Université Paul Sabatier
Licence L3 ESR 2017–2018
Arithmétique

Examen du jeudi 17 mai 2018, 14 h - 16 h

Exercice 1. Soit a un entier relatif non carré. On se propose de démonter qu'alors, il existe une infinité de nombres premiers modulo lesquels a n'est pas un carré. On s'autorisera pour cela à utiliser non seulement la loi de réciprocité quadratique [1], mais aussi le théorème de la progression arithmétique [2].

On va distinguer trois cas, selon la parité des exposants r_i dans la décomposition

$$a = (-1)^{r_0} 2^{r_1} p_2^{r_2} \dots p_m^{r_m}$$

(où les p_i sont des nombres premiers impairs distincts). Au moins un r_i est impair donc on peut supposer (quitte à permuter les p_i) que r_0, r_1 ou r_2 est impair.

Les trois questions sont indépendantes.

1) On suppose dans cette question que r_2 est impair.
   (a) Montrer qu'il existe un entier x non carré modp_2 et congru à à 1 mod $8p_3 \dots p_m$.
   (b) Montrer qu'il existe alors une infinité de nombres premiers p congrus à x mod $8p_2 \dots p_m$ et que modulo chacun de ces p, l'entier a n'est pas un carré.
2) On suppose maintenant que $r_2, \dots, r_m$ sont pairs et r_1 impair. Montrer qu'il existe une infinité de nombres premiers p congrus à -3 mod 8 et que pour une infinité d'entre eux, $\left(\frac{a}{p}\right) = -1$.
3) On suppose enfin que a est l'opposé d'un carré. Montrer qu'il existe une infinité de nombres premiers p congrus à -1 mod 4 et que pour une infinité d'entre eux, $\left(\frac{a}{p}\right) = -1$.

Solution : Wikiversité, Introduction à la théorie des nombres, Exercices sur les résidus quadratiques, exercice 4-15.

Exercice 2.

1) Quels sont les nombres premiers modulo lesquels -2 est un carré ?
2) Soient $n = x^2 + 2y^2$ (avec x, y entiers) et p, congru à -1 ou -3 mod 8, un diviseur premier de n.
   (a) Déduire de la question précédente que p divise y (donc aussi x).
   (b) En déduire que l'exposant de p dans la décomposition de n en facteurs premiers est pair.
3) Montrer que la forme principale q_{-8} est la seule forme positive réduite de discriminant -8.
4) Soit m un entier sans facteur carré, et sans diviseur premier congru à -1 ou -3 mod 8. Déduire de la question précédente que m est de la forme $x^2 + 2y^2$.
5) Déduire de tout ce qui précède une condition nécessaire et suffisante pour qu'un entier $n \in \mathbb{N}^*$ soit de la forme $x^2 + 2y^2$.

Solution : Wikiversité, Introduction à la théorie des nombres, Exercices sur les formes quadratiques entières, exercice 5-14.

---

[1] Rappel de la loi de réciprocité quadratique : pour p et q premiers impairs distincts,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} = \begin{cases} 1 \text{ si, mod 4, } p \text{ ou } q \equiv 1 \\ -1 \text{ si, mod 4, } p \text{ et } q \equiv -1 \end{cases}$$

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

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 \text{ si } p \equiv \pm 1 \bmod 8 \\ -1 \text{ si } p \equiv \pm 3 \bmod 8. \end{cases}$$

[2] Rappel du théorème de la progression arithmétique de Dirichlet : pour tout entier n non nul et tout entier m premier avec n, il existe une infinité de nombres premiers congrus à m mod n (on pourrait, avec un peu plus d'astuce, se passer ici de ce résultat très puissant).