(n)$. Alors $\sigma(mn) \leq \sigma(m)$.*

Preuve : On note $s = \sigma(m) = \sigma(n)$. Soit $z \in \mathbb{N}$.
Onécrit z commme somme de s carrés en disposant de $a_1, a_2, \ldots, a_s \in \mathbb{N}$ et $b_1, b_2, \ldots, b_s \in \mathbb{N}$ tels que :

$$z \equiv \sum_{i=1}^{s} a_i^2 [m]$$

$$z \equiv \sum_{i=1}^{s} b_i^2 [n]$$

D'après le lemme chinois, il existe alors $c_1, c_2, \ldots, c_s \in \mathbb{N}$ tels que

$$\forall i \in \{1, \ldots, s\}, \begin{cases} c_i \equiv a_i & [m] \\ c_i \equiv b_i & [n] \end{cases}$$

Ils vérifient

$$z \equiv \sum_{i=1}^{s} c_i^2 [mn]$$

.

□

Proposition 1.5 (Multiplicativité bis)**.** *Soit $m, n \in \mathbb{N}$ deux entiers premiers entre eux. Alors $\sigma(mn) = \max(\sigma(m), \sigma(n))$.*

Preuve : Sans perte de généralité $\sigma(n) \geq \sigma(m)$.
D'après la proposition 1.2, $\sigma(n) \leq \sigma(mn)$, donc $\sigma(mn) \geq \max(\sigma(m), \sigma(n))$.
D'autre part, d'après la remarque initiale, toute somme de $\sigma(m)$ carrés est une somme de $\sigma(n)$ carrés. On peut alors utiliser le même argument que pour la proposition 1.4, pour montrer que $\sigma(mn) \leq \max(\sigma(m), \sigma(n))$. □

Fort de ces observations, on s'attaque au cas où n est une puissance d'un nombre premier. Le cas où $p = 2$ découle des propositions 1.3 et 1.1 :

$$\begin{cases} \sigma(2) = 1 \\ \sigma(4) = 2 \\ \sigma(2^r) = 4 \quad \text{si } r \geq 3 \end{cases}$$

Proposition 1.6. *Soit p un nombre premier impair. Alors $\sigma(p) = 2$.*

Preuve : L'ensemble des carrés de $\mathbb{Z}/p\mathbb{Z}$ est :

$$S = \left\{ x^2, x \in \left[\!\left[0, \frac{p-1}{2} \right]\!\right] \right\}$$

Puisque p est impair, chaque carré non nul de $\mathbb{Z}/p\mathbb{Z}$ est l'image par l'application $x \mapsto x^2$ définie sur $\mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ d'exactement deux antécédents. Donc S est de cardinal $\frac{p+1}{2}$.

Soit $z \notin S$. Les ensembles $\left\{ z - x^2, x \in \left[\!\left[0, \frac{p-1}{2} \right]\!\right] \right\}$ et $\left\{ y^2, y \in \left[\!\left[0, \frac{p-1}{2} \right]\!\right] \right\}$ sont de cardinal $\frac{p+1}{2}$ donc ne peuvent pas être disjoints.

Il existe donc $x, y \in \left[\!\left[0, \frac{p-1}{2} \right]\!\right]$ tels que $z = x^2 + y^2$. Par conséquent, $\sigma(p) = 2$. □

Pour étendre le résultat aux puissances de p, on utilise le lemme de Hensel.

Lemme 1.1 (Lemme de Hensel)**.** *Soit P un polynôme à coefficients dans $\mathbb{Z}_p$. Soit $x_0 \in \mathbb{Z}_p$ tel que $P(x_0) \equiv 0[p]$ et $P'(x_0) \not\equiv 0[p]$, alors il existe $x \in \mathbb{Z}_p$ tel que $P(x) = 0$ et $x \equiv x_0$.*

Proposition 1.7. *Soit $p \in \mathbb{P}$ un nombre premier impair, $\alpha \in \mathbb{N}^*$ et $z \in \mathbb{N}, p \nmid z$. Alors z est un carré module p si et seulement si z est un carré modulo p^α.*

Preuve : On applique le lemme de Hensel avec $P = X^2 - z$. □

Proposition 1.8. *Soit $p \in \mathbb{P}, p \equiv 1[4]$ et $\alpha \in \mathbb{N}^*$. Alors $\sigma(p^\alpha) = 2$.*

Preuve : Soit $z \in \mathbb{N}$. On écrit $z = p^r z'$ avec $r \in \mathbb{N}, z' \in \mathbb{N}$ et $p \nmid z'$.

D'après la proposition 1.6, il existe $x_0, y_0 \in \mathbb{Z}$ tels que $z' \equiv x_0^2 + y_0^2[p]$. p ne peut pas diviser à la fois x_0 et y_0, sinon il diviserait z', ce qui est exclus. Sans perte de généralité, p ne divise pas x_0, et donc $p \nmid z' - y_0^2$.

On peut alors appliquer la proposition 1.7 : $z' - y_0^2$ est un carré modulo p^α, donc z' est la somme de deux carrés dans $\mathbb{Z}/p^\alpha Z$.

D'autre part, on observe que p^r vérifie les conditions du théorème 1.2 (théorème des deux carrés), donc p^r est une somme de deux carrés dans $\mathbb{Z}$ et donc dans $\mathbb{Z}/p^r\mathbb{Z}$.

Pour conclure, on invoque l'identité de Lagrange $(a^2+b^2)(c^2+d^2) = (ac-bd)^2+(ad+bc)^2$, encore vraie dans $\mathbb{Z}/p^r\mathbb{Z}$ pour écrire z comme somme de deux carrés.

□

Proposition 1.9. *Soit $p \in \mathbb{P}, p \equiv 3[4]$ et $\alpha \in \mathbb{N}, \alpha \geq 2$. Alors $\sigma(p^\alpha) = 3$.*

Preuve : On procède en deux temps.

$\sigma(p^\alpha) \geq 3$. D'après la proposition 1.2, il suffit d'étudier le cas $\alpha = 2$. Il suffit d'exhiber $z \in \mathbb{N}$ qui ne soit pas une somme de deux carrés modulo 2. On propose $z = p$ et on se donne par l'absurde $x, y \in \mathbb{N}$ tels que $p \equiv x^2 + y^2[p^2]$. Alors on a $k \in \mathbb{Z}$ tel que $x^2 + y^2 = p + kp^2 = p(1 + kp)$. Donc la valuation p-adique $v_p(x^2 + y^2) = 1$. L'entier $x^2 + y^2$ est une somme de deux carrés pour lequel $p \equiv 3[4]$ est un diviseur qui apparaît à une puissance impaire. Cela contredit le théorème 1.2.

$\sigma(p^\alpha) \leq 3$. On observe que $p \equiv 3[4]$ implique $p^r \equiv 1, 3$ ou $-1[8]$ et $2p^r \equiv 2$ ou $-2[8]$. Soit $z \in \mathbb{N}$.

- Si z est impair, alors l'un des entiers z ou $z+2p^r$ est impair non congru à -1 modulo 8. D'après le théorème des trois carrés 1.3, il s'écrit comme somme de trois carrés, ce que l'on peut réduire modulo p^r.
- Si z est pair, alors l'un des entiers $z + p^r$ ou $z + 3p^r$ est impair non congru à -1 modulo 8. D'après le théorème des trois carrés 1.3, il s'écrit comme somme de trois carrés, ce que l'on peut réduire modulo p^r.

□

Conclusion

On connaît ainsi σ pour les puissances de nombre premier :

$$\begin{cases} \sigma(2) = 1 \\ \sigma(4) = 2 \\ \sigma(2^r) = 4 & \text{si } r \geq 3 \\ \sigma(p) = 2 & \text{si } p \in \mathbb{P} \\ \sigma(p^r) = 2 & \text{si } p \in \mathbb{P}, p \equiv 1[4], r \in \mathbb{N}^* \\ \sigma(p^r) = 3 & \text{si } p \in \mathbb{P}, p \equiv 3[4], r \in \mathbb{N}^*, r \geq 2 \end{cases}$$

Grâce à la proposition 1.5, on a alors déterminé $\sigma(n)$ pour $n \geq 2$.