Entiers de la forme $x^2 + ky^2$

Deux niveaux de difficulté/longueur :

— Piste bleue : questions **1)** à **5)**.

— Piste rouge : tout le devoir.

On s'attache dans ce devoir à décrire les ensembles $\mathscr{E}_k = \left\{ n \in \mathbb{N}^* \mid \quad \exists\, x, y \in \mathbb{Z}, \quad n = x^2 + ky^2 \right\}$ pour $k \in \{1, 2, 3\}$.

1) Montrer, en travaillant dans $\mathbb{C}$, que $\mathscr{E}_k$ est *stable par produit* pour tout $k \in \{1, 2, 3\}$, i.e. que : $\quad \forall m, n \in \mathscr{E}_k, \quad mn \in \mathscr{E}_k$.

1 Lemme de Thue

On doit le lemme suivant au mathématicien norvégien Axel Thue (1863-1922).

Théorème (Lemme de Thue) Soient $n \in \mathbb{N}^*$ et $a \in \mathbb{Z}$. Il existe des entiers x et y pour lesquels :

$$0 < |x| \leqslant \sqrt{n}, \qquad |y| \leqslant \sqrt{n} \qquad \text{et} \qquad y \equiv ax\ [n].$$

2) Soient $n \in \mathbb{N}^*$ et $a \in \mathbb{Z}$. On pose $e = \left\lfloor \sqrt{n} \right\rfloor$ et on note f l'application de $[\![0, e]\!]^2$ dans $[\![0, n-1]\!]$ qui associe à (x, y) le reste de la division euclidienne de $ax - y$ par n.

a) Comparer $\left|[\![0, e]\!]^2\right|$ et $\left|[\![0, n-1]\!]\right|$. Quelle propriété de f en déduit-on ?

b) En déduire le lemme de Thue.

2 Diviseurs de $x^2 + ky^2$ pour $x \wedge y = 1$

3) Soient $k \in \{1, 2, 3\}$, $x, y \in \mathbb{Z}$ premiers entre eux et $n \in \mathbb{N}^*$. On suppose que n divise $x^2 + ky^2$ sans être le carré d'un entier.

a) Justifier l'existence d'un entier z pour lequel $k \equiv -z^2\ [n]$.

D'après le lemme de Thue, il existe des entiers a et b pour lesquels : $\quad |a| \leqslant \sqrt{n}, \quad 0 < |b| \leqslant \sqrt{n} \quad$ et $\quad a \equiv bz\ [n]$.

b) Montrer que $n \in \mathscr{E}_k$ si $k \in \{1, 2\}$.

On suppose à présent que $k = 3$ et que n est impair.

c) Montrer que si $a^2 + 3b^2 = 2n$, alors a et b ont la même parité et dénicher une contradiction.

d) En déduire que $n \in \mathscr{E}_3$.

3 Entiers de la forme $x^2 + y^2$

4) Montrer que tout élément impair de $\mathscr{E}_1$ est congru à 1 modulo 4.

5) Soit $p \in \mathbb{P} \smallsetminus \{2\}$. On pose $r = \dfrac{p-1}{2}$.

a) Montrer que : $\quad \forall x \in [\![1, p-1]\!], \quad \exists!\, x^\star \in [\![1, p-1]\!], \quad xx^\star \equiv 1\ [p]. \quad$ Pour quels x a-t-on $x^\star = x$?

b) En déduire le *théorème de Wilson* : $\quad (p-1)! \equiv -1\ [p]$.

c) Montrer, grâce au produit $\displaystyle\prod_{k=1}^{r} k(p-k)$, que $r!^2 \equiv (-1)^{r+1}\ [p]$.

d) En déduire que si $p \equiv 1\ [4]$, alors $p \in \mathscr{E}_1$.

En résumé :

Théorème (Théorème des deux carrés) Un nombre premier autre que 2 est la somme de deux carrés d'entiers si et seulement s'il est congru à 1 modulo 4.

La caractérisation des sommes de deux carrés d'entiers a agité les mathématiciens dès l'Antiquité, mais le premier énoncé général — sans preuve ! — du théorème des deux carrés date du 17ème siècle. On le doit au mathématicien français Pierre de Fermat. Un siècle plus tard, le mathématicien suisse Leonhard Euler (1707-1783) démontre le théorème. De nombreuses preuves et généralisations suivront.

6) Montrer que $\mathscr{E}_1$ est l'ensemble des entiers naturels non nuls n pour lesquels $v_p(n)$ est pair pour tout $p \in \mathbb{P}$ congru à 3 modulo 4. Ce résultat plus précis est lui aussi appelé le *théorème des deux carrés*.

4 Entiers de la forme $x^2 + 2y^2$

7) Montrer que tout élément impair de $\mathscr{E}_2$ est congru à 1 ou 3 modulo 8.

8) Soit $p \in \mathbb{P} \smallsetminus \{2\}$. On pose $r = \dfrac{p-1}{2}$.

a) Montrer que l'application $k \longmapsto p-k$ est bijective de $[\![1, r]\!] \cap (2\mathbb{Z}+1)$ sur $[\![r+1, p-1]\!] \cap 2\mathbb{Z}$.

b) En déduire la congruence : $\displaystyle\prod_{k=1}^{r} \left((-1)^k k\right) \equiv 2^r r! \, [p]$, puis la *loi complémentaire de Gauss* : $2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \, [p]$.

c) En déduire que si $p \equiv 3 \, [8]$, alors -2 est un carré modulo p, puis que $p \in \mathscr{E}_2$.

En poussant les choses un peu plus loin, on montre de même que si $p \equiv 1 \, [8]$, alors $p \in \mathscr{E}_2$, mais quelques connaissances supplémentaires sur les carrés modulo p sont requises.

En résumé, un nombre premier autre que 2 peut être écrit sous la forme x^2+2y^2 avec $x, y \in \mathbb{Z}$ si et seulement s'il est congru à 1 ou 3 modulo 8. Il n'est pas dur d'en déduire, comme en **6)**, que $\mathscr{E}_2$ est l'ensemble des entiers naturels non nuls n pour lesquels $v_p(n)$ est pair pour tout $p \in \mathbb{P}$ congru à 5 ou 7 modulo 8.

Concernant les entiers de la forme x^2+3y^2, on peut montrer les résultats suivants. Un nombre premier autre que 3 peut être écrit sous la forme x^2+3y^2 avec $x, y \in \mathbb{Z}$ si et seulement s'il est congru à 1 modulo 3. Enfin, $\mathscr{E}_3$ est l'ensemble des entiers naturels non nuls n pour lesquels $v_p(n)$ est pair pour tout $p \in \mathbb{P}$ congru à 2 modulo 3.