Université Paul Sabatier
Licence L3 ESR 2017–2018
Arithmétique

TD 5 : Formes quadratiques entières.

Exercice 1.

1) Soit $q(x,y) = ax^2 + bxy + cy^2$. Montrer que $q(\mathbb{Z}^2) \subset \mathbb{Z}$ (si et) seulement si $a, b, c \in \mathbb{Z}$.
2) Trouver un polynôme $P \in \mathbb{Q}[X] \setminus \mathbb{Z}[X]$ tel que $P(\mathbb{Z}) \subset \mathbb{Z}$.

Exercice 2. Montrer que $\operatorname{pgcd}(a,b,c)$ est le pgcd de tous les entiers représentés par $ax^2 + bxy + cy^2$.

Exercice 3. Soient $q(x,y) = ax^2 + bxy + cy^2$ et $d = b^2 - 4ac$.

1) Montrer que s'il existe un entier représenté par q et premier avec d, alors q est primitive.
2) Pourquoi est-ce une généralisation de la règle (évidente) « si a et b sont premiers entre eux, alors q est primitive » ?
3) (facultatif) Réciproquement, on suppose q primitive. Montrer que pour tout entier $n \neq 0$, il existe un entier premier avec n et représenté par q.

Exercice 4. Calculer $\widetilde{h}(-31)$ et $h(-31)$.

Exercice 5. Vous allez, dans cet exercice, démontrer le théorème des deux carrés « de Fermat » : un entier $n > 0$ est somme de deux carrés si et seulement si, dans sa décomposition en facteurs premiers, les exposants de tous les facteurs premiers congrus à 3 mod 4 sont pairs.

1) Démontrer le sens direct (« seulement si ») de l'équivalence. (Indication : montrer d'abord que si un nombre premier $p \equiv 3 \bmod 4$ divise une somme de deux carrés $x^2 + y^2$, alors p divise x et y.)
2) Montrer que $\widetilde{h}(-4) = 1$.
3) Soit m un entier sans facteur carré, et sans facteur premier congru à 3 mod 4. Montrer que -4 est un carré mod$4m$ et en déduire (grâce à la question précédente) que m est une somme de deux carrés.
4) En déduire le sens réciproque (« si ») de l'équivalence.

Exercice 6. (facultatif)

1) Vérifier (dans tout anneau commutatif) l'identité de Brahmagupta :
$$\left(p^2 - dq^2\right)\left(r^2 - ds^2\right) = (pr + dqs)^2 - d\,(ps + qr)^2\,.$$
2) Montrer que pour tout discriminant d, l'ensemble $q_d\left(\mathbb{Z}^2\right)$ des entiers représentés par la forme principale de discriminant d contient 1 et est stable par produit. (Dans le cas $d \equiv 1 \bmod 4$, on pourra vérifier puis utiliser que $q_d(x,y) = \frac{(2x+y)^2 - dy^2}{4}$.)

Exercice 7.

1) Montrer que $h(-3) = 1$.
2) En déduire que tout nombre premier congru à 1 mod 3 est de la forme $x^2 + xy + y^2$.
3) (Facultatif) Caractériser de même les nombres premiers de la forme $q_d(x,y)$, pour
$$d = -4, -7, -8, -11, -19, -43, -67, -163.$$

Exercice 8. Identifier les classes pour $d = -12$. En déduire que tout nombre premier congru à 1 mod 3 est de la forme $x^2 + 3y^2$.

Exercice 9. Montrer que $h(-20) = 2$ et qu'un nombre premier est de la forme $x^2 + 5y^2$ si et seulement s'il est congru à 1 ou 9 mod 20.

Exercice 10. (facultatif ; exercice sur 12 pts (4+2+3+3) de l'examen sur 30 pts de janvier 2017)
Soit un nombre premier $p > 3$.

1) Montrer que -6 est un carré mod$p$ si et seulement si p est congru soit à ± 1 mod 8 et à 1 mod 3, soit à ± 3 mod 8 et à -1 mod 3.
2) Montrer que les deux seules formes (quadratiques entières positives) réduites de discriminant -24 sont $x^2 + 6y^2$ et $2x^2 + 3y^2$.
3) En déduire que p est de la forme $x^2 + 6y^2$ si et seulement s'il est congru à 1 ou 7 mod 24, et qu'il est de la forme $2x^2 + 3y^2$ si et seulement s'il est congru à 5 ou 11 mod 24.
4) Montrer que si deux entiers N_1, N_2 sont représentés tous deux par $x^2 + 6y^2$ ou tous deux par $2x^2 + 3y^2$ alors $N_1 N_2$ est représenté par $x^2 + 6y^2$, et que si l'un est représenté par $x^2 + 6y^2$ et l'autre par $2x^2 + 3y^2$ alors $N_1 N_2$ est représenté par $2x^2 + 3y^2$.

Exercice 11.

1) Montrer que pour toute représentation propre $q(\alpha, \gamma) = m > 0$, il existe une unique équivalence propre $q(\alpha x + \beta y, \gamma x + \delta y) = mx^2 + nxy + ly^2$ telle que $-m < n \leq m$.
2) Déterminer les racines carrées de -1 mod 65.
3) En déduire les couples d'entiers (n, l) tels que $-65 < n \leq 65$ et $n^2 - 4 \times 65l = -4$.
4) En déduire que 65 est somme de deux carrés d'exactement deux façons (à interversion près des deux carrés), que l'on précisera.

Exercice 12. (facultatif) Soit q une forme quadratique entière de discriminant d. Montrer que les trois propriétés suivantes sont équivalentes :

1) d est un carré parfait (éventuellement nul) ;
2) q s'annule en d'autres points (de $\mathbb{Z}^2$) que le point $(0, 0)$;
3) q est le produit de deux formes linéaires (de $\mathbb{Z}^2$ dans $\mathbb{Z}$).