Théorie des nombres
FEUILLE DE TD N°5

Exercice 1

Trouver, si elles existent, les racines carrées de 2 dans $\mathbf{F}_{113}$.

Exercice 2

Calculer les symboles de Jacobi suivants :

$$\left(\frac{7}{15}\right), \left(\frac{7}{45}\right), \left(\frac{11}{45}\right), \left(\frac{30}{77}\right), \left(\frac{55}{273}\right).$$

Exercice 3

Théorème des 2 carrés.
On cherche à trouver les nombres p premiers s'écrivant sous la forme

$$p = x^2 + y^2.$$

1. Montrer que si $p = 3 \mod 4$, alors p n'est pas somme de deux carrés.
   On supposera dans la suite que $p = 1 \mod 4$.
2. Montrer qu'il existe $u_0 \in \mathbf{N}$ tel que $u_0^2 = -1 \mod p$. Montrer que pour tout x, $x^2 + (u_0 x)^2 = 0 \mod p$.
3. On considère l'ensemble

   $$E = \{u_0 x - y \mid 0 \leq x < \sqrt{p}, 0 \leq y < \sqrt{p}\}.$$

   Montrer qu'il existe z_1 et z_2 dans E tels que $z_1 = z_2 \mod p$.
4. En déduire qu'il existe x et y dans $\mathbf{N}$ tels que $x^2 + y^2 = p$.

Exercice 4

Écrire $2425 = 5^2 \cdot 97$ et $754 = 2 \cdot 13 \cdot 29$ comme sommes de deux carrés.
Écrire $323 = 17 \cdot 19$ et $1265 = 5 \cdot 11 \cdot 23$ comme sommes de quatre carrés.

Exercice 5

Théorème de Minkowski :
Soit C un convexe de $\mathbf{R}^n$ symétrique par rapport à 0 et de volume strictement supérieur à 2^n. Alors il existe $u_0 \neq 0$ tel que $u_0 \in C \cap \mathbf{Z}^n$.

1. Notons $D = [0,1[^n$. Vérifier que $\mathbf{R}^n = \bigcup_{u \in \mathbf{Z}^n} (D + u)$.
2. Soit $A \subset \mathbf{R}^n$ un ensemble de volume strictement supérieur à 1. Pour $u \in \mathbf{Z}^n$, on note $A_u = (A \cap (D + u)) - u$. Montrer que pour tout u, $A_u \subset D$ et que $Vol(A) = \sum_{u \in \mathbf{Z}^n} Vol(A_u)$.

3. En déduire qu'il existe $u, v \in \mathbf{Z}^n$, $u \neq v$ tels que $A_u \cap A_v \neq \emptyset$.
4. Posons $C' = \frac{1}{2}C$. Montrer qu'il existe $x_0, y_0 \in C'$ tels que $x_0 - y_0 \in \mathbf{Z}^n \setminus \{0\}$.
5. Montrer que $C = \{x - y \mid x, y \in C'\}$. En déduire que $u_0 = x_0 - y_0 \in C \cap \mathbf{Z}^n \setminus \{0\}$.

Exercice 6

Soit $p = 13$. On remarque que pour $a = 5$, on a $a^2 = -1 \mod p$. En considérant le réseau de $\mathbf{Z}^2$ engendré par $(1, a)$ et $(0, p)$ trouver x et y tels que $p = x^2 + y^2$.

Même question pour $p = 61$ et $a = 11$.

Exercice 7

1. On cherche les nombres premiers p s'écrivant sous la forme $p = x^2 + 2y^2$.
   - Montrer qu'un tel p vérifie $(\frac{-2}{p}) = 1$, *i.e.* $p = 2$ ou $p = 1$ ou $3 \mod 8$.
   - Supposons que -2 est un carré dans $\mathbf{F}_p$. On a a tel que $a^2 = -2 \mod p$. En considérant le réseau engendré par $(a, 1)$ et $(p, 0)$ et l'ellipse définie pour un certain r par $x^2 + 2y^2 = r^2$ (le volume défini par une telle ellipse est $V_r = \frac{\pi r^2}{\sqrt{2}}$), montrer qu'il existe x et y tels que $x^2 + 2y^2 = p$.
2. On cherche maintenant tous les entiers n s'écrivant sous la forme $n = x^2 + 2y^2$.
   - Montrer que l'ensemble de ces entiers est stable par multiplication.
   - Trouver toutes les formes réduites de discriminant 2.
   - En déduire qu'un tel entier n est de la forme $n = k^2 m$ où chaque facteur premier de m est soit égal à 2, soit congru à 1 ou 3 modulo 8.
   - Appliquer le résultat à $n = 198$.

Exercice 8

En utilisant la même méthode montrer que les entiers n s'écrivant sous la forme

$$n = x^2 + 3y^2$$

sont les entiers de la forme $n = k^2 m$, où tout facteur premier de m est égal à 3 ou congru à 1 modulo 6.
Application : écrire 84 sous cette forme.

Exercice 9

1. On cherche les nombres premiers p s'écrivant sous la forme

$$p = x^2 + 5y^2.$$

   (a) Montrer que -5 est un carré modulo p si et seulement si $p = 2$, $p = 5$ ou $p = 1, 3, 7$ ou 9 modulo 20.

   (b) À l'aide de la méthode de Minkowski, montrer que pour de tels nombres p il existe x et y tels que $x^2 + 5y^2 = p$ ou $x^2 + 5y^2 = 2p$.

(c) En raisonnant modulo 5, en déduire que les nombres p cherchés sont les nombres de la forme $p = 5$ ou $p = 1$ ou 9 modulo 20.

2. On cherche désormais les entiers n s'écrivant sous la forme

$$n = x^2 + 5y^2.$$

(a) Montrer que les seules formes réduites de discriminant 5 sont $x^2 + 5y^2$ et $2x^2 + 2xy + 3y^2$.

(b) Montrer que si p est représenté par une telle forme, alors -5 est un carré modulo p.

(c) Réciproquement, montrer que si -5 est un carré modulo p, alors p est représenté par l'une des formes réduites ci-dessus.

(d) Vérifier que

$$\begin{aligned}(2x^2 + 2xy + 3y^2)(2x'^2 + 2x'y' + 3y'^2) &= (2xx' + xy' + x'y + 3yy')^2 + 5(xy' - x'y)^2\\ (x^2 + 5y^2)(x'^2 + 5y'^2) &= (xx' + 5yy')^2 + 5(xy' - x'y)^2.\end{aligned}$$

(e) Déduire de tout cela qu'un entier n s'écrit sous la forme $n = x^2 + 5y^2$ si et seulement si n se décompose sous la forme

$$n = m^2 m_1 m_2,$$

où m_1 est le produit de nombres premiers égaux à 5 ou congrus à 1 ou 9 modulo 20, et m_2 est le produit d'un nombre pair de nombres premiers égaux à 2 ou congrus à 3 ou 7 modulo 20.

3. Vérifier le résultat sur des exemples.