Théorie des nombres

FEUILLE DE TD N°3

Exercice 1

1 Montrer que dans un anneau factoriel, un élément irréductible engendre un idéal premier et un élément réductible engendre un idéal non-premier.

2 Montrer que dans un anneau principal, les idéaux premiers sont les idéaux maximaux.

Exercice 2

1 Donner toutes les solutions dans $\mathbf{Q}^2$ de l'équation $x^2+2y^2=6$. On pourra en exploitant la solution $(2,1)$ chercher (x,y) sous la forme $(2+X, 1+tX)$.

2 Donner toutes les solutions dans $\mathbf{Q}^2$ des équations suivantes :

$$x^2+y^2=11 \qquad x^2-6y^2=-1.$$

On pourra raisonner par congruence.

3 Montrer que l'équation $2x^2+2y^2=1$ n'a pas de solution dans $\mathbf{Z}^2$, mais qu'elle en a dans $\mathbf{Q}^2$.

Exercice 3

On considère l'anneau $A=\mathbf{Z}[i]=\mathbf{Z}[X]/(X^2+1)\mathbf{Z}[X]$. On rappelle que A est euclidien. Soit p un nombre premier impair. On rappelle que (-1) est un carré dans $\mathbf{F}_p$ si et seulement si $(-1)^{\frac{p-1}{2}}=1 \mod p$, si et seulement si $p=1 \mod 4$.

1 Peut-on écrire 11 comme somme de deux carrés dans $\mathbf{Z}$? et 13 ?

2 Montrer que l'anneau quotient A/pA est isomorphe à $\mathbf{F}_p/(X^2+1)\mathbf{F}_p$.

3 Montrer que si $p=-1 \mod 4$, p est irréductible dans A.

4 On suppose que $p=1 \mod 4$ et on considère une racine carré $\alpha=[A]_p$ de -1 dans $\mathbf{F}_p$. Montrer que l'application $A=\mathbf{Z}[i]\to\mathbf{F}_p$, $a+ib\mapsto[a]_p+\alpha[b]_p$ est un morphisme d'anneaux, surjectif et que son noyau est engendré par un élément a de A. Montrer que p s'écrit ab dans A avec ni a ni b inversibles dans A. En déduire que $N(a)=p$.

5 Montrer que p est la somme de deux carrés dans $\mathbf{Z}$ si et seulement si $p=1 \mod 4$.

Exercice 4

1 Soit n un entier et $a=n^2+n+1$. Montrer que tout facteur premier de a distinct de 3 est congru à 1 modulo 3.

2 Soient $p_1,\dots p_r$ des nombres premiers. Que peut-on dire des facteurs premiers de :

$$(3p_1\dots p_r)^2+3p_1\dots p_r+1?$$

En déduire qu'il y a une infinité de nombres premiers congrus à 1 modulo 3.

3 Généralisation. Soit q un nombre premier impair. Montrer que pour tout p premier distinct de q, on a les équivalences suivantes :

$$p\equiv 1[q] \iff \mathbf{F}_p \text{ contient une racine primitive } q \text{ -ième de l'unité}$$

$\iff$ le polynôme $\dfrac{X^q-1}{X-1} = X^{q-1}+X^{q-2}+\cdots+1$ a une racine de l'unité dans $\mathbf{F}_q$.

En déduire qu'il y a une infinité de nombres premiers congrus à 1 modulo q.

Exercice 5

Le but de cet exercice est de démontrer la version du théorème de Fermat où l'anneau $\mathbf{Z}$ est remplacé par un anneau de polynômes. Soit $n \geq 3$ un entier. On cherche des triplets (A, B, C) d'éléments de $\mathbf{C}[T]$, premiers entre eux (un tel triplet est dit primitif) et vérifiant l'équation

$$A^n + B^n = C^n.$$

Un tel triplet sera dit trivial si ses éléments sont constants. On va montrer que les seuls triplets primitifs d'éléments de $\mathbf{C}[T]$ solutions de l'équation sont les triplets triviaux. Pour cela on utilise la méthode de descente infinie. Pour tout triplet (A, B, C) de $\mathbf{C}[T]^3$ on pose

$$h(A, B, C) := \max(\deg(A), \deg(B), \deg(C)).$$

On suppose l'ensemble $\mathcal{E}$ des triplets primitifs solutions non triviaux non vide. On peut alors choisir $(A_0, B_0, C_0) \in \mathcal{E}$ tel que $h(A_0, B_0, C_0)$ soit minimal dans $\mathcal{E}$.

1 On note μ_n l'ensemble des racines n-èmes de l'unité. Montrer que les polynômes $C_0 - \zeta B_0$, $\zeta \in \mu_n$ sont deux à deux premiers entre eux, et que pour tout $\zeta \in \mu_n$, il existe un polynôme P_ζ vérifiant $P_\zeta^n = C_0 - \zeta B_0$.

2 Soient $\zeta_1, \zeta_2, \zeta_3$ trois éléments distincts de μ_n. Montrer qu'il existe un triplet $(a_1, a_2, a_3) \in \mathbf{C}^3$ tel que l'on ait

$$(a_1 P_{\zeta_1})^n + (a_2 P_{\zeta_2})^n = (a_3 P_{\zeta_3})^n.$$

3 Conclure.

4 Peut-on remplacer $\mathbf{C}$ par un corps quelconque ?

Exercice 6

On rappelle que tous les triplets pythagoriciens primitifs avec Y pair, sont de la forme $X = m^2-n^2, Y = 2mn, Z = m^2+n^2$ $1 \leq n < m$, m et n premiers entre eux, m ou n pair.

Soit (x, y, z) une solution de l'équation $x^4 + y^4 = z^2$ avec $x \geq 1, y \geq 1, z \geq 1$ et z minimal.

1 Montrer que (x^2, y^2, z) est un triplet pythagoricien primitif. On peut supposer que x est impair (et donc y pair) et on écrira avec m et n premiers entre eux, m ou n pair et $1 \leq n < m$, $x^2 = m^2 - n^2, y^2 = 2mn, z = m^2 + n^2$.

2 Montrer que (x, n, m) est un triplet pythagoricien primitif avec x impair. On peut donc écrire $x = a^2-b^2, n = 2ab, m = a^2+b^2$, $1 \leq b < a$, a et b premiers entre eux, a ou b pair. Montrer que a, b, m sont deux à deux premiers entre eux. Calculer abm et montrer que a, b et m sont des carrés. On écrira $a = A^2$, $b = B^2$ et $m = M^2$.

3 Montrer que (A, B, M) est une solution de l'équation initiale avec $1 \leq M < z$.

4 En déduire que les seules solutions de l'équation $x^4 + y^4 = z^2$ et donc de l'équation $x^4 + y^4 = z^4$ sont avec $x = 0$ ou $y = 0$.